public / öffentlich

Final Version / Endfassung

GLOBALTRUST® Certificate Policy

[GCP - VDA Policy]

Autor: Hans G. Zeger

Version 2.0g / 3rd April 2020

OID-Number/Nummer: 1.2.40.0.36.1.1.8.1
History/Historie OID-Number/Nummer: 1.2.40.0.36.1.1.8.99

Policy Online: http://www.globaltrust.eu/certificate-policy.html

Contact: http://www.globaltrust.eu/impressum.html

Limits: http://www.globaltrust.eu/limitation.html

Suspension(Sperre) / Revocation(Widerruf): http://www.globaltrust.eu/revocation.html

Editorial note: This document has been provided with an qualified signature. The date of signature can deviate from the date of the start of the validity of this document for different legal and organisational reasons. The signature does not give information about the start of the validity of the document, but confirms the integrity of the content.

Redaktioneller Hinweis: Das vorliegende Dokument ist mit einer qualifizierten Signatur versehen. Das Datum der Signatur kann aus verschiedenen rechtlichen und organisatorischen Gründen vom Datum des Gültigkeitsbeginns des Dokuments abweichen. Die Signatur gibt keine Auskunft über den Gültigkeitsbeginn des Dokuments, sondern bestätigt nur die Unversehrtheit des Inhalts.

CONTENT/ INHALT

APPENDIX / ANHANG

1. INTRODUCTION / EINLEITUNG

Management-Statement

Certification services, in particular digital electronic signatures and digital certificates, are seen as key technologies for the production of reliable global business processes. The secure management of confidential certification data, the long-term sustainability of certification procedures and the verifiability of certification processes are of central importance to the business activity of the Certification Authority (CA).

Information security is understood to be, alongside the security of IT infrastructure, the secure usage of all information relevant to certification services outside of IT.

The fundamental principles of information security are confidentiality, integrity and availability.

In this sense, the provision of appropriate technology and resources is of central importance. The performance of certification services is considered the principle task of the operator. All objectives of or changes to certification services, including changes to policies regarding certification services, take place upon the instruction of the management, taking strict information security standards into account.

The foundation of these strict information security standards is that certification services are performed exclusively on the basis of defined business models.

In the implementation of new business processes or the adaptation of existing business processes, their effects on the existing information security concept is first reviewed, and the implementation is conceived so that the

Zertifizierungsdienste, insbesondere digitale elektronische Signaturen und digitale Zertifikate werden als Schlüsseltechnologien zur Herstellung vertrauenswürdiger globaler Geschäftsprozesse angesehen. Der sicheren Verwaltung vertraulicher Zertifizierungsdaten, die langfristige Nachvollziehbarkeit der Zertifizierungsvorgänge und die Überprüfbarkeit der Zertifizierungsdienste hat damit zentrale Bedeutung in der Geschäftstätigkeit des Vertrauensdienstanbieters (VDA).

Als Informationssicherheit wird neben der Sicherheit der IT-Infrastruktur auch die sichere Verwendung aller zu den Zertifizierungsdiensten relevanten Informationen außerhalb der IT verstanden.

Grundlagen der Informationssicherheit sind die Gewährleistung der Vertraulichkeit, Integrität und Verfügbarkeit.

In diesem Sinn kommt der Bereitstellung geeigneter Techniken und Hilfsmittel zentrale Bedeutung zu. Die Erbringung von Zertifizierungsdiensten wird als zentrale Aufgabe des Betreibers angesehen. Alle Vorgaben oder Änderungen der Zertifizierungsdienste inklusive Änderungen in den die Zertifizierungsdienste betreffenden Policies erfolgen auf Grund von Anweisungen der Geschäftsführung unter besonderer Bedachtnahme strenger Informationssicherheitsmaßstäbe.

Grundlage dieser strengen Informationssicherheitsmaßstäbe ist, dass Zertifizierungsdienste ausschließlich auf Basis definierter Geschäftsmodelle erbracht werden.

Bei der Implementierung neuer Geschäftsprozesse bzw. der Anpassung bestehender Geschäftsprozesse werden deren Auswirkungen auf das bestehende Informationssicherheitskonzept vorab geprüft und die

existing security concept (GLOBALTRUST® Certificate Security Policy, OID: 1.2.40.0.36.1.2.2.1[1]) is adhered to. This document is not publicly available. The security concept describes the Information Security Management System (ISMS) for all certification services for which the operator assumes responsibility (either as the CA or the contractor of the CA).

The operation and adaptation of existing business processes and the implementation of new business processes is performed using the PDCA[2] model, in which PDCA cycles are arranged in appropriate time periods. Independent of the pre-defined standard PDCA cycle, unforeseen events can necessitate additional or shortened PDCA cycles (in particular during adaptations of essential technical, personnel, commercial or legal parameters). Sub-processes, as well as sub-PDCA processes, are organised insofar as they are materially applicable.

Furthermore, information security is ensured organisationally using a clear role concept (⇨ GLOBALTRUST® Certificate Security Policy), in which a certification committee is assigned a central role in the planning of certification services. All functions relevant to certification are represented in the certification committee. Changes in the certificate policies are approved by the certification committee.

In the certification committee, sufficient financial funding for information security measures is established, in consideration of legal guidelines and commercial resources.

Implementierung so konzipiert, dass das bestehende Sicherheitskonzept (GLOBALTRUST® Certificate Security Policy, OID-Nummer: 1.2.40.0.36.1.2.2.1[1]) eingehalten wird. Dieses Dokument ist nicht öffentlich verfügbar. Das Sicherheitskonzept beschreibt das Informations-Sicherheits-Management-System (ISMS) für alle Zertifizierungsdienste für die der Betreiber verantwortlich zeichnet (entweder als VDA oder als Dienstleister für VDAs).

Der Betrieb und die Anpassung bestehender und die Implementierung neuer Geschäftsprozesse erfolgt nach dem PDCA[2]-Modell, wobei die PDCA-Zyklen sich nach sachlich sinnvollen Zeitperioden orientieren. Unabhängig vom vordefinierten Standard-PDCA-Zyklus können unvorhergesehene Ereignisse (insbesondere bei Änderung wesentlicher technischer, personeller, wirtschaftlicher oder rechtlicher Rahmenbedingungen) zusätzliche oder verkürzte PDCA-Zyklen erfordern. Teilprozesse werden, soweit sachlich anwendbar, ebenfalls als Teil-PDCA-Zyklen organisiert.

Informationssicherheit wird weiters durch ein klares personelles Rollenkonzept (⇨ GLOBALTRUST® Certificate Security Policy) organisatorisch gesichert, wobei dem Zertifizierungs-Ausschuss eine zentrale Rolle in der Planung der Zertifizierungsdienste zukommt. Im Zertifzierungs-Ausschuss sind alle für die Zertifizierung relevanten Funktionen repräsentiert. Änderungen in den Certificate Policies werden durch den Zertifizierungs-Ausschuss genehmigt und freigegeben.

Im Zertifizierungs-Ausschuss erfolgt unter Berücksichtigung der rechtlichen Vorgaben und der wirtschaftlichen Ressourcen die ausreichende finanzielle Dotierung von Informationssicherheitsmaßnahmen.

---

1 The GLOBALTRUST® Certificate Security Policy is not publicly available. / Die GLOBALTRUST® Certificate Security Policy ist nicht öffentlich verfügbar

2 PDCA = Plan (planning phase), Do (development and implementation phase), Act (operation phase), Check (review phase with the objective of identifying potiential for improvement) / PDCA = Plan (Planungsphase), Do (Entwicklungs-, Umsetzungs- oder Implementierungsphase), Act (Betriebsphase), Check (Überprüfungsphase mit dem Ziel Verbesserungspotentiale zu identifizieren)

For the purpose of motivating all employees and achieving an optimal role model function, the management and the members of the certification committee commit themselves to regularly taking part in training events and observing security regulations faithfully. All employees are obliged to maintain confidentiality.

Im Sinne der Motivation aller Mitarbeiter und um eine optimale Vorbildfunktion zu erreichen, verpflichten sich Geschäftsführung und die Mitglieder des Zertifizierungs-Ausschuss selbst zur erforderlichen Teilnahme an Schulungsveranstaltungen und der Beachtung aller Sicherheitsregeln. Alle Mitarbeiter werden zur Einhaltung des Datengeheimnisses verpflichtet.

To maintain information security, all employees holding responsibilities conduct tests of the information security processes, in which internal and external audits have an important role. Recognised vulnerabilities lead invariably to consequences. Vulnerabilities and consequences are documented. The management commits itself to regular evaluation of the suitability, up-to-dateness and appropriateness of the security objectives and guidelines.

Zur Aufrechterhaltung der Informationssicherheit führen alle zuständigen Funktionsträger regelmäßig Prüfungen der Informationssicherheitsprozesse durch, wobei in ternen und externen Audits eine wichtige Rolle zukommt. Erkannte Schwachstellen führen ausnahmslos zu Konsequenzen, Schwachstellen und Konsequenzen werden dokumentiert. Die Geschäftsführung verpflichtet sich zur regelmäßigen Evaluation der Eignung, Aktualität und Angemessenheit der Sicherheitsziele und -leitlinien.

The flow of information, the required reports at management level and the required documentation are stipulated within the framework of the accountability concept (⇨ GLOBALTRUST® Certificate Security Policy). The internal documentation of certification services takes place through an internal Content Management System. The documents are accessible to all responsible personnel. Those parts of the documentation that are necessary for the recovery of the IT system in the event of emergency are kept ready in printed form. Through a complex and on-going enhanced authority and keyword process documents can be assigned flexibly designated themes and tasks or designated usage groups (for example, technical documents, user documents, contract and certification documents, instructions, reports and so on).

Im Rahmen des Rollenkonzepts (⇨ GLOBALTRUST® Certificate Security Policy) wird sowohl der Informationsfluss, die erforderlichen Berichte an die Leitungsebene und die erforderlichen Dokumentationen festgelegt. Die interne Dokumentation der Zertifizierungsdienste erfolgt mittels eines internen Content Management Systems, die Dokumente sind allen zuständigen Personen zugänglich. Für Notfälle werden jene Dokumentationsteile in gedruckter Form bereit gehalten, die für die Wiederherstellung der IT-Infrastruktur unerlässlich sind. Durch ein komplexes und laufend erweitertes Berechtigungs- und Schlagwortkonzept können Dokumente flexibel bestimmten Themen und Aufgaben bzw. bestimmten Nutzungsgruppen zugeordnet werden (z.B. technische Dokumente, Anwendungsunterlagen, Vertrags- und Zertifizierungsunterlagen, Weisungen, Berichte usw.).

The CA conducts the necessary audits to ensure the conformity of its certification services with the documents listed under ⇨ 8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS / Prüfung der Konformität und andere Beurteilungen (p168). The audit reports are published or otherwise made

Der VDA führt die erforderlichen Audits durch, um die Konformität seiner Zertifizierungsdienste mit den unter ⇨ 8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS / Prüfung der Konformität und andere Beurteilungen (p168) gelisteten Dokumenten sicher zu stellen. Soweit

available as necessary.

The VDA will regularly execute safety analyses of its public and internal certification network. The analyses will be executed due to the requirements of supervisory authorities, or due to agreements with third parties, the CA/Browser Forum or similar institutions, due to system or network changes, once in the quarter at the mininum. As far as the checks will be executed due to requirements by the supervisory authorities or a third party, the check can take place in one week.

erforderlich werden die Auditreports veröffentlicht bzw. zur Verfügung gestellt.

Der VDA führt regelmäßig sicherheitstechnische Analysen seines gesamten öffentlichen und internen Zertifizierungs-Netzwerkes durch. Die Prüfung erfolgt auf Grund von Vorgaben von Aufsichtsstellen, auf Grund von Vereinbarungen mit Dritten, des CA/Browser Forums oder vergleichbarer vom VDA anerkannter Einrichtungen, auf Grund von System- oder Netzwerkänderungen, jedenfalls zumindest einmal im Quartal. Soweit die Überprüfungen auf Grund Anforderungen durch die Aufsichtsbehörde oder Dritte erfolgt, kann die Überprüfung innerhalb einer Woche erfolgen.

1.1 Overview / Übersicht

The operator offers all certification services as defined by this document.

The GLOBALTRUST® Certificate Policy (GCP) governs all requirements of the operator's certification services. If regulations are provided for individual products in the applicable practice statement (in particular the GLOBALTRUST® Certificate Practice Statement), these are to be understood as supplementary within the framework of this policy.

The GLOBALTRUST® Certificate Policy described in this document is referred to henceforth as the "Policy". This Policy is to be understood as the foundation within which the certification services are performed. Additional restrictions in the applicability of the policy can be agreed, in particular, cases of certification and signature procedures. However, this in no way affects legal foundations (in particular [eIDAS-VO], [SVG], [SVV], ...) or technical foundations (in particular [CWA-14167-1], [ETSI TS 101 456], including successors: [ETSI EN 319 401], [ETSI EN 319 411-1], [ETSI EN 319 411-2], [ETSI TS 102 042], including successors [ETSI EN 319 411-3], ...). The terms and conditions of the CA or additional agreements with

Der Betreiber bietet sämtliche Zertifizierungsdienste im Sinne dieses Dokuments an.

Die GLOBALTRUST® Certificate Policy (GCP) regelt alle Anforderungen der Zertifizierungsdienste des Betreibers. Soweit für einzelne Produkte Regelungen im jeweils anzuwendenden Practice Statement (insbesoondere dem GLOBALTRUST® Certificate Practice Statement) vorgenommen werden, sind diese als Ergänzungen im Rahmen dieser Policy zu verstehen.

Die in diesem Dokument beschriebene GLOBALTRUST® Certificate Policy wird im Folgenden kurz als "Policy" bezeichnet. Diese Policy ist als Grundlage zu verstehen, innerhalb derer die Zertifizierungsdienste erbracht werden. Zusätzliche Beschränkungen in der Anwendbarkeit der Policy auf bestimmte Zertifizierungsfälle und Signaturvorgänge ist durch Vereinbarungen möglich. Dies betrifft jedoch in keinem Fall eine Änderung gesetzlicher (insbesondere [eIDAS-VO], [SVG], [SVV], ...) oder technischer (insbesondere [CWA-14167-1], [ETSI TS 101 456] inklusive Nachfolger: [ETSI EN 319 401], [ETSI EN 319 411-1], [ETSI EN 319 411-2],...) Grundlagen. Die AGB des VDA oder zusätzliche

partner companies cannot render the Policy fully or partially invalid.

All processes necessary for certification services are documented by the operator internally.

The GLOBALTRUST® Certificate Policy, the GLOBALTRUST® Certificate Practice Statement and the GLOBALTRUST® Certificate Security Policy together constitute the foundation of the operation concept as submitted to the regulator for licensing. The implementation of the technical procedures of the operation concept is ensured by the internal documentation system.

Changes to or new developments of business processes take place according to written documentation and always contain the following information: description of the planned changes or new developments, date of initialisation, participating employees, expected duration, interim results, and information on the date of completion, on-going adjustment of the date of completion, including information on work to be completed and the personnel responsible for acceptance and documentation of the completed business process.

Changes or new developments are to be initiated by the personnel responsible according to ⇨ GLOBALTRUST® Certificate Security Policy. In the event of doubt, permission must come directly from the management.

Vereinbarungen der Partnerunternehmen können jedoch nicht die vorliegende Policy ganz oder teilweise außer Kraft setzen.

Alle für die Erbringung der Zertifizierungsdienste notwendigen Prozesse sind vom Betreiber intern dokumentiert.

Die GLOBALTRUST® Certificate Policy, das GLOBALTRUST® Certificate Practice Statement und die GLOBALTRUST® Certificate Security Policy sind gemeinsam Grundlage des der Aufsichtsbehörde zur Genehmigung vorgelegten Betriebskonzepts. Die Umsetzung der technischen Abläufe des Betriebskonzepts ist durch das interne Dokumentationssystem sichergestellt.

Änderungen oder Neuentwicklungen von Geschäftsprozessen erfolgen gemäß schriftlicher Dokumentation und enthält jedenfalls folgende Angaben: Beschreibung der geplanten Änderungen oder Neuentwicklungen, Initialisierungsdatum, beteiligte Mitarbeiter, voraussichtliche Dauer, Zwischenergebnisse und Angaben zum Fertigstellungstermin, eine laufende Anpassung des Fertigstellungsstatus inkl. Angaben der offenen Arbeiten und der verantwortlichen Person für die Abnahme, Dokumentation des fertig gestellten Geschäftsprozesses.

Änderungen oder Neuentwicklungen sind von verantwortlicher Stelle gemäß ⇨ GLOBALTRUST® Certificate Security Policy zu veranlassen. Im Zweifel ist die Genehmigung direkt durch die Geschäftsführung erforderlich.

1.2 Document name and identification / Dokumenttitel und -identifikation

Document title: "GLOBALTRUST® Certificate Policy“ (GCP)

This policy is valid for GLOBALTRUST® and has the OID: 1.2.40.0.36.1.1.8.1.

Dokumententitel: "GLOBALTRUST® Certificate Policy" (GCP)

Diese für GLOBALTRUST® gültige Policy hat die OID-Number/Nummer: 1.2.40.0.36.1.1.8.1).

This document becomes valid on the day that it is published on the website of the operator. Where not otherwise indicated, the validity of the earlier version of the document ends as the new version becomes valid.

This document was compiled in conformity with RFC3647.

External documents are cited in square brackets [] and can be found in ⇨ Appendix A: I Bibliography (p109) listed with bibliographic information. They are cited with the date 1 February 2015, but the respectively valid versions or the applicable subsequent standards apply.

Unless otherwise indicated, the validity of weblinks refers to the day upon which editing of the document was completed.

The certificate policy contains all rules for the issuance and application of certificates for simple, advanced and qualified signatures.

Changes on the grounds of legal changes become effective from the time at which the legal provisions come into force. Other changes become effective through announcement on the website of GLOBALTRUST®.

Where legal changes or changes to those documents and standards for which certification services require conformity necessitate a change of the GLOBALTRUST® Certificate Policy,
the GLOBALTRUST® Certificate Practice Statements
or the GLOBALTRUST® Certificate Security Policy, adaptation ensues in a timely fashion sufficient to ensure that the changed requirements can be fulfilled.

Das vorliegende Dokument tritt mit dem Tag der Veröffentlichung auf der Website des Betreibers in Kraft. Sofern nicht anders vermerkt endet die Gültigkeit der früheren Version des Dokuments mit Beginn der Gültigkeit der neuen Version.

Das vorliegende Dokument wurde konform [RFC3647] erstellt.

Fremd-Dokumente werden in eckigen Klammern [] zitiert und finden sich im ⇨ Appendix / Anhang A: 1 Bibliography / Bibliographie (p192) mit den bibliographischen Angaben gelistet. Sie werden mit Stand 3rd April 2020 zitiert, aber in der jeweils gültigen Fassung bzw. zutreffenden Folgestandards angewandt.

Die Gültigkeit von Weblinks bezieht sich, sofern nicht ausdrücklich anders vermerkt auf den Redaktionsschluss dieses Dokuments.

Die vorliegende Certificate Policy enthält alle Regeln für die Ausstellung und Verwendung von Zertifikaten für einfache, fortgeschrittene und qualifizierte Signaturen.

Änderungen auf Grund gesetzlicher Änderungen werden zum Zeitpunkt des Inkrafttretens der gesetzlichen Bestimmungen wirksam, sonstige Änderungen nach Verlautbarung auf der Website von GLOBALTRUST®.

Sofern gesetzliche Änderungen oder Änderungen jener Dokumente und Standards, für die die Zertifizierungsdienste Konformität beanspruchen, eine Änderung der GLOBALTRUST® Certificate Policy,
des GLOBALTRUST® Certificate Practice Statements oder
der GLOBALTRUST® Certificate Security Policy erfordern, erfolgt die Anpassung so zeitgerecht, dass die geänderten Anforderungen erfüllt werden können.

History of changes

Drafts 1.0 to 1.4 were internal versions and never entered into force.

Version 1.5 Original Version 10th August 2006

Version 1.6 Changes I 12th April 2007

- Explanation of the trademark GLOBALTRUST®
- OID given for the English translation of the Policy
- Conformity with [ETSI TS 102 042] established
- Newly added key management subscriber
- Various editorial corrections of spelling and phrasing errors

Version 1.7 Changes II 1st April 2014

- New structure of the document according to [RFC3647]
- Description of detailed certification procedures in ⇨ GLOBALTRUST® Certificate Practice Statement
- Addition of the issuance of qualified certificates for advanced and qualified signatures
- Operation of time stamp service defined
- Operation of mobile certification services defined
- Change of Certification Service Provider
- Additions and corrections in the bibliography
- Regulation of the labelling of simple certifications from 1.7.2014 (⇨ GLOBALTRUST® Certificate Practice Statement).
- Editorial correction of spelling and phrasing errors

Änderungshistorie

Die Vorversionen 1.0 bis 1.4 waren interne Fassungen und traten nie in Kraft.

Version 1.5 Stammfassung 10. August 2006

Version 1.6 Änderungen I 12. April 2007

- Erläuterungen zur Marke GLOBALTRUST®
- OID-Nummer für englische Übersetzung der Policy vergeben
- Konformität mit [ETSI TS 102 042] hergestellt
- Neu hinzugefügt Schlüsselverwaltung Signator
- Diverse redaktionelle Korrektur von Schreib- und Formulierungsfehlern

Version 1.7 Änderungen II 1. April 2014

- Neustrukturierung des Dokuments gemäß [RFC3647]
- Darstellung der detaillierten Zertifizierungsabläufe in ⇨ GLOBALTRUST® Certificate Practice Statement
- Erweiterung für die Ausstellung qualifizierter Zertifikate für fortgeschrittene und qualifizierte Signaturen
- Betrieb des Zeitstempeldienstes definiert
- Betrieb mobiler Zertifizierungsdienste definiert
- Änderung des Vertrauensdienstanbieters
- Ergänzungen und Korrekturen in der Literaturliste
- Regelung zur Kennzeichnung von einfachen Zertifikaten ab 1.7.2014 (⇨ GLOBALTRUST® Certificate Practice Statement).
- Redaktionelle Korrektur von Schreib- und Formulierungsfehlern

Version 1.8 Changes III 1st June 2014
- Proposed version RTR
- Editorial correction of spelling and phrasing errors

Version 1.8a Changes IV 1st October 2014
- Adjustment based on insights from 10 September 2014 from RTR
- Editorial correction of spelling and phrasing errors

Version 1.8b Changes V 1st February 2015
- Adjustments based on meeting on 15 January 2015 at the RTR
- Specification of used key and hash algorithms
- Editorial correction of spelling and phrasing errors

Version 1.8c Changes VI 1st June 2015
- Integration of english translation
- Editorial correction of spelling and phrasing errors

Version 1.8d Changes VI 1st June 2016
- internal Version, not activated

Version 1.8 Änderungen III 1. Juni 2014
- Antragsversion RTR
- Redaktionelle Korrektur von Schreib- und Formulierungsfehlern

Version 1.8a Änderungen IV 1. Oktober 2014
- Anpassungen auf Grund der Einschau vom 10. September 2014 durch RTR
- Redaktionelle Korrektur von Schreib- und Formulierungsfehlern

Version 1.8b Änderungen V 1. Februar 2015
- Anpassungen auf Grund der Besprechung am 15. Jänner 2015 bei RTR
- Präzisierung der verwendeten Schlüssel- und Hashalgorithmen
- Redaktionelle Korrektur von Schreib- und Formulierungsfehlern

Version 1.8c Änderungen VI 1. Juni 2015
- Integration der englischen Übersetzung
- Redaktionelle Korrektur von Schreib- und Formulierungsfehlern

Version 1.8d Änderungen VI 1. Juni 2016
- interne Version, nicht in Kraft gesetzt

Version 2.0 Changes VII 1st June 2017
- Description of allowed and suitable Common Names (CN)
- Procedure in case of dispute
- Disclaimer of warranties for the browser suppliers
- Clarification of the responsibility for company certificates
- Change to the european regulation on signatures [eIDAS-VO], the austrian law "Signatur- und Vertrauensdienstgesetz" [SVG] and the austrian regulation "Signatur- und Vertrauensdiensteverordnung" [SVV]
- Use of the term "Vertrauensdiensteanbieter (VDA)" instead of "Zertifizierungsdiensteanbieter"
- Editorial correction of spelling and phrasing errors

Version 2.0b Changes VIII 13th August 2018
- Reduction validity period new server certificates according CA Browserforum [CABROWSER-BASE]
- Consideration of CAA-Records according CA Browserforum [CABROWSER-BASE]
- More detailed definitions of identification procedure during certificate delivery
- Editorial correction of spelling and phrasing errors

Version 2.0c Changes 15th January 2019
- Additional clarifications accorting issuing- und check-processes
- Editorial correction of spelling and phrasing errors, update of citations

Version 2.0d Changes 19th April 2019
- internal Version, not activated

Version 2.0 Änderungen VII 1. Juni 2017
- Beschreibung erlaubter und geeigneter Common Names (CN)
- Vorgangsweise bei Streitfragen
- Haftungsfreistellung der Browseranbieter
- Klärung Verantwortung bei Company-CAs
- Umstellung auf EU Signatur-Verordnung [eIDAS-VO], Signatur- und Vertrauensdienstegesetz [SVG], Signatur- und Vertrauensdiensteverordnung [SVV]
- Verwendung der Bezeichnung Vertrauensdiensteanbieter (VDA) statt Zertifizierungsdiensteanbieter
- Redaktionelle Korrektur von Schreib- und Formulierungsfehlern

Version 2.0b Änderungen VIII 13. August 2018
- Reduktion Laufzeit neuer Server-Zertrifikate gemäß CA Browserforum [CABROWSER-BASE]
- Berücksichtigung CAA-Records gemäß CA Browserforum [CABROWSER-BASE]
- Präzisierung der Beschreibung des Identifikationsverfahrens bei Zertifikatszustellung
- Redaktionelle Korrektur von Schreib- und Formulierungsfehlern

Version 2.0c Änderungen IX 15. Jänner 2019
- Ergänzende Klarstellungen in den Ausstellungs- und Prüfprozessen
- Redaktionelle Korrektur von Schreib- und Formulierungsfehlern, Aktualisierung von Zitierungen

Version 2.0d Änderungen 19. April 2019
- interne Fassung, nicht in Kraft gesetzt

Version 2.0e Changes 25th June 2019
- Definition of videobased online identification
- Description of qualified server certificates
- Description of EV certificates
- Clarifications concerning key pair generation
- Editorial correction of spelling and phrasing errors

Version 2.0f Changes 13th December 2019
- Update Business address
- Precision of email validation procedure
- Description of disseminating status information in case of CA-key compromise
- Beschreibung Certificate Transparency
- Editorial correction of spelling and phrasing errors

Version 2.0g Changes 3rd April 2020
- Permitted Subject Names of CA-certificates restricted
- Clarifications on the use of EKU constraints
- Server certificate validity period limited to 397 days
- organizationIdentifier (OID: 2.5.4.97) and cabfOrganizationIdentifier (OID: 2.23.140.3.1) introduced
- Editorial correction of spelling and phrasing errors

Version 2.0e Änderungen 25. Juni 2019
- Identifizierung durch videogestützte Onlineidentifikation definiert
- Beschreibung qualifizierte Serverzertifikate
- Beschreibung EV-Zertifikate
- Klarstellungen bei der Schlüsselerzeugung
- Redaktionelle Korrektur von Schreib- und Formulierungsfehlern

Version 2.0f Änderungen 13. Dezember 2019
- Aktualisierung Büroaddresse
- Konkretisierung Email-Validierung
- Verteilung Widerrufsstatus im Fall der Kompromittierung eines CA-Schlüssels beschrieben
- Beschreibung Certificate Transparency
- Redaktionelle Korrektur von Schreib- und Formulierungsfehlern

Version 2.0g Änderungen 3. April 2020
- Zulässige Subject Einträge von CA-Zertifikaten begrenzt
- Ergänzende Klarstellungen zu EKU-Verwendung
- Laufzeit von Serverzertifikaten auf 397 Tage begrenzt
- organizationIdentifier (OID: 2.5.4.97) und cabfOrganizationIdentifier (OID: 2.23.140.3.1) eingeführt
- Redaktionelle Korrektur von Schreib- und Formulierungsfehlern

1.3 PKI participants / Beteiligte

1.3.1 Certification authorities / Vertrauensdienstanbieter

Issuer and Certification Authority (CA)

The issuer of this Policy and Certification Authority (CA) is e-commerce monitoring GmbH, a company listed on the commercial register according to Austrian law, with its place of business in Vienna (commercial court

Herausgeber und Vertrauensdienstanbieter (VDA)

Herausgeber dieser Policy und Vertrauensdienstanbieter (VDA) ist die e-commerce monitoring GmbH, ein nach österreichischem Recht im Firmenbuch eingetragenes Unternehmen mit Sitz in Wien

Vienna FN 224536 a). e-commerce monitoring performs all certification services attributed to GLOBALTRUST® (Certification Services Provider responsible). The CA runs the website http://www.globaltrust.eu. The CA fulfills all requirements of a trustworthy organisation, in particular making available sufficient financial and personnel resources to fulfil all obligations in the framework of the certification services.

(Handelsgericht Wien FN 224536 a), und ist Erbringer aller zu GLOBALTRUST® zugeordneten Zertifizierungsdienste (verantwortlicher Vertrauensdienstanbieter). Der VDA betreibt die Website http://www.globaltrust.eu. Der VDA erfüllt alle Voraussetzungen einer zuverlässigen Organisation, insbesondere verfügt er über eine ausreichende finanzielle und personelle Ausstattung um alle im Rahmen der Zertifizierungsdienste eingegangenen Verpflichtungen zu erfüllen.

1.3.2 Registration authorities / Registrierungsstelle

Registration authority

The business offices of the CA and certification partners authorised by the CA. The registration authority acts in the framework of the standards of the CA. Provided that independent registration authorities are established, they must have completed all audits that are relevant for their area of activity, according to GLOBALTRUST® Certificate Practice Statements, the GLOBALTRUST® Certificate Security Policy and this GLOBALTRUST® Certificate Policy.

Registrierungsstelle

Die Geschäftsstellen des VDA und weitere vom VDA autorisierte Zertifizierungspartner. Die Registrierungsstelle agiert im Rahmen der Vorgaben des VDA. Sofern unabhängige Registrierungsstellen eingerichtet werden, müssen sie über alle erforderlichen Audits gemäß des GLOBALTRUST® Certificate Practice Statements, der GLOBALTRUST® Certificate Security Policy und dieser GLOBALTRUST® Certificate Policy verfügen, die für ihren Tätigkeitsbereich relevant sind.

Certification partner

Persons who are authorised to receive and review certification applications (including verification of identity) in the commission of the CA.

Zertifizierungspartner

Personen, die zur Entgegennahme und Prüfung der Zertifizierungsanträge (inklusive Identitätsprüfung) im Auftrag des VDA berechtigt sind.

Authorised person

A natural person who is authorised to review certification applications and conduct full or partial certification services. This can be employees of the CA (authorised employees), of the registration authority, a contractor, a contractually authorised certification partner or employees of the provider of commerical identification services. The scope of activity is demonstrably adhered to in the framework of instructions, descriptions of activities, contractual agreements and other appropriate documentation, documented and can be made available to authorised interested third

Autorisierte Person

Natürliche Person, die zur Prüfung von Zertifizierungsanträgen und zur Durchführung von Zertifizierungsdiensten oder Teilen davon berechtigt ist. Dies können Mitarbeiter des VDA (autorisierte Mitarbeiter), einer Registrierungsstelle, eines Dienstleisters, eines vertraglich berechtigten Zertifizierungspartners oder Mitarbeiter von Anbietern kommerzieller Identifizierungsdienste sein. Der Tätigkeitsumfang wird im Rahmen von Dienstanweisungen, Tätigkeitsbeschreibungen, vertraglichen Vereinbarungen und anderen geeigneten Dokumentationen

parties, should they exist. Authorised employees of the CA are specifically trained and are particularly trustworthy.

nachweisbar festgehalten, dokumentiert und kann bei Vorliegen berechtigter Interessen Dritten zur Verfügung gestellt werden. Autorisierte Mitarbeiter des VDA werden spezifisch geschult und sind besonders vertrauenswürdig.

1.3.3 Subscribers / Signator

Applicant

A person who submits an application for the issuance of a certificate on the basis of a valid certificate policy and applicable additional agreements, either for themselves personally or for a private, public or international organisation.

Subscriber

A person who possesses a signature-creation device and who acts either in their own name or in the capacity of the position occupied by them or in the name of a legal or natural person.

Antragsteller

Person, die auf Basis einer gültigen Certificate Policy und allfälliger zusätzlicher Vereinbarungen einen Antrag auf Ausstellung eines Zertifikats für sich persönlich oder für eine private, eine öffentliche oder internationale Organisation stellt.

Signator, Unterzeichner

Eine Person, die eine Signaturerstellungseinheit besitzt und die entweder im eigenen Namen oder im Namen der von ihr vertretenen Stelle oder juristischen oder natürlichen Person handelt. Die Begriffe Signator und Unterzeichner werden synonym verwendet.

1.3.4 Relying parties / Nutzer

Relying party

A natural person who uses the services or products of the operator or uses services or products produced with the services and products of the operator. This usage can take place with or without a contract with the operator. In particular, every relying party who uses a public key validated with a certificate from the operator or receives electronically signed information.

Participants

All persons and entities subject to this GLOBALTRUST® Certificate Policy and the applicable GLOBALTRUST® Certificate Practice Statement. This is, in particular, the CA, registration and validation authorities, contractors and certification partners with regard to application review, issuance,

Nutzer

Eine natürliche Person, die Dienste, Produkte des Betreibers oder mit Diensten oder Produkten des Betreibers hergestellte Dienste oder Produkte benutzt. Die Nutzung kann mit oder ohne Vertrag mit dem Betreiber erfolgen. Insbesondere ist jeder Nutzer der einen mit Zertifikat des Betreibers bestätigten öffentlichen Schlüssel benutzt oder Empfängers von elektronisch signierten Informationen ist.

Beteiligte

Alle Personen und Einrichtungen, die dieser GLOBALTRUST® Certificate Policy und dem anzuwendenden GLOBALTRUST® Certificate Practice Statement unterworfen sind. Insbesondere sind dies der VDA, Registrierungs- und Bestätigungsstellen,

archiving and revocation of certificates for the purposes of this GLOBALTRUST® Certificate Policy. Also, the subscriber in the context of the usage of the certificate (in particular for electronic signatures) and all relying parties.

Dienstleister und Zertifizierungspartner in Hinblick auf Antragsprüfung, Ausgabe, Archivierung und Widerruf von Zertifikaten im Sinne dieser GLOBALTRUST® Certificate Policy. Weiters der Signator im Zusammenhang der Anwendung des Zertifikats (insbesondere bei elektronischen Signaturen) und die Nutzer.

1.3.5 Other participants / Weitere Beteiligte

Operator

This describes the role of the CA as service provider. If the CA is contracted by other certification service providers, it is obliged to treat technical and organisational procedures identically to the described GLOBALTRUST® Certificate Policy. Where the independent performance of certification services (CA) as well as the performance of services as a contractor is referred to, this is referred to comprehensively as “operator” in this document

Betreiber

Betreiber beschreibt die Rolle des VDA als Dienstleister. Soweit der VDA als Dienstleister für andere Vertrauensdienstanbieter tätig ist, verpflichtet er sich die technischen und organisatorischen Abläufe ident zu der beschriebenen GLOBALTRUST® Certificate Policy zu behandeln. In den Fällen, in denen sowohl auf die eigenständige Erbringung von Zertifizierungsdiensten (VDA), als auch auf die Erbringung als Dienstleister verwiesen werden soll, wird in diesem Dokument umfassend von "Betreiber" gesprochen.

Service Provider

Further entities or natural Persons who have been fully or partially entrusted with the technical or commercial implementation of certification services by the CA. The issuer of this document acts as a conractor if it performs certification servicesunder the instruction of another certificate authority (“contractor of a CA”).

Dienstleister

Weitere Einrichtungen oder natürliche Personen, die vom VDA mit der technischen oder wirtschaftlichen Umsetzung von Zertifizierungsdiensten teilweise oder ganz betraut werden. Dienstleister ist der Herausgeber, wenn er Zertifizierungsdienste im Auftrag eines anderen Vertrauensdienstanbieters erbringt ("Dienstleister eines VDA").

Reseller

Entities that have specific agreements with the CA regarding distribution. A list of resellers is available on the website of the CA.

Vertriebspartner

Einrichtungen, die mit dem VDA spezifische Vereinbarungen zum Vertrieb von Zertifizierungsdiensten haben. Eine Liste von Vertriebspartnern ist über die Website des VDA abrufbar.

Regulator

A regulator responsible for the certification services of the CA by law.

Aufsichtsbehörde

Eine für die Zertifizierungsdienste des VDA auf Grund gesetzlicher Vorgaben zuständige Aufsichtsbehörde.

Confirmationauthority

Bestätigungsstelle

A confirmation authority as established by the Austrian Signature Law [SVG] ("Bestätigungsstelle"), or confirmation authority for secure signature-creation devices as established by legal provisions in other States issued on the basis of the EU signature regulation [eIDAS-VO].

Nach dem österreichischen Signatur- und Vertrauensdienstegesetz [SVG] eingerichtete Bestätigungsstelle oder eine nach einer auf Basis der EU Signatur-Verordnung [eIDAS-VO] erlassenen gesetzlichen Bestimmung in einem anderen Staat eingerichtete Bestätigungsstelle für sichere Signaturerstellungseinheiten.

Competent independent auditor

An auditor that is competent to audit certification authorities according to at least one of the following or a stricter criterion:
- [[ETSI EN 319 401], [ETSI EN 319 411-1], [ETSI EN 319 411-2]
- [eIDAS-VO]
- [SVG] + [SVV]
- [CABROWSER-BASE]
- [CABROWSER-EV]
- [MOZILLA-CAPOL]
- [WEBTRUST-CA]
- [WEBTRUST-EV]

The auditor employs employees with the competence to examine PK infrastructure, IT security technology and IT security, as audited and accredited by a third partyThe auditor is accredited to audit to ETSI standards, according to ETSI TS 119 403, and to conduct ISO 27001 audits (or similar), according to ISO 27006. The auditor acts on the basis of a legal warrant, according to public guidelines, or follows the guidelines of a professional association. If the auditor does not act in the framework of a legal warrant, it has liability insurance available to it with an indemnity limit of at least 1 000 000 USD.

In the event of an audit, the auditor announces the criteria under which the audit will be conducted and under which criteria it acts and is accredited.

kompetente unabhängige Auditstelle

Auditstelle, die befähigt ist Zertifizierungsstellen nach zumindest einem der folgenden oder einem strengerem Kriterium zu prüfen:
- [ETSI EN 319 401], [ETSI EN 319 411-1], [ETSI EN 319 411-2]
- [eIDAS-VO]
- [SVG] + [SVV]
- [CABROWSER-BASE]
- [CABROWSER-EV]
- [MOZILLA-CAPOL]
- [WEBTRUST-CA]
- [WEBTRUST-EV]

Die Auditstelle beschäftigt Mitarbeiter die die Fähigkeit in der Prüfung von PK-Infrastruktur, IT-Sicherheits Techniken, IT-Sicherheits durch Audits und Akreditierung von Dritten haben. Die Auditstelle ist akredidiert nach ETSI TS 119 403 zur Prüfung von ETSI-Standards, nach ISO 27006 zur Durchführung von ISO 27001 Audits (oder vergleichbar). Die Auditstelle handelt auf Grund einer gesetzlichen Befugnis, nach öffentlichen Richtlinien oder folgt den Richtlinien eines Berufsverbandes. Die Auditstelle - soweit sie nicht im Rahmen einer gesetzlichen Befugnis tätig ist - verfügt über eine Haftpflichtvericherung mit einer Deckungssumme von mindestens USD 1.000.000.

Im Falle einer Prüfung gibt die Auditstelle bekannt, nach welchen Kriterien sie die Prüfung durchführte und nach welchen Kriterien sie tätig und akredidiert ist.

Concerned party

Betroffener

All persons whose personal data is stored and/or processed by the operator.

Alle Personen zu denen der Betreiber personenbezogene Daten verwaltet.

1.4 Certificate usage / Verwendungszweck der Zertifikate

1.4.1 Appropriate certificate uses / Verwendungszweck

Legitimate uses are derived from the certificate's contents, the GLOBALTRUST® Certificate Policy and the applicable GLOBALTRUST® Certificate Practice Statement.

Die zulässigen Verwendungszwecke ergeben sich aus den Einträgen im Zertifikat, dieser GLOBALTRUST® Certificate Policy und dem anzuwendenden GLOBALTRUST® Certificate Practice Statement.

Legitimate formats of data to be signed can be listed in the document ⇨ Appendix / Anhang A: 3 supported signature creation unitS / Unterstützte Signaturerstellungsprodukte (p211), in the respectively applicable certificate policy or on the website of the CA. If restrictions regarding specific formats exist, they are included in the document. Reference to publications of regulators with regard to acceptable and/or recommended data formats is also permissible.

Die zulässigen Formate der zu signierenden Daten können im Dokument ⇨ Appendix / Anhang A: 3 supported signature creation unitS / Unterstützte Signaturerstellungsprodukte (p211), in der jeweils anzuwendenden Certificate Policy oder auf der Website des VDA gelistet werden. Sofern bei Formaten Einsatzbeschränkungen bestehen, werden diese im Dokument angeführt. Zulässig ist dabei auch ein Verweis auf Publikationen der Aufsichtsstellen bezüglich zulässiger und/oder empfohlener Datei-Formate.

With regard to signature-creation devices, there are no obligatory technical guidelines for advanced signatures. The subscriber is free to use the signature-creation device at his discretion, but must ensure sole personal control of the signatures assigned to him as is legally compulsory.

Bezüglich der Signaturerstellungseinheiten fortgeschrittener Signaturen werden keine zwingenden technischen Vorgaben gemacht. Der Signator ist im Einsatz der Signaturerstellungseinheiten frei, er muss jedoch rechtlich verbindlich die persönliche und alleinige Kontrolle über die ihm zugeordnete Signatur zusichern.

Binding transactions with a value over 100 000 EUR require a qualified certificate for electronic signatures.

Verbindliche Rechtsgeschäfte mit einem Wert von mehr als 100.000,- Euro erfordern ein qualifiziertes Zertifikat für elektronische Signaturen.

If it is not possible to verify the certificate of an electronic signature, it is the sole responsibility of the relying party whether or not they recognise the validity of the signature. The CA holds no responsibility in this regard.

Ist die Überprüfung eines Zertifikates zu einer elektronischen Signatur nicht möglich, liegt es in der alleinigen Verantwortung des Nutzers, ob er die Gültigkeit der Signatur anerkennt, eine Haftung des VDA ist ausdrücklich ausgeschlossen.

It is permissible to announce limitations on the use or validity of the certificate on the website or in otherwise published conditions (in particular

Es ist zulässig über die Website oder sonstwie veröffentliche Bedingungen Einschränkungen in der Nutzung bzw. Gültigkeit des

notice of the maximum transaction value for which the signature can be validly issued). The responsibility of the CA is also limited in line with the given limitations and maximum amounts.

Zertifikats (insbesondere Beachtung von Betragsobergrenzen bis zu denen die Signatur gültig ausgestellt wird festzulegen). Gemäß dieser eingetragenen Einschränkungen und Obergrenzen beschränkt sich auch die Haftung des VDA.

Additional limitations can also arise from the type of certificate issued and its usage.

Zusätzliche Einschränkungen können sich aus dem Typus des ausgestellten Zertifikates und des Verwendungszweckes ergeben.

The subscriber is required to use the Key Pair only in accordance with this Policy and to use only the key generation algorithms and parameters described in this Policy.

Der Signator ist verpflichtet, das Schlüsselpaar nur im Einklang mit dieser Policy zu verwenden und nur die in dieser Policy beschriebenen Algorithmen und Parameters zur Schlüsselgenerierung zu verwenden.

1.4.2 Prohibited certificate uses / Untersagte Nutzung der Zertifikate

Where it is technically feasible and appropriate, usage restrictions are included in the certificates in a form compliant with the standard. Restrictions on permissible domain names and IP addresses are given on enduser-sub-certificates intended for the issuance of server certificates.

Dort wo dies technisch machbar und sinnvoll ist werden Verwendungsbeschränkungen direkt in den Zertifikaten in der dem Standard entsprechenden Form eingetragen. Bei Endkunden-Sub-Zertifikaten die zur Ausstellung von Serverzertifikaten vorgesehen sind, erfolgt eine Beschränkung der zulässigen Domainnamen und IP-Adressen.

1.5 Policy administration /Policy Verwaltung

1.5.1 Organization administering the document /Zuständigkeit für das Dokument

This document is the sole responsibility of the operator.

Das vorliegende Dokument unterliegt der alleinigen Verantwortung des Betreibers.

1.5.2 Contact person / Kontaktperson

Queries regarding this document can be directed to the operator. Current contact details are listed on the operator's website. (⇨ Contact details: http://www.globaltrust.eu/impressum.html).

Anfragen zum Dokument sind an den Betreiber zu richten. Die aktuellen Kontaktdaten sind auf der Website des Betreibers gelistet (⇨ Contact: http://www.globaltrust.eu/impressum.html) .

Requests for revocation should be sent as soon as possible via https://www.globaltrust.eu/revocation.html. Alternatively, revocations can also be requested by email to revocation@globaltrust.eu or by phone. In any case, sufficient revocation authorization must be demonstrated, for example through online authentication.

In the case of certificate-related problems, such as suspected misuse, everyone involved can contact the operator via abuse@globaltrust.eu or by phone. A Certificate Problem Report must contain at least:

- An indication that allow a unique identification oft he certificate
- An understandable statement of the circumstances
- The contact details of the sender

Both requests for revocation and Certificate Problem Reports are taken seriously and are given priority.

Anträge auf Widerruf sollten so rasch als möglich via https://www.globaltrust.eu/revocation.html übermittelt werden. Alternativ können Widerrufe auch per email an revocation@globaltrust.eu oder telefonisch beantragt werden. In jedem Fall ist eine ausreichende Berechtigung zum Widerruf nachzuweisen, zum Beispiel durch online-Authentisierung.

Bei zertifikatsbezogenen Problemen, zum Beispiel bei Verdacht auf Missbrauch, kann sich jeder Beteiligte an abuse@globaltrust.eu oder telefonisch mit dem Betreiber in Verbindung setzen.. Ein Problembericht muss mindestens enhalten:

- Eine Angabe, die zur ununterscheidbaren Identifizerung des Zeritfikats geeignet ist, vorzugsweise die Seriennummer
- Eine verständliche Darlegung der Umstände auf die er sich bezieht
- Die Kontaktdaten des Absenders

Sowohl Widerrufsanträge als auch sonstige Problemberichte werden grundsätzlich ernst genommen und mit Priorität behandelt.

1.5.3 Person determining CPS suitability for the policy / Person die die Eignung der CPS bestätigt

GLOBALTRUST® Certificate Practice Statements are assigned and accepted by the certification committee in accordance with the accountability concept (⇨ GLOBALTRUST® Certificate Security Policy.

GLOBALTRUST® Certificate Practice Statements werden gemäß Rollenkonzept (⇨ GLOBALTRUST® Certificate Security Policy durch den Zertifizierungs-Ausschuss in Auftrag gegeben und durch den Zertifizierungs-Ausschuss abgenommen.

1.5.4 CPS approval procedures / Verfahren zur Freigabe der CPS

GLOBALTRUST® Certificate Practice Statements are verified and issued by regular members of the certification committee. Acceptability is confirmed by a representative of the management and at least one further member of the certification committee.

GLOBALTRUST® Certificate Practice Statements werden durch die regulären Mitglieder des Zertifizierungs-Ausschusses geprüft und freigegeben. Die Eignung des GLOBALTRUST® Certificate Practice Statements wird durch einen

Vertreter der Geschäftsführung und zumindest ein weiteres Mitglied des Zertifizierungs-Ausschusses bestätigt und intern dokumentiert.

1.6 Definitions and acronyms / Definitionen und Kurzbezeichnungen

Business process

A logical unit of measures and procedures towards a defined objective. The ⇨ certification services are a subgroup of all the business processes of the operator.

Certification services

All services performed by the operator, in particular the following principle services:

- Administration of applicants for certificates (including identification of applicants)
- Issuing of certificates (including suspension and revocation of certificates)
- Distribution of certificates
- Administration of applications for suspension and revocation
- Distribution of information on suspension and revocation

Further certification services include, in particular

- Provisioning and distribution of signature-creation devices
- Time stamp services
- Other signature services, such as signature services via mobile devices (“mobile signature”), other server-based signature services, in particular document archive services that are run by the operator.

Certification services are performed according to EU signature regulation [eIDAS-VO], [SVG] and [CWA-14167-1], and include simple, advanced and qualified electronic signatures, qualified or simple certificates and qualified or simple time stamp services.

Geschäftsprozess

Logische Einheit aller Maßnahmen und Abläufe zur Erreichung eines inhaltlich definierten Zieles. Die ⇨ Zertifizierungsdienste sind eine Untergruppe aller Geschäftsprozesse des Betreibers.

Zertifizierungsdienste

Gesamtheit aller Dienstleistungen, die der Betreiber erbringt, insbesondere sind dies folgende zentrale Dienste:

- Verwaltung von Antragstellern für Zertifikate (inkl. Identifikation der Antragsteller)
- Ausstellen von Zertifikaten (inkl. Sperre und Widerruf von Zertifikaten)
- Ausliefern von Zertifikaten
- Verwaltung von Sperr- und Widerrufsanträgen
- Verbreitung von Sperr- und Widerrufsinformationen

Weitere Zertifizierungsdienste sind insbesondere

- Erstellen und Ausliefern von Signaturerstellungseinheiten
- Zeitstempeldienste
- sonstige Signaturdienste, wie Signaturdienste mittels mobile Devices ("Handysignatur"), sonstige serverbasierte Signaturdienste, insbesondere Dokumentenarchivierungsdienste die vom Betreiber selbst betrieben werden.

Die Erbringung erfolgt insbesondere gemäß EU Signaturverordnung [eIDAS-VO], [SVG] und [CWA-14167-1] und umfasst sowohl Dienstleistungen zur einfachen, fortgeschrittenen oder qualifizierten elektronischen Signatur, zu qualifizierten oder einfachen Zertifikaten, zu

Individual services are organised as ⇨ business processes.

Server-based signature services

Services of the operator in administration, archiving, creation, verification or delivery of signed documents. The documents can be signed by the relying party, the operator, authorised third parties or a combination of the above-named groups. Qualified or non-qualified certificates can be used as proof of authenticity. The server-based signature service may also be offered as a part of the operator's services, for example in the context of pseudonymisation and anonymisation services.

Electronic signature

Data in electronic form according to EU signature regulation [eIDAS-VO], which is attached or logically linked to electronic data and authenticates it.

Certificate data

All data, in particular identification data, which is necessary for issuance, audit or revocation of certificates.

Simple electronic signature

An electronic signature that conforms to the requirements of neither the advanced electronic signature nor the qualified electronic signature.

Advanced electronic signature

An electronic signature that fulfils the following criteria:
a) it is assigned exclusively to the subscriber;
b) it enables the identification of the subscriber;
c) it is created by means that the subscriber can keep under their sole control;

qualifizierten oder einfachen Zeitstempeldiensten.

Die einzelnen Dienste sind als ⇨ Geschäftsprozesse organisiert.

serverbasierte Signaturdienste

Dienstleistungen des Betreibers zur Verwaltung, Archivierung, Erstellung, Verifizierung oder Zustellung signierter Dokumente. Die Dokumente können individuell durch den Nutzer, den Betreiber, autorisierte Dritte oder einer Kombination aus den genannten Personengruppen signiert werden. Es können zum Nachweis der Authentizität qualifizierte oder nicht qualifizierte Zertifikate verwendet werden. Der serverbasierte Signaturdienst kann auch nur Teil eines Dienstangebots des Betreibers sein, etwa im Rahmen von Pseudonymisierungs- und Anonymisierungsdiensten.

elektronische Signatur

Daten in elektronischer Form im Sinne EU Signaturverordnung [eIDAS-VO], die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen.

Zertifikatsdaten

Gesamtheit aller Daten, insbesondere Identifikationsdaten, die für Ausstellung, Prüfung oder Widerruf von Zertifikaten erforderlich sind.

einfache elektronische Signatur

Elektronische Signatur, die weder den Anforderungen der fortgeschrittenen elektronischen Signatur, noch denen der qualifizierten elektronischen Signatur entspricht.

fortgeschrittene elektronische Signatur

Eine elektronische Signatur, die folgende Anforderungen erfüllt:
a) sie ist ausschließlich dem Unterzeichner zugeordnet;
b) sie ermöglicht die Identifizierung des Unterzeichners;
c) sie wird mit Mitteln erstellt, die der Unterzeichner unter seiner alleinigen Kontrolle halten kann;

d) it is linked to the data to which it refers in such a way that later changes to the data can be recognised.

Governmental signature ("Amtssignatur")

Advanced electronic signature according to the E-Government Law [E-GOVG], in particular taking [ASZ] and similar documentation with a governmental character into account.

Qualified electronic signature

An electronic signature that fulfils the following criteria:
- all criteria of an advanced electronic signature,
- that is based upon a qualified certificate and
- has been created by a secure signature-creation device (SSCD).

Certificate

An electronic attestation that assigns signature verification data to a subscriber and confirms the identity of that signatory, the legal entity he represents, or a system controlled by him or his legal entity.

The name of the issuing certificate for which this policy is valid is set out in detail in the GLOBALTRUST® Certificate Practice Statement.

Server certificate

A certificate for website authentication and SSL/TLS that has been issued in accordance with [CABROWSER-BASE] or [CABROWSER-EV].

The name of the issuing certificate for which this policy is valid is set out in detail in the GLOBALTRUST® Certificate Practice Statement.

d) sie ist so mit den Daten, auf die sie sich bezieht, verknüpft, dass eine nachträgliche Veränderung der Daten erkannt werden kann.

Amtssignatur

Fortgeschrittene elektronische Signatur gemäß E-Governmentgesetz [E-GOVG], insbesondere unter Berücksichtigung von [ASZ] und vergleichbarer Dokumentationen mit amtlichen Charakter.

qualifizierte elektronische Signatur

Elektronische Signatur die folgende Anforderungen erfüllt:
- alle Anforderungen der fortgeschrittenen elektronischen Signatur,
- die auf einem qualifizierten Zertifikat beruht und
- von einer sicheren Signaturerstellungseinheit (SSCD) erstellt wird.

Zertifikat

Eine elektronische Bescheinigung, mit der Signaturprüfdaten einem Signator zugeordnet werden und die Identität dieses Signators, der von ihm vertretenen juristischen Person oder einem von ihm oder der von ihm vertretenen juristischen Person kontrollierten System bestätigt wird.

Die Bezeichnung der ausstellenden Zertifikate für die diese Policy gültig ist wird detailliert im GLOBALTRUST® Certificate Practice Statement dargelegt.

Serverzertifikat

Zertifikat, das der Website-Authentisierung und SSL/TLS-Verwendung dient und das gemäß [CABROWSER-BASE] oder [CABROWSER-EV] ausgestellt wurde.

Die Bezeichnung der ausstellenden Zertifikate für die diese Policy gültig ist wird detailliert im GLOBALTRUST® Certificate Practice Statement dargelegt.

Simple certificate

A certificate that does not fulfil the criteria of a qualified certificate. Simple certificates contain at least the following entries:

The subject is encoded according to UTF-8 if it contains umlauts or special characters. PrintableString can be used if it does not contain umlauts or special characters.

The subject can contain the following inputs: countryName (mandatory), localityName (mandatory), stateOrProvinceName (optional), organizationName (if the certificate is being issued for an organisation), organizationalUnitName (optional), commonName or pseudonym or givenName (it is mandatory to fill in one), title (optional), serialNumber (optional). Each field can only be used for those inputs which are defined according to the applicable standards and norms.

Further information in the certificate:

- X509v3 Key Usage: critical e.g. Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment
- X509v3 Extended Key Usage: mandatory at least one entry e.g. emailProtection. AnyExtendedKeyUsage is not used.
- X509v3 Subject Alternative Name, e.g. z.B. email:my@other.address,URI:http://my.url.here/

- CA Issuers - URI:http://service.globaltrust.eu/static/globaltrust-NN-**-der.cer[3]

einfaches Zertifikat

Zertifikat, das nicht den Kriterien eines qualifizierten Zertifikates entspricht. Einfache Zertifikate enthalten zumindest folgende Angaben:

Die Kodierung des Subjects erfolgt gemäß UTF-8 wenn Umlaute/Sonderzeichen enthalten sind, printableString kann verwendet werden, wenn Umlaute/Sonderzeichen nicht enthalten sind.

Das Subject kann folgende Einträge enthalten: countryName (verpflichtend), localityName (verpflichtend), stateOrProvinceName (optional), organizationName (sofern Zertifikat für eine Organisation ausgestellt wird), organizationalUnitName (optional), commonName oder pseudonym oder givenName (eines ist verpflichtend), title (optional), serialNumber (optional). Jedes Feld kann nur für jene Einträge verwendet werden, für das es gemäß der anzuwendenden Standards und Normen definiert ist.

Weitere Angaben im Zertifikat:

- X509v3 Key Usage: critical , z.B. Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment
- X509v3 Extended Key Usage: zwingend zumindestens ein Eintrag z.B. emailProtection, nicht verwendet wird der Eintrag anyExtendedKeyUsage.
- X509v3 Subject Alternative Name z.B. z.B. email:my@other.address,URI:http://my.url.here/
- CA Issuers - URI:http://service.globaltrust.eu/static/globaltrust-NN-**[3]-der.cer

[3] NN== Identifier of a product line of the CA, for example, server, advanced, client, ...,
== continual numbers, beginning with 1, to differentiate different CA certificates in the same product line (in the future), for example GLOBALTRUST ADVANCED 1 uses the file http://service.globaltrust.eu/static/globaltrust-qualified-1**-der.cer as certificate URL and http://service.globaltrust.eu/static/globaltrust-**qualified-1**.crl as revocation list. A detailed description of which policy, CRL, LDAP service and OCA service belongs to which product can be found under ⇨ Policy Online: http://www.globaltrust.eu/certificate-policy.html
NN == Bezeichnung der Produktlinie des VDA, z.B. server, advanced, client, ...,

- X509v3 CRL Distribution Points: Full Name: URI:http://service.globaltrust.eu/static/globaltrust-NN-**.crl
- OCA - URI:http://OCA-NN-**[4].globaltrust.eu
- X509v3 Certificate Policies: Policy: 1.2.40.0.36.1.1.8.1
- CPS: http://www.globaltrust.eu/certificate-policy.htm
- Policy: 1.2.40.0.36.4.1.10 (Certificates that had been issued between 1.7.2014 and 1st April 2019 and whose keys have not been generated in a signature creation device that do not comply with at least FIPS-140 2 L2 or CC Protection Profile CWA 14169)
- Administration attribute "Verwaltungseigenschaft" (OID 1.2.40.0.10.1.1.1): Administration identifier (optional)
- Operator attribute "Dienstleistereigenschaft" (OID 1.2.40.0.10.1.1.2): NULL (optional)
- Official attribute "Organwaltereigenschaft" (OID 1.2.40.0.10.3.4): Administration identifier (optional)
- Attribute of signature for electronic authority (OID 1.2.40.0.10.1.7.2): NULL (optional)
- Signature algorithm used for end-user certifcates: SHA2 (sha256WithRSAEncryption or higher)

Qualified certificate for electronic signatures

A certificate for the creation of electronic signatures that it is issued with the latest technology and fulfils, in particular, the requirements in [eIDAS-VO] Appendix I and is provided by a Certification Service Provider (CA) that fulfils the requirements in [eIDAS-VO].

- X509v3 CRL Distribution Points: Full Name: URI:http://service.globaltrust.eu/static/globaltrust-NN-**.crl
- OCA - URI:http://OCA-NN-**[4].globaltrust.eu
- X509v3 Certificate Policies: Policy: 1.2.40.0.36.1.1.8.1
- CPS: http://www.globaltrust.eu/certificate-policy.htm
- Policy: 1.2.40.0.36.4.1.10 (Zertifikate die zwischen 1.7.2014 und 1.4.2019 ausgestellt wurden und deren Schlüssel nicht in einer Signaturerstellungseinheit erzeugt wurden, die nicht zumindest FIPS-140 2 L2 oder CC Protection Profile CWA 14169 entspricht)
- Verwaltungseigenschaft (OID 1.2.40.0.10.1.1.1): Verwaltungskennzeichen (optional)
- Dienstleistereigenschaft (OID 1.2.40.0.10.1.1.2): NULL (optional)
- Organwaltereigenschaft (OID 1.2.40.0.10.3.4): Verwaltungskennzeichen (optional)
- Eigenschaft zur Signatur von elektronischer Vollmachten (OID 1.2.40.0.10.1.7.2): NULL (optional)
- Verwendeter Signature Algorithm für Zertifikate, die an Enduser ausgestellt werden: SHA2 (sha256WithRSAEncryption oder höher)

qualifiziertes Zertifikat für elektronische Signaturen

Ein Zertifikat, das zur Erstellung elektronischer Signaturen dient und das dem Stand der Technik ausgestellt wurde und insbesondere die Anforderungen der [eIDAS-VO] Anhang I erfüllt und von einem Zertifizierungsdiensteanbieter (VDA) bereitgestellt wird, der die Anforderungen der [eIDAS-VO] erfüllt.

** == laufende Nummer, beginnend mit 1 zur (zukünftigen) Unterscheidung unterschiedlicher CA-Zertifikate derselben Produktlinie, z.B. GLOBALTRUST QUALIFIED 1 verwendet die Dateien http://service.globaltrust.eu/static/globaltrust-**qualified-1**-der.cer als Zertifikats-URL und http://service.globaltrust.eu/static/globaltrust-**qualified-1**.crl als Widerrufsliste. Die detaillierte Darstellung zu welchem Produkt welche Policy, welche CRL, welcher LDAP-Dienst und welches OCA-Service zugeordnet ist findet sich unter ⇨ Policy Online: http://www.globaltrust.eu/certificate-policy.html

4 -NN-**== in the event of OCA responder, the CA reserves the right to leave the string "-NN-**" empty.
-NN-** == im Fall der OCA-Responder behält sich der VDA vor den String "-NN-**" leer zu lassen.

The content follows [ETSI EN 319 412]. The validity period of the qualified certificate for electronic signatures is limited to 5 years by law and can be shortened by the CA for legal or other important reasons at any time.

Der Inhalt folgt [ETSI EN 319 412]. Die Laufzeit des qualifizierten Zertifikats für elektronische Signaturen ist auf Grund der rechtlichen Vorgaben auf maximal 5 Jahre limitiert und kann vom VDA auf Grund geänderter rechtlicher Rahmenbedingungen oder anderer wichtiger Gründe jederzeit verkürzt werden.

Qualified server certificate

A certificate for website authentication that it is issued with the latest technology and fulfils, in particular, the requirements in [eIDAS-VO] Appendix IV as well as [CABROWSER-EV] and is provided by a Certification Service Provider (CA) that fulfils the requirements in [eIDAS-VO].

The content follows [ETSI EN 319 412] as well as [CABROWSER-EV] The validity period of the qualified server certificate is limited to 825 days by law and can be shortened by the CA for legal or other important reasons at any time. Qualified server certificates issued on or after 1st September 2020 will have a validity period no greater than 397 days.

qualifiziertes Serverzertifikat

Ein Zertifikat, das zur Websiteauthentifizierung dient und das dem Stand der Technik ausgestellt wurde und insbesondere die Anforderungen der [eIDAS-VO] Anhang IV sowie [CABROWSER-EV] erfüllt und von einem Zertifizierungsdiensteanbieter (VDA) bereitgestellt wird, der die Anforderungen der [eIDAS-VO] erfüllt.

Der Inhalt folgt [ETSI EN 319 412] sowie [CABROWSER-EV] Die Laufzeit des qualifizierten Serverzertifikats ist auf Grund der rechtlichen Vorgaben auf maximal 825 Tage limitiert und kann vom VDA auf Grund geänderter rechtlicher Rahmenbedingungen oder anderer wichtiger Gründe jederzeit verkürzt werden. Die Laufzeit von qualifizierten Serverzertifikaten, die ab 1.9.2020 ausgestellt werden, ist mit 397 Tagen limitiert.

Qualified certificate

The certificate can be issued either as a qualified certificate for electronic signatures or as a qualified server certificate and contains a reference to the certificate policy under which the certificate has been issued and which clearly identifies it as a qualified certificate.

The subject is encoded according to UTF-8 if it contains umlauts or special characters. PrintableString can be used if it does not contain umlauts or special characters.

The subject can contain the following inputs: countryName (mandatory), localityName (mandatory), stateOrProvinceName (optional),

qualifiziertes Zertifikat

Kann entweder als qualifiziertes Zertifikat für elektronische Signaturen oder als qualifiziertes Serverzertifikat ausgestellt werden und enthält einen Hinweis auf die Certificate Policy unter der das Zertifikat ausgestellt wurde und die es eindeutig als qualifiziertes Zertifikat kennzeichnet.

Die Kodierung des Subjects erfolgt gemäß UTF-8 wenn Umlaute/Sonderzeichen enthalten sind, printableString kann verwendet werden, wenn Umlaute/Sonderzeichen nicht enthalten sinnd.

Das Subject kann folgende Einträge enthalten: countryName (verpflichtend), localityName (verpflichtend), stateOrProvinceName

organizationName (if the certificate is being issued for an organisation), organizationalUnitName (optional), commonName or pseudonym or givenName (it is mandatory to fill in one), title (optional), serialNumber (mandatory), businessCategory (mandatory in case of qualified server certificates), jurisdictionLocalityName and/or jurisdictionStateOrProvinceName and/or jurisdictionCountryName (only in case of qualified server certificates, usage according to [CABROWSER-EV]) Each field can only be used for those inputs which are defined according to the applicable standards and norms.

Further information in the certificate:

- X509v3 Key Usage: critical Digital Signature and Key Encipherment (in case of qualified server certificates)
- X509v3 Extended Key Usage: mandatory at least one entry, e.g. TLS Web Server Authentication and/or TLS Web Client Authentication AnyExtendedKeyUsage is not used.

- CA Issuers - URI:http://service.globaltrust.eu/static/globaltrust-NN-**-der.cer
- X509v3 CRL Distribution Points: Full Name: URI:http://service.globaltrust.eu/static/globaltrust-NN-**.crl
- OCA - URI:http://OCA-NN-**.globaltrust.eu
- X509v3 Certificate Policies: Policy: 1.2.40.0.36.1.1.##.1
- CPS: http://www.globaltrust.eu/certificate-policy.htm Policy: 0.4.0.1456.1.1 (qualified certifiactes for electronic signatures) or 0.4.0.194112.1.4 (qualified server certificates) and 2.23.140.1.1 (qualified server certificates with additional EV treatment)

- 1.2.40.0.36.4.1.3: [Serial number of the signature-creation device as ASN1 OCTET STRING]
- qcStatements:

(optional), organizationName (sofern Zertifikat für eine Organisation ausgestellt wird), organizationalUnitName (optional), commonName oder pseudonym oder givenName (eines ist verpflichtend), title (optional), serialNumber (verpflichtend), businessCategory (verpflichtend, nur bei qualifizierten Serverzertifikaten), jurisdictionLocalityName und/oder jurisdictionStateOrProvinceName und/oder jurisdictionCountryName (nur bei qualifizierten Serverzertifikaten, Einsatz gemäß [CABROWSER-EV]) Jedes Feld kann nur für jene Einträge verwendet werden, für das es gemäß der anzuwendenden Standards und Normen definiert ist.

Weitere Angaben im Zertifikat:

- X509v3 Key Usage: critical Digital Signature und bei qualifizierten Serverzertifikaten zusätzlich: Key Encipherment
- X509v3 Extended Key Usage: zwingend mindestens ein Eintrag, z.B. TLS Web Server Authentication und/oder TLS Web Client Authentication. Nicht verwendet wird der Eintrag anyExtendedKeyUsage.
- CA Issuers - URI:http://service.globaltrust.eu/static/globaltrust-NN-**-der.cer
- X509v3 CRL Distribution Points: Full Name: URI:http://service.globaltrust.eu/static/globaltrust-NN-**.crl
- OCA - URI:http://OCA-NN-**.globaltrust.eu
- X509v3 Certificate Policies: Policy: 1.2.40.0.36.1.1.##.1
- CPS: http://www.globaltrust.eu/certificate-policy.htm Policy: 0.4.0.1456.1.1 (qualifizierte Zertifikate für elektronische Signaturen) oder 0.4.0.194112.1.4 (qualifizierte Serverzertifikate) und 2.23.140.1.1 (qualifizierte Serverzertifikate, wenn auch EV)

- 1.2.40.0.36.4.1.3: [Seriennummer der Signaturerstellungseinheit als ASN1 OCTET STRING]
- qcStatements:

- id-etsi-qcs-QcCompliance (OID 0.4.0.1862.1.1),
- id-etsi-qcs-QcLimitValue: QcEuLimitValue (OID 0.4.0.1862.1.2) (optional)
- id-etsi-qcs-QcRetentionPeriod: QcEuRetentionPeriod (OID 0.4.0.1862.1.3) (optional)
- id-etsi-qcs-QcSSCD (OID 0.4.0.1862.1.4)

- id-etsi-qcs-QcType (OID 0.4.0.1862.1.6)
- id-etsi-qct-web (OID 0.4.0.1862.1.6.3)
- Administration attribute "Verwaltungseigenschaft" (OID 1.2.40.0.10.1.1.1): Administration identifier (optional)
- Operator attribute "Dienstleistereigenschaft" (OID 1.2.40.0.10.1.1.2): NULL (optional)
- Official attribute "Organwaltereigenschaft" (OID 1.2.40.0.10.3.4): Administration identifier (optional)
- Attribute of signature for electronic authority (OID 1.2.40.0.10.1.7.2): NULL (optional)
- further OID inputs if they are in accordance with the conditions for qualified certificates (optional)

Signature algorithm used: SHA2 (sha256WithRSAEncryption or higher)

Root certificate

A certificate that is used exclusively by the CA in the creation of certification services, which can only be signed by itself as the root of the certificate hierarchy (also self-signed certificate).

The root certificates of the issuer and user (applicant) have identical information.

The private key of the root certificate is generated for use using RSA and with a minimum length of 4096 bits. The hash algorithm used is for the

- id-etsi-qcs-QcCompliance (OID 0.4.0.1862.1.1),
- id-etsi-qcs-QcLimitValue: QcEuLimitValue (OID 0.4.0.1862.1.2) (optional)
- id-etsi-qcs-QcRetentionPeriod: QcEuRetentionPeriod (OID 0.4.0.1862.1.3) (optional)
- id-etsi-qcs-QcSSCD (OID 0.4.0.1862.1.4)

- id-etsi-qcs-QcType (OID 0.4.0.1862.1.6)
- id-etsi-qct-web (OID 0.4.0.1862.1.6.3)
- Verwaltungseigenschaft (OID 1.2.40.0.10.1.1.1): Verwaltungskennzeichen (optional)
- Dienstleistereigenschaft (OID 1.2.40.0.10.1.1.2): NULL (optional)

- Organwaltereigenschaft (OID 1.2.40.0.10.3.4): Verwaltungskennzeichen (optional)
- Eigenschaft zur Signatur von elektronischer Vollmachten (OID 1.2.40.0.10.1.7.2): NULL (optional)
- weitere OID-Einträge sofern im Einklang mit den Bestimmungen zu qualifizierten Zertifikaten (optional)

Verwendeter Signature Algorithm: SHA2 (sha256WithRSAEncryption oder höher)

Root-Zertifikat

Zertifikat das vom VDA ausschließlich zur Erbringung von Zertifizierungsdiensten verwendet wird und dass als oberste Instanz nur von sich selbst unterschrieben wird (auch Self-Signed-Zertifikat bzw. Wurzel-Zertifikat).

Die Root-Zertifikate sind in den Angaben von Herausgeber und Anwender (Antragsteller) ident und Root-Zertifikate weisen im Herausgeber- und Subject-Feld idente Angaben auf.

Der private Schlüssel von Root-Zertifikaten wird für die Verwendung mittels RSA und mit einer Mindestlänge von 4096 bit generiert, der

root certificate SHA1. For root certificates that have been created since 1 October 2014, this is at least SHA256.

Root certificates are used only to sign CA certificates and revocation lists of the certification operations. Other uses are not allowed by the processes of the CA.

CA certificate

Certificates of the CA necessary to perform certification services. CA certificates can be self-signed certificates of the CA (root certificate) or sub-certificates issued under self-signed certificates that are intended for the performance of certification services. The fingerprints of the CA certificates and applicable policy are published on the website of the CA and the regulators responsible are notified (⇨ http://www.globaltrust.eu/certificate-policy.html).

The private keys of any CA certificates are generated using RSA and with a minimum length of 4096 bits. The hash algorithm used is at least SHA256.

CA certificates that are issued from February 1st, 2020, contain no more than the following subject data: two-digit country name according to ISO 3166-1 of the country in which the VDA is based, organization name of the VDA according to the commercial register entry and an a CN field eintry that allows precise differentiation from other CA certificates.

Further information in the certificate is at least:
- X509v3 Basic Constraints: critical, CA:TRUE

verwendete Hash-Algorithmus ist für Root-Zertifikate SHA1, für Root-Zertifikate, die nach dem 1. Oktober 2014 erstellt werden zumindest SHA256.

Root-Zertifikate werden ausschließlich zum Signieren von CA-Zertifikaten und Widerrufslisten. Andere Verwendungen sind auf Grund der Betriebsorganisation des VDA ausgeschlossen.

CA-Zertifikat

Zertifikate des VDA, die zur Erbringung von Zertifizierungsdiensten erforderlich sind. CA-Zertifikate können Self-Signed-Zertifikate des VDA sein (Root-Zertifikat) oder unter einem Self-Signed-Zertifikat ausgestellte Sub-Zertifikate, die zur Erbringung von Zertifizierungsdiensten vorgesehen sind. Die Fingerprints der CA-Zertifikate und die anzuwendende Policy sind auf der Website des VDA und bei den zuständigen Aufsichtsstellen hinterlegt (⇨ http://www.globaltrust.eu/certificate-policy.html).

Der private Schlüssel von CA-Zertifikaten wird für die Verwendung mittels RSA mit einer Mindestlänge von 4096 bit generiert, der verwendete Hash-Algorithmus ist zumindest SHA256.

CA-Zertifikate die ab 1.2.2020 ausgestellt werden, enthalten im Subject String nicht mehr als folgende Daten: zweistellige Länderbezeichnung gemäß ISO 3166-1 jenes Landes, in dem der VDA seinen Sitz hat, Organisationsbezeichnung des VDA laut Firmenbucheintrag[5] sowie einenEintrag im CN-Feld, der eine präzise Unterscheidung von anderen CA-Zertifikaten ermöglich

Weitere Angaben im Zertifikat sind jedenfalls:
- X509v3 Basic Constraints: critical, CA:TRUE

[5] In the case of X509v3 certificates, the CA uses the following issuer information (issuer data): C=AT und O= (company name according to commercial register)
Im Falle von X509v3-Zertifikaten verwendet der VDA folgende Herausgeberangaben (Issuer-Daten): C=AT und O= (Firmenbezeichnung lt. Firmenbuch)

- X509v3 Key Usage: critical Certificate Sign, CRL Sign

CA-certificates (with the exception of root certifcates), created on or after 1st January 2019, contain a least one X509v3 Extended Key Usage entry that indicates the permitted EKU-entries in end user certificates. The anyExtendedKeyUsage must not be used. Id-kp-serverAuth and id-kp-emailProtection must not be combined in the same CA-certificate.

CA certificates are used exclusively for signing (CA) certificates and revocation lists. Other uses are not allowed by the processes of the CA.

End user certificate

A certificate that has been signed by a CA certificate and can be used for signature and/or encryption purposes. Such a certificate cannot be used for the issuance of further (subordinate) certificates.

Sub-certificate

A certificate that has been signed by a CA certificate and can be used by the VDA to issue further certificates.

enduser-sub-certificate

Certificate signed by a sub-certificate of the operator and made available to the subscriber for issuing own end user certificates. In any case, it contains technical limitations, such as the name of the issuing company, domain names that the company demonstrably owns or country restrictions. These restrictions can be assigned alone or in combination, but country restrictions alone are not sufficient. Further, at least one entry in the extension field extendedKeyUsage is present.

- X509v3 Key Usage: critical Certificate Sign, CRL Sign

CA-Zertifikate (ausgenommen Root-Zertfikate), die ab 1.1.2019 ausgestellt werden, enthalten zumindest einen Eintrag im Feld X509v3 Extended Key Usage, der die möglichen EKU-Werte von Endzertifikaten enthält. Diese Erweiterung enthält niemals den Wert anyExtendedKeyUsage. Die Werte id-kp-serverAuth und id-kp-emailProtection werden nicht im selben CA-Zertifkat kombiniert

CA-Zertifikate werden ausschließlich zum Signieren von ausgestellten Zertifikaten, von CA-Zertifikaten und Widerrufslisten verwendet. Andere Verwendungen sind auf Grund der Betriebsorganisation des VDA ausgeschlossen.

Endkundenzertifikat

Zertifikat, dass von einem CA-Zertifikat unterschrieben ist und für Signatur- und/oder Verschlüsselungszwecke verwendet werden kann. Es erlaubt keine Ausstellung weiterer (untergeordneter) Zertifikate.

Sub-Zertifikat

Zertifikat, das von einem CA-Zertifikat unterschrieben ist und vom VDA auch für die Ausstellung weiterer Zertifikate verwendet werden kann.

Endkunden-Sub-Zertifikat

Spezielles Endkundenzertifikat, das von einem Sub-Zertifikat des Betreibers unterschrieben wird und das dem Signator zur Ausstellung eigener Endkundenzertifikate zur Verfügung gestellt wird. Es enthält jedenfalls technische Beschränkungen, zum Beispiel auf den Namen des ausstellenden Unternehmens, Domainnamen über die das Unternehmen nachweislich verfügt oder Länderbeschränkungen. Diese Beschränkungen können alleine oder kombiniert vergeben werden, wobei Länderbeschränkungen alleine nicht ausreichend sind. Weiters ist zumindest ein Eintrag im Feld extendedKeyUsage (zum Beispiel eMailProtection) vorhanden.

Time stamp

A signed data structure comprising the hash code of a document and the time of signature. The format and method of the generation of the time stamp complies with the standard [RFC3161] including the addition [RFC5816]. Information on the current operating data of the time stamp service (including accuracy and time stamp process) can be found on the website http://www.globaltrust.eu/produkte.html.

Qualified time stamp service

A service which generates time stamps using a qualified certificate or an equivalent process that ensures the correctness and authenticity of the time information contained.

Operation

All activities of the CA in performing certification services.

Operations concept

All documents on the operation of certification services that are audited and authorised by the ⇨ regulator.

Certification system

Technical system that enables the processing of certification services, in particular the issuance or revocation of certificates.

Administrative system

Administrative system used for verifying and generating data that is necessary for the issuance or revocation of certificates.

Information Security Management System (ISMS)

All technical and organisational measures for the planning, establishment, maintenance and change of the information security of the operator.

Zeitstempel, Timestamp

Signierte Datenstruktur bestehend jedenfalls aus dem Hashcode eines Dokuments und dem Zeitpunkt der Unterzeichnung. Format und Methode der Erzeugung des Zeitstempels entspricht dem Standard [RFC3161] inklusive der Ergänzung [RFC5816]. Angaben zu den aktuellen Betriebsdaten des Zeitstempeldienstes (inkl. Zeitgenauigkeit, Zeitstempelverfahren) finden sich auf Website http://www.globaltrust.eu/produkte.html. Die Begriffe Zeitstempel und Timestamp werden synonym verwendet.

qualifizierter Zeitstempeldienst

Dienst der Zeitstempel durch ein qualifiziertes Zertifikat oder ein vergleichbares Verfahren erzeugt, das die Richtigkeit und Unverfälschtheit der Zeitangabe sicherstellt.

Betrieb

Gesamtheit aller Tätigkeiten des VDA zur Erbringung der Zertifizierungsdienste.

Betriebskonzept

Gesamtheit aller Dokumente zum Betrieb der Zertifizierungsdienste die durch die ⇨ **Aufsichtsstelle** geprüft und genehmigt wurden.

Zertifizierungssystem

Technisches System, dass die Abwicklung von Zertifizierungsdiensten, insbesondere Ausstellung oder Widerruf von Zertifikaten, ermöglicht.

Administratives System

Verwaltungssystem zur Prüfung und Erzeugung der für die Ausstellung oder den Widerruf von Zertifikaten erforderlichen Daten.

Informationssicherheitsmanagementsystem, ISMS

Gesamtheit aller technischen und organisatorischen Maßnahmen zur Planung, Herstellung, Aufrechterhaltung, Änderung der

Private, public and international organisations

Private organisations are entities that have been established according to applicable regulations of private and civil law.

Public organisations are entities that have been established by the law of their respective lands, such as authorities, state administrations, municipal, regional or national offices.

International organisations are entities that have been established on the basis of treaties in the realm of public international law.

Signature creation data

Distinct data such as codes or private cryptographic keys that are used by the subscriber to create an electronic signature.

Activation data

Information belonging to the subscriber that is necessary for the implementation of a signature, at least a part of which is confidential and only known to the subscriber or is only in the possession of the subscriber (for example, signature PIN or password).

Signature-creation device

Configured software, hardware or a combination of the two that is used to implement signature creation data.

HSM

A Hardware Security Module (HSM), a hardware ⇨ signature-creation device.

Secure signature-creation device, secure key

A state-of-the-art signature-creation device that fulfils the requirements in EU signature regulation [eIDAS-VO] Appendix II (secure signature creation

Informationssicherheit des Betreibers.

Private, öffentliche und internationale Organisationen

Private Organisationen sind Einrichtungen die in ihren Ländern nach den jeweils geltenden Regeln des Privat- bzw. Zivilrechts eingerichtet sind.

Öffentliche Organisationen sind Einrichtungen, die in ihren Ländern kraft Gesetz eingerichtet sind, etwa Behörden, staatliche Verwaltungen, Gemeinde-, Landes- oder Bundesdienststellen.

Internationale Organisationen sind Einrichtung, die auf Grund völkerrechtlicher Vereinbarungen eingerichtet sind.

Signaturerstellungsdaten

Eindeutige Daten wie Codes oder private kryptographische Schlüssel, die vom Unterzeichner (Signator) zur Erstellung einer elektronischen Signatur verwendet werden.

Aktivierungsdaten

Informationen des Signators, die er zur Durchführung einer Signatur benötigt, zumindest Teile davon sind vertraulich und nur dem Signator bekannt bzw. nur im Besitz des Signators (z.B. Signatur-PIN bzw. Passwort).

Signaturerstellungseinheit

Eine konfigurierte Software, Hardware oder Kombination aus beiden, die zur Implementierung der Signaturerstellungsdaten verwendet wird.

HSM

Hardware-Sicherheitsmodul oder englisch Hardware Security Module (HSM), Hardwareprodukt im Sinne ⇨ Signaturerstellungseinheit.

Sichere Signaturerstellungseinheit, sicherer Schlüssel

Eine Signaturerstellungseinheit, die dem Stand der Technik entspricht und jedenfalls die Anforderungen EU Signaturverordnung [eIDAS-VO]

device, SSCD), the comments of the BSI, A-SIT, similar entities and regulators are noted).

Signature verification data

Data such as codes or public cryptographic keys that are used to verify an electronic signature.

Product for electronic signatures

Hardware or software or their specific components that are used by the certificate authority (CA) for the provision of services for electronic signatures or for the creation and verification of electronic signatures.

Signature regulations

All documents applicable to the certification services described, in particular provisions formulated in [SVG], [SVV], [eIDAS-VO], including documents cited in the provisions.

24/7/365, round-the-clock service, office hours

Services are provided all year round, seven days a week and 24 hours a day. Service disruptions or failures are documented. In isolated cases, additional limitations on availability can be defined, such as a tolerated disruption period of 1% per month or year.

Where not otherwise described in the respective GLOBALTRUST® Certificate Practice Statement, published on the website of the operator or one of the websites referred to in the respective certificate policy, the following minimum office hours apply for every kind of query, application or order, including applications for suspension and revocation: working days, Monday to Friday 9:00 – 17:00.

Anhang II erfüllt (secure signature creation device, SSCD), Hinweise des BSI, der A-SIT, vergleichbarer Einrichtungen und der Aufsichtstellen werden beachtet).

Signaturprüfdaten

Daten wie Codes oder öffentliche kryptographische Schlüssel, die zur Überprüfung einer elektronischen Signatur verwendet werden.

Produkt für elektronische Signaturen

Hard- oder Software bzw. deren spezifische Komponenten, die von einem Zertifizierungsdiensteanbieter (VDA) für die Bereitstellung von Diensten für elektronische Signaturen verwendet werden oder die für die Erstellung und Überprüfung elektronischer Signaturen verwendet werden.

Signaturbestimmungen

Gesamtheit der in den für die beschriebenen Zertifizierungsdienste zutreffenden Dokumente, insbesondere [SVG], [SVV], [eIDAS-VO] formulierten Bestimmungen inklusive den in den Bestimmungen zitierten Dokumenten.

24/7/365, Permanenzdienst, Bürozeiten

Dienste werden ganzjährig, sieben Tage die Woche und 24 Stunden täglich bereitgestellt. Ausfälle bzw. Fehler in der Bereitstellung werden dokumentiert. Im Einzelfall können zusätzlich Beschränkungen der Verfügbarkeit definiert werden, etwa tolerierte Ausfallszeiten von 1% pro Monat oder Jahr.

Soweit nicht im jeweiligen GLOBALTRUST® Certificate Practice Statement eines Dienstes abweichend beschrieben, nicht auf der Website des Betreibers oder auf einer in der jeweiligen Certificate Policy angegebenen Website abweichend veröffentlicht, gelten folgende Mindest-Bürozeiten für jede Form von Anfragen, Anträgen und Bestellungen, inkl. Anträgen zu Sperren und Widerrufen: werktags Mo-Fr 9:00 - 17:00

Outside of these times an on-call service is available to address technical disruptions, defects or other emergencies that are critical to certification services.

Cross certification

The confirmation of the certificate of another certification authority, from a regulator by the CA or vice versa.

End user key, end user signature-creation device

A key for end users (subscriber) from the CA, which is created and issued for creating electronic signatures. In the case of asymmetric encryption, "end user key" describes a pair of keys comprising a private and a public key.

Secure environment

All technical and organisational measures that enable controlled operation of certification services.

Product addition

Additional information that describes the certification services and types of certificate and is a part of the certificate issued by the CA. In connection with the certificates issued according to the standard X.509v3, this is an additional part of the CN of a CA certificate following the term GLOBALTRUST, for example, GLOBALTRUST ADVANCED. Product additions can be defined and assigned in the framework of the business activity of the operator, as long as they are not misleading or potentially in conflict with the product additions used in this policy.

EV certificates

Specific certificates that have been issued based on guidelines published by the CA/browser forum, "CA/Browser Forum Guidelines for Extended Validation Certificates" ([CABROWSER-EV].

Außerhalb dieser Zeiten besteht ein Bereitschaftsdienst zur Behebung zertifizierungskritischer technischer Störungen, Gebrechen und sonstiger Notfälle.

Cross-Zertifizierung

Bestätigung eines Zertifikats eines anderen Zertifizierungsdiensteanbieters, eines Zertifikates einer Aufsichtstelle durch den VDA oder umgekehrt.

Endkundenschlüssel, Endkunden-Signaturerstellungseinheit

Schlüssel der vom VDA für Endkunden (Signator, Unterzeichner) für die elektronische Signatur erstellt und ausgeliefert wird. Bei asymetrischen Verschlüsselungen beschreibt "Endkundenschlüssel" das Schlüsselpaar des privaten und öffentlichen Schlüssels.

gesicherte Umgebung

Gesamtheit aller technischen und organisatorischen Maßnahmen, die den kontrollierten Zertifizierungsbetrieb ermöglichen.

Produktzusatz

Ergänzende Angabe, die zur Beschreibung der Zertifizierungsdienste und Zertifikatsarten dient und Teil des vom VDA ausgegebenen Zertifikates ist. Im Zusammenhang mit Zertifikaten nach dem X.509v3-Standard ist der Produktsatz jener ergänzende Teil des CN eines CA-Zertifikates, der auf „GLOBALTRUST" folgt, z.B. „ADVANCED" bei „GLOBALTRUST ADVANCED". Produktzusätze können im Rahmen der Geschäftstätigkeit des Betreibers definiert und vergeben werden, wobei sie nicht irreführend sein oder im Konflikt zu den in dieser Policy verwendeten Produktzusätzen sein dürfen.

EV Zertifikate

Bezeichnet Zertifikate, die auf Basis der vom CA/Browser Forum publizierten Richtlinien „CA/Browser Forum Guidelines for Extended Validation Certificates" [CABROWSER-EV] ausgegeben worden sind.

The terms are otherwise used corresponding to [SVG], [SVV], [eIDAS-VO], [X.509v3], [CWA-14167-1], [ETSI EN 319 401], [ETSI EN 319 411-1], [ETSI EN 319 411-2], [RFC3161], [RFC3739] and [RFC3647] or others named in ⇨ Appendix A: 1 Bibliography (p192).

Ansonsten werden die Begriffe sinngemäß nach [SVG], [SVV], [eIDAS-VO], [X.509v3], [CWA-14167-1], [ETSI EN 319 401], [ETSI EN 319 411-1], [ETSI EN 319 411-2], [RFC3161], [RFC3739] und [RFC3647] oder anderer in ⇨ Appendix / Anhang A: 1 Bibliography / Bibliographie (p192) genannten Dokumente verwendet.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES / VERÖFFENTLICHUNG UND AUFBEWAHRUNG

2.1 Repositories / Aufbewahrung

The current version of this document is available on the website of the operator on a 24/7/365 basis (⇨ http://www.globaltrust.eu/certificate-policy.html).

Previous versions of this document are available from the regulator or on the website of the operator under the OID 1.2.40.0.36.1.1.8.99.

Changes made to the GLOBALTRUST® Certificate Policy will be announced in a timely fashion on the website or by email, if provided by the certificate holders.

Die aktuelle Version dieses Dokuments ist auf Basis 24/7/365 über die Website des Betreibers abrufbar (⇨ http://www.globaltrust.eu/certificate-policy.html).

Historische Versionen des Dokuments sind bei der Aufsichtsstelle abzurufen oder unter der OID-Nummer 1.2.40.0.36.1.1.8.99 auf der Website des Betreibers abgelegt.

Über die Website(⇨ http://www.globaltrust.eu) bzw. sofern von den Zertifikatsinhabern verfügbar per E-Mail wird zeitgerecht über Änderungen informiert, die in der GLOBALTRUST® Certificate Policy vorgenommen werden.

2.2 Publication of certification information / Veröffentlichung von Zertifizierungsinformationen

All documents necessary to perform certification services are published on the website of the operator, as well as the CA certificates used and their hash sums.

Information on services offered and procedures used is made available.

Testwebsites are available via the operator's website at http://globaltrust.eu/certificate-policy/

The CA makes conditions for the use of certificates available to the subscribers and other users who place their trust in the services of

Über die Website des Betreibers werden alle für die Erbringung der Zertifizierungsdienste erforderlichen Dokumente veröffentlicht, ebenso die verwendeten CA-Zertifikate und geeignete Prüfsummen.

Weiters werden Informationen zu den angebotenen Diensten und die verwendeten Verfahren zugänglich gemacht.

Testwebseiten sind über die Website des Betreibers (⇨http://globaltrust.eu/certificate-policy/) abrufbar.

Der VDA macht den Signatoren und den Benutzern, die auf die Zuverlässigkeit der GLOBALTRUST® Dienste vertrauen, die Bedingungen,

GLOBALTRUST® by publishing the following documents on the website:

1. the certificate policy. If necessary, additional certificate policies described in this document
2. general terms and conditions of use
3. additional descriptions of individual certification services
4. where applicable – a reference to the notification of certification services at the regulating authority
5. other communications
6. all cross-certificates that identify the CA as the holder and have been issued according to an agreement with the CA or have been accepted by the CA

The subscriber is notified of changes through announcement on the website of the CA or by email or post as circumstances require.

Further, CA certificates are disclosed via the Common CA Database (https://www.ccadb.org/) within 7 days of their creation.

die die Benutzung des jeweiligen Zertifikats betreffen, durch Veröffentlichung folgender Dokumente auf der Website des Betreibers zugänglich:

1. die gegenständliche Certificate Policy, sofern für einen Dienst erforderlich weitere in diesem Dokumenten bezeichnete Certificate Policies
2. Allgemeine Betriebs- und Nutzungsbedingungen
3. ergänzende Beschreibungen zu den einzelnen Zertifizierungsdiensten
4. - sofern anwendbar - ein Verweis auf die Anzeige des Zertifizierungsdienstes bei der Aufsichtsbehörde
5. sonstige Mitteilungen
6. alle Crosszertifikate die den VDA als Inhaber identifizieren und aufgrund einer Vereinbarung des VDA erstellt wurden oder von diesem akzeptiert wurden

Änderungen werden dem Signator mittels Bekanntmachung auf der Website des VDA und ggf. zusätzlich per E-Mail oder brieflich mitgeteilt.

Weiters werden CA-Zertifikate binnen 7 Tagen nach ihrer Erstellung in die Common CA Database (https://www.ccadb.org/) eingetragen.

2.3 Time or frequency of publication / Häufigkeit der Veröffentlichung

Binding agreements are published before they enter into force and are valid until revoked. Any limitations on time, in particular the validity of certificates, are communicated in an appropriate fashion. Other information is published promptly during office hours.

Changes are published promptly.

Verbindliche Vereinbarungen werden fristgerecht vor Inkrafttreten veröffentlicht und gelten bis Widerruf. Im Falle von Befristungen, insbesondere der Gültigkeit von Zertifikaten, wird darauf in geeigneter Weise hingewiesen. Sonstige Informationen werden unverzüglich während der Bürozeiten veröffentlicht.

Änderungen werden unverzüglich veröffentlicht.

2.4 Access controls on repositories / Zugangsbeschränkungen

No measures are taken to restrict access to public information.

Internal information is safeguarded according to the GLOBALTRUST® Certificate Security Policy.

Es werden keine Maßnahmen zur Beschränkung des Zugriffs auf die öffentlichen Informationen ergriffen.

Interne Informationen werden gemäß GLOBALTRUST® Certificate Security Policy gesichert.

3. IDENTIFICATION AND AUTHENTICATION / IDENTIFIZIERUNG UND AUTHENTIFIKATION

All certification data is verified according to plausibility, factual and technical correctness and compliance with legal and other juridical requirements, in particular information on signature creation devices used, information on the issuance of private keys, certificate requirements (for example a certificate signing request) and applicable policies.

In addition, the CA can make use of external services and experts. If evidence of legitimate control of individual components and confidential information is necessary (in particular signature creation devices, private keys, etc), the subscriber must produce this. If the CA has good reason to question the explanations provided, it can request additional confirmation and credentials. Certificates cannot be delivered before this has been successfully verified.

Alle Zertifikatsdaten, insbesondere Angaben über verwendete Signaturerstellungeinheiten, Angaben zur Erzeugung von privaten Schlüsseln, Zertifikatsanforderungen (wie ein Certificate Signing Request), anzuwendende Policies werden nach Plausibilität, sachlicher und technischer Richtigkeit und nach Übereinstimmung mit gesetzlichen und sonstigen rechtlichen Vorgaben geprüft.

Dazu kann sich der VDA auch externer Dienste und Sachverständiger bedienen. Soweit ein Nachweis über die rechtmäßige Verfügungsgewalt über einzelne Komponenten und vertrauliche Informationen erforderlich ist (insbesondere Signaturerstellungseinheiten, private Schlüssel usw.) sind jedenfalls Erklärungen vom Signator vorzulegen. Der VDA kann bei berechtigten Zweifel an den abgegebenen Erklärungen zusätzliche Bestätigungen und Bescheinigungen anfordern. Eine Zustellung von Zertifikaten vor erfolgreichen Abschluss der Prüfung erfolgt nicht.

3.1 Naming /Benennung

Names are chosen so that they express facts or correspond to the name of the person or entity. They can be in any preferred language. Misleading, erroneous or unlawful names and designations are not accepted by the operator.

Bezeichnungen werden so gewählt, dass sie den beschreibenden Sachverhalt ausdrücken oder dem Namen einer Person oder Einrichtung entsprechen. Sie können in beliebiger Sprache erfolgen. Irreführende, fehlerhafte oder rechtswidrige Bezeichnungen und Benennungen werden vom Betreiber nicht akzeptiert.

3.1.1 Types of names / Arten der Benennung

Certificate names will be checked for uniqueness for one applicant.

Zertifikatsbezeichnungen (CommonName, CN) werden auf Eindeutigkeit

Certification applications from different applicants with identical certificate names will not be accepted. Certification applications from the same applicant with the same certificate names will be accepted, if the information is still correct at the date of the reissue.

Names will only be accepted in certificates that
- are legitimately available to the applicant or
- in the case of other unprotected terms and names, as long as they are not misleading or breach legal regulations.

im Bezug zu einem Antragsteller geprüft. Zertifikatsanträge unterschiedlicher Antragsteller mit identen Zertifikatsbezeichnungen werden nicht akzeptiert. Idente Zertifikatsbezeichnungen desselben Antragstellers werden akzeptiert, sofern die Angaben zum Zeitpunkt der Neuausstellung eines Zertifikates noch korrekt sind.

In den Zertifikaten werden ausschließlich Bezeichnungen zugelassen,
- über die der Antragsteller rechtmäßig verfügt oder
- im Falle sonstiger nicht geschützter Begriffe und Bezeichnungen, soweit sie nicht irreführend sind oder gegen gesetzliche Bestimmungen verstoßen.

3.1.2 Need for names to be meaningful / Notwendigkeit für aussagekräftige Namen

Names in certificates must be meaningful if intended to fulfil a purpose.

Suitable names are:
- the proven name of the applicant including titles, professional titles and academic titles
- the proven name of the organisation for which the applicant gets issued the certificate, including proven details of the organisational unit
- legally required information
- trade names and product names, that verifiably belong to the applicant or the applying organisation, including domain, eMail and server names
- technical data (e.g. serial number of the smartcard) that are obviously connected to the certificate and that can be assigned or checked by the VDA,
- Functional and organisational names that inform about the use and/or the meaning of a certificate.

Soweit für die Erfüllung eines Zweckes erforderlich werden aussagekräftige Bezeichnungen und Namen in den Zertifikaten verlangt.

Geeignete Bezeichnungen und Namen sind:
- der nachgewiesene Namen des Antragstellers inklusive Titel, Berufstitel, akademische Grade und Berufsbezeicchnungen soweit sie nachgewiesen werden,
- der nachgewiesene Namen jener Organisation, für die der Antragsteller ein Zertifikat ausgestellt erhält inklusive Abteilungsangaben soweit sie nachgewiesen werden,
- Angaben auf Grund gesetzlicher Vorschriften,
- Markennamen und Produktbezeichnungen über die der Antragsteller oder die antragstellende Organisation nachweislich verfügt, inklusive Domain-, eMail- und Serverbezeichnungen,
- technische Angaben (zB Seriennummer der verwendeten Smartcard) die eindeutig mit dem Zertifikat verknüpft sind und vom VDA vergeben oder geprüft werden können,
- Funktions- und Organisationsbezeichnungen die den Empfänger eines Zertifikates über Verwendung und/oder Bedeutung eines Zertifikates informieren.

3.1.3 Anonymity or pseudonymity of subscribers / Behandlung von Anonymität oder Pseudonymen von Antragstellern

Certification services can be performed so that persons, organisations or organs of organisations making an application are not publicly named, as long as this is permitted by legal and technical standards. In this event, internal documentation clearly matches the certification services provided to the individual or organisation making the application.

Zertifizierungsdienste können - sofern rechtlich und den technischen Standards entsprechend zulässig - auch in einer Form erbracht werden, bei denen die antragstellenden Personen, Organisationen oder Organe der antragstellenden Organisationen nicht öffentlich aufscheinen. In diesem Fall erfolgt eine interne Dokumentation in der die in Anspruch genommenen Zertifizierungsdienste eindeutig einer antragstellenden Person oder Organisation zugeordnet werden kann.

Pseudonyms are designated as such in qualified certificates, according to technical standards.

Pseudonyme werden jedenfalls bei qualifizierten Zertifikaten als solche eingetragen bzw. gemäß den technischen Standards gekennzeichnet.

In the event of a certified or proven legal interest or obligation, the identity of the individual or organisation making an application is made available, including organs and representative entities.

Im Falle eines bescheinigten oder nachgewiesenen rechtlichen Interesses oder einer rechtlichen Verpflichtung werden die Identitätsdaten einer antragstellenden Person oder Organisation, inklusive den Organen oder Vertretungen bekannt gegeben.

3.1.4 Rules for interpreting various name forms / Interpretationsregeln für verschiedene Benennungsformen

If several name forms are equally valid, it is left to the applicant to choose.

Sind mehrere Benennungsformen gleichermaßen zulässig, dann wird grundsätzlich dem Antragsteller die Wahl gelassen, welche Benennungsform er wählt.

This procedure is abandoned if a name form is essentially simpler and clearer.

Von dieser Vorgangsweise wird abgegangen, wenn eine Benennungsform wesentlich einfacher und eindeutiger ist.

In the event of disagreement over names, the operator suggests the most appropriate name.

Im Fall von Benennungskonflikten schlägt der Betreiber die geeignetste Benennung vor.

3.1.5 Uniqueness of names / Einmaligkeit von Benennungen

Certificates are not provided for different subscribers using one and the

Es werden keine Zertifikate für unterschiedliche Signatoren erbracht, die

same name. It is ensured that certification services are differentiated using at least a serial number or equivalent identifier.

dieselbe Bezeichnung haben. Jedenfalls wird sichergestellt, dass sich Zertifizierungsdienste durch eine Seriennummer oder eine vergleichbare Kennzeichnung unterscheiden.

3.1.6 Recognition, authentication and role of trademarks / Berücksichtigung und Authentifikation von Markennamen

It is permitted to enter a publically registered trademark as the name of an organisation, provided that the applicant can demonstrate that the trademark may be used and that the official name of the company holding the trademark is given afterwards in brackets. In the interest of limiting the length of the field organizationName, abbreviations are permitted, provided that they are not misleading.

Es ist zulässig, eine öffentlich registrierte Markenbezeichnug als Organisationsname einzutragen, sofern der Antragsteller nachweisen kann, diese verwenden zu dürfen und der offizielle Firmenname der Markenbezeichnung in Klammern nachgestellt wird. Um die Länge des organizationName Feldes zu begrenzen sind Abkürzungen erlaubt, sofern sie nicht irreführend sind.

3.2 Initial identity validation / erstmalige Identitätsfeststellung

All information on the certificate holder that is contained in the certificate, in particular their identity, is verified for accuracy in every form of certification. In the event that an applicant appears as a representative or organ of a certificate holder, in particular in connection with the issuance of certificates for particular organisations or domain names, the capacity of this person to act as a representative or organ is verified.

Alle Angaben zum Zertifikatsinhaber, die im Zertifikat enthalten sind - insbesondere die Identitätsangaben - werden in jeder Zertifikatsvariante auf ihre Richtigkeit hin geprüft. In den Fällen, indenen ein Antragsteller als Vertreter oder Organ eines Zertifikatsinhabers auftritt, insbesondere im Zusammenhang mit der Ausstellung von Zertifikaten für bestimmte Organisationen oder Domainnamen, wird auch die Vertretungs- bzw. Organbefugnis der Person geprüft.

Upon the initial application for a qualified, advanced or EV certificate, personal identity is confirmed by the CA or a person authorised by the CA.

Im Falle der Erstantragsstellung erfolgt bei qualifizierten fortgeschrittenen oder EV-Zertifikaten eine persönliche Identitätsfeststellung durch den VDA oder eine vom VDA authorisierte Person.

3.2.1 Method to prove possession of private key / Nachweis über den Besitzes des privaten Schlüssels

Provided that the private key has not been issued by the operator, the operator requires proof from the subscriber that they are indeed in possession of the private key. Proof can be provided by technical

Sofern der private Schlüssel nicht durch den Betreiber erzeugt wird, verlangt der Betreiber einen Nachweis vom Signator, dass er tatsächlich im Besitz des privaten Schlüssels ist. Der Nachweis kann durch

procedures. Suitable technical methods are in particular the transmission of a Certificate Signing Request (CSR) signed with the private key.

technische Verfahren erfolgen. Geeignete technische Verfahren sind insbesondere die Übermittlung eines mit dem privatem Schlüssel signierten Certificate Signing Request (CSR).

3.2.2 Authentication of organization identity / Authentifikation der Organisation

If an application contains information about an organisation, this data is verified. Likewise, it is verified as to whether the person making the application is authorised to request certificates for the organisation.

The measures and procedures to identify and register the applicant depend on the respective certification service and its juridical and in particular its legal requirements. They can also differ functionally as well as regionally.

All authorities and organisations recognised by the state that maintain public registers and verify identity before recording an entity in these registers are qualified to confirm the validity of an organisation.

Soweit ein Antrag Angaben zu einer Organisation enthält, werden diese Daten geprüft. Ebenso, ob die antragstellende Person tatsächlich berechtigt ist für diese Organisation Zertifikate zu beantragen.

Die Maßnahmen und Abläufe zur Identifikation und Registrierung des Antragstellers orientieren sich am jeweiligen Zertifizierungsdienst und seinen rechtlichen, insbesondere gesetzlichen Vorgaben und können sowohl sachliche, als auch regionale Unterschiede aufweisen.

Als Auskunftsstelle für die Gültigkeit einer Organisation sind grundsätzlich alle staatlich anerkannten Behörden und Organisationen geeignet, die öffentliche Verzeichnisse führen und vor Aufnahme in diese Verzeichnisse eine Identitätsprüfung durchführen.

3.2.3 Authentication of individual identity / Identitätsprüfung von Personen

The applicant must provide information about the type of official identification document, its number, information on the issuing authorities and the date of issuance.

a) Case Verification in person

If the identity of the applicant is verified by an authorised person (for example, the applicant is personally present in the offices of the CA or registration authority), the official identification document must be presented in original or as a notarised copy. Notarised copies must be submitted. The identity of the applicant, the kind of official personal document, its number, the issuing authority and the date of issue of the original documents are recorded. A submitted document can be rejected if

Vom Antragsteller sind die Angabe der Art des amtlichen Personaldokuments, die Dokumentennummer, die Identitätsangaben der ausstellenden Behörde und das Ausstellungsdatum erforderlich.

a) Case Verification in person / Fall Überprüfung vor Ort

Findet die Überprüfung der Identität des Antragstellers durch eine autorisierte Person statt (z.B. Antragsteller ist in den Räumlichkeiten des VDA oder einer Registrierungsstelle persönlich anwesend) dann ist das amtliche Personaldokument im Original oder als beglaubigte Kopie vorzulegen. Beglaubigte Kopien sind auszuhändigen, von einem Originaldokument sind - neben den Identitätsangaben des Antragstellers - jedenfalls Art des amtlichen Personaldokuments, die

it does not unequivocally establish the identity of the person, if it is not valid or no longer valid, or if the official character of the document is questionable. If the applicant cannot produce any suitable documents, the application is rejected on the basis that the authentication of identity has failed.

Requires the applicant informations about an organisation in the certificate and he isn't authorizied to act for the organisation, it's mandatory to obtain an authority by an official representant of the organisation, which should included in the certificate.

b) Case Verification not in person

If the identity of the applicant cannot be verified by their presence, the identity information and the information contained in the identification document, such as the type of official personal document, its number, the identity of the issuing authority and the date of issuance is collected. Furthermore, the information is checked for plausibility using submitted copies of the documents (an attestation is not necessary). If the plausibility check is not successful or concerns persist regarding the submitted documents, additional documents and contact points can be submitted or enquiries can be made at trustworthy public sources. If the applicant cannot sufficiently clarify this in spite of requests, the application is rejected on the basis that plausibility checks have failed.

The following information is obligatory for qualified certificates in addition to the minimum information described above:

- date and place of birth
- a nationally recognised identification number or an equivalent

Nummer ,die Identitätsangaben der ausstellenden Behörde und das Ausstellungsdatum zu erfassen. Ein vorgelegtes Dokument kann abgelehnt werden, wenn auf Grund dieses Dokument die Person nicht zweifelsfrei identifiziert werden kann, das Dokument nicht(mehr) gültig ist oder der amtliche Charakter des Dokuments zweifelhaft ist. Kann der Antragsteller keine geeigneten Dokumente vorlegen, dann wird der Antrag auf Grund fehlgeschlagener Identitätsprüfung abgelehnt.

Verlangt der Antragsteller "vor Ort" Angaben zu einer Organisation im Zertifikat und es handelt sich nicht um eine zur Vertretung nach außen befugte Person, dann wird zwingend eine Vollmacht durch eine zur Vertretung nach außen befugte Person dieser Organisation eingefordert.

b) Case Verification not in person / Fall Überprüfung nicht vor Ort

Kann die Identität des Antragstellers nicht auf Grund seiner persönlichen Anwesenheit geprüft werden, werden die Identitätsangaben und Angaben zum amtlichen Personaldokument, wie Art des amtlichen Personaldokuments, die Nummer ,die Identitätsangaben der ausstellenden Behörde und das Ausstellungsdatum auf Grund der Angaben des Antragstellers erfasst. Weiters erfolgt eine Plausibilitätsprüfung der Angaben auf Basis vorgelegter Kopien der Dokumente (eine Beglaubigung ist nicht erforderlich). Ist die Plausibilitätsprüfung nicht erfolgreich oder bestehen Bedenken bei den vorgelegten Dokumente können zusätzliche Unterlagen, zusätzliche Kontakte oder Anfragen in vertrauenswürdigen öffentlichen Quellen erfolgen. Kann der Antragsteller trotz Aufforderung offene Fragen nicht ausreichend aufklären, dann wird der Antrag auf Grund fehlgeschlagener Plausibilitätsprüfung abgelehnt.

Bei qualifizierten Zertifikaten sind zusätzlich zu den oben beschriebenen Mindestangaben folgende Informationen zur Person des Signators obligatorisch:

- Geburtstag und -ort
- Eine national anerkannte Identifikationsnummer oder ein

attribute which can be used to distinguish the person from another person with the same name.

Authentication of identity is completed when the application takes place in person at a registration authority and the applicant submits an official personal document in original or validation of identity can be confirmed by a certified legal opinion, especially authenticated validation of identity in original submitted by a court or notary (⇨ a) verification in person).

In all other cases of (b) verification not in person) the authentication of identity is completed during the processing of the application (⇨ 6.1.2 Private key delivery to subscriber / Zustellung privater Schlüssel an den Signator, p132) or through videobased online-identification (⇨ GLOBALTRUST® Certificate Practice Statement 3.2.3 Authentication of individual identity / Identitätsprüfung von Personen).

The certificate can contain additional information on the subscriber: telephone number, fax number and e-mail address, information on profession and qualifications, and if necessary, further information. Individual information can be optional or obligatory depending on the certification service.

vergleichbares Attribut, mit der die Person von anderen Personen gleichen Namens unterschieden werden kann.

Die Identitätsprüfung ist abgeschlossen, sofern der Antrag persönlich in einer der Registrierungsstellen erfolgte und vom Antragsteller ein amtliches Personaldokument im Original vorgelegt wurde oder durch ein geprüftes Rechtsgutachten der Identitätsnachweis erbracht wurde, insbesondere ein durch Gericht oder Notar beglaubigter Identitätsnachweis im Original ausgehändigt wurde (⇨ a) Case Verification in person / Fall Überprüfung vor Ort).

In allen anderen Fällen (b) Case Verification not in person / Fall Überprüfung nicht vor Ort) erfolgt der Abschluss der Identitätsprüfung im Zuge der Antragsbearbeitung (⇨ 6.1.2 Private key delivery to subscriber / Zustellung privater Schlüssel an den Signator, p132) oder durch eine videogestützte Online-Identifikation (⇨ GLOBALTRUST® Certificate Practice Statement 3.2.3 Authentication of individual identity / Identitätsprüfung von Personen).

Im Zertifikat können zusätzliche Angaben zur Person des Signators enthalten sein:
Telefonnummer, Faxnummer und E-Mailadresse, Berufs- und Qualifikationsangaben, allenfalls weitere Daten. Abhängig vom Zertifizierungsdienst können einzelne Angaben optional oder obligatorisch sein.

3.2.4 Non-verified subscriber information / Nicht-verifizierte Antragstellerdaten

The certificates inludes
a) Either certificates do not contain non-verified information (required in the case of qualified or EV certificates) or
b) if non-verified information is permitted (for example, the certificates are marked as test certificates), the Certificates are issued under

Die Zertifikate enthalten
a) entweder keine nicht-verifizierten Angaben (jedenfalls bei qualifizierten Zertifikaten oder EV-Zertifikaten) oder
b) sofern nicht-verifizierte Angaben zulässig sind (z.B. bei Zertifikaten die als Testzertfifikate gekennzeichnet sind), werden die Zertifikate

separate test-CAs.

However, all designations are excluded that are misleading or evidently not permitted for other legal reasons. If the subscriber wishes to enter a trademark, the right to use the trademark is verified.

unter eigenen Test-CAs ausgestellt .

Ausgeschlossen sind jedoch in allen Fällen Angaben, die irreführend oder aus sonstigen rechtlichen Gründen offensichtlich unzulässig sind. Wird die Führung von Markennamen beansprucht, erfolgt jedenfalls eine Verifizierung.

3.2.5 Validation of authority / Nachweis der Vertretungsbefugnis

The registration authority conducts the verification of authority and information/documents of the persons named in the application.

If the certification services have been requested on behalf of persons or organisations or evidence should be given of the power of authority to act for a third party, this is only possible if the requested representations on behalf of the third party are verified. The scope of authority and proof of authority for this kind of representation must comply with the law of the state in which the person or organisation, for which the certification services are undertaken, has domicile.

The CA or persons authorised to perform the certification will reject an application if doubt exists regarding the legal power of the agent to act on behalf of a third party. If the CA or persons authorised to perform the certification are informed after the fact of reasons that mean the agent cannot act as a representative, the certification services will be immediately suspended and the certificates revoked.

Die Registrierungsstelle übernimmt die Prüfung der Vertretungsbefugnis und der Angaben/Unterlagen der im Antrag genannten Personen.

Werden Zertifizierungsdienste in Vertretung von Personen oder Organisationen beantragt oder soll in Zertifizierungsdiensten die Vertretungsmacht für Dritte bescheinigt werden, dann ist das nur möglich, wenn die beanspruchten Vertretungen nachgewiesen werden. Vollmachtsumfang und Nachweis der Vollmacht für derartige Vertretungen müssen den gesetzlichen Bestimmungen jenes Staates entsprechen, in dem die Person oder Organisation für die die Zertifizierungsdienste erbracht werden sollen, seinen Sitz hat.

Der VDA bzw. zur Zertifizierung autorisierte Personen haben bei Zweifel an einer rechtlich zulässigen Vertretungsmacht einen entsprechenden Antrag abzulehnen. Werden dem VDA bzw. zur Zertifizierung autorisierte Personen im nachhinein Gründe bekannt, die eine gültige Vertretungsmacht ausschließen, sind die Zertifizierungsdienste unverzüglich einzustellen und Zertifikate zu widerrufen.

3.2.6 Criteria for interoperation / Kriterien für Interoperabilität

All cross certifications are disclosed if the CA has initiated and/or accepted the cross certification.

Alle Cross-Zertifizierungen werden offengelegt, sofern der VDA die Cross-Zertfierung veranlasst und/oder akzeptiert hat.

3.3 Identification and authentication for re-key requests / Identifikation und Authentifikation für Schlüsselerneuerung

All information on the certificate holder, in particular identity information, will be verified for correctness when the key is renewed.

Alle Angaben zum Zertifikatsinhaber - insbesondere die Identitätsangaben - werden bei Schlüsselerneuerung auf ihre Richtigkeit hin geprüft.

Provided that the applicant does not request any changes, only the information that is subject to change since the initial application is verified for correctness, in particular control of domain names, design and trademark rights, place of business and the existence of the company.

Sofern keine Änderungen des Antragstellers begehrt werden, werden nur jene Angaben auf ihre Richtigkeit hin überprüft, die seit der Erstantragstellung einer Änderung unterliegen können, insbesondere die Verfügung über Domainnamen, Muster- und Markenrechte, Angaben zum Firmensitz und dem Bestehen der Firma.

Changes requested by the applicant will be treated the same as an initial application (⇨ 3.2 Initial identity validation / erstmalige Identitätsfeststellung, p50).

Änderungen die der Antragsteller begehrt werden so behandelt, wie im Fall der Erstantragstellung (⇨ 3.2 Initial identity validation / erstmalige Identitätsfeststellung, p50).

3.3.1 Identification and authentication for routine re-key / Identifikation und Authentifikation für routinemäßige Schlüsselerneuerung

Procedures as in ⇨ 3.3 Identification and authentication for re-key requests / Identifikation und Authentifikation für Schlüsselerneuerung (p55).

Vorgehen wie ⇨ 3.3 Identification and authentication for re-key requests / Identifikation und Authentifikation für Schlüsselerneuerung (p55).

3.3.2 Identification and authentication for re-key after revocation / Identifikation und Authentifikation für Schlüsselerneuerung nach Widerrufen

Procedures as in ⇨ 3.3 Identification and authentication for re-key requests / Identifikation und Authentifikation für Schlüsselerneuerung (p55).

Vorgehen wie ⇨ 3.3 Identification and authentication for re-key requests / Identifikation und Authentifikation für Schlüsselerneuerung (p55).

3.4 Identification and authentication for revocation request / Identifikation und Authentifikation für Widerrufsanträge

⇨ 4.9.2 Who can request revocation / Berechtigte für Antrag auf Widerruf (p83)

⇨ 4.9.2 Who can request revocation / Berechtigte für Antrag auf Widerruf (p83)

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS / ANFORDERUNGEN ZERTIFIKATSLEBENSZYKLUS

Certification services take place exclusively on the basis of defined business processes. The status of a certificate, a certification service and the status of the issuance of a certificate are documented using defined status values and is clearly documented at every point during the life cycle.

Critical disruptions, interruptions and failures are handled according to defined, internally documented business processes approved by the management. Irrespective of the remedy, an analysis and development of improvement measures to avoid such incidents in the future takes place in any case. In any case, in the event of any type of CA key being compromised (including algorithm compromise), the measures also include the revocation of the affected CA certificates.

A certificate, a signature creation device or equivalent product is only personalised and delivered after the administrative activities necessary for this service have been completed, in particular the successful completion of the necessary identity authentication.

The issuing of certificates to organizations that for whatever reason could lead to conflicts of interest is excluded.

Die Erbringung der Zertifizierungsdienste erfolgt ausschließlich auf Basis definierter Geschäftsprozesse, der Status eines Zertifikates, eines Zertifizierunsdienstes bzw. der Status der Zertifikatsausstellung wird durch definierte Statuswerte dokumentiert und ist zu jedem Zeitpunkt des Lebenszyklus des Zertifikates eindeutig definiert.

Die Behandlung von kritischen Betriebsstörungen, Unterbrechungen und Ausfällen erfolgt nach definierten, intern dokumentierten und von der Geschäftsführung freigegebenen Geschäftsprozessen. Unabhängig von der Behebung erfolgt in jedem Fall eine Analyse und eine Erarbeitung von Verbesserungsmaßnahmen zur Vermeidung solcher Vorälle in der Zukunft. Im Fall der Kompromittierung jeglicher Art von CA-Schlüsseln (inklusive Komrpmittierung von Algorithmen) umfassen die Maßnahmen jedenfalls auch den Widerruf der betroffenen CA-Zertifikate.

Die Personalisierung und Zustellung eines Zertifikats, einer Signaturerstellungseinheit oder vergleichbarer Produkte erfolgt erst nach Abschluss der für diese Dienstleistung erforderlichen administrativen Tätigkeiten, insbesondere nach erfolgreichem Abschluss der erforderlichen Identitätsfeststellungen.

Die Ausstellung von Zertifikaten an Organisationen, bei denen aus welchen Gründen auch immer Interessenkonflikte bestehen könnten, ist augeschlossen.

4.1 Certificate Application / Antragstellung

The existing policy describes the basic application process, which can be elaborated upon pursuant to practical or legal circumstances. Every

Die vorliegende Policy beschreibt den grundlegenden Ablauf der Antragsbearbeitung, der im Einzelfall auf Grund sachlicher oder

certificate issuance is preceded by an application.

rechtlicher Gegebenheiten verfeinert werden kann. Jeder Zertifikatsausstellung geht ein Antrag voraus.

4.1.1 Who can submit a certificate application / Berechtigung zur Antragstellung

Natural persons und organisations (especially corporations, societies, authorities, businesses) can submit applications or orders for certification services as they wish. There are no regional or practical limitations. In order to provide access to certification services for persons with disabilities in accordance with ETSI EN 319 549, applications can be submitted in any form (web form, email, port, telephone, fax ...). There is no support for the use of signature products.

Natürliche Personen und Organisationen (insbesondere Unternehmen, Vereine, Behörden, Betriebe) können Anträge und Bestellungen zur Erbringung von Zertifizierungsdiensten vorbringen. Es bestehen keine regionalen oder sachlichen Einschränkungen. Um gemäß ETSI EN 319 549 Personen mit Behinderungen den Zugang zu Zertifizierungsdiensten zu ermöglichen, können Anträge in jeder beliebigen Form (Webformular, eMail, Post, Telefon, Fax…) eingebracht werden. Für die Verwendung von Signaturprodukten besteht keine Unterstützungsmöglichkeit.

If the identity of the applicant has not yet been established, the applications are handled as anonymous. Authentication of identity takes place before a certificate is issued. The scope of this authentication is defined by the applicable certificate policy.

Solange die Identität eines Antragstellers nicht festgestellt ist, werden die Anträge grundsätzlich als anonym gestellt betrachtet. Vor Ausgabe eines Zertifikats erfolgt jedenfalls eine Identitätsfeststellung. Der Umfang der Identitätsfeststellung erfolgt gemäß der jeweils anzuwendenden Certificate Policy.

The time at which the application was made and the method by which the certificate data has been distributed (publicly accessible or not) is recorded in the application data.

Zu den Antragsdaten wird Zeitpunkt des Antrags und Art der Verbreitung der Zertifikatsdaten (öffentlich zugänglich oder nicht) aufgezeichnet.

4.1.2 Enrollment process and responsibilities / Anmeldungsverfahren und Verantwortlichkeiten

Applications from organisations must be submitted by an authorised person. Persons submitting an application from the same address as the organisation concerned are presumed to have authority to act on behalf of the organisation. If the person making the application and the organisation concerned have different addresses, a person authorised to represent the organisation externally must confirm the authority of the person making the application.

Anträge von Organisationen müssen von einem befugten Organ gestellt werden, wobei bei Personen die einen Antrag unter derselben Anschrift wie die betroffene Organisation stellen, grundsätzlich die Vermutung der Befugnis gegeben ist. Bei abweichenden Anschriftangaben des antragstellenden Organs und der betroffenen Organisation muss eine nach außen vertretungsbefugte Person die Berechtigung des antragstellenden Organs bestätigen.

Before the contract between the subscriber and the CA is completed, the policy and all other possible conditions (general terms and conditions, individual agreements) on the use of the certificate will be made available to the subscriber electronically or in written documents.

The following information will be retained:
- all documents und other information that concern the application process, including applications for the issuance or renewal of a certificate.
- all information that concern the approval of applications.

Bevor der Vertrag zwischen dem Signator und dem VDA abgeschlossen wird, werden dem Signator die Policy, und allfällige sonstige Bestimmungen (allgemeine Geschäftsbedingungen, individuelle Vereinbarungen) zur Nutzung des Zertifikats elektronisch oder durch schriftliche Unterlagen zugänglich gemacht.

Es werden jedenfalls die folgenden Informationen festgehalten:
- Alle Unterlagen und Ereignisse, die die Antragsbearbeitung betreffen, inklusive Anträge auf Zertifikatsausstellung und -verlängerung.
- Alle Ereignisse die die Freigabe von Anträgen betreffen.

4.2 Certificate application processing / Bearbeitung von Zertifkatsanträgen

The data of the applicant will be verified on the basis of the following documents and sources of information[6]:
(1) confirmation by the applicant
(2) legal opinion
(3) confirmation from an auditor
(4) QIIS - Qualified independent information service
(5) QGIS - Qualified government information service
(6) QTIS - Qualified tax information service

The registration authority undertakes the following review of applications:
- Examination of the organisation and trademarks used by the

Die Daten des Antragstellers werden auf Basis folgender Dokumente und Informationsquellen[7] geprüft:
(1) Bestätigung vom Antragsteller
(2) Rechtsgutachten
(3) Bestätigung eines Wirtschaftsprüfers
(4) Qualifizierte unabhängige Informationsquelle (QIIS - Qualified independent information service)
(5) Qualifizierte behördliche Informationsquelle (QGIS - Qualified government information service)
(6) Qualifizierte behördliche Steuerinformationsquelle (QTIS - Qualified tax information service)

Die Registrierungsstelle nimmt folgende Überprüfungen des Antrags vor:
- Prüfung der Organisation bzw. von ihr verwendeter Markennamen

[6] In case of examination an applicant for EV-certificates, the documents fulfill the requirements as defined in [WEBTRUST-EV] and [CABROWSER-EV]. The requierements ar internal documented and can presented regulatory authorities and auditors.

[7] Im Falle der Prüfung eines Antragstellers für ein EV-Zertifikat entsprechen die Dokumente und Informationsquellen jedenfalls den Anforderungen gemäß [WEBTRUST-EV] und [CABROWSER-EV]. Die Anforderungen sind intern dokumentiert und können auf Wunsch Aufsichtsbehörden vorgelegt werden.

organisation (according to credible certificates submitted by the applicant, as per disclosure (inc. requests to databases) from a qualified official source of information or with the assistance of a qualified independent source of information, especially the databases of trustworthy third parties)

- if a certificate can be used to sign emails, all email addresses entered in the certificate will be checked as to whether the applicant has control of these addresses or is authorised to use them by their owner. This can take place through sending a randomly generated 18-digit value to these addresses and obtaining a confirming response of the applicant, containing the value.
- if a certificate is suitable for SSL encryption on servers, all domain names entered in the certificate will be checked as to whether the applicant is the owner of the domain names or is authorised by the owner to use them. All IP addresses entered will be checked as to whether the applicant can use them. This can take place through direct communication with the owner of the domain or address according to publicly available databases. In any case specifications of the domain name records (DNS) observed. The check is in any case conducted by the operator itself.

- If a certificate is suitable for SSL encryption on servers, its contents will be verified for up-to-dateness and correctness at least every 825 days. For certificates issued on or after 1st September 2020, this verification will take place at least every 397 days.

(gemäß vom Antragsteller vorgelegter unbedenklicher Bescheinigungen, lt. Auskunft (inkl. Datenbankabfrage) einer qualifizierten behördlichen Informationsquelle oder anhand von qualifizierten unabhängige Informationsquellen, insbesondere Datenbanken vertrauenswürdiger Dritter).

- Sofern sich ein Zertifikat für die Signatur von E-Mails eignet, wird bei allen im Zertifikat einzutragenden E-Mail Adressen geprüft, ob der Antragsteller die Kontrolle über diese Adressen besitzt, oder von deren Inhaber autorisiert ist. Dies kann insbesondere durch direkte Kommunikation mit diesen Adressen erfolgen (Bestätigungsmail).

- Sofern sich ein Zertifikat für die SSL-Verschlüsselung auf Servern eignet, wird bei allen im Zertifikat einzutragenden Domain Namen geprüft, ob der Antragsteller dessen Inhaber des Domainnamens ist, oder von diesem autorisiert wurde und die Kontrolle über diese besitzt. Bei allen einzutragenden IP-Adressen wird geprüft, ob der Antragsteller die Kontrolle über diese besitzt. Dies kann insbesondere durch eine direkte Kommunikation mit dem Inhaber der Domain bzw. der Adresse laut öffentlich zugänglicher Datenbanken erfolgen. Jedenfalls werden Vorgaben gemäß Domain-Records (DNS) beachtet. Die Prüfung erfolgt jedenfalls durch eine Registrierungsstelle des Betreibers.
- Sofern sich ein Zertifikat für die SSL Verschlüsselung auf Servern eignet, wird dessen Inhalt mindestens alle 825 Tage auf dessen Aktualität und Korrektheit hin geprüft. Für ab 1.9.2020 ausgestellte Zertifikate findet diese Prüfung mindestens alle 397 Tage statt.

4.2.1 Performing identification and authentication functions / Durchführung Identifikation und Authentifikation

For advanced signatures, governmental signatures or qualified certificates, authentication of the personal identity of the applicant is undertaken by the operator or by a person authorised by the operator or an entity that is

Im Falle von fortgeschrittenen Signaturen, Amtssignaturen oder qualifizierten Zertifikaten erfolgt eine persönliche Identitätsfeststellung des Antragstellers durch den Betreiber oder eine vom Betreiber

authorised to authenticate identity, especially courts, notaries, delivery services that also offer authentication of identity for the delivery of documents (in Austria in particular, this is POST AG) or similar entities.

In all cases, authentication of identity of the applicant requires
- submission of official identification papers or
- personal recognition from the authority authenticating identity (persons authorised by the operator or employees of the authority), whereby the authority vouches for the identity of the person beyond doubt, documents the authentication and confirms this with a signature.

If the authentication is undertaken by an entity authorised to do so, this is regarded as completed when the necessary confirmation has been signed and returned to the operator with a memorandum provided by the authority.

authorisierte Person oder eine Prüfstelle, die zur Identitätsfeststellung befugt ist, insbesondere Gerichte, Notare, Zustelldienste, die auch eine Identitätsprüfung bei der Übergabe von Dokumenten anbietet (in Österreich ist das insbesondere die POST AG) oder vergleichbare Einrichtungen.

In allen Fällen erfolgt die Identitätsfeststellung des Antragstellers
- durch Vorlage eines amtlichen Ausweises oder
- durch persönliche Bekanntheit mit dem Prüforgan (vom Betreiber authorisierte Person oder Mitarbeiter einer Prüfstelle), wobei sich das Prüforgan für die zweifelsfreie Identitätsfeststellung verbürgt, die Prüfung schriftlich dokumentiert und mit Unterschrift bestätigt.

Wenn die Prüfung von einer Prüfstelle- vorgenommen wird, dann gilt sie als abgeschlossen, wenn die erforderliche Bestätigung unterfertigt und mit Prüfvermerk der Prüfstelle versehen an den Betreiber retourniert wurde.

4.2.2 Approval or rejection of certificate applications / Annahme oder Ablehnung von Zertifikatsanträgen / Approval or rejection of certificate applications

A certificate is issued only when the authentication procedures necessary for the respective type of certificate have been successfully completed.

After authentication, the application data is
(a) approved so that a certificate can be created or
(b) the applicant receives a request for further documents or
(c) the applicant is informed that the application has been rejected.

If the applicant does not meet the request to provide further documents even after a reminder, the application is rejected.

Ein Zertifikat wird erst dann ausgestellt, wenn alle für den jeweiligen Zertifikatstyp notwendigen Prüfschritte erfolgreich abgeschlossen wurden.

Nach Prüfung der Antragsdaten werden Zertifikatsanträge:
(a) entweder zur Zertifikatserstellung freigegeben oder
(b) der Antragsteller erhält den Auftrag weitere Unterlagen beizubringen oder
(c) der Antragsteller wird von der Ablehnung seines Antrags verständigt.

Kommt ein Antragsteller der Aufforderung zur Ergänzung der Unterlagen auch nach Mahnung nicht nach, dann wird der Antrag abgelehnt.

4.2.3 Time to process certificate applications / Fristen für die Bearbeitung von Zertifkatsanträgen

Applications for certificates are processed as per law, contractual agreements and the processing times given on the website.

Zertifikatsanträge werden gemäß gesetzlicher Vorgaben, vertraglicher Vereinbarungen und den auf der Website zugesicherten Fristen bearbeitet.

4.3 Certificate issuance / Zertifikatsausstellung

The CA issues certificates based on a reviewed and approved application and the public key of the applicant.

Der VDA stellt Zertifikate auf Basis eines geprüften und freigegebenen Antrags und des öffentlichen Schlüssels des Antragstellers aus.

The operator issues certificates as per the respective notice of the regulatory authority or based on the product description published on its website. In particular, these certificates are in X.509v3 format.

Der Betreiber erstellt Zertifikate gemäß der jeweiligen Anzeige bei der Aufsichtsbehörde oder auf Grund der auf seiner Website veröffentlichten Produktbeschreibung. Insbesondere sind dies Zertifikate im X.509v3 Format.

Certificates are only issued in a secure environment using predefined processes (security profiles and configurations) that check the authenticity of the certificate request and the integrity of the application data provided and proceed as per the applicable certificate policy.

Die Zertifikatserstellung erfolgt ausschließlich in einer gesicherten Umgebung durch vorgegebene Prozesse (Sicherheitsprofile und Konfigurationen), die vor der Zertifikatserstellung die Authentizität der Zertifikatsanforderung und die Integrität der freigegebenen Antragsdaten prüfen und gemäß der zutreffenden Certificate Policy ablaufen.

The structure and content of the certificates comply with the applicable certificate policy. Qualified certificates for electronic signatures include all information necessary for electronic signatures and identification of the subscriber. Qualified server certificates include all information necessary for website authentication.

Aufbau und Inhalt der Zertifikate hat der jeweils anzuwendenden Certificate Policy zu entsprechen. Qualifizierte Zertifikate für elektronische Signaturen enthalten jedenfalls alle zur elektronischen Signatur erforderlichen und den Signator identifizierenden Angaben. Qualifizierte Serverzertifikate enthalten jedenfalls alle zur Websiteauthentifizierung erforderlichen Angaben.

The certificate issuance procedures described in this section apply to

⇨ 4.6 Certificate renewal / Neuaustellung Zertifikat (p72)

Die in diesem Abschnitt beschriebenen Abläufe für die Zertifikatsausstellung gelten sinngemäß auch für

⇨ 4.6 Certificate renewal / Neuaustellung Zertifikat (p72)

⇨ 4.7 Certificate re-key / Neuausstellung des Zertifikats mit Erzeugung eines neuen Schlüsselpaares (p74)
⇨ 4.8 Certificate modification / Zertifikatsänderung (p76)

⇨ 4.7 Certificate re-key / Neuausstellung des Zertifikats mit Erzeugung eines neuen Schlüsselpaares (p74)
⇨ 4.8 Certificate modification / Zertifikatsänderung (p76)

4.3.1 CA actions during certificate issuance / Vorgehen des VDA bei der Ausstellung von Zertifikaten

The processes (security profiles and configurations) necessary for the issuance of certificates are approved by the responsible authority as per ⇨ GLOBALTRUST® Certificate Security Policy.

Die zur Zertifikatserstellung erforderlichen Prozesse (Sicherheitsprofile und Konfigurationen) werden von der gemäß ⇨ GLOBALTRUST® Certificate Security Policy zuständigen Stelle freigegeben.

The certificate is provided with the signature verification data of the operator and is electronically signed by the operator. The signature creation data used for this signature have been generated according to the requirements of [eIDAS-VO] and other legal and technical standards.

Das Zertifikat wird mit Signaturprüfdaten des Betreibers versehen und ist von ihm elektronisch signiert. Die dafür verwendeten Signaturerstellungsdaten wurden gemäß den Anforderungen der [eIDAS-VO] und anderer rechtlicher und technischer Vorgaben erzeugt.

The formats of the certificates, especially qualified certificates, are defined in the applicable certificate policy. If there is no individual definition provided, [RFC5280] is applicable. Qualified certificates contain the information necessary as per [eIDAS-VO] Appendix I or Appendix IV and [ETSI EN 319 412]. In case of qualified server certificates, in addition [CABROWSER-EV] applies.

Die Formate der Zertifkate, insbesondere der qualifizierten Zertifikate sind in der jeweils anzuwendenden Certificate Policy definiert. Sofern keine eigene Definition erfolgt, gilt [RFC5280]. Qualifizierte Zertifikate enthalten jedenfalls die erforderlichen Angaben gemäß [eIDAS-VO] Anhang I bzw. Anhang IV und [ETSI EN 319 412]. Bei qualifizierten Serverzertifikaten wird zudem [CABROWSER-EV] beachtet.

A protocol is created when issuing a certificate. The protocol can be submitted to regulatory authorities, accreditation organisations and other verification authorities upon request. Furthermore, all issuance procedures are logged that concern subscriber certificates, certificates and keys used by the operator for their signatures, cross-certificates and certificates containing identification and infrastructure keys.

Bei Ausstellung eines Zertifikates wird ein Protokoll erstellt. Das Protokoll kann Aufsichtstellen, Akkreditierungseinrichtungen oder sonstigen Prüfstellen bei Bedarf vorgelegt werden. Weiters werden alle ausstellungsrelevanten Schritte der Signator-Zertifikate, der zur Signatur vom Betreiber verwendeten Zertifikate und Schlüssel, der Cross-Zertifikate und der Zertifikate der Identifikations- und Infrastrukturschlüssel protokolliert .

Data necessary for certification is transferred to the certification system via secure paths. The confidentiality and integrity of the information is also ensured. Secure paths include the use of, in particular, external data carriers intended solely for the purpose of delivering data, dedicated VPN

Die Übergabe der zur Zertifizierung erforderlichen Daten an das Zertifizierungssystem erfolgt über gesicherte Pfade. Dabei wird die Vertraulichkeit und die Integrität der Informationen sicher gestellt. Als gesicherte Pfade gelten insbesondere die Verwendung ausschließlich für

tunnels between the administrative system and the certification system or equivalent, state-of-the-art measures. Requests for certificates are electronically signed.

All certificates are signed with a private key of the CA. Only CA certificates, cross-certificates, certificates for infrastructure assignments and internal certificates are issued with a root certificate.

According to Certificate Transparency (defined in [RFC6962]) server-certificates are disclosed on at least three audit-proof logservers operated by external entities. (Certificate Transparency according to [RFC6962]

den Zweck der Übergabe vorgesehene externe Datenträger, dedizierte VPN-Tunnel zwischen administrativem System und Zertifizierungssystem oder durch vergleichbare, dem Stand der Technik entsprechende Maßnahmen. Die Anforderung von Zertifikaten wird elektronisch signiert.

Alle Zertifikate werden mit einem privaten Schlüssel des VDA signiert. Mit einem Root-Zertifikat werden ausschließlich CA-Zertifikate, Cross-Zertifikate, Zertifikate für Infrastrukturaufgaben oder interne Zertifikate ausgestellt.

Bei der Ausstellung von Serverzertifikaten erfolgt eine Veröffentlichung auf mindestens drei revisionssicheren Logservern die von externen Stellen betrieben werden (Certificate Transparency gemäß [RFC6962])

4.3.2 Benachrichtigung des Signators über die Ausstellung des Zertifikats / Notification to subscriber by the CA of issuance of certificate

The subscriber is immediately informed by appropriate means that the certificate has been issued.

Appropriate means for informing the subscriber include, in particular

- by email (provided that an address has been given in the application or is known because of a previous business relationship) or
- by post or fax or
- on the phone or in person.

It is permitted to use more than one form of communication simultaneously.

This communication never contains confidential information that would allow use of the certificate on its own.

Der Signator wird nach Ausstellung des Zertifikates unverzüglich in geeigneter Form informiert.

In geeigneter Form erfolgt die Information insbesondere

- durch Verständigung per E-Mail (sofern eine Adresse im Antrag angegeben wurde oder auf Grund einer früheren Geschäftsbeziehung bekannt ist) oder
- durch Zustellung eines Briefes oder Faxes oder
- durch telefonische oder persönliche Mitteilung.

Es ist zulässig mehrere Verständigungsformen parallel zu wählen.

In keinem Fall enthält die Verständigung geheime Informationen, die für sich allein genommen die Nutzung eines Zertifikates erlauben.

4.4 Certificate acceptance / Zertifikatsannahme

The subscriber should confirm that he has received the certificate and corresponding conditions of use, in particular this GLOBALTRUST® Certificate Policy and the corresponding GLOBALTRUST® Certificate Practice Statement.

Der Signator hat die Annahme des Zertifikates und der dazugehörigen Nutzungsbestimmungen, insbesondere diese GLOBALTRUST® Certificate Policy und das zugehörige GLOBALTRUST® Certificate Practice Statement zu bestätigen.

4.4.1 Conduct constituting certificate acceptance / Verfahren zur Zertifikatsannahme

Confirmation that the certificate has been received is given either in written or electronic form, in compliance with the law.

Die Bestätigung der Zertifikatsannahme erfolgt schriftlich oder elektronisch, jedenfalls in Übereinstimmung mit gesetzlichen Vorgaben.

4.4.2 Publication of the certificate by the CA / Veröffentlichung der Zertifikate

The necessary verification data, such as, in particular, the public signature key, hash values and further information on the operator, are published on the website of the operator or in the link given in the applicable GLOBALTRUST® Certificate Practice Statement. Every certificate contains a reference to the publicly accessible authority where the verification data can be accessed and requested.

Die erforderlichen Prüfdaten, wie insbesondere öffentliche Signaturschlüssel, Hash-Werte, weitere Angaben zum Betreiber werden auf der Website des Betreibers oder im anzuwendenden GLOBALTRUST® Certificate Practice Statement genannten Link veröffentlicht. Jedes ausgestellte Zertifikat enthält einen Verweis auf eine öffentlich zugängliche Stelle über die diese Prüfdaten abgerufen oder angefordert werden können.

4.4.3 Notification of certificate issuance by the CA to other entities / Benachrichtigung von Dritten über die Zertifikatsaustellung

Other organisations are informed immediately by the operator,

- if the certificate issued affects their activities or
- this has been contractually agreed or
- other legal conditions necessitate that they be informed.

Sonstige Einrichtungen werden vom Betreiber unverzüglich benachrichtigt,

- sofern ein ausgestelltes Zertifikat Auswirkungen auf ihre Tätigkeit hat oder
- es vertraglich vereinbart ist oder
- sonstige rechtliche Bestimmungen die Benachrichtigung erfordern.

4.5 Key pair and certificate usage / Schlüsselpaar und Zertifikatsnutzung

4.5.1 Subscriber private key and certificate usage / Nutzung des privaten Schlüssels und des Zertifikates durch den Signator

The CA contractually obligates the subscriber to comply with the following commitments.

All contractual conditions will be made available to the applicant on the website of the CA Website. The applicant confirms that he has received and accepted these simultaneous to sending the order form.

The subscriber is obligated to:

1. input complete and correct information in compliance with the requirements of this policy, especially during the registration procedure.
2. verify that all information in the certificate is correct directly after successful delivery
3. retain the private key to a hardware unit to which the subscriber has sole access (for example, encrypted storage of a private key using a password, signature PIN or passphrase, special signature creation devices that prevent or essentially complicate the reading of a private key). For simple signatures, for example GLOBALTRUST® CLIENT, limitations on access and organisational measures that limit access to the computer that contains the key and the certificate are also understood to be sufficient security measures for the purpose of this policy.
4. in the case of self-generation of a private key, appropriate secure procedures should be applied to ensure a sufficient quality of randomness in the generation of keys. In particular, these are hardware components explicitly intended for this purpose, such as

Der VDA bindet den Signator vertraglich an die Einhaltung der nachfolgend angeführten Verpflichtungen.

Dem Antragsteller werden alle Vertragsbedingungen auf der Website des VDA zugänglich gemacht. Gleichzeitig mit dem Absenden des Bestellformulars bestätigt er deren Kenntnisnahme und Akzeptanz.

Die dem Signator auferlegten Verpflichtungen umfassen:

1. Die Angabe vollständiger und korrekter Informationen in Übereinstimmung mit den Anforderungen dieser Policy insbesondere anlässlich des Vorgangs der Registrierung.
2. Die Prüfung der Korrektheit aller Angaben im Zertifikat auf deren Korrektheit unmittelbar nach erfolgter Zustellung
3. Die Aufbewahrung des privaten Schlüssels in einer Hardware-Einheit, zu der der Signator den alleinigen Zugriff hat (z.B. verschlüsseltes Abspeichern des privaten Schlüssels mittels Passwort, Signatur-PIN bzw. Passphrase, spezielle Signaturerstellungseinheiten, die das Auslesen des privaten Schlüssels verhindern oder wesentlich erschweren).
   Im Fall einfacher Signaturen, wie zum Beispiel GLOBALTRUST® CLIENT, sind auch Zutrittsbeschränkungen und organisatorische Maßnahmen, die den Zugang zum Computer beschränken der den Schlüssel und das Zertifikat enthält, als ausreichende Sicherheitsmaßnahmen im Sinne dieser Policy zu verstehen.
4. Im Falle der Selbstgenerierung des privaten Schlüssels werden geeignete sichere Verfahren angewandt, die eine ausreichende Zufallsqualität bei der Schlüsselerzeugung gewährleisten, insbesondere sind dies ausdrücklich dafür vorgesehene

HSM modules, or software components, which allow their user to increase the quality of randomness through system events (in particular the entry of files with random numbers, the performance of movements of the mouse or keystrokes during key generation). The CA reserves the right to require full disclosure of information on the key generation procedure from the subscriber and to reject a certification application if concerns arise over the quality of randomness of the key. Inappropriate key procedures are detailed on the website of the operator and may not be used.

5. use appropriate caution to prevent the unauthorised use of the private key.
6. use server certificates exclusively on devices that are accessible from the addresses listed in the certificate (for X.509v3 in the subjectAltName extension).
7. inform the operator immediately if one or more of the following circumstances arise before the validity of the certificate has expired:
   - the private key or its activation data has been lost.
   - the private key of the subscriber or its activation data may have been compromised,
   - exclusive control over the private key has been lost,
   - the information in the certificate is incorrect or has changed,
8. completely remove the key from operation immediately as soon as the subscriber becomes aware that it has been compromised.
9. completely remove the keyfrom operation if informed by the operator that the CA key has been compromised.
10. the secure safekeeping of the key remains the sole responsibility of the

Hardwarekomponenten, wie HSM-Module oder Softwarekomponenten, die es erlauben durch Systemereignisse die Zufallsqualität zu erhöhen (insbesondere Angabe von Dateien mit Zufallszahlen, Durchführen von Mausbewegungen oder Tastaturanschlägen während der Schlüsselgenerierung). Der VDA behält sich vor, vom Signator vollständige Auskunft über den Schlüsselgenerierungsvorgang zu verlangen und bei Bedenken bezüglich der Zufallsqualität des Schlüssels einen Zertifizierungsantrag abzulehnen. Ungeeignete Schlüsselverfahren werden auf der Website des Betreibers bekannt gemacht und dürfen nicht verwendet werden.

5. Die Anwendung entsprechender Vorsicht, um den unbefugten Gebrauch des privaten Schlüssels zu verhindern.
6. Die Verwendung von Serverzertifikaten ausschließlich auf Geräten, die über die im Zertifikat eingetragenen Adressen (bei X.509v3 in der subjectAltName-Erweiterung) erreichbar sind.
7. Die unverzügliche Benachrichtigung des Betreibers, wenn vor Ablauf der Gültigkeitsdauer eines Zertifikats eine oder mehrere der folgenden Bedingungen eintreten:
   - Der private Schlüssel oder dessen Aktivierungsdaten gingen verloren.
   - der private Schlüssel des Signators oder dessen Aktivierungsdaten wurden möglicherweise kompromittiert,
   - die alleinige Kontrolle über den privaten Schlüssel ging verloren,
   - die im Zertifikat beinhalteten Informationen sind inkorrekt oder haben sich geändert,
8. Die unverzügliche vollständig Außerbetriebnahme des Schlüssels, sobald er Kenntnis über dessen Kompromitierung erhält .
9. Die unverzügliche vollständig Außerbetriebnahme des Schlüssels, wenn ihm vom Betreiber eine Kompromitierung des CA-Schlüssels zur Kenntnis gebracht wird.
10. Die sichere Verwahrung des Schlüssels liegt in der ausschließlichen

subscriber.

11. destroy invalid keys. This also applies for keys saved on signature creation devices. An appropriate method of destruction includes returning the signature creation device to the operator with a request to destroy the invalid key.

12. The subscriber should inform the user of signed data of his obligations for the purpose of this policy in a suitable way. He may not conclude agreements or provide explanations to a third party that contradict this policy, the applicable standards, the valid juridical, in particular legal, conditions, or the GLOBALTRUST® Certificate Practice Statement.

13. The following limitations apply to the issuance of qualified certificates for electronic signatures:
    The key pair may only be used for the generation of electronic signatures. All further limitations on the administration of keys of which the subscriber is informed should likewise be observed.
    The certificate may only be used for electronic signatures that have been generated with the SSCD corresponding to the certificate.

14. In the event that the CA key or subscriber key has been compromised, the subscriber should follow the instructions of the CA within 48 hours. This time span is shortened if specific security risks are expected. In this event, the subscriber will be informed of the shortened reaction time by telephone, email or other suitable means.

15. The subscriber accepts that the CA can revoke a certificate in the event of a violation of the conditions of this policy, other agreements concluded with the subscriber, or the use of the certificate for criminal

Verantwortung des Signators.

11. Ungültige Schlüssel sind zu vernichten, dies gilt auch für auf Signaturerstellungeinheiten gespeicherte Schlüssel. Eine geeignete Vernichtung besteht auch in der Retournierung der Signaturerstellungseinheit an den Betreiber mit dem Auftrag die ungültigen Schlüssel zu vernichten.
12. Der Signator hat den Nutzer signierter Dateien in geeigneter Weise auf seine Pflichten im Sinne dieser Policy hinzuweisen. Er darf keine Vereinbarungen abschließen oder Erklärungen gegenüber Dritten abgeben, die im Widerspruch zu dieser Policy, den anzuwendenden Standards, den gültigen rechtlichen, insbesondere gesetzlichen Bestimmungen oder dem GLOBALTRUST® Certificate Practice Statement stehen.
13. Im Falle der Ausgabe qualifizierter Zertifikate für elektronische Signaturen gelten folgende Einschränkungen:
    Das Schlüsselpaar darf ausschließlich für die Erstellung elektronischer Signaturen eingesetzt werden. Alle weiteren dem Signator bekanntgegebenen Einschränkungen der Schlüsselverwaltung sind ebenfalls zu beachten.
    Das Zertifikat darf nur für elektronische Signaturen verwendet werden, die mit der dem Zertifikat zugehörigen SSCD erstellt wurden.
14. Im Falle der Kompromitierung eines CA- oder des Signator-Schlüssels hat der Signator die Anweisungen des VDA innerhalb von 48 Stunden auszuführen. Diese Zeitspanne kann verkürzt werden, wenn spezifische Sicherheitsrisken zu erwarten sind. In diesem Fall wird der Signator von der verkürzten Reaktionszeit telefonisch, per E-Mail oder auf sonstige geeignete Weise verständigt.
15. Der Signator akzeptiert, dass der VDA ein Zertifikat im Falle der Mißachtung der Bestimmungen dieser Policy, anderer mit dem Signator geschlossenen Vereinbarungen oder im Falle der

or fraudulent activities. Compensation will not be paid for a certificate revoked on these grounds or for resulting damages.

Enduser-sub-certificates whose private keys are under the control of the subscriber must fulfill additional conditions below the restrictions listed in ⇨ 7.1.2 Certificate extensions / Zertifikatserweiterungen (p161).

These certificates contain an OID as a policy entry, with which it is shown that the user complies with the conditions and policies of a third party with whom the CA has concluded an agreement to recognise the CA certificates in advance. These are the [CABROWSER-BASE] and [MS-CA] conditions. Furthermore, there is no “anyPolicy” entry in the certificate, in particular for x.509v3 certificates.

If the subscriber can issue certificates in the context of a enduser-sub-certificate assigned to him using an automated process, all inputs for email addresses, domain names and IP addresses may only originate from a predefined range that has been verified and agreed by a registration authority.

Additional conditions for the use of readable data carriers for private keys:

If the private key is stored in readable data carriers (floppy disk, USB stick, hard drive, etc), the subscriber is obligated to keep the necessary passwords separately and to take particular care of the data carrier. Transportable data carriers (floppy disk, USB stick, CD, ...) should be kept in secure containers that are only accessible to the subscriber. Built-in, fixed data carriers (hard drive) should only be usable by the subscriber. System administrators should be contractually obligated to secure the confidentiality of the private key. It should be ensured that copies are only

Zertifkatsverwendung für kriminelle oder betrügerische Aktivitäten jederzeit widerrufen kann. Ein Kostenersatz für aus diesen Gründen widerrufene Zertifikat oder daraus resultierten Schäden gebührt nicht.

Endkunden-Sub-Zertifikate, bei denen der private Schlüssel unter Kontrolle des Signators ist, haben zu den unter ⇨ 7.1.2 Certificate extensions / Zertifikatserweiterungen (p161) genannten Einschränkungen nachstehende zusätzliche Bedingungen zu erfüllen.

Solche Zertifikate enthalten als Policy-Eintrag eine OID mit der angezeigt wird, dass der Nutzer die Bestimmungen und Policies Dritter einhält, mit denen der VDA Vereinbarungen zur Vorabanerkennung der CA-Zertifikate abgeschlossen hat, jedenfalls sind dies die Bestimmungen [CABROWSER-BASE] und [MS-CA]. . Darüber hinaus ist im Zertifikat keinesfalls ein Eintrag im Sinne "beliebige Policy" vorhanden, insbesondere ist bei x.509v3-Zertifikaten kein anyPolicy Eintrag vorgesehen.

Sofern der Signator über einen automatisierten Vorgang Zertifikate im Rahmen eines ihm zugewiesenen Endkunden-Sub-Zertifikates ausstellen kann, dürfen Einträge von E-Mail-Adressen, Domain Namen und IP-Adressen lediglich einem vorab definierten und von einer Registrierungsstelle geprüften und vereinbarten Bereich entstammen.

Additional conditions / Ergänzende Bestimmungen bei Einsatz auslesbarer Datenträger für private Schlüssel:

Soweit der private Schlüssel in auslesbaren Datenträgern gespeichert ist (Diskette, USB-Stick, Festplatte usw.), verpflichtet sich der Signator zur getrennten Verwahrung erforderlicher Passwörter und zur besonders sorgfältigen Verwahrung des Datenträgers. Bei transportablen Datenträgern (Diskette, USB-Stick, CD, ...) erfolgt die Aufbewahrung in verschlossenen, nur für den Signator zugänglichen Behältern, bei fix eingebauten Datenträgern (Festplatten) ist die Verwendung auf den Signator beschränkt. Systemadministratoren sind vertraglich zur

made when requested by the subscriber (this also applies for back-up copies).

Furthermore, the subscriber should ensure as per the current state of the art that the data carrier is free from malware that could read, copy or otherwise change the private key. In particular, the subscriber should undertake sufficient protection measures against malware of any kind, especially viruses, worms, programmes with trapdoor functions or spyware programmes that could compromise the private key, the certificate or another part of the signature process.

Sicherung der Vertraulichkeit des privaten Schlüssels zu verpflichten. Es ist sicherzustellen, dass nur vom Signator veranlasste Kopien erstellt werden (gilt auch für Backupkopien).

Weiters stellt der Signator nach dem Stand der Technik sicher, dass der verwendete Datenträger frei von Schadprogrammen ist, die den privaten Schlüssel auslesen, kopieren oder sonstwie verändern können. Insbesondere unternimmt der Signator ausreichende Schutzmaßnahmen gegen Malware jeglicher Art, insbesondere Viren, Würmer, Programme mit Trapdoorfunktionen und Spyware-Programme, die den privaten Schlüssel, das Zertifikat oder einen sonstigen Teil eines Signaturvorganges beeinträchtigen können.

4.5.2 Relying party public key and certificate usage / Nutzung des öffentlichen Schlüssels und des Zertifikates durch Nutzer

Electronic signatures that use certificates that have been issued by the CA are only valid in the framework of this policy. Electronic signatures in this meaning are also timestamps, issued from the CA. Users of certificates and electronically signed information (including Timestamps) must therefore observe the following verification procedures:

- the verification will be documented to the extent necessary to record the facts,
- binding transactions of a value more than 100 000 EUR require a qualified signature.
- The user of the electronic signature must document the verification in written form and the verification should be performed by at least two persons working independently from one another.
  The revocation status of a certificate is to be checked by the services provided by the CA.
- if the verification of a certificate for an electronic signature is not possible, it is the responsibility of the user whether he recognises the validity of the signatures. The CA or a third party is explicitly not

Elektronische Signaturen die Zertifikate verwenden, die vom VDA herausgegeben wurden, sind nur im Rahmen dieser Policy gültig. Als elektronische Signatur in diesem Sinne sind auch die vom VDA erbrachten Zeitstempel zu verstehen. Nutzer von Zertifikaten und elektronisch signierten Informationen inklusive Zeitstempel müssen folgende Prüfschritte beachten:

- die Überprüfung wird in dem Umfang dokumentiert als dies zur Sicherung rechtlicher Sachverhalte erforderlich ist,
- verbindliche Rechtsgeschäfte mit einem Wert von mehr als 100.000,- Euro erfordern eine qualifizierte Signatur
- der Nutzer der elektronischen Signatur hat die Prüfung jedenfalls schriftlich zu dokumentieren und die Prüfung hat unabhängig voneinander durch zumindest zwei Personen zu erfolgen,
- Der Widerrufsstatus eines Zertifikates ist durch die vom VDA bereitgestellten Dienste zu überprüfen.
- ist die Überprüfung eines Zertifikates zu einer elektronischen Signatur nicht möglich, liegt es in der alleinigen Verantwortung des Nutzers, ob er die Gültigkeit der Signatur anerkennt, eine Haftung

responsible for this.
- Observance of the limitations on the use or validity of the certificate (especially observance of upper limits for amounts for which valid signatures can be issued), as given in the certificate (inc. reference to the applicable certificate policy) or in the published terms and conditions. The liability of the CA is also limited as per these limitations and upper limits.
- All precautions prescribed in agreements or elsewhere must be observed.

The user registers, that because of the fast progress of the cryptography technique and the improvement of computer systems, signatures and keys may get uncertain, even if at the time of issuing, the security of the signature was certain. It is advised to check the VDA website on "limits" to find constraints of the validity of signatures and certificates, that can not be published by revocation and / or the certificate content. This regards especially older signatures, in any case signatures that are older than 12 months.

In case of receiving a time stamp, the user has the same check duties as for other signatures. Furthermore, possible technical limitations that result from the issuing of the time stamp (⇨ 6.8 Time-stamping / Zeitstempel p151 and ⇨ GLOBALTRUST® Certificate Practice Statement 6.8 Time-stamping / Zeitstempel) must be considered.

If doubts over the validity of the certificate arise, especially if the means provided to request the status of suspension and revocation are not available, the CA should be contacted directly. The appropriate measures

des VDA oder Dritter ist ausdrücklich ausgeschlossen,
- Beachtung der im Zertifikat (inkl. Verweis auf die anzuwendende Certificate Policy) oder in den veröffentlichten Geschäftsbedingungen dargelegten Einschränkungen in der Nutzung bzw. Gültigkeit des Zertifikats (insbesondere Beachtung von Betragsobergrenzen, bis zu denen die Signatur gültig ausgestellt wird). Gemäß dieser eingetragenen Einschränkungen und Obergrenzen beschränkt sich auch die Haftung des VDA.
- Sämtliche Vorkehrungen die in Vereinbarungen oder anderswo verordnet wurden, müssen eingehalten werden.

Der Nutzer nimmt zur Kenntnis, dass auf Grund des raschen Fortschritts der kryptographischen Technik und der raschen Steigerung der Leistungsfähigkeit von Computersystemen Signaturen und Schlüssel unsicher werden können, auch wenn zum Zeitpunkt der Ausstellung der Signatur von der Sicherheit des Signaturverfahrens ausgegangen werden konnte. Es wird daher dringend empfohlen die Website des VDA zum Thema Limits zu konsultieren, um allfällige Beschränkungen in der Gültigkeit von Signaturen und Zertifikaten erkennen zu können, die sich nicht durch Widerruf- und/oder Zertifikatsinhalt darstellen lassen. Dies gilt insbesondere bei Signaturen älteren Datums, jedenfalls bei Signaturen, die länger als 12 Monate zurück liegen.

Im Falle des Erhalts eines Zeitstempels gelten für den Nutzer bezüglich der Signatur des Zeitstempels dieselben Prüfpflichten, wie für jede andere Signatur. Zusätzlich sind jedoch allfällige technische Beschränkungen zu beachten, die sich durch die Ausgabe des Zeitstempels ergeben (⇨ 6.8 Time-stamping / Zeitstempel p151 und ⇨ GLOBALTRUST® Certificate Practice Statement 6.8 Time-stamping / Zeitstempel).

Bestehen Zweifel an der Gültigkeit des Zertifikats, insbesondere wenn die bereitgestellten Abfragemöglichkeiten zu Sperr- und Widerrufsstatus nicht verfügbar sind, ist mit dem VDA direkt Kontakt aufzunehmen. Es

will then be taken to clarify the validity of the certificate.

The VDA registers all of the issued time stamps. In case of doubt about the validity of a time stamp, the VDA can check if the time stamp for a specific document was really issued by its service. For this purpose, the user only has to send the hash value of the document to the VDA. Than the user receives information whether and when a time stamp had been requested for this hash value.

werden dann geeignete Maßnahmen zur Klärung der Gültigkeit des Zertifikats gesetzt.

Der VDA registriert alle erbrachten Zeitstempel. Bestehen Zweifel an der Gültigkeit eines Zeitstempels kann der VDA feststellen, ob der Zeitstempel zu einem bestimmten Dokument tatsächlich mit seinem Service erbracht wurde. Dazu ist es ausreichend den Hash-Wert des zu prüfenden Dokuments an den VDA zu senden. Der Nutzer erhält auf diesem Weg Auskunft ob und wenn ja, wann ein Zeitstempel zu diesem Hash-Wert angefordert wurde.

4.6 Certificate renewal / Neuaustellung Zertifikat

The CA issues certificates as part of the renewal of a certificate on the basis of a reviewed and approved application and the public key of the applicant.

An existing certificate is not extended. It is however permitted to make a new certificate with a new duration and new certificate data using an existing key or an existing CSR (Certificate Signing Request), provided that the algorithms used comply with the current state of the art.

Der VDA stellt Zertifikate im Zuge der Neuausstellung eines Zertifikat auf Basis eines geprüften und freigegebenen Antrags und des öffentlichen Schlüssels des Antragstellers aus.

Ein bestehendes Zertifikat wird nicht verlängert, es ist jedoch zulässig zu einem bestehenden Schlüssel bzw. zu einem bestehenden CSR (Certificate Signing Request) ein neues Zertifikat mit neuer Laufzeit und neuen Zertifikatsangaben zu machen, sofern die verwendeten Algorithmen noch dem aktuellen technischen Standard entsprechen.

4.6.1 Circumstance for certificate renewal / Umstände für Neuaustellung eines Zertifikats

The renewal of a certificate is permitted if
- the kind of certificate allows this legally and
- there are no distinct reasons against renewal.

Eine Neuausstellung eines Zertifikates ist zulässig, wenn
- die Art des Zertifikates es rechtlich zulässt und
- keine individuellen Gründe gegen eine Neuausstellung sprechen.

4.6.2 Who may request renewal / Berechtigte für Antrag auf Neuaustellung Zertifikat

The original applicant is authorised to apply for a renewal.

Für einen Antrag auf Neuausstellung ist der ursprüngliche Antragsteller berechtigt.

4.6.3 Processing certificate renewal requests / Bearbeitung eines Antrags auf Neuausstellung Zertifikat

It is ensured that applications from applicants who are already registered from a previous certificate issuance are complete, correct and properly authorised using the following measures:

- The registration authority verifies the data in the certificate for its current validity.
- Possible changes to the existing policy, terms and conditions and other agreements will be communicated.

Durch folgende Maßnahmen wird sicher gestellt, dass Anträge von Antragstellern, die anlässlich einer vorhergehenden Zertifikatsausstellung bereits registriert wurden, vollständig, korrekt und ordnungsgemäß autorisiert sind:

- Die Registrierungsstelle prüft die im Zertifikat enthaltenen Daten hinsichtlich ihrer aktuellen Gültigkeit.
- Allfällige Änderungen in der vorliegenden Policy, in den Geschäftsbedingungen und in den sonstigen Vereinbarungen werden zur Kenntnis gebracht.

Information for server certificates issued before 1st September 2020 may be used again without renewed verification, provided that it is not older than 825 days.

Informationen für vor 1.9.2020 ausgestellte Serverzertifikate dürfen ohne neuerliche Prüfung wiederverwendet werden, sofern sie nicht älter als 825 Tage sind

Information for server certificates issued on or after 1st September 2020 may be used again without renewed verification, provided that it is not older than 397 days.

Informationen für ab 1.9.2020 ausgestellte Serverzertifikate dürfen ohne neuerliche Prüfung wiederverwendet werden, sofern sie nicht älter als 397 Tage sind.

The CA renews certificates for which the key pair is retained on the basis of a reviewed and approved application and the public key of the applicant.

Der VDA führt Zertifikatsneuausstellung mit Beibehaltung des Schlüsselpaares auf Basis eines geprüften und freigegebenen Antrags und des öffentlichen Schlüssels des Antragstellers aus.

4.6.4 Notification of new certificate issuance to subscriber / Benachrichtigung des Signators über die Neuausstellung Zertifikat

Notification of a renewal is subject to the same procedures and restrictions as ⇨ 4.3.2 Benachrichtigung des Signators über die Ausstellung des Zertifikats / Notification to subscriber by the CA of issuance of certificate

Die Benachrichtigung der Neuausstellung unterliegt denselben Verfahren und Beschränkungen wie ⇨ 4.3.2 Benachrichtigung des Signators über die Ausstellung des Zertifikats / Notification to

(p64).

subscriber by the CA of issuance of certificate (p64).

4.6.5 Conduct constituting acceptance of a renewal certificate / Verfahren zur Annahme nach Neuausstellung Zertifikat

The procedure for accepting certificates after renewal is subject to the same procedures and restrictions as in ⇨ 4.4.1 Conduct constituting certificate acceptance / Verfahren zur Zertifikatsannahme (p65).

Das Verfahren zur Zertifikatsannahme nach Neuausstellung unterliegt denselben Verfahren und Beschränkungen wie ⇨ 4.4.1 Conduct constituting certificate acceptance / Verfahren zur Zertifikatsannahme (p65).

4.6.6 Publication of the renewal certificate by the CA / Veröffentlichung der Neuausstellung Zertifikat durch VDA

Publication of renewal is subject to the same procedures and restrictions as in ⇨ 4.4.2 Publication of the certificate by the CA / Veröffentlichung der Zertifikate (p65).

Die Veröffentlichung der Neuausstellung unterliegt denselben Verfahren und Beschränkungen wie ⇨ 4.4.2 Publication of the certificate by the CA / Veröffentlichung der Zertifikate (p65).

4.6.7 Notification of certificate issuance by the CA to other entities / Benachrichtigung von Dritten über die Ausstellung eines Zertifikates

Notification of renewal is subject to the same procedures and restrictions as in ⇨ 4.4.3 Notification of certificate issuance by the CA to other entities / Benachrichtigung von Dritten über die Zertifikatsaustellung (p65).

Die Benachrichtigung der Neuausstellung unterliegt denselben Verfahren und Beschränkungen wie ⇨ 4.4.3 Notification of certificate issuance by the CA to other entities / Benachrichtigung von Dritten über die Zertifikatsaustellung (p65).

4.7 Certificate re-key / Neuausstellung des Zertifikats mit Erzeugung eines neuen Schlüsselpaares

Certificate re-key is subject to the same procedures and restrictions as in ⇨ 4.6 Certificate renewal / Neuaustellung Zertifikat (p72).

Zertifikatsneuausstellung mit Erzeugung eines neuen Schlüsselpaares unterliegen denselben Verfahren und Beschränkungen wie ⇨ 4.6 Certificate renewal / Neuaustellung Zertifikat (p72).

4.7.1 Circumstances for certificate re-key / Umstände für Neuausstellung Zertifikat mit Erzeugung eines neuen Schlüsselpaares

Certificate re-key is permitted if

Eine Neuausstellung eines Zertifikates mit Erzeugung eines neuen Schlüsselpaares ist zulässig, wenn

- the type of certificate allows this legally and
  there are no distinct reasons against a renewal.

- die Art des Zertifikates es rechtlich zulässt und
- keine individuellen Gründe gegen eine Neuausstellung sprechen.

4.7.2 Who may request certification of a new public key / Berechtigte für Antrag auf Neuaustellung Zertifikat mit Erzeugung eines neuen Schlüsselpaares

The subscriber is authorised to make an application for renewal.

Für einen Antrag auf Neuausstellung ist der Signator berechtigt.

4.7.3 Processing certificate re-keying requests / Bearbeitung eines Antrags auf Neuausstellung Zertifikat mit Erzeugung eines neuen Schlüsselpaares

The processing of an application for re-keying is subject to the same procedures and restrictions as in ⇨ 4.6.3 Processing certificate renewal requests / Bearbeitung eines Antrags auf Neuausstellung Zertifikat (p73).

Die Bearbeitung eines Antrag auf Neuausstellung mit Erzeugung eines neuen Schlüsselpaares unterliegt denselben Verfahren und Beschränkungen wie ⇨ 4.6.3 Processing certificate renewal requests / Bearbeitung eines Antrags auf Neuausstellung Zertifikat (p73).

4.7.4 Notification of new certificate issuance to subscriber / Benachrichtigung über die Neuausstellung Zertifikat mit Erzeugung eines neuen Schlüsselpaares

Notification of the renewal of a re-keyed certificate is subject to the same procedures and restrictions as 4.6.4 Notification of new certificate issuance to subscriber / Benachrichtigung des Signators über die Neuausstellung Zertifikat (p73).

Die Benachrichtigung der Neuausstellung eines Zertifikates mit Erzeugung eines neuen Schlüsselpaares unterliegt denselben Verfahren und Beschränkungen wie ⇨ 4.6.4 Notification of new certificate issuance to subscriber / Benachrichtigung des Signators über die Neuausstellung Zertifikat (p73).

4.7.5 Conduct constituting acceptance of a re-keyed certificate / Verfahren zur Zertifikatsannahme nach Neuausstellung Zertifikat mit Erzeugung eines neuen Schlüsselpaares

The procedure for accepting a certificate after renewal is subject to the same procedures and restrictions as in ⇨ 4.6.5 Conduct constituting acceptance of a renewal certificate / Verfahren zur Annahme nach Neuausstellung Zertifikat (p74).

Das Verfahren zur Zertifikatsannahme nach Neuausstellung unterliegt denselben Verfahren und Beschränkungen wie ⇨ 4.6.5 Conduct constituting acceptance of a renewal certificate / Verfahren zur Annahme nach Neuausstellung Zertifikat (p74).

4.7.6 Publication of the re-keyed certificate by the CA / Veröffentlichung der Neuausstellung Zertifikat mit Erzeugung eines neuen Schlüsselpaares durch VDA

Publication of a re-keyed certificate is subject to the same procedures and restrictions as in ⇨ 4.6.6 Publication of the renewal certificate by the CA / Veröffentlichung der Neuausstellung Zertifikat durch (p74).

Die Veröffentlichung der Neuausstellung mit Erzeugung eines neuen Schlüsselpaares unterliegt denselben Verfahren und Beschränkungen wie ⇨ 4.6.6 Publication of the renewal certificate by the CA / Veröffentlichung der Neuausstellung Zertifikat durch (p74).

4.7.7 Notification of certificate issuance by the CA to other entities / Benachrichtigung von Dritten über Neuausstellung Zertifikat mit Erzeugung eines neuen Schlüsselpaares

Notification of the issuance of a re-keyed certificate is subject to the same procedures and restrictions as in ⇨ 4.6.7 Notification of certificate issuance by the CA to other entities / Benachrichtigung von Dritten über die Ausstellung eines Zertifikates (p74).

Die Benachrichtigung der Neuausstellung mit Erzeugung eines neuen Schlüsselpaares unterliegt denselben Verfahren und Beschränkungen wie ⇨ 4.6.7 Notification of certificate issuance by the CA to other entities / Benachrichtigung von Dritten über die Ausstellung eines Zertifikates (p74).

4.8 Certificate modification / Zertifikatsänderung

Certificate modification is subject to the same procedures and restrictions as in ⇨ 4.6 Certificate renewal / Neuaustellung Zertifikat (p72)

Zertifikatsänderungen unterliegt denselben Verfahren und Beschränkungen wie ⇨ 4.6 Certificate renewal / Neuaustellung Zertifikat (p72)

4.8.1 Circumstances for certificate modification / Umstände für Zertifikatsänderung

Certificate modification is permitted if
- the type of certificate legally permits this and
- there are no distinct reasons against a renewal.

Eine Zertifikatsänderung ist zulässig, wenn
- die Art des Zertifikates es rechtlich zulässt und
- keine individuellen Gründe gegen eine Neuausstellung sprechen.

4.8.2 Who may request certificate modification / Berechtigte für Antrag auf Zertifikatsänderung

The subscriber and persons authorised to represent the company as listed in the certificate are authorised to make an application for a modification.

Für einen Antrag auf Änderung ist der Signator und vertretungsbefugte Personen jenes Unternehmens berechtigt, das im Zertifikat eingetragen ist.

4.8.3 Processing certificate modification requests / Bearbeitung eines Antrags auf Zertifikatsänderung

Certificate modifications are subject to the same procedures and restrictions as in ⇨ 4.6.3 Processing certificate renewal requests / Bearbeitung eines Antrags auf Neuausstellung Zertifikat (p73)

In addition, modified data is reviewed in the same way as new certificate applications.

Zertifikatsänderungen unterliegt denselben Verfahren und Beschränkungen wie ⇨ 4.6.3 Processing certificate renewal requests / Bearbeitung eines Antrags auf Neuausstellung Zertifikat (p73)

Ergänzend gilt: Geänderte Daten werden genauso geprüft, wie bei neuen Zertifikatsanträgen.

4.8.4 Notification of new certificate issuance to subscriber / Benachrichtigung über die Zertifikatsänderung

Notification of certificate modification is subject to the same procedures and restrictions as in 4.3.2 Benachrichtigung des Signators über die Ausstellung des Zertifikats / Notification to subscriber by the CA of issuance of certificate (p38).

Die Benachrichtigung der Zertifikatsänderung unterliegt denselben Verfahren und Beschränkungen wie ⇨ 4.3.2 Benachrichtigung des Signators über die Ausstellung des Zertifikats / Notification to subscriber by the CA of issuance of certificate (p38).

4.8.5 Conduct constituting acceptance of modified certificate / Verfahren zur Zertifikatsannahme nach Zertifikatsänderung

The procedure for accepting certificates after modification is subject to the same procedures and restrictions as in ⇨ 4.4.1 Conduct constituting certificate acceptance / Verfahren zur Zertifikatsannahme (p65).

Das Verfahren zur Zertifikatsannahme nach Zertifikatsänderung unterliegt denselben Verfahren und Beschränkungen wie ⇨ 4.4.1 Conduct constituting certificate acceptance / Verfahren zur Zertifikatsannahme (p65).

4.8.6 Publication of the modified certificate by the CA / Veröffentlichung der Zertifikatsänderung

Publication of the certificate modification is subjected to the same

Die Veröffentlichung der Zertifikatsänderung unterliegt denselben

procedures and restrictions as in ⇨ 4.4.2 Publication of the certificate by the CA / Veröffentlichung der Zertifikate (p65).

Verfahren und Beschränkungen wie ⇨ 4.4.2 Publication of the certificate by the CA / Veröffentlichung der Zertifikate (p65).

4.8.7 Notification of certificate issuance by the CA to other entities / Benachrichtigung über die Zertifikatsänderung

Notification of certificate modification is subject to the same procedures and restrictions as in ⇨ 4.4.3Notification of certificate issuance by the CA to other entities / Benachrichtigung von Dritten über die Zertifikatsaustellung (p65).

Die Benachrichtigung der Zertifikatsänderung unterliegt denselben Verfahren und Beschränkungen wie ⇨ 4.4.3 Notification of certificate issuance by the CA to other entities / Benachrichtigung von Dritten über die Zertifikatsaustellung (p65).

4.9 Certificate revocation and suspension / Zertifikatswiderruf und -sperre

A two-tier revocation concept is used to ensure the most practical usage of the certificate possible:

- suspension of the validity of the certificate
- declaration of invalidity of the certificate (revocation)

Applications for suspension and revocation are made through the published channels and the subscriber must make sure that the application has been received.

The CA makes the follow options available:

(a) Suspension
The validity of a certificate is temporarily suspended. This can be prompted manually or automatically and is at maximum valid for the legally and technically permitted duration.

(b) Revocation
This leads to the certificate being declared invalid early.

A revocation leads to the early termination of the validity of a certification. Reactivation is not possible. The revocation is performed under the control of at least two people as per the role concept as defined in ⇨ GLOBALTRUST® Certificate Security Policy.

Certificate suspensions can be recorded in a suspension list. The

Um eine möglichst praxisnahe Nutzung der Zertifikate zu gewährleisten, wird ein zweistufiges Widerrufskonzept angewandt:

- Aussetzung der Gültigkeit eines Zertifikates (Sperre)
- ungültig Erklären eines Zertifikates (Widerruf)

Sperr- und Widerrufsantrag haben auf den bekannt gegebenen Kanälen zu erfolgen und der Signator hat sich zu vergewissern, dass der Antrag auch tatsächlich eingelangt ist.

Der VDA stellt folgende Möglichkeiten zur Verfügung:

(a) Suspension/Sperre
Die Gültigkeit eines Zertifikates wird vorläufig aussetzt, kann manuell oder automatisiert ausgelöst werden und ist maximal für die rechtlich und technisch zulässige Dauer gültig ist

(b) Revocation/Widerruf
Führt zum vorzeitigen ungültig Erklären eines Zertifikates.

Ein Widerruf führt zur vorzeitigen Beendigung der Gültigkeit eines Zertifikats, eine Re-Aktivierung ist ausgeschlossen. Der Widerruf erfolgt unter Kontrolle von zumindest zwei Personen gemäß dem in ⇨ GLOBALTRUST® Certificate Security Policy definierten Rollenkonzept.

Zertifikatssperren können in einer eigenen Sperrliste eingetragen

suspension indicates that the certificate may have been compromised. A suspension can be lifted. A subscriber is informed that a certificate suspension has been received and is requested to confirm or lift the suspension.

Electronic signatures that have been issued before suspension or revocation retain their validity.

The information that a certificate has been suspended or revoked is publicly available.

Server certificates cannot be suspended.

The third party may report suspected problems or abuse of the certificates. The CA follows up on this report and revokes or suspends the corresponding certificates if needed.

If an event that could make a revocation necessary has not been conclusively verified, an application for suspension of the certificate should be made.

If a certificate is to be revoked, a revocation protocol is generated (⇨ Appendix / Anhang A: 2 Content Certification-Protocols / Inhalt Ausstellungs-, Sperr-, Entsperr- und Widerrufs-Protokoll für Zertifikate) The revocation protocol can be submitted to regulatory authorities, accreditation organisations or other authorised authorities if necessary. Furthermore, all procedures relevant to revocation of subscriber certificates, certificates and keys used by the CA for signature purposes, cross certificates and the certificates for identification and infrastructure keys will be recorded.

Subscribers are informed of the suspension or revocation of their certificate by appropriate means. Appropriate means include, in particular, information sent to a verified email address that the subscriber has given and that has not been documented as invalid, information given by telephone using a telephone number given by the subscriber or by fax, if a

werden. Die Sperre informiert über eine mögliche Kompromittierung eines Zertifikates. Eine Sperre kann aufgehoben werden. Der Signator wird über das Einlangen der Zertifikatssperre verständigt und um Bestätigung oder Aufhebung der Sperre ersucht.

Elektronische Unterschriften, die vor Widerruf oder Sperre ausgestellt wurden, behalten ihre Gültigkeit.

Die Tatsache der Sperre oder des Widerrufs eines Zertifkates ist öffentlich verfügbar.

Bei Server-Zertifikaten ist eine Sperre nicht möglich.

Es existiert außerdem die Möglichkeit für Dritte, vermutete Probleme oder den Missbrauch von Zertifikaten zu melden. Der VDA wird diesen Hinweisen nachgehen und bei Bedarf die entsprechenden Zertifkate widerrufen oder sperren.

Wenn ein Ereignis, das einen Widerruf erforderlich machen kann, noch nicht abschliessend geprüft ist, hat ein Antrag auf Sperre des Zertifikates zu erfolgen.

Bei Widerruf eines Zertifikates wird ein Widerrufsprotokoll erstellt (⇨ Appendix / Anhang A: 2 Content Certification-Protocols / Inhalt Ausstellungs-, Sperr-, Entsperr- und Widerrufs-Protokoll für Zertifikate (p209). Das Widerrufsprotokoll kann Aufsichtstellen, Akkreditierungseinrichtungen oder sonstigen befugten Prüfstellen bei Bedarf vorgelegt werden. Weiters werden alle widerrufsrelevanten Schritte der Signator-Zertifikate, der zur Signatur vom VDA verwendeten Zertifikate und Schlüssel, der Cross-Zertifikate und der Zertifikate der Identifikations- und Infrastrukturschlüssel protokolliert.

Signatoren werden über Sperre oder Widerruf ihres Zertifikates in geeigneter Form verständigt. Geeignet ist insbesondere die Information an eine geprüfte E-Mail-Adresse, die der Signator selbst bekannt gegeben hat und die nicht als ungültig dokumentiert ist, eine telefonische Information an eine vom Signator bekannt gegebene

fax number has been provided by the subscriber. In all other cases, the subscriber is informed by post.

Telefonnummer oder eine Verständigung per Fax, sofern die Faxnummer vom Signator bekannt gegeben wurde. In allen anderen Fällen erfolgt eine Verständigung auf dem Postweg.

4.9.1 Circumstances for revocation / Umstände für Zertifikatswiderruf

A certificate is revoked if the further use of the key in the sense of this policy is no longer ensured.

Reasons for revocation include:

1. The subscriber or applicant makes a written application.
2. A communication from the applicant that the original certificate application was not sufficiently authorised and that he has not subsequently granted this authorisation.
3. The operator receives proof that the private key used has been compromised or no longer complies with current technical requirements.
4. The operator receives proof that the certificate has been misused.
5. The operator becomes aware that the subscriber has violated the terms of use, the Certificate Policy, the Certificate Policy Statement or another contractual agreement.
6. The operator becomes aware that the subscriber is no longer legally authorised to use a designation in the certificate, in particular an email address, domain name or an IP address.
7. The operator becomes aware that a wild card certificate has been used to authenticate a subdomain with fraudulent intent or intent to deceive.
8. The operator becomes aware of a significant change to the information recorded in the certificate.
9. The operator establishes that the information recorded in the certificate is inaccurate or misleading.

Ein Zertifikat ist zu widerrufen, wenn die weitere Verwendung des Schlüssels im Sinne dieser Policy ist nicht mehr gewährleistet ist.

Widerrufsgründe sind jedenfalls:

1. Der Signator oder der Antragsteller stellt einen schriftlichen Antrag.
2. Eine Verständigung vom Antragsteller, dass der ursprüngliche Zertifikatsantrag nicht hinreichend autorisiert war und er diese Autorisierung nicht nachträglich erteilt.
3. Der Betreiber erhält einen Beweis, dass der verwendete private Schlüssel kompromittiert wurde oder nicht mehr den aktuellen technischen Anforderungen entspricht.
4. Der Betreiber erhält einen Beweis, dass das Zertifikat missbräuchlich verwendet wurde
5. Der Betreiber erhält Kenntnis davon, dass der Signator die Nutzungsbedingungen, die Certifcate Policy, das Certificate Practice Statement oder eine sonstige vertragliche Vereinbarung verletzt hat.
6. Der Betreiber erhält Kenntnis darüber, dass der Signator nicht länger rechtlich befugt ist, eine im Zertifikat eingetragene Bezeichnung, insbesondere eine eMail-Adresse, einen Domainnamen oder eine IP-Adresse, zu verwenden.
7. Der Betreiber erhält Kenntnis davon, dass ein Wildcardzertifikat dazu verwendete wurde um eine Subdomain in betrügerisch täuschender Absicht zu authentifizieren.
8. Der Betreiber erhält Kenntnis von einer signifikanten Änderung bezüglich der im Zertifkat eingetragenen Informationen.
9. Der Betreiber stellt fest, dass eine im Zertifikat eingetragene Information ungenau oder täuschend ist.

10. The CA discontinues its operations and has not concluded an agreement with another operator to continue operations.
11. The operator loses the right to issue the respective type of certificate, unless it has concluded an agreement to continue the revocation status service.
12. The operator receives proof that the private key of a CA certificate has been compromised.
13. Circumstances arise that make the technical content or format of the certificate an unacceptable security risk.

14. The operator has evidence of use of the certificate by the subscriber that is contrary to the contract. In particular, this includes breaches of this policy, the GLOBALTRUST® Certificate Practice Statement, the agreed GTCs or other individual agreements (inc. service and payment obligations).

15 The operator obtains evidence that a validation that had been performed in order to issue a certificate can not be relied upon.

16 The operator becomes aware that a certificate has been issued in violation of this policy, the GLOBALTRUST® Certificate Practice Statement or any of the then current requirements listet in (⇨ 8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS / Prüfung der Konformität und andere Beurteilungen, p168

The subscriber accepts that the operator can revoke a certificate in the event of the violation of the conditions of this policy, other agreements concluded with the subscriber or the use of the certificate for criminal or fraudulent activities at any time. Compensation for certificates revoked on these grounds or resulting damages will not be paid.

Certificates for keys that have been issued according to procedures that are

10. Der VDA stellt seinen Betrieb ein, und hat mit keinem anderen Betreiber eine Vereinbarung zu einer Fortführung geschlossen.
11. Der Betreiber verliert das Recht, den jeweiligen Zertifikatstyp auszustellen, außer er er hat eine Vereinbarung geschlossen, den Widerrufsstatusdienst fortzuführen.
12. Der Betreiber erhält einen Beweis, dass der verwendete private Schlüssel des CA-Zertifikates kompromittiert wurde.
13. Es werden Gründe bekannt, die den technischen Inhalt oder das Format des Zertifikates zu einem inakzeptablen Sicherheitsrisiko machen.
14. Der Betreiber hat qualifizierte Hinweise auf eine vertragswidrige Verwendung eines Zertifikats durch den Signator. Vertragswidrige Verwendung sind insbesondere Verstöße gegen diese Policy, gegen das GLOBALTRUST® Certificate Practice Statement, gegen die vereinbarten AGBs oder sonstigen individuellen Vereinbarungen (inkl. Leistungs- und Zahlungsverpflichtungen).
15. Der Betreiber erhält einen Beweis, dass auf eine bei Zertifikatsausstellung erfolgte Validierung nicht vertraut werden kann
16. Der Betreiber erhält Kenntnis davon, dass das Zertifkat nicht im Einklang mit dieser Policy, dem GLOBALTRUST® Certificate Practice Statement oder einer der in (⇨ 8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS / Prüfung der Konformität und andere Beurteilungen, p168 genannten Vorgaben in der im Ausstellungszeitpunkt gültigen Fassung.ausgestellt wurde.

Der Signator akzeptiert, dass der Betreiber ein Zertifikat im Falle der Mißachtung der Bestimmungen dieser Policy, anderer mit dem Signator geschlossenen Vereinbarungen oder im Falle der Zertifkatsverwendung für kriminelle oder betrügerische Aktivitäten jederzeit widerrufen kann. Ein Kostenersatz für aus diesen Gründen widerrufene Zertifikat oder daraus resultierten Schäden gebührt nicht.

Zertifikate zu Schlüsseln, die mit Verfahren erstellt werden, die gemäß

no longer seen as secure as defined by legal conditions, especially the Signature Act ([SVV]) or a decision of a regulatory authority or recognised standardisation regimes (in particular as per the special recommendations [ETSI TS 119 312]) or on the grounds of internal knowledge, will be revoked by the operator and all affected parties will be informed of this.

The operator has the right to revoke a certificate for organisational or technical reasons at any time. If a certificate is revoked on these grounds prior to the contractually agreed duration of validity of the certificate and the subscriber is not responsible for this, the subscriber is entitled to an equivalent certificate to be issued using secure procedures for the remaining duration of the contractually agreed term. Other reimbursement or compensation is not envisaged.

A CA-certificate or enduser-sub-certificate will be revoked within 7 days (unless shorter time limit is mandatory in this policy specified) if one of the following criteria has been fulfilled:

1. A written application by the applicant.
2. A communication from the applicant that the original certificate application was not sufficiently authorised and that he has not subsequently granted authority.
3. The operator receives credible evidence that the private key used has been compromised or no longer complies with current technical requirements.
4. The operator receives evidence that the certificate has been misused.
5. The operator becomes aware that the subscriber has violated the terms of use, the Certificate Policy, the Certificate Practice Statement, the agreement on the use of the enduser-sub-certificate, a compulsory technical standard (especially [CABROWSER-BASE]) or another

gesetzlicher Bestimmungen, insbesondere Signatur- und Vertrauensdiensteverordnung ([SVV]) oder der Entscheidung der Aufsichtsstelle oder anerkannter Standardisierungsgremien (insbesondere gemäß den speziellen Empfehlungen [ETSI TS 119 312]) oder auf Grund interner Erkenntnisse als nicht mehr sicher anzusehen sind, werden vom Betreiber widerrufen und alle betroffenen Parteien darüber in Kenntnis gesetzt.

Der Betreiber hat das Recht ein Zertifikat jederzeit aus organisatorischen oder technischen Gründen zu widerrufen. Erfolgt ein derartiger Widerruf aus Gründen die der Signator nicht zu verantworten hat und vor Ablauf der vertraglich vereinbarten Gültigkeitsdauer des Zertifikats, dann hat der Signator für die Dauer der vertraglich vereinbarten Restlaufzeit Anspruch auf Ausstellung eines gleichwertigen, mit sicheren Verfahren hergestellten Zertifikats. Sonstige Entschädigungen oder Kostenersätze sind nicht vorgesehen.

Ein CA-Zertifikat oder Endkunden-Sub-Zertifikat wird jedenfalls nach spätestens 7 Tagen widerrufen (sofern nicht auf Grund dieser Policy kürzere Widerrufsfristen zwingend erforderlich sind) wenn eines der folgenden Kriterien erfüllt ist:

1. Schriftlicher Antrag des Antragstellers.
2. Eine Verständigung vom Antragsteller, dass der ursprüngliche Zertifikatsantrag nicht hinreichend autorisiert war und er diese Autorisierung nicht nachträglich erteilt.
3. Der Betreiber erhält einen glaubhaften Hinweis, dass der verwendete private Schlüssel kompromittiert wurde oder nicht mehr den aktuellen technischen Anforderungen entspricht.
4. Der Betreiber erhält einen Beweis, dass das Zertifikat missbräuchlich verwendet wurde.
5. Der Betreiber erhält Kenntnis davon, dass der Signator die Nutzungsbedingungen, die Certifcate Policy, das Certificate Practice Statement, die Vereinbarung zur Verwendung des Endkunden-Sub-Zertifikates, einen vorgeschriebenen technischen Standard

contractual agreement.

6. The CA establishes that the information in the certificate is erroneous, incorrect or misleading.
7. The operator of the enduser-sub-certificate discontinues his activities and has not made provisions for them to be transferred elsewhere.

8. The agreement with the operator that the enduser-sub-certificate can be used to issue certificates has expired, unless an additional agreement is made that the revocation service will continue.

9. A further item in this Certificate Policy or GLOBALTRUST® Certificate Practice Statement requires the revocation.
10. Circumstances arise that make the technical content or format of the certificate an unacceptable security risk.

11 The operator becomes aware that a certificate has been issued in violation of this policy, the GLOBALTRUST® Certificate Practice Statement or any of the then-current requirements listed in (⇨ 8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS / Prüfung der Konformität und andere Beurteilungen, p168

(insbesondere [CABROWSER-BASE]) oder eine sonstige vertragliche Vereinbarung verletzt hat.
6. Der VDA stellt fest, dass eine im Zertifikat eingetragen Information fehlerhaft, ungenau oder täuschend ist.
7. Der Betreiber des Endkunden-Sub-Zertifikates stellt seine operative Tätigkeit ein, und hat keine Vorkehrungen für eine Übernahme der Tätigkeit getroffen.
8. Die Vereinbarung mit dem Betreiber dass dieser das Endkunden-Sub-Zertifikat zur Ausstellung von Zertifikaten verwenden darf ist abgelaufen, außer es besteht eine Zusatzvereinbarung, dass der Widerrufsdienst weiterhin betrieben wird.
9. Ein sonstiger Punkt dieser Certificate Policy bzw. des GLOBALTRUST® Certificate Practice Statements verlangt den Widerruf.
10. Es werden Gründe bekannt, die den technischen Inhalt oder das Format des Zertifikates zu einem inakzeptablen Sicherheitsrisiko machen.
11. Der Betreiber erhält Kenntnis davon, dass das Zertifkat nicht im Einklang mit dieser Policy, dem GLOBALTRUST® Certificate Practice Statement oder einer der in (⇨ 8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS / Prüfung der Konformität und andere Beurteilungen, p168 genannten Vorgaben.in der im Ausstellungszeitpunkt gültigen Fassung ausgestellt wurde.

4.9.2 Who can request revocation / Berechtigte für Antrag auf Widerruf

The following are authorised to revoke and suspend certificates:
- the subscriber,
- the applicant,
- in all cases in which the subscriber is acting on the behalf of another person or an organisation and the certificate has been issued for this purpose, this person or an authorised representative of the

Zum Widerruf und zur Zertifikatssperre berechtigt sind folgende Stellen:
- der Signator,
- der Antragsteller,
- für die Fälle, bei denen der Signator in Vertretung einer anderen Person oder einer Organisation handelt und das Zertifikat zu diesem Zweck ausgestellt ist, diese Person bzw. ein ausgewiesener

organisation,
- the operator, as per the conditions in ⇨ 4.9.1 Circumstances for revocation / Umstände für Zertifikatswiderruf (p46),
- other regulatory or control entities, if this is necessary because of compulsory requirements.

If an application for revocation is made by someone other than the operator, a complete verification of identity and authorisation to request revocation is compulsory.

Vertreter der Organisation,
- der Betreiber, gemäß den Bedingungen ⇨ 4.9.1 Circumstances for revocation / Umstände für Zertifikatswiderruf (p46),
- sonstige Aufsichts- und Kontrollstellen, sofern dies auf Grund zwingender Bestimmungen erforderlich ist.

Wird ein Widerruf von einer anderen Stelle als dem Betreiber beantragt, ist zwingend eine vollständige Identitätsprüfung und Prüfung der Widerrufsberechtigung erforderlich.

4.9.3 Procedure for revocation request / Stellung eines Widerrufantrages

A revocation request can be made on the telephone, by fax, by email, in written form (⇨ Contact information/ Contact: http://www.globaltrust.eu/impressum.html) or on the website (⇨ Suspension or revocation/ Suspension(Sperre) / Revocation(Widerruf): http://www.globaltrust.eu/revocation.html), stating the relevant certificate information and identifiers (product name, serial number, fingerprint, ..) that clearly identify the certificate and sufficient proof of authorisation to make the request.

The CA retains the right to request further proof of authorisation and to suspend a certificate rather than revoke it, if there is doubt as to whether the person making the request is authorised to do so.

If the authorised applicant so wishes, the certificate can be revoked immediately.

Ein Widerrufsantrag kann formlos telefonisch, per Fax, per E-Mail, schriftlich (⇨ Contact: http://www.globaltrust.eu/impressum.html) oder über die Website (⇨ Suspension(Sperre) / Revocation(Widerruf): http://www.globaltrust.eu/revocation.html) unter Angabe geeigneter Zertifikatsangaben und Kennzeichen (Produktbezeichnung, Seriennummer, Fingerprint, ...), die das Zertifikat eindeutig identifizieren und eines ausreichenden Nachweises der Berechtigung eingebracht werden.

Der VDA behält sich vor bei Zweifel der Berechtigung weitere Nachweise zu verlangen und stattdessen nur eine Sperre durchzuführen.

Sofern der berechtigte Antragsteller es wünscht, kann sofort der Widerruf durchgeführt werden.

4.9.4 Revocation request grace period / Informationsfrist für Antragstellung auf Widerruf

If a natural or legal person as per ⇨ 4.9.2 Who can request revocation / Berechtigte für Antrag auf Widerruf (p83) has information that could lead to revocation as per ⇨ 4.9.1 Circumstances for revocation / Umstände für Zertifikatswiderruf (p80), this should be provided to the operator. For

Liegen einer natürlichen oder juristischen Person laut ⇨ 4.9.2 Who can request revocation / Berechtigte für Antrag auf Widerruf (p83) Informationen vor, die einen Widerruf gemäß einem der in⇨ 4.9.1 Circumstances for revocation / Umstände für Zertifikatswiderruf

qualified certificates this should be done immediately. For all other kinds of certificates operated in accordance [ETSI EN 319 411-1], this should be done as soon as possible. A certificate can be suspended independently of this, at any time and without reason.

In such a case, the VDA will decide within 24 hours whether a revocation or other action should be taken, taking into account the nature of the reported circumstance, the number of reports on a particular certificate, the organization that issues the report and the relevant legislation.

(p80) angeführten Gründe zur Folge haben kann, so sind diese dem Betreiber bei qualifizierten Zertifikaten unverzüglich, bei allen anderen Zertifikatsformen so rasch als möglich zu belegen. Davon unabhängig ist die Sperre, die ohne Begründung jederzeit beantragt werden kann.

Der VDA entscheidet in einem solchen Fall binnen 24 Stunden, ob eine Widerruf oder eine sonstige Maßnahme vorzunehmen ist unter Berücksichtigung der Art des berichteten Umstandes, der Anzahl der Berichte zu einem bestimmten Zertifikat, der Organisation, die den Bericht einbringt sowie der einschlägigen Gesetzgebung

4.9.5 Time within which CA must process the revocation request / Reaktionszeit des VDAs auf einen Widerrufsantrag

Requests by telephone, fax, post and email will be received and processed within the office hours given in the GLOBALTRUST® Certificate Practice Statement and will be subject to all necessary reviews after completion.

Anträge per Telefon, Fax, Post und E-Mail werden während der Bürozeiten entgegen genommen und bearbeitet und unverzüglich nach Abschluss aller erforderlichen Prüfungen durchgeführt.

Revocation requests can be made via a web interface around the clock.

Widerrufsanträge via Webinterface werden rund um die Uhr entgegen genommen.

The maximum duration permitted between receiving the request and performing it depends on the current legal conditions, but is less than 24 hours.

Die maximal zulässige Zeitdauer zwischen Einlangen des Widerrufs bzw. der Sperre und der Durchführung richtet sich nach den aktuellen gesetzlichen Bestimmungen, ist aber jedenfalls kleiner als 24 Stunden.

For qualified certificates, the revocation is executed within three hours of the request on business days from 9am to 5pm, with the exception of Saturdays. Outside of these times, a suspension is performed within six hours.

Im Falle qualifizierter Zertifikate erfolgt die Durchführung des Widerrufs an Werktagen, ausgenommen Samstag, von 9 bis 17 Uhr spätestens innerhalb von drei Stunden ab Bekanntwerden des Widerrufsgrundes. Außerhalb dieser Zeit erfolgt die Sperre jedenfalls innerhalb von sechs Stunden.

If the applicant cannot provide sufficient information to reliably confirm his identity and authorisation to request a revocation between the time of the request and the maximum permitted response time, the revocation will be rejected and a suspension performed instead.

Kann der Antragsteller in der Zeit zwischen Antragstellung und maximal zulässiger Reaktionszeit keine ausreichenden Angaben zu seiner zuverlässigen Identifizierung und Widerrufsberechtigung machen, dann wird der Widerruf abgelehnt und eine Sperre durchgeführt.

The applicant must provide sufficient information to reliably confirm his

Der Antragsteller hat für die maximal zulässige Dauer der Sperre (⇨ **(a)**

identity and authorisation to request a revocation within the maximum permitted duration of suspension (⇨(a) Suspension, p78). If this is not possible within this time, the suspension will be lifted.

In the processing of revocation and suspension requests, individual cases may be treated with priority due to their underlying risk. If proof of prosecutable behaviour is found, the relevant authorities may be notified.

Confirmation of receipt may be delivered automatically or manually during the subsequent office hours. In the event of doubt, the subscriber should repeat his request for suspension or revocation. Confirmation of receipt is not confirmation that the request has been processed. Confirmation that the revocation has been processed can be obtained from the CA manually during the office hours subsequent to the request, is automatically available as an entry in the corresponding revocation list and takes place - if applicable - via an eMail to the subscriber Confirmation of the rejection of a revocation request requires a review by authorised personnel and takes place during the office hours following the request.

Suspension/Sperre, p78) Gelegenheit ausreichende Angaben zu seiner zuverlässigen Identifizierung und Widerrufsberechtigung vorzulegen. Ist das innerhalb dieser Zeit nicht möglich, erfolgt die Aufhebung der Sperre.

Bei der Abarbeitung von Widerrufs- und Sperranträgen können einzelne Fälle aufgrund des ihnen zugrunde liegenden Risikos prioritär behandelt werden. Im Falle eines Hinweises auf strafbare Handlungen, können die zuständigen Behörden verständigt werden.

Eine Bestätigung des Einlangens kann automatisiert unverzüglich oder manuell im Zuge der nächsten Bürozeiten erfolgen. Im Zweifel hat der Signator seinen Sperr- oder Widerrufsantrag zu wiederholen. Die Bestätigung des Einlangens ist jedoch keine Bestätigung der tatsächlichen Durchführung. Die Bestätigung der Durchführung eines Widerrufsantrags kann manuell beim VDA während der dem Antrag folgenden Bürostunden eingeholt werden, ist automatisiert als Eintrag in der entsprechenden Widerrufsliste ablesbar, und erfolgt - sofern anwendbar - per eMail an den Signator. Die Bestätigung der Ablehnung eines Widerrufsantrags bedarf immer eine Prüfung durch autorisiertes Personal und erfolgt während der dem Antrag folgenden Bürostunden.

4.9.6 Revocation checking requirement for relying parties / Verpflichtung der Nutzer zur Widerrufsprüfung

Revoked (or suspended) certificates can be confirmed using the associated suspension or revocation lists.

The user must carefully examine the validity of the certificate by looking at the suspension and revocation status and using the request channels provided by the CA (⇨ 4.5.2 Relying party public key and certificate usage / Nutzung des öffentlichen Schlüssels und des Zertifikates durch Nutzer, p70).

Widerrufene (bzw. gesperrte) Zertifikate können anhand der jeweils vorgesehenen Sperr- bzw. Widerrufsliste(n) validiert werden.

Sorgfältige Überprüfung der Gültigkeit des Zertifikates mittels des Sperr- und Widerrufsstatus unter Verwendung der vom VDA bereitgestellten Abfragemöglichkeiten ist im Rahmen der durch den Nutzer durchgeführten Prüfung (⇨ 4.5.2 Relying party public key and certificate usage / Nutzung des öffentlichen Schlüssels und des Zertifikates durch Nutzer, p70) obligatorisch.

4.9.7 CRL issuance frequency (if applicable) / Frequenz der CRL-Erstellung

Suspension and revocation lists (CRL, Certificate Revocation List) are updated according to technical standards, the law, the GLOBALTRUST® Certificate Practice Statement and the applicable certificate policy. If conditions given in these sources contradict each other, the lists will be updated according to the shortest time necessary. Updated revocation information is available at the latest within an hour.

Die Aktualisierung der Sperr- bzw. Widerrufslisten (CRL, Certificate Revocation List) erfolgt gemäß technischer Standards, rechtlicher Vorgaben, des GLOBALTRUST® Certificate Practice Statement, der anzuwendenden Certificate Policy, jedenfalls bei einer Sperre bzw. Widerruf eines Zertifikates. Im Falle widersprüchlicher Bestimmungen erfolgt die Aktualisierung gemäß der kürzesten erforderlichen Zeit . Aktualisierte Widerrufsinformationen sind jedenfalls innerhalb einer Stunde verfügbar.

Suspension or delta revocation lists (if available) are issued on a daily basis or more often, as far as technically and legally required. As a rule, the delta revocation lists are empty and serve to document the up-to-dateness of the CRL. The revocation lists for root certificates (CARL) are issued for a period of one year and renewed within this period, at least if a revocation occurs.

Die Sperrlisten oder die Delta-Widerrufslisten (sofern vorhanden) werden - sofern technisch oder rechtlich erforderlich - auf täglicher Basis oder öfter erstellt. Der Inhalt der Delta-Widerrufslisten ist im Regelfall leer und dient zur Dokumentation der Aktualität der CRL. Die Widerrufslisten zu Rootzertifikaten (CARL) werden für die Dauer eines Jahres ausgestellt und innerhalb dieses Zeitraumes erneuert, jedenfalls aber wenn es zu einem Widerruf kommt.

In the case of cross certificates, the CARL will be created for at least 31 days and renewed within this period, or at least if a revocation occurs. If the cross-certified CA is no longer active, all certificates and CRLs relating to it will be revoked immediately.

Bei Cross-Zertifkaten werden die CARL zumindest für die Dauer von 31 Tagen erstellt und innerhalb dieses Zeitraums erneuert, jedenfalls aber wenn es zu einem Widerruf kommt. Wenn die cross-zertifizierte CA nicht mehr tätig ist, werden alle Zertifikate und CRL, die sich auf die Stelle beziehen, unverzüglich widerrufen.

Suspension and revocation lists are updated immediately after a suspension or revocation of a qualified certificate has been completed. This also automatically updates the OCSP[8] answers.

Sperr- und Widerrufslisten werden im Falle einer Sperre oder eines Widerrufs von qualifizierten Zertifikaten sofort nach Abschluss von Sperre oder Widerruf aktualisiert. Dies führt auch zur sofortigen Aktualisierung der OCSP-Antworten.

Revocation and suspension lists for server-certificates (EV included) are valid for a maximum of 10 days (and updated at least every 7 days). OCSP

Bei allen Server-Zertifikaten (inklusive EV) beträgt die maximale Gültigkeitsdauer der Widerrufs- bzw. Sperrliste 10 Tage (wobei eine

[8] OCSP = Online Certificate Status Protocol

answers are valid for 10 days (the data for which is updated every 4 days).	Aktualisierung mindestens alle 7 Tage erfolgt), die von OCSP-Antworten 10 Tage (wobei die zu Grunde liegenden Daten mindestens alle 4 Tage aktualisiert werden).
Information on revoked certificates is kept until at least the expiry of the certificate.	Informationen über widerrufene Zertifikate bleiben zumindest bis zum Zeitpunkt des regulären Endes des Zertifkates bestehen.
The time used for revocation services is synchronized with public time servers at least every hour by appropriate technical procedures.	Die für Widerrufsdienste verwendete Zeit wird durch geeignete technische Verfahren zumindest jede Stunde mit öffentlichen Zeitservern synchronisiert.

4.9.8 Maximum latency for CRLs (if applicable) / Maximale Verzögerung der Veröffentlichung der CRLs

Suspension and revocation lists accessible on the internet are updated after every suspension and revocation.	Die über das Internet abrufbaren Sperr- und Widerrufslisten werden nach jeder Sperre bzw. Widerruf aktualisiert.

4.9.9 On-line revocation/status checking availability / Möglichkeit der online Widerrufsprüfung

The registry for suspension and revocation lists is publically and internationally available. It is not possible to prevent the publication of revocations and suspensions.	Die Verzeichnisdienste für Sperr- und Widerrufslisten sind öffentlich und international zugänglich. Eine Veröffentlichungssperre von widerrufenen oder gesperrten Zertifikaten ist nicht möglich.

4.9.10 On-line revocation checking requirements / Voraussetzungen für die online Widerrufsprüfung

It is ensured that the entire revocation list chain for EV certificates can be downloaded over an analogue telephone line within 3 seconds under normal circumstances. The response times for CRL and OCSP requests remain under 10 seconds under normal circumstances.	Es wird sichergestellt, dass die gesamte Widerrufslisten Kette für EV-Zertifikate bei Normalbedingungen über eine analoge Telefonleitung in höchstens 3 Sekunden heruntergeladen werden kann.Die Antwortzeiten für CRL- und OCSP-Anfragen bleiben im Normalfall unter 10 Sekunden.

4.9.11 Other forms of revocation advertisements available / Andere verfügbare Widerrufsdienste

The operator reserves the right to provide further revocation services. These are announced on the website of the operator.	Der Betreiber behält sich vor - soweit technisch möglich und rechtlich zulässig - weitere Widerrufsdienste bereit zu stellen. Diese werden über

die Website des Betreibers angekündigt.

The current status of a qualified certificate can be requested using OCSP. OCSP Stapling is not supported.

Im Falle qualifizierter Zertifikate kann der aktuelle Status eines Zertifikates jedenfalls mittels OCSP abgefragt werden. OCSP Stapling wird nicht unterstützt.

Users can request the current status of an issued certificate from the operator, regardless of the technical availability of revocation services.

Unabhängig von der technischen Verfügbarkeit von Widerrufsdiensten kann der Nutzer den aktuellen Status eines ausgestellten Zertifikates beim Betreiber erfragen.

4.9.12 Special requirements re-key compromise / Spezielle Anforderung bei Kompromittierung des privaten Schlüssels

If it is suspected that a private key has been compromised, this must be reported to the CA immediately. Revocation of compromised private keys is given priority.

Besteht der Verdacht der Komprimitierung des privaten Schlüssels ist dies unverzüglich dem VDA zu melden. Widerrufe auf Grund der Komprimitierung des privaten Schlüssels werden bevorzugt behandelt.

4.9.13 Circumstances for suspension / Umstände für Zertifikatssperre

Reasons for suspension include:

1. The subscriber or applicant makes a written request.
2. A communication from the applicant that the original certificate application was not sufficiently authorised and that he has not subsequently granted authorisation.
3. The operator receives notice that a used private key has been compromised or no longer complies with current technical requirements.
4. The operator receives notice that the certificate has been misused.
5. The operator receives notice that the subscriber has violated the terms of use, the Certificate Policy, the Certificate Practice Statement or another contractual agreement.
6. The operator receives notice that the subscriber is no longer legally authorised to use a name that has been entered into the certificate, especially a domain name or an IP address.

Gründe für eine Sperre sind jedenfalls:

1. Der Signator oder der Antragsteller stellt einen schriftlichen Antrag.
2. Eine Verständigung vom Antragsteller, dass der ursprüngliche Zertifikatsantrag nicht hinreichend autorisiert war und er diese Autorisierung nicht nachträglich erteilt.
3. Der Betreiber erhält einen Hinweis, dass der verwendete private Schlüssel kompromittiert wurde oder nicht mehr den aktuellen technischen Anforderungen entspricht.
4. Der Betreiber erhält einen Hinweis, dass das Zertifikat missbräuchlich verwendet wurde.
5. Der Betreiber erhält einen Hinweis, dass der Signator die Nutzungsbedingungen, die Certifcate Policy, das Certificate Practice Statement oder eine sonstige vertragliche Vereinbarung verletzt hat.
6. Der Betreiber erhält einen Hinweis, dass der Signator nicht länger rechtlich befugt ist, eine im Zertifikat eingetragene Bezeichnung, insbesondere ein Domainname oder eine IP-Adresse, zu

7. The operator receives notice that a wild card certificate has been used to authenticate a subdomain with fraudulent intent or intent to deceive.
8. The operator receives notice of a significant change that affects the information in the certificate.
9. The operator suspects that the information in the certificate is incorrect or misleading.
10. The operator receives notice that the used private key of a CA certificate has been compromised.
11. The operator has evidence that the subscriber has used the certificate contrary to the contract. Use contrary to the contract includes, in particular, breaches of this policy, the GLOBALTRUST® Certificate Practice Statement, the agreed GTCs or other individual agreements (inc. service and payment obligations).

verwenden.
7. Der Betreiber erhält einen Hinweis, dass ein Wildcardzertifikat dazu verwendete wurde um eine Subdomain in betrügerisch täuschender Absicht zu autentifizieren.
8. Der Betreiber erhält einen Hinweis von einer signifikanten Änderung bezüglich der im Zertifkat eingetragenen Informationen.
9. Der Betreiber hat die Vermutung, dass eine im Zertifikat eingetragen Information ungenau oder täuschend ist.
10. Der Betreiber erhält einen Hinweis, dass der verwendete private Schlüssel des CA-Zertifikates kompromittiert wurde.
11. Der Betreiber hat Hinweise auf eine vertragswidrige Verwendung eines Zertifikats durch den Signator hat. Vertragswidrige Verwendung sind insbesondere Verstöße gegen diese Policy, gegen das GLOBALTRUST® Certificate Practice Statement, gegen die vereinbarten AGBs oder sonstigen individuellen Vereinbarungen (inkl. Leistungs- und Zahlungsverpflichtungen).

4.9.14 Who can request suspension / Berechtigte für Antrag auf Sperre

The following are authorised to request suspension:
- the subscriber or applicant
- if the subscriber is acting on the behalf of another person or an organisation and the certificate has been issued for this purpose, this person or an authorised representative of the organisation,
- the operator, as per the conditions ⇨ 4.9.1 Circumstances for revocation / Umstände für Zertifikatswiderruf (p80),
- other regulatory or control authorities, if this is legally required according to compulsory requirements

Zur Zertifikatssperre berechtigt sind folgende Stellen:
- der Signator oder der Antragsteller
- für die Fälle, bei denen der Signator in Vertretung einer anderen Person oder einer Organisation handelt und das Zertifikat zu diesem Zweck ausgestellt ist, diese Person bzw. ein ausgewiesener Vertreter der Organisation,
- der Betreiber, gemäß den Bedingungen ⇨ 4.9.1 Circumstances for revocation / Umstände für Zertifikatswiderruf (p80),
- sonstige Aufsichts- und Kontrollstellen, sofern dies auf Grund zwingender Bestimmungen rechtlich erforderlich ist.

4.9.15 Procedure for suspension request / Stellung eines Antrages auf Sperre

A suspension request can be made by giving the relevant certificate information and identifiers (product identifier, serial number, fingerprint) and credible proof of authorisation.

Ein Sperrantrag kann formlos unter Angabe geeigneter Zertifikatsangaben und Kennzeichen (Produktbezeichnung, Seriennummer, Fingerprint, ...) und einer glaubhaft Machung der Berechtigung eingebracht werden.

Suspension requests made via the web interface are automatically processed, if they are sufficiently specific and the relationship between the applicant and the certificate concerned can be established (otherwise they will be treated like emails).

Sperranträge die via Webinterface einlangen werden - sofern ausreichend spezifiziert und eine eindeutige Zuordnung des Antragstellers und des betroffenen Zertifikates möglich ist - sofort automatisiert bearbeitet (ansonsten werden sie wie E-Mails behandelt).

A suspension comes into effect automatically after the suspension request has been made. Identity can also be automatically verified, for example, using login data that has been issued by the CA or data that is known or accessible only to the subscriber. If the certificate is not suspended or suspended late or otherwise erroneously, the applicant can contact the CA, who will examine the cause of the erroneous suspension.

Eine Zertifikatssperre wird nach Einlangen des Sperrantrags automatisiert wirksam. Eine Identitätsprüfung kann in diesem Fall auch automatisiert, etwa unter Verwendung von Zugangsdaten, die vom VDA vergeben wurden oder von Daten, die üblicherweise nur dem Signator bekannt und/oder zugänglich sind, erfolgen. Erfolgt die Sperre nicht, verspätet oder sonstwie fehlerhaft, dann steht dem Antragsteller eine Kontaktmöglichkeit zum VDA zur Verfügung, der die Ursache der fehlerhaften Sperre überprüft.

The procedure is otherwise identical to the ⇨ 4.9.3 Procedure for revocation request / Stellung eines Widerrufantrages (p84).

Im übrigen ist der Ablauf ident zu ⇨ 4.9.3 Procedure for revocation request / Stellung eines Widerrufantrages (p84).

4.9.16 Limits on suspension period / Dauer einer Zertifikatssperre

A suspension becomes a revocation if the suspension is confirmed, there is no response or there is no request made to lift the suspension within the legal maximum suspension period.

Eine Zertifikatssperre wird zu einem Widerruf des Zertifikates, wenn innerhalb der rechtlich maximal zulässigen Dauer einer Zertifikatssperre eine Bestätigung der Sperre erfolgt, keine Reaktion erfolgt oder keine Aufhebung der Zertifikatssperre verlangt wird.

If a suspension is lifted, a protocol will be issued with the same information as in the case of a suspension.

Wenn eine Sperre aufgehoben wird, wird ein Protokoll mit den selben Informationen wie bei einer Sperre erstellt.

4.10 Certificate status services / Zertifikatsstatusdienste

The operator provides sufficient services to establish the status of the certificate.

Apart from the standardised provision of the registry and revocation services, the status of an issued certificate can be obtained on a case-by-case basis. This can be obtained orally, by phone, by email or by other electronic means. Further standards can be provided according to legal, customer-specific or other requirements. The reliability and integrity of this disclosure is also given together with the status of the certificate. Disclosures electronically signed by the CA are binding until their expiry or revocation.

The CA can confirm the subscriber for whom a qualified certificate has been issued and the validity of the certificate within the duration legally provided for, which is at least 35 years after issuance.

All certificates issued by GLOBALTRUST® will be made available to subscribers and users using the following means:

1. On principle, all certificates are published in the registry of the CA. User details are published on the website of the CA (⇨ http://www.globaltrust.eu/directory.html).
2. The CA makes all parties concerned aware of the conditions of use of a certificate through the GLOBALTRUST® Certificate Policy together with the corresponding GLOBALTRUST® Certificate Practice Statement.
3. The registry is a ⇨ permanent service. Interruptions of more than 24

Der Betreiber stellt ausreichende Dienste zur Feststellung des Status der Zertifikate bereit.

Unabhängig von der standardisierten Bereitstellung des Verzeichnis- und Widerrufsdienstes kann im Einzelfall der Status eines ausgestellten Zertifikates individuell beauskunftet werden. Zulässige Auskunftsmöglichkeiten sind mündlich, per Telefon, per Post, per eMail oder auf einem sonstigen elektronischen Übertragungsweg. Weitere Standards können auf Grund gesetzlicher, kundenspezifischer oder sonstiger Anforderungen bereitgestellt werden. Im Zusammenhang mit der Beauskunftung des Status eines ausgestellten Zertifikates erfolgt auch eine Angabe zur Zuverlässigkeit bzw. Integrität der Auskunft. Durch den VDA elektronisch signierte Auskünfte gelten bis zu deren Ablaufdatum bzw. Widerruf als verbindlich.

Der VDA kann bei von ihm ausgestellten qualifizierten Zertifikaten für die gesetzlich vorgesehene Dauer, zumindest jedoch bis 35 Jahre nach dem Zeitpunkt der Ausstellung den Signator für den das Zertifikat ausgestellt wurde und die Gültigkeit des Zertifikates bestätigen.

Es werden alle von GLOBALTRUST® ausgestellte Zertifikate den Signatoren und Nutzern folgendermaßen verfügbar gemacht:

1. Grundsätzlich werden alle Zertifikate in den Verzeichnisdienst(en) des VDA veröffentlicht. Die Nutzungsdetails werden auf der Website (⇨ http://www.globaltrust.eu/directory.html) des VDA veröffentlicht.
2. Die Bedingungen für die Benutzung eines Zertifikats werden vom VDA allen Beteiligten in Form der GLOBALTRUST® Certificate Policy in Verbindung mit dem zutreffenden GLOBALTRUST® Certificate Practice Statement zur Kenntnis gebracht.
3. Der Verzeichnisdienst ist als ⇨ Permanenzdienst verfügbar.

hours will be logged as failures. Interruptions for qualified certificates of more than 30 minutes will be logged as failures. This documentation is available to regulatory authorities and auditors. The documents will also be made available to a third party within a relevant timeframe, if they possess a legitimate interest.

4. The registry is publicly and internationally accessible.

An omission is made from the registry if

- the subscriber wishes this or other substantial reasons exist and
- the type of certification service permits this (as constrained by the content of the announcement at the regulatory authority and the requirements of standards and laws or other binding legal requirements)

Information on the holder of a certificate that has not been automatically published in the registry will be disclosed if the person requesting the information proves that they have a legitimate interest.

It is not possible to prevent suspended or revoked certificates from being published in the registry.

Unterbrechungen von mehr als 24h werden als Störfälle dokumentiert. Im Falle qualifizierter Zertifikate werden Störfälle ab einer Unterbrechung von 30 Minuten dokumentiert. Diese Dokumentation ist für Aufsichts- und Auditstellen zugänglich, bei Vorhandensein berechtigter Interessen werden für einen relevanten Zeitraum die Unterlagen auch Dritten bereit gestellt.

4. Die Verzeichnisdienste sind öffentlich und international zugänglich.

Eine Aufnahme in den Verzeichnisdienst unterbleibt, wenn

- der Signator es wünscht oder andere gewichtige Gründe vorliegen und
- die Art des Zertifizierungsdienstes es erlaubt (wesentlich sind der Inhalt der Anzeige bei der Aufsichtsbehörde, Vorgaben durch Standards und Gesetze oder sonstige verbindliche rechtliche Vorgaben).

Auch zu den Zertifikaten die nicht im Verzeichnisdienst automatisiert veröffentlicht werden, wird Auskunft über den Inhaber erteilt, sofern der Auskunftssuchende ein berechtigtes Interesse glaubhaft macht.

Die Aufnahme in die Liste der gesperrten oder widerrufenen Zertifikate kann nicht unterbunden werden.

4.10.1 Operational characteristics / Betriebliche Voraussetzungen

Access to publicly accessible data, such as the registry, revocation lists, suspension lists, certification status services, information on the applicable certificate policy, information services etc, is controlled and uses a firewall configured to the state of the art.

Der Zugriff auf öffentlich zugängliche Daten, wie den Verzeichnisdienst, Widerrufslisten, Sperrlisten, Zertifizierungsstatusdienste, Informationen zur jeweils anzuwendenden Certificate Policy, Auskunftsdiensten usw. ist kontrolliert und erfolgt über eine nach dem Stand der Technik konfigurierte Firewall.

4.10.2 Service availability / Verfügbarkeit

Certificate status services, and in particular suspension and revocation lists, are available 24/7/365.

Die Zertifikatsstatusdienste, insbesondere Sperr und Widerrufsdienste werden auf Basis von 24/7/365 betrieben.

4.10.3 Optional features / Zusätzliche Funktionen

The operator reserves the right to specify further features in the GLOBALTRUST® Certificate Practice Statement.

Der Betreiber behält sich vor weitere Funktionen im GLOBALTRUST® Certificate Practice Statement zu spezifizieren.

4.11 End of subscription / Vertragsende

Certificates are issued with a limited validity period. The maximum duration possible is the duration of the certificate that signs the issued certificate. The maximum duration of qualified certificates is set by legal requirements.

Zertifikate werden befristet ausgestellt, die maximal mögliche Laufzeit ist die Dauer jenes Zertifikates, dass das ausgestellte Zertifikat elektronisch signiert. Bei qualifizierten Zertifikaten ist die maximale Laufzeit auf gesetzliche Vorgaben begrenzt.

Changes are permitted if they are set out in the applicable GLOBALTRUST® Certificate Practice Statement and do not contradict legal or technical requirements. If the duration of a certificate is longer than the duration of the signing certificate, it retains its validity, as long as it was issued during the validity period of the signing certificate and has not been revoked.

Abweichungen sind dann zulässig, wenn sie im jeweils anzuwendenden GLOBALTRUST® Certificate Practice Statement festgelegt werden und gesetzlichen und technischen Vorgaben nicht widersprechen. Ist die Laufzeit eines Zertifikats länger als die Laufzeit des unterschreibenden Zertifikates, dann behält es trotzdem seine Gültigkeit, sofern es innerhalb der Laufzeit des unterschreibenden Zertifikates ausgestellt und nicht widerrufen wurde.

Expired certificates are not revoked. Electronic signatures that were generated during a certificate's validity period retain their validity after the certificate has expired.

Abgelaufene Zertifikate werden nicht widerrufen, elektronische Signaturen, die innerhalb der Gültigkeitsdauer eines Zertifikates erstellt wurden, behalten auch nach Ablauf des Zertifikates ihre Gültigkeit.

The obligations for the CA, operator and subscriber that come from this GLOBALTRUST® Certificate Policy and the GLOBALTRUST® Certificate Practice Statement persist after the end of the validity period of the certificate for the applicable duration.

Die Verpflichtungen die sich aus dieser GLOBALTRUST® Certificate Policy und dem GLOBALTRUST® Certificate Practice Statement für VDA, Betreiber und Signator ergeben, bleiben nach Ende der Laufzeit des Zertifikates für die für das jeweilige Zertifikat anwendbare Dauer bestehen.

4.12 Key escrow and recovery / Schlüsselhinterlegung und -wiederherstellung

Features for recovery or archiving of keys are not provided. Keys suitable

Es werden keine Funktionen zur Wiederherstellung oder Archivierung

for qualified electronic signatures are saved only in the appropriate security hardware and provided to the subscriber. All other keys are kept as encrypted data only until delivery to the subscriber is complete.

von Schlüsseln bereitgestellt. Schlüssel, die für die qualifizierte elektronische Signatur geeignet sind werden ausschließlich in der dafür geeigneten Sicherheitshardware gespeichert und dem Signator bereit gestellt, alle anderen Schlüssel werden als verschlüsselte Datei nur solange bereit gehalten, bis die Zustellung zum Signator abgeschlossen ist.

4.12.1 Key escrow and recovery policy and practices / Policy und Anwendung von Schlüsselhinterlegung und -wiederherstellung

Key escrow features are not provided.

Es werden keine Schlüssel-Treuhandfunktionen ("key-escrow") zur Verfügung gestellt.

4.12.2 Session key encapsulation and recovery policy and practices / Policy und Anwendung für den Einschluß und die Wiederherstellung von Session keys

Session key encapsulation and recovery features are not provided.

Es werden keine Funktionen zu Einschluß und Wiederherstellung von Session keys bereit gestellt.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS / ANFORDERUNGEN STANDORT, MANAGEMENT UND BETRIEB

The CA is responsible for the organisation and documentation of all processes in the context of certification services (including time stamp services). This also applies to services outsourced to a contracted partner. The documentation formats used are a part of the GLOBALTRUST® Certificate Security Policy. The documentation method used is internally documented.

The tasks and assigned responsibilities of the contracted partner are clearly regulated. In addition, controls are established to check that activities are performed properly.

The certification service includes the technical (automated) permanent availability of the revocation list. This also applies to the automated acceptance of revocation requests.

The availability of central certification services
- distribution of CA certificates
- suspension and revocation management and
- distribution of revocation statuses

uses redundant system components and is subject to continual supervision. The availability target of the central certification services is 99.9% in a month. Availability is measured and recorded by the operational monitoring. The records are kept for at least a year and register the start and end points of failures. If the availability target has not been reached in a particular month, additional organisational and technical measures are deployed to improve availability.

Der VDA ist für die Gestaltung und Dokumentation aller Prozesse im Rahmen der Zertifizierungsdienste (inklusive Zeitstempeldienste) verantwortlich; dies gilt auch für die an Vertragspartner ausgelagerten Dienste. Die eingesetzten Dokumentationsformate sind Teil der GLOBALTRUST® Certificate Security Policy, die verwendeten Dokumentationsmittel sind intern dokumentiert.

Die Aufgaben und zugeordneten Verantwortlichkeiten der Vertragspartner sind klar geregelt, weiters sind Kontrollen zur Überprüfung der ordnungsgemäßen Tätigkeit eingerichtet.

Der Zertifizierungsdienst ist inklusive der technischen (automatisierten) Verfügbarkeit der Widerrufslisten als Permanenzdienst organisiert. Dies gilt auch für die automatisierte Entgegennahme von Widerrufsanträgen.

Die Verfügbarkeit der zentralen Zertifizierungsdienste
- Verbreitung der VDA-Zertifikate,
- Sperr- und Widerrufsmanagement und
- Verbreitung des Widerrufsstatus

erfolgt durch redundante Systemkomponenten und unterliegt einer laufenden Betriebsüberwachung. Angestrebt wird die Verfügbarkeit dieser zentralen Zertifizierungsdienste von 99,9% auf Monatsbasis. Gemessen wird die Verfügbarkeit durch Aufzeichnungen aus der Betriebsüberwachung. Diese Aufzeichnungen werden zumindest für die Dauer eines Jahres bereit gehalten und erlauben jedenfalls Beginn und Ende von Ausfällen zu erkennen. Wird die angestrebte Verfügbarkeit in einem Monat nicht erreicht, werden zusätzliche organisatorische und technische Maßnahmen gesetzt, die eine Verbesserung der Verfügbarkeit erwarten lassen.

If availability does not comply with the requirements of the regulatory authority or the law, this will be communicated according to legal requirements and agreements. Failures are documented internally and, as far as possible, measures are developed to prevent them in the future.

Entspricht die Verfügbarkeit nicht den Vorgaben der Aufsichtstellen oder der Gesetzeslage, erfolgt eine Mitteilung im Rahmen der rechtlichen Vorgaben und Vereinbarungen. Jedenfalls werden Störungen intern dokumentiert und - sofern erforderlich und technisch möglich - Maßnahmen zur künftigen Vermeidung entwickelt.

Approaches fundamental to security are documented in this policy. In addition to this, the CA deploys specific security measures as set out in the non-public GLOBALTRUST® Certificate Security Policy. These security measures are deployed in compliance with security targets and guidelines as per the GLOBALTRUST® Certificate Practice Statement.

Die für die Sicherheit grundlegenden Vorgehensweisen sind in dieser Policy dokumentiert. Zusätzlich setzt der VDA spezifische Sicherheitsmaßnahmen wie sie in der nicht öffentlichen GLOBALTRUST® Certificate Security Policy festgelegt sind. Diese Sicherheitsmaßnahmen werden entsprechend der Sicherheitsziele und -leitlinien gemäß GLOBALTRUST® Certificate Practice Statement gesetzt.

All operational procedures are documented and are subject to this GLOBALTRUST® Certificate Policy, the GLOBALTRUST® Certificate Security Policy and the applicable GLOBALTRUST® Certificate Practice Statement.

Alle betrieblichen Abläufe sind dokumentiert und unterliegen dieser GLOBALTRUST® Certificate Policy, der GLOBALTRUST® Certificate Security Policy und dem jeweils anzuwendenden GLOBALTRUST® Certificate Practice Statement.

5.1 Physical controls / Bauliche Sicherheitsmaßnahmen

The certification services are conducted only in appropriate premises. The details are as set out in the GLOBALTRUST® Certificate Security Policy.

Die Zertifizierungsdienste werden ausschließlich in geeigneten Räumlichkeiten erbracht. Die Details sind in der GLOBALTRUST® Certificate Security Policy geregelt.

5.1.1 Site location and construction / Standortlage und Bauweise

The management of the CA decides where the certification services take place, taking the requirements of the GLOBALTRUST® Certificate Security Policy into account.

Die Geschäftsführung des VDA entscheidet, an welchem Ort die Zertifizierungsdienste stattzufinden haben, dabei werden die Vorgaben der GLOBALTRUST® Certificate Security Policy beachtet.

5.1.2 Physical access / Zutritt

It is ensured that access to the premises in which functions critical to security are performed is restricted and that the risk of physical damage to facilities is minimised.

In particular, the following security measures apply:

1. Access to devices upon which certification and revocation services are performed is restricted to authorised personnel only. The systems that issue certificates are physically protected from the threat of environmental disasters.
2. Security measures are taken to prevent the loss, damage or compromising of facilities and interruption of operations.

Es ist sicher gestellt, dass der Zutritt zu Räumlichkeiten, in denen sicherheitskritische Funktionen ausgeübt werden, beschränkt ist und die Risken einer physischen Beschädigung von Anlagen minimiert sind.

Insbesondere gelten folgende Sicherheitsmaßnahmen:

1. Der Zugriff zu den Geräten, in denen Zertifizierungs- und Widerrufsdienste erbracht werden, ist auf autorisiertes Personal beschränkt. Die Systeme, welche Zertifikate ausstellen, sind vor Gefährdung durch Umweltkatastrophen baulich geschützt.
2. Es werden Maßnahmen ergriffen, um den Verlust, die Beschädigung oder die Kompromittierung von Anlagen und die Unterbrechung des Betriebes zu verhindern.

5.1.3 Power and air conditioning / Stromnetz und Klimaanlage

Power and air conditioning are available in sufficient quantity. Details are given in the GLOBALTRUST® Certificate Security Policy.

Stromversorgung und Klimanalage sind in ausreichender Kapazität verfügbar. Die Details sind in der GLOBALTRUST® Certificate Security Policy geregelt.

5.1.4 Water exposures / Gefährdungspotential durch Wasser

The location of components critical to certification is selected so that water damage is unlikely. Details are provided in the GLOBALTRUST® Certificate Security Policy.

Die Auswahl des Standortes der zertifizierungskritischen Komponenten erfolgt unter Bedachtnahme der Unwahrscheinlichkeit einer Gefährdung durch Wasser. Die Details sind in der GLOBALTRUST® Certificate Security Policy geregelt.

5.1.5 Fire prevention and protection / Brandschutz

Sufficient precautions are made to protect against fire. Details are given in the GLOBALTRUST® Certificate Security Policy.

Es sind ausreichende Vorkehrungen zum Brandschutz getroffen. Die Details sind in der GLOBALTRUST® Certificate Security Policy geregelt.

5.1.6 Media storage / Aufbewahrung von Speichermedien

Media is stored securely away from components critical to certification. Necessary measures are detailed in the GLOBALTRUST® Certificate Security Policy.

Speichermedien werden entfernt vom Betriebsstandort der zertifizierungskritischen Komponenten aufbewahrt und gesichert. Die erforderlichen Maßnahmen sind in der GLOBALTRUST® Certificate Security Policy geregelt.

5.1.7 Waste disposal / Abfallentsorgung

Waste is disposed according to local legal requirements.

Technische Systems and Documents that - for whatever reason - are to be taken out of service are disposed of securely. This includes the separation of parts containing confidential data (e.g., disks such as hard disks, ...) and other hardware components. Those parts which contain confidential data are so far destroyed under the supervision of an employee of the operator that a data reconstruction is impossible. All components are disposed of in accordance with existing waste management regulations.

Die Abfallentsorgung erfolgt gemäß den örtlichen gesetzlichen Bestimmungen.

Technische Systeme und Dokumente, die - aus welchen Gründen auch immer - außer Betrieb zu nehmen sind, werden gesichert entsorgt. Dies umfasst die Trennung von Teilen, die vertrauliche Daten enthalten (z.B. Datenträger, wie Festplatten, ...) und sonstigen Hardwarekomponenten. Jene Teile die vertrauliche Daten enthalten werden unter Aufsicht eines Mitarbeiters des Betreibers hardwaretechnisch soweit zerstört, dass eine Datenrekonstruktion unmöglich ist. Alle Komponenten werden gemäß den bestehenden Abfallwirtschaftsbestimmungen entsorgt.

5.1.8 Off-site backup / Offsite Backup

Backups are stored away from components critical to certification. Necessary measures are given in the GLOBALTRUST® Certificate Security Policy.

Backups werden entfernt vom Betriebsstandort der zertifizierungskritischen Komponenten aufbewahrt und gesichert. Die erforderlichen Maßnahmen sind in der GLOBALTRUST® Certificate Security Policy geregelt.

5.2 Procedural controls / Prozessanforderungen

Certification services (particularly application, issuance, processing and revocation of certificates) are performed under a strict separation of

Die Erbringung der Zertifizierungsdienste (insbesondere Antragstellung, Ausstellung, Ablauf und Widerruf von Zertifikaten) erfolgt unter strikter

administrative and technical operations.

Organisational measures for secure management are of central importance to the operator. Particularly in the event of failure or unforeseen events (“stress” situations), appropriate strategies and general measures should cover instances that could not fully be defined as business processes beforehand.

Main general measures include:
a) four-eyes principle for critical processes
b) motivated employees
c) clear and distinct distribution of responsibilities
d) comprehensive documentation of operational events
e) cooperative exchange of information in the context of an institutionalised certification committee

All administrative business processes relevant to certification are documented in an internal content management and monitoring system. These processes are described, administered and used in internal documentation.

All management activities involving category 1 keys, in particular the activation of the systems required for certification, key generation, backup, activation, deactivation and destruction of keys, are based on protocols, audits, defined roles and four-eyes principle, and are subject to specific internal policies documentation. Reports are signed by the responsible persons. Before starting any activity, it is checked to see if the system is in an intact, correct and untampered status.

Trennung von administrativen und technischen Tätigkeiten.

Für den Betreiber kommen organisatorische Maßnahmen zur gesicherten Betriebsführung zentrale Bedeutung zu. Besonders im Störfall oder bei unvorhergesehenen Ereignissen ("Stress"-Situation) sollen geeignete Strategien und allgemeine Maßnahmen auch jene Fälle abdecken, die nicht vorausschauend vollständig als Geschäftsprozesse definiert werden konnten.

Zu diesen zentralen allgemeinen Maßnahmen gehören:
a) 4-Augen-Prinzip bei kritischen Prozessen
b) motivierte Mitarbeiter
c) klare und eindeutige Aufgabenverteilung
d) umfassende Dokumentation des betrieblichen Geschehens
e) kollegialer Informationsaustausch im Rahmen eines institutionalisierten Zertifizierungs-Ausschusses

Alle für die Zertifizierung relevanten administrativen Geschäftsprozesse werden in einem internen Content-Management- und Monitoring-System dokumentiert. Beschreibung, Verwaltung und Nutzung dieser Prozesse erfolgt in der internen Betriebsdokumentation.

Alle Managementaktivitäten, die Schlüssel der Kategorie 1 betreffen, wie insbesondere die Aktivierung der für die Zertifizierung erforderlichen Systeme, Schlüsselerzeugung, Backup, Aktivierung, Deaktivierung und Zerstörung der Schlüssel, erfolgen auf Basis von Protokollen, Audits, festgelegten Rollen und dem Mehraugenprinzip und unterliegen besonderen internen Dokumentationen. Protokolle werden von den verantwortlichen Personen unterzeichnet. Vor Beginn jeder Aktivität wird geprüft, ob das System sich in einem unversehrten, korrekten und nicht manipulierten Zustand befindet.

5.2.1 Trusted roles / Rollenkonzept

The role concept, role description and role responsibilities are defined in

Das Rollenkonzept, die Rollenbeschreibung und die Berichtspflichten

the ⇨ GLOBALTRUST® Certificate Security Policy. Changes in the distribution of roles are to be carried out so that all the activities necessary in this practice statement and in the certificate policies can be fulfilled and a satisfactory replacement provided.

sind in der ⇨ GLOBALTRUST® Certificate Security Policy definiert. Änderungen in der Rollenverteilung sind so vorzunehmen, dass alle in diesem Practice-Statement und in den Certificate-Policies erforderlichen Tätigkeiten erfüllt werden können und ausreichende Vertretungen vorgesehen sind.

5.2.2 Number of persons required per task / Mehraugenprinzip

Critical processes are subject to the four-eyes principle. The persons involved are documented.

Kritische Prozesse unterliegen dem 4-Augenprinzip. Die beteiligten Personen werden dokumentiert.

5.2.3 Identification and authentication for each role / Identifikation und Authentifikation der Rollen

Employees authenticate themselves clearly during certification services. If an employee has been logged out, they must re-authenticate. All authentication identifiers are unique and only assigned once. The authentication identifiers of former employees are deactivated and documented.

Im Zuge der Zertifizierungsdienste authentifizieren sich die Mitarbeiter eindeutig, erfolgt zwischenzeitlich ein Log-Out, erfolgt eine Re-Authentifizierung. Alle vergebenen Authentifikationskennzeichen werden eindeutig und einmalig vergeben. Authentifikationskennzeichen ausgeschiedener Mitarbeiter werden deaktiviert, jedoch weiterhin dokumentiert.

Authorised employees identify themselves to the certification system using multi-factor-autentication, at least a hardware token (with an identification key) and a password. This fulfils the requirements described in ⇨ 6. TECHNICAL SECURITY CONTROLS / Technische Sicherheitsmaßnahmen (p120) for identification keys (⇨ **Category/Kategorie 3**, p121)

Zur Zertifizierung berechtigte Mitarbeiter weisen sich gegenüber dem Zertifizierungssystem durch mehrere Faktoren aus, mindestens einen Hardware-Token (mit Identifikationsschlüssel) und ein Passwort. Dieser erfüllt die Anforderungen wie unter ⇨ 6. TECHNICAL SECURITY CONTROLS / Technische Sicherheitsmaßnahmen (p120) für Identifikationsschlüssel (⇨ **Category/Kategorie 3**, p121) beschrieben.

5.2.4 Roles requiring separation of duties / Rollenausschlüsse

All employees are engaged only in the roles that have been defined for them and are briefed and trained in the necessary operational procedures. They receive only the access rights and tokens necessary to undertake their role.

Alle Mitarbeiter sind ausschließlich im Rahmen der für sie definierten Rollen tätig und werden in die erforderlichen betrieblichen Abläufe eingewiesen und geschult. Sie erhalten nur die für ihre Tätigkeit erforderlichen Zugangsberechtigungen und Token.

5.3 Personnel controls / Mitarbeiteranforderungen

All employees engaged in certification services have the necessary expertise, in particular employees who administer the orders of signature products, supervise technical operations and conduct development of certification products.

Alle im Zusammenhang mit Zertifizierungsdiensten tätigen Mitarbeiter, dies sind insbesondere jene Mitarbeiter, die die Bestellungen von Signaturprodukten verwalten, den technischen Betrieb betreuen und die Neu- und Weiterentwicklung der Zertifizierungsprodukte durchführen weisen die erforderliche Fachkenntnis auf.

The management of the CA can task suitable authorised persons or suitable contractors according to the role concept in this policy (⇨ GLOBALTRUST® Certificate Security Policy) for the purpose of performing certification services. These persons or contractors plan and implement all operative measures including the establishment of necessary documentation, certification guidelines and operational premises.

Die Geschäftsführung des VDA kann für die Erbringung der Dienste gemäß dieser Policy im Rahmen des Rollenkonzeptes (⇨ GLOBALTRUST® Certificate Security Policy) geeignete bevollmächtigte Personen oder geeignete Dienstleister beauftragen. Diesen obliegen die Festlegung und Umsetzung aller operativen Maßnahmen inkl. der Festlegung der erforderlichen Dokumentationen, Zertifizierungsrichtlinien und Betriebsstandorte.

In any case, the role concept describes the roles Security Officer, Registration Officer (including revocation), System Auditor and System Administrator. The functions are staffed separately. Details and actual responsibility are documented internally.

Das Rollenkonzept beschreibt jedenfalls die Rollen Security Officer, Registration Officer (inklusive Widerruf), System Auditor und Systemadministrator. Die Funktionen sind personell getrennt. Details und aktuelle Zuständigkeiten sind intern dokumentiert.

All employees working in connection with certification services only perform the tasks assigned to them in the context of the role concept and are independent, in particular free of pressure from the management.

Alle im Zusammenhang mit Zertifizierungsdiensten tätigen Mitarbeiter üben nur die ihnen im Rahmen des Rollenkonzept zugewiesenen Aufgaben aus und sind in ihrem Wirkungsbereich unabhängig, insbesondere frei von Druck durch die Geschäftsführung.

The system administrators and other persons charged with certification tasks are contractually obliged to comply with data security requirements as per the existing laws and standards.

Die Systemadministratoren und sonstige mit Zertifizierungsaufgaben betraute Personen werden zur Einhaltung der Datensicherheitsbestimmungen gemäß der bestehenden Gesetze und Standards vertraglich verpflichtet.

The employees of the CA are particularly suitable as qualified personnel to implement and secure the requirements anchored in this policy.

Die Mitarbeiter des VDAs sind als qualifiziertes Personal besonders geeignet, die in dieser Policy verankerten Bestimmungen umzusetzen und zu gewährleisten.

A certificate committee is established to govern certification services and meets on request. More detailed criteria regarding the composition and calling of meetings are defined in the role concept (⇨ GLOBALTRUST® Certificate Security Policy).

Zur Steuerung der Zertifizierungsdienste ist ein Zertifizierungs-Ausschuss eingerichtet, der nach Anforderung zusammentritt. Die näheren Kriterien bezüglich Zusammensetzung und Einberufung sind in Rollenkonzept (⇨ GLOBALTRUST® Certificate Security Policy) definiert.

The employees of the TSP receive only the necessary user and administrator rights for their work. The rights granted are reviewed at least quarterly and adjusted if necessary. Rights not needed are deactivated promptly.

Die Mitarbeiter des VDA erhalten ausschließlich die für ihre Tätigkeit erforderlichen Benutzer- und Administratorrechte. Die vergebenen Rechte werden zumindest quartalsweise überprüft und bei Bedarf angepasst. Werden Rechte nicht mehr benötigt, werden sie unverzüglich deaktiviert.

All employees involved in certification services are independent of other companies and organizations.

Alle im Zusammenhang mit Zertifizierungsdiensten tätigen Mitarbeiter sind von anderen Unternehmen und sonstigen Organisationen unabhängig.

5.3.1 Qualifications, experience, and clearance requirements / Anforderungen an Qualifikation, Erfahrung und Zuverlässigkeit

The requirements are described in the role concept (⇨ GLOBALTRUST® Certificate Security Policy).

- Functions and responsibilities relevant to security are documented in internal job descriptions and in the internal role plan. Functions that are essential for the security of certification services are clearly defined.
- Job descriptions stating responsibilities, access rights and competences are developed for all employees of the CA.
- All management functions are occupied by persons who have experience in the technology of electronic signatures and encryption.
- The CA does not employee persons who have committed prosecutable acts that indicate that they would be unsuitable for a position of trust.
- The identity and trustworthiness of all people involved in the operation

Die Anforderungen werden im Rahmen des Rollenkonzepts (⇨ GLOBALTRUST® Certificate Security Policy) beschrieben.

- Sicherheitsrelevante Funktionen und Verantwortlichkeiten werden in den internen Stellenbeschreibungen und im internen Rollenplan dokumentiert. Jene Funktionen, von denen die Sicherheit der Zertifizierungsdienste abhängt, sind eindeutig identifiziert.
- Für die Mitarbeiter des VDAs sind klare Stellenbeschreibungen ausgearbeitet, in denen die Pflichten, Zugriffsrechte und Kompetenzen dargelegt sind.
- Alle Leitungsfunktionen sind mit Personen besetzt, die über Erfahrung mit der Technologie elektronischer Signaturen und Verschlüsselungen verfügen.
- Der VDA beschäftigt keine Personen, die strafbare Handlungen begangen haben, welche sie für eine vertrauenswürdige Position ungeeignet erscheinen lassen.
- Alle in den Betrieb des Zertifizierungsdienstes involvierte Menschen

of certification services is checked before they are employed.

- The identity of employees, others contracted by the operator and persons involved in the issuance of certificates is checked.
- Employees, others contracted by the operator, and persons involved in the issuance of certificates undergo a background check, in which previous employees, references and the highest level of or most relevant education is checked.
- In the role plan, roles designated as essential or key roles are always occupied.
- Care is taken to ensure that there are no conflicts of interest or incompatibilities in functions and responsibilities relevant to security.

durchlaufen vor ihrem Engagement eine Identitätsprüfung sowie eine Prüfung ihrer Vertrauenswürdigkeit.

- Angestellte und andere vom Betreiber beauftragte und in die Ausstellung von Zertifikaten involvierte Personen durchlaufen eine Identitätsprüfung.
- Angestellte und andere vom Betreiber beauftragte und in die Ausstellung von Zertifikaten involvierte Personen durchlaufen eine Hintergrundcheck, in dem vorige Arbeitgeber, Referenzen und die höchste oder relevanteste Ausbildung geprüft werden.
- Im Rollenplan als notwendig oder als Schlüsselrolle ausgezeichnete Rollen sind stets besetzt.
- Bei sicherheitsrelevante Funktionen und Verantwortlichkeiten wird darauf geachtet, dass keine Interessenskonflikte bzw. Unvereinbarkeiten entstehen.

5.3.2 Background check procedures / Durchführung von Backgroundchecks

Employees undergo satisfactory and effective security checks depending on requirements and roles.

Die Mitarbeiter werden, abhängig von den Anforderungen und Aufgaben ausreichenden und effektiven Sicherheitsüberprüfungen unterzogen.

All employees must also provide a binding declaration of their integrity, the scope of which can be limited as per legal requirements to specific prosecutable offences. Sentences that have been erased, reversed or cleared according to relevant provisions are not considered.

Weiters haben alle Mitarbeiter eine verbindliche Erklärung bezüglich ihrer Unbescholtenheit abzugeben, wobei der Umfang der Erklärung auf Grund gesetzlicher Bestimmungen auf bestimmte strafbare Sachverhalte beschränkt werden kann. Nicht zu berücksichtigen sind Verurteilungen die nach einschlägigen Bestimmungen als getiligt, aufgehoben oder gelöscht anzusehen sind.

5.3.3 Training requirements / Schulungen

Employees are entrusted with certification tasks only after sufficient training.

Die Mitarbeiter werden mit Zertifizierungsaufgaben ausschließlich nach ausreichender Einschulung betraut.

5.3.4 Retraining frequency and requirements / Häufigkeit von Schulungen und Anforderungen

Operations personnel are continually trained in the use of monitoring tools and other tools necessary for certification services.

Das Betriebspersonal wird laufend in der Verwendung der Monitoring-Instrumente und sonstiger für die Erbringung der Zertifizierungsdienste erforderlichen Instrumente geschult.

In addition, ad hoc training is provided, in particular in the event of an incident relevant to security, a change in legal or technical requirements or the introduction of a new procedure.

Zusätzlich erfolgen anlassbezogene Schulungen, insbesondere bei Vorliegen sicherheitsrelevanter Vorfälle, bei geänderten rechtlichen oder technischen Voraussetzungen und bei Einführung neuer Verfahrensweisen.

5.3.5 Job rotation frequency and sequence / Häufigkeit und Abfolge Arbeitsplatzrotation

Job rotation is not envisaged, but new employees go through all positions necessary to complete their tasks.

Es ist keine Arbeitsplatzrotation vorgesehen, neue Mitarbeiter durchlaufen jedoch alle notwendigen Stationen, die zur Erfüllung ihrer Aufgaben erforderlich sind.

5.3.6 Sanctions for unauthorized actions / Strafmaßnahmen für unerlaubte Handlungen

Unauthorised actions by employees are penalised according to the requirements of employment law. For other contracted persons, punishment and damages are decided appropriately according to the risk ensuing from the activities of this person.

Unerlaubte Handlungen von Mitarbeitern werden gemäß den Bestimmungen des Angestelltengesetzes geahndet. Bei sonstigen vertraglich gebundenen Personen werden Straf- und Schadenersatzleistungen angemessen zum von der Tätigkeit der Person ausgehenden Risiko vereinbart.

In the case of unauthorized actions, the employee is deducted from activities related to the certification. In case of suspicion of unauthorized actions, the deduction is in any case until the clarification of the incident.

Bei unerlaubten Handlungen wird der Mitarbeiter jedenfalls von Tätigkeiten, die die Zertifizierung betreffen, abgezogen. Beim Verdacht auf unerlaubte Handlungen erfolgt der Abzug jedenfalls bis zur Klärung des Vorfalls.

5.3.7 Independent contractor requirements / Anforderungen an Dienstleister

The operator can employ a service-provider for all of its certification

Der Betreiber kann sich für alle seine Zertifizierungsdienste (vollständig

services (fully or partially). In this instance, the contractor will be subject to all the requirements applicable for the respective certification service.

oder teilweise) Dienstleister bedienen. In diesem Fall werden die für den jeweiligen Zertifizierungsdienst gültigen Anforderungen vollständig dem Dienstleister überbunden.

service-providers are chosen with care and are bound contractually to comply with the requirements applicable for their task.

Depending on the nature of the agreement, the obligations incumbent upon the service provider are written maintained, in particular compliance with the requirements set out in 8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS / Prüfung der Konformität und andere Beurteilungen, p168.

Dienstleister werden sorgfältig ausgewählt und zur Einhaltung der für ihre Tätigkeit anwendbaren Bestimmungen vertraglich verpflichtet. Abhängig von der Art der Vereinbarung werden die den Dienstleister treffenden Pflichten schriftlich festgehalten, insbesondere die Einhaltung der in (⇨ 8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS / Prüfung der Konformität und andere Beurteilungen, p168 genannten Vorgaben.

The CA retains in any case responsibility for the proper performance of certification services.

Die Verantwortung für die ordnungsgemäße Erbringung der Zertifizierungsdienste bleibt in jedem Fall beim VDA.

If the contractor is involved in the issuance of server certificates, the operator conducts an annual internal examination as to whether the contractor is complying with the requirements of [CABROWSER-BASE]. Domain validation, including validation of the domain portain of an eMail address, and the authentication for an IP address are in any case conducted by the operator itself and may not be transferred to a contractor.

Sofern ein Dienstleister in die Erstellung von Serverzertifikaten involviert ist, wird vom Betreiber jährlich durch eine interne Prüfung ermittelt, ob dieser die Bestimmungen von [CABROWSER-BASE] einhält. Die Verifizierung von Domainnamen (inkl. des Domainteils von eMailadressen) und IP-Adressen darf nicht an einen Dienstleister übertragen werden.

A contractor may never conduct an identity check for the certificate application of an organisation over which it has influence.

Ein Dienstleister darf niemals die Identitätsprüfung für einen Zertifikatsantrag einer Organisation durchführen auf die er bestimmenden Einfluss hat.

The transmission of registration data to or from contractors acting as registration authority is done exclusively encrypted through secure connections.

Die Übermittlung von Registrierungsdaten an oder durch Dienstleister, die als Registrierungsstelle tätig sind, erfolgt ausschließlich verschlüsselt über gesicherte Verbindungen.

5.3.8 Documentation supplied to personnel / Zur Verfügung gestellte Unterlagen

Employees are demonstrably made aware of the necessary documents and processes for certification services.

Die zum Betrieb der Zertifizierungsdienste erforderlichen Dokumente und Prozesse werden nachweislich den Mitarbeitern zur Kenntnis gebracht.

The management of the CA approves the necessary documentation and

Die Geschäftsführung des VDA genehmigt die notwendigen

certification guidelines and appoints those persons and external contractors responsible for the implementation of certification services as per the internal role concept (⇨ GLOBALTRUST® Certificate Security Policy). If guidelines are established or authorisation is granted to persons, this is documented in written form.

Dokumentationen und Zertifizierungsrichtlinien und ernennt jene Personen und externe Vertragspartner, die für die Umsetzung der Zertifizierungsdienste gemäß internen Rollenkonzept (⇨ GLOBALTRUST® Certificate Security Policy) verantwortlich sind. Verabschiedung von Richtlinien und Ernennung von autorisierten Personen werden schriftlich dokumentiert.

5.4 Audit logging procedures / Betriebsüberwachung

5.4.1 Types of events recorded / Zu erfassende Ereignisse

The issuing of private keys for a root certificate that has been issued since 9.7.2013 and is used for the issuance of certificates is observed by a competent and independent auditor.

Audit reports from a competent and independent auditor contain the following information:

a) The procedure for root certificate key issuance and the corresponding protection measures are documented as per the GLOBALTRUST® Certificate Policy, and where necessary, the applicable Certificate Practice Statement (CPS).

b) The procedural protocol contains sufficient details on key generation (inc. technical scripts used).

c) Item a) is observed and fully and correctly performed.

The following events are subject to special documentation:

- Exceptional situations in operation (inc. maintenance, system failures,...) are documented by the monitoring system and additional comments and explanations can be added if required. The monitoring

Die Erstellung eines privaten Schlüssels für ein Root-Zertifikat, welcher nach dem 9.7.2013 erstellt wurde und für die Ausstellung von Zertifikaten verwendet wird, wird von einer kompetenten und unabhängigen Auditstelle überwacht.

Auditreports kompetenter und unabhängiger Auditstellen enthalten folgende Angaben :

a) Der Vorgang der Root-Zertifikat Schlüsselerstellung und die zugehörigen Schutzmaßnahmen werden gemäß der GLOBALTRUST® Certificate Policy und - sofern erforderlich - dem jeweils anzuwendendem Certificate Practice Statement (CPS) dokumentiert.

b) Das Ablaufprotokoll enthält ausreichende Details zur Schlüsselgenerierung (inkl. der verwendeten technischen Skripts).

c) Die Vorgaben a) wurden eingehalten, vollständig und korrekt durchgeführt.

Folgende Ereignisse unterliegen besonderen Dokumentationen:

- Außergewöhnliche Betriebssituationen (inkl. Wartungen, Systemausfälle, ...) werden durch das Überwachungssystem dokumentiert und können bei Bedarf durch zusätzliche

data is regularly signed and archived.

- All relevant events that occur in the course of certificate issuance are logged, in particular all events that concern the life cycle of issued certificates and cross-certificates.

- All events that concern applications for new certificates, applications for the renewal of certificates and the approval of applications are documented.

Anmerkungen und Erklärungen ergänzt werden. Die Überwachungsdaten werden regelmäßig signiert und archiviert.

- Alle im Zuge der Zertifikatserstellung relevanten Ereignisse werden protokolliert. Das sind insbesondere alle Ereignisse die den Lebenszyklus von ausgestellten Zertifikaten sowie Cross-Zertifikate betreffen.
- Alle Ereignisse die den Antrag auf neue Zertifikate, den Antrag auf Verlängerung von Zertifikaten oder die Bestätigung von Anträgen betreffen, werden dokumentiert.

5.4.2 Frequency of processing log / Überwachungsfrequenz

Monitoring tools that continually show operational status are made available to operational personnel. These monitoring tools are continually adapted and optimised according to current requirements and operational experiences.

The monitoring frequency is oriented to the operational requirements of individual processes and is documented internally. This can be adapted if required.

Dem Betriebspersonal stehen Monitoring-Instrumente zur Verfügung, die laufend den Betriebsstatus anzeigen. Diese Monitoring-Instrumente werden laufend aktuellen Anforderungen und betrieblichen Erfahrungen angepasst und optimiert.

Die Überwachungsfrequenz orientiert sich an den betrieblichen Anforderungen der einzelnen Prozesse und ist intern dokumentiert. Es erfolgt bei Bedarf eine Anpassung.

5.4.3 Retention period for audit log / Aufbewahrungsfrist für Überwachungsaufzeichnungen

Records necessary for auditing are retained for as long as necessary until the audit has been completed and confirmed. This does not affect longer legal or contractual retention periods.

Die Aufbewahrungszeit für Aufzeichnungen die für Audits erforderlich sind, ist jedenfalls so lange, bis ein Audit durchgeführt und bestätigt wurde. Davon unberührt sind allenfalls längere gesetzliche oder vertragliche Aufbewahrungszeiten.

5.4.4 Protection of audit log / Schutz der Überwachungsaufzeichnungen

Failures and other operational incidents are documented as a security precaution in static data formats or in data formats without dynamic elements, in particular text formats, graphic formats, for example JPG,

Die Dokumentation der Sicherheitsvorkehrungen, von Störfällen und besonderen Betriebssituationen erfolgt in statischen Dateiformaten bzw. in Dateiformaten ohne dynamische Elemente, insbesondere in Text-

TIFF, GIF or PNG, or PDF formats without dynamic elements (in particular PDF/A format). Documentation data with special requirements is provided with a time stamp or another suitable form of electronic signature, especially if this is specified in the GLOBALTRUST® Certificate Security Policy or the applicable Certificate Policy.

Formaten, in grafischen Formaten, wie beispielsweise JPG, TIFF, GIF oder PNG oder im PDF-Format ohne dynamische Elemente (insbesondere PDF/A-Format). Dokumentationsdaten mit besonderen Archivierungserfordernissen, insbesondere wenn gesetzlich, durch die GLOBALTRUST® Certificate Security Policy oder durch die anzuwendende Certificate Policy vorgegeben, werden mit einem Zeitstempel oder einer anderen geeigneten Form der elektronischen Signatur versehen.

The precise configuration of the monitoring system is documented internally. In this monitoring system, verification measures that can be manually implemented in the event of the failure of the automated monitoring system are also documented.

Die konkrete Ausgestaltung des Überwachungssystems ist intern dokumentiert. Im Rahmen dieser Überwachungsdokumentation sind auch jene Prüfmaßnahmen dokumentiert, die bei Ausfall des automatisierten Überwachungssystems manuell gesetzt werden können.

The monitoring system is monitored as per the role concept (⇨ GLOBALTRUST® Certificate Security Policy) during regular office operations. In the event that critical services fail, on-call staff are informed by SMS. The on-call service reacts according to a defined escalation strategy as per the GLOBALTRUST® Certificate Security Policy. In particular, the section “failure scenarios” establishes that critical services for qualified services (signature, revocation, certificate, time stamp services…) have a maximum reaction time of three hours within office hours and a maximum reaction time of six hours otherwise. In any event, reaction times as required by law are observed, especially if they are shorter.

Während des regulären Bürobetriebes wird das Überwachungssystem laufend gemäß Rollenkonzept (⇨ GLOBALTRUST® Certificate Security Policy) kontrolliert. Bei Ausfall kritischer Dienste erfolgt eine automatisierte Verständigung des Bereitschaftsdienstes per SMS. Der Bereitschaftsdienst reagiert im Rahmen einer festgelegten Eskalationsstrategie gemäß GLOBALTRUST® Certificate Security Policy, insbesondere Abschnitt "Ausfallsszenarien" wobei für kritische Dienste im Rahmen qualifzierter Angebote (Signatur-, Widerrufs-, Zertifikats-, Zeitstempeldienst, ...) während der Bürozeiten eine maximale Reaktionszeit von drei Stunden, außerhalb der Bürozeiten von maximal sechs Stunden festgelegt ist, jedenfalls werden gesetzliche vorgesehene Reaktionszeiten, insbesondere wenn sie kürzer sind, eingehalten.

Security incidents are passed on to supervisory authorities, audit offices, partners, customers and other relevant bodies immediately after ascertaining the exact facts. If an issue can not be conclusively assessed, a preliminary notification to the supervisory authorities will be issued within 24 hours.

Sicherheitsvorkommnisse werden an Aufsichtsstellen, Audit-Stellen, Partner, Kunden und sonstige relevante Stellen unverzüglich nach Feststellen des genauen Sachverhalts weiter gegeben.Kann ein Sachverhalt nicht abschließend beurteilt werden, dann erfolgt gegenüber den Aufsichtstellen jedenfalls innerhalb von 24 Stunden eine vorläufige Mitteilung.

Access to certification facilities is logged and regularly checked. In addition,

Zugriffe auf Zertifizierungseinrichtungen werden protokolliert und

monitoring services are activated that report implausible or critical access attempts.

regelmäßig geprüft. Zusätzlich sind Überwachungs- und Monitoringdienste aktiviert, die unplausible bzw. kritische Zugriffsversuche elektronisch melden.

5.4.5 Audit log backup procedures / Sicherung des Archives der Überwachungsaufzeichnungen

Archives for the audit log are securely stored away from components critical to certification services. The necessary measures are given in the GLOBALTRUST® Certificate Security Policy.

Archive der Überwachungsaufzeichnungen werden entfernt vom Betriebsstandort der zertifizierungskritischen Komponenten aufbewahrt und gesichert. Die erforderlichen Maßnahmen sind in der GLOBALTRUST® Certificate Security Policy geregelt.

5.4.6 Audit collection system (internal vs. external) / Betriebsüberwachungssystem

The operator uses a system for collecting the operationally relevant data, which is activated at system startup. This system allows detection of system states and malfunctions, unauthorized or irregular access and incidents. The monitoring is continuous, redundant and includes also the start and stop of the monitoring system itself. The testing and monitoring cycles are based on the requirements of the respective services and are regulated in the GLOBALTRUST® Certificate Security Policy. In the event of certification-critical incidents, a notification is sent to the responsible persons.

Der Betreiber setzt ein System zur Sammlung der betriebsrelevanten Daten ein, welches beim Systemstart aktiviert wird Dieses System erlaubt insbesondere die Erkennung Systemzustände und Störungen, unautorisierte oder irreguläre Zugriffe und Vorfälle zu erkennen. Die Überwachung erfolgt kontinuierlich, wird redundant geführt und umfasst auch Start und Stop des Überwachungssystems selbst. Die Prüf- und Überwachungszyklen orientieren sich an den Anforderungen der jeweiligen Dienste und sind in der GLOBALTRUST® Certificate Security Policy geregelt. Bei zertifizierungskritischen Vorfällen erfolgt eine Benachrichtigung an die zuständigen Personen.

5.4.7 Notification to event-causing subject / Benachrichtigung des Auslösers

Not applicable

Nicht zutreffend

5.4.8 Vulnerability assessments / Gefährdungsanalyse

Certification services undergo an annual risk analysis. The risk analysis is

Die Zertifizierungsdienste werden einer jährlichen Risikoanalyse

carried out by identifying, naming and describing threats, by identifying weak points and by determining the likelihood of occurrence and potential damage.

unterzogen. Die Risikoanalyse erfolgt durch Ermitteln, Benennen und Beschreiben von Bedrohungen und Gefährdungen, durch Identifikation von Schwachstellen und durch Ermittlung von Eintrittswahrscheinlichkeit und potentieller Schadenshöhe.

The risk assessment is carried out by estimating the impact of an incident on the operator's business, taking into account the legal obligationsThe results and necessary measures are documented in the GLOBALTRUST® Certificate Security Policy.

Die Risikobewertung erfolgt durch Abschätzung der Auswirkungen eines Vorfalls auf die Geschäftstätigkeit des Betreibers unter Bedachtnahme der gesetzlichen Verpflichtungen. Die Ergebnisse und die erforderlichen Maßnahmen sind in der GLOBALTRUST® Certificate Security Policy dokumentiert.

An inventory of the material and intangible assets of the TSP takes place at least once a year. Certification-relevant contracts and agreements are audited once every quarter. The GLOBALTRUST® Certificate Security Policy is approved by the management

Eine Inventur der materiellen und immateriellen Güter des VDA findet mindestens einmal jährlich statt. Zertfizierungsrelevante Verträge und Vereinbarungen werden jedenfalls einmal im Quartal geprüft.Die GLOBALTRUST® Certificate Security Policy wird von der Geschäftsführung in Kraft gesetzt.

5.5 Records archival / Aufzeichnungsarchivierung

All certification-relevant information, data, measures, decisions, agreements, instructions etc, including every key pair generation that is induced by the CA, are documented in written form. “Written form” is understood to mean all record formats that permit the documentation to be safely reconstructed later, in particular written records (inc. print-outs), entries in appropriate databases intended for this purpose, electronic log records of systems used or emails.

Alle zertifizierungsrelevanten Informationen, Daten, Maßnahmen, Entscheidungen, Vereinbarungen, Anweisungen usw., einschließlich jeder vom VDA veranlasster Schlüsselgenerierung, werden beleghaft dokumentiert. Als "beleghaft" werden alle Aufzeichnungsformen verstanden, die eine zuverlässige spätere Rekonstruktion der Dokumentation erlaubt, insbesondere sind dies schriftliche Aufzeichnungen (inkl. Ausdrucke), Eintragungen in entsprechende, dafür vorgesehene Datenbanken, elektronische Protokollaufzeichnungen der eingesetzten Systeme oder E-Mails.

Depending on individual requirements, these documents can be signed electronically or by hand or their integrity can be established using other measures, such as time stamping.

Abhängig von den individuellen Anforderungen können diese Dokumente elektronisch oder handschriftlich signiert sein oder es kann die Integrität durch andere Maßnahmen, wie Zeitstempel gesichert sein.

Logs and historical versions are stored in an archive system for which access is restricted. When data is removed from storage in backup systems

Protokolle und historische Versionen werden in einem beschränkt zugänglichen Archivsystem aufbewahrt. Im Zuge der Auslagerung in

(for example, tape library), it is subject to a verification procedure.

In the backup plan, electronically administered documents and information are administered by the person responsible as per the role concept (⇨ GLOBALTRUST® Certificate Security Policy). Data secured in this way is sufficient to restore the system.

The availability of the backups is tested in a regularly manner and documented internaly.

Incident and certification service logs (⇨ Appendix / Anhang A: 2 Content Certification-Protocols / Inhalt Ausstellungs-, Sperr-, Entsperr- und Widerrufs-Protokoll für Zertifikate) that concern the operation of certification services are kept for 35 years.

Backupsysteme (z.B. Bandarchiv) werden die ausgelagerten Dateien einem Verifikationsverfahren unterzogen.

Elektronisch verwaltete Unterlagen und Informationen werden im Rahmen eines Backupplans durch eine verantwortliche Person gemäß Rollenkonzept (⇨ GLOBALTRUST® Certificate Security Policy) verwaltet. Die so gesicherten Daten sind ausreichend, um den aktuellen Systemstand wiederherzustellen.

Die Verfügbarkeit der Backups wird regelmäßig getestet und intern dokumentiert.

Die den Betrieb des Zertifizierungsdienstes betreffenden Ereignis- und Zertifizierungsdienstprotokolle (⇨ Appendix / Anhang A: 2 Content Certification-Protocols / Inhalt Ausstellungs-, Sperr-, Entsperr- und Widerrufs-Protokoll für Zertifikate, p209) werden 35 Jahre aufbewahrt.

5.5.1 Types of records archived / Zu archivierende Aufzeichnungen

Processes and procedures relevant to certification, orders and contracts, are logged and subject to a change log, where reasonable. This affects, in particular, developments in certification services and their technical documentation.

Documents and data necessary for the verification of existing, expired or revoked certificates, data necessary to check timestamps, including certificates, revocation status information and the documentation of failures and special operational incidents are archived as per the requirements of the respective certification policy, in particular information requirements concerning duration and form of filing. This can be in databases intended for this purpose, on central servers, on external data carriers or manually filed.

Archived documents are filed in a structured way and are searchable.

Zertifizierungsrelevante Vorgänge oder Abläufe, Bestellungen und Verträge, werden protokolliert und unterliegen - soweit sinnvoll - einer Änderungshistorie. Dies betrifft insbesondere Entwicklungen zu den Zertifizierungsdiensten und deren technische Dokumentationen.

Unterlagen und Daten, die zur Prüfung bestehender, abgelaufener oder widerrufener Zerifikate erforderlich sind, Daten die zur Prüfung vergebener Zeitstempel erforderlich sind, einschließlich Zertifikate, Widerrufsstatusinformationen und der Dokumentation von Störfällen und besonderen Betriebssituationen, werden gemäß den Vorgaben der jeweiligen Certification Policy, insbesondere was Dauer und Ablageform betrifft, in dafür vorgesehenen Datenbanken, auf zentralen Servern, auf externen Datenträgern oder als manuelle Ablage archiviert .

Archivierte Unterlagen werden strukturiert abgelegt und sind durchsuchbar.

5.5.2 Retention period for archive / Aufbewahrungsfristen für archivierte Daten

The retention period is 35 years from the issuance of the document/occurrence of the event, unless otherwise noted in the applicable GLOBALTRUST® Certificate Practice Statement.

Die Aufbewahrungszeit ist, sofern nicht im jeweils anzuwendenden GLOBALTRUST® Certificate Practice Statement anders vermerkt, die Dauer von 35 Jahren ab Erstellung des Dokuments/Eintreten des Ereignisses.

A legally stipulated minimum retention time applies to documents important for qualified certificates. All archived documents are marked with a time, which refers to the documented event.

Für Unterlagen, die für qualifizierte Zertifikate von Bedeutung sind, gilt jedenfalls die gesetzlich vorgesehene Mindestaufbewahrungszeit. Alle archivierten Unterlagen sind mit Zeitangaben versehen, die sich auf das dokumentierte Ereignis beziehen.

Audit and log data from operations are kept for three months online in operative systems, after them as long as they are needed for the monitoring of operations. In any case, certification-relevant files that are stored on backed-up data carriers are kept for 7 years beyond the validity of the respective certificate.

Betriebsbedingt anfallende Audit- und Logdateien werden drei Monate online in operativen Systemen bereit gehalten, darüber hinaus jedenfalls so lange aufbewahrt, wie sie zur Überwachung des Betriebs erforderlich sind. Zertifizierungsrelevante Dateien, die auf gesicherte Datenträger ausgelagert werden, werden jedenfalls 7 Jahre nach Ablauf der Gültigkeit des jeweiligen Zertifikates aufbewahrt.

5.5.3 Protection of archive / Schutz der Archive

Documents are stored according to the current state of the art. If kept, print-outs (paper print-outs, hard copies) are kept in lockable premises. Electronically archived documents are kept in common data formats (plain text, XML, PDF (inc. PDF/A, TIFF, JPG, GIF, PNG etc) which can be viewed and read in the future. If it is foreseeable that a particular format will not be readable in the future, a document will be converted in a timely fashion into a format that will be readable in the future.

Die Aufbewahrung richtet sich nach dem aktuellen Stand der Technik. Soweit Ausdrucke aufbewahrt werden (Papierausdrucke, Hardcopies) werden sie in versperrbaren Räumlichkeiten aufbewahrt. Elektronisch archivierte Dokumente werden in gängigen Datenformaten aufbewahrt (unter anderem in Plain-Text, XML, PDF (inkl. PDF/A), TIFF, JPG, GIF, PNG usw), von denen auch in Zukunft eine einfache Darstellbarkeit und Lesbarkeit erwartet werden kann. Sofern absehbar ist, dass bestimmte Formate in Zukunft nicht mehr lesbar sind, erfolgt zeitgerecht eine Konvertierung in zukunftssichere Formate.

Private information, in particular passwords and private keys for certification services, is not archived. Confidential information, in particular information necessary for operations, is archived and access to it is

Geheime Informationen, insbesondere Passwörter und private Schlüssel der Zertifizierungsdienste unterliegen keiner Archivierung, vertrauliche Informationen, insbesondere betrieblich erforderliche Informationen

restricted as per ⇨ "Confidential" level / **Stufe "vertraulich"** (p175)

unterliegen einer Archivierung, deren Zugriff gemäß der ⇨ "Confidential" level / **Stufe "vertraulich"** (p175) beschränkt ist.

5.5.4 Archive backup procedures / Sicherung des Archives

The fundamental principles of archiving are:

- **Functionality:** backups are only made with a view to specific, defined uses.
- **Integrity:** Backups are secured in the same way as archives, using appropriate measures, in particular electronic signature of archived data, restricted access (authentication procedures), reference documents/ hash procedures or a combination of these methods.
- **Confidentiality:** As a principle, keeping backups of private information (such as passwords, private keys etc) is avoided. If this is unavoidable, this information is stored in encrypted form. The algorithms used comply with the state of the art, in particular the requirements of [ETSI TS 119 312] and legal requirements.
- **Reliability:** backups are made using suitable software and hardware components that allow the data to be stored safely over the necessary time period.
- **External storage:** backups are stored externally according to their functionality in such a way as to ensure sufficient secure storage and availability. On principle, backup data is stored at a sufficient distance away from the original copies. Long-term backups are stored in premises other than those in which the server is operated. Online security and operation backups are stored on systems other than the systems that contain the original data. In any event, access is restricted and physical and technical barriers must be surmounted to access the backup data.

Die Grundprinzipen der Archivierung sind:

- **Funktionalität:** Backups werden ausschließlich in Hinblick auf bestimmte, definierte Anwendungen erstellt.
- **Integrität:** Backups werden vergleichbar den Archiven durch geeignete Maßnahmen, insbesondere durch elektronische Signatur von archivierten Dateien, durch Zugriffsrestriktionen (Authentisierungsverfahren), durch Referenzdokumentationen/Hashverfahren oder durch eine Kombination der genannten Methoden gesichert.
- **Vertraulichkeit:** Grundsätzlich wird vermieden, dass Backups geheime Informationen (wie Passwörter, private Schlüssel usw.) enthalten. Sofern dies unumgänglich ist, erfolgt deren Speicherung in verschlüsselter Form. Die verwendeten Algorithmen entsprechen dem Stand der Technik, insbesondere den Vorgaben von [ETSI TS 119 312] und gesetzlichen Bestimmungen.
- **Zuverlässigkeit:** Backups werden durch geeignete Soft- und Hardwarekomponenten erstellt, die eine zuverlässige Aufbewahrung über die erforderlichen Zeiträume erwarten lassen.
- **Auslagerung:** Backups werden entsprechend ihrer Funktionalität so ausgelagert, dass eine der Funktionalität entsprechende ausreichende sichere Aufbewahrung und Verfügbarkeit gegeben ist. Es wird dabei das Prinzip der ausreichenden Entfernung vom Originaldatenbestand verfolgt. Die Aufbewahrung der Langzeit-Backups erfolgt in anderen Räumlichkeiten, als den Räumen, in denen die Server betrieben werden, Online-Sicherheits- und Betriebsbackups auf anderen Systemen, als die Systeme, die die Originaldaten enthalten. In allen Fällen ist der Zugang beschränkt

- **Reconstructability:** random samples of backups are tested for their reconstructability and availability. This can also be requested by management. The procedure for requesting this is internally documented.

und zur Erlangung des Zugangs zu den Backupdaten ist die Überwindung physischer und/oder technischer Hindernisse erforderlich.

- **Rekonstruierbarkeit:** Backups werden stichprobenweise auf ihre Rekonstruierbarkeit und Verfügbarkeit getestet, diese kann auch durch die Geschäftsführung beauftragt werden. Die Vorgangsweise zur Beauftragung ist intern dokumentiert.

5.5.5 Requirements for time-stamping of records / Anforderungen zum Zeitstempeln von Aufzeichnungen

Depending on operational requirements, these documents can be signed electronically or by hand or their integrity can be ensured using other measures, such as timestamping.

Electronic documents are administered in appropriate systems that use integrity checks to recognise data errors and avoid data loss. A timestamp is generated for electronically archived documents soon after they are issued. This timestamp documents the time of documentation and integrity of the document. The time of the timestamp is synchronized with public time servers at least once per hour by appropriate technical measures. Data is otherwise secured as per the GLOBALTRUST® Certificate Security Policy.

Abhängig von den betrieblichen Anforderungen können diese Dokumente elektronisch oder handschriftlich signiert sein oder es kann die Integrität durch andere Maßnahmen, wie Zeitstempel gesichert sein.

Die elektronischen Dokumente werden in geeigneten Systemen verwaltet, die durch Integritätsprüfungen Datenfehler erkennen und Datenverlust vermeiden können. Zu elektronisch archivierten Dokumenten wird zeitnah zum Ereignis ein Zeitstempel generiert, der den Zeitpunkt der Archivierung und die Unversehrtheit des Dokuments dokumentiert. Die Uhrzeit der Zeitstempel wird durch geeignete technische Verfahren zumindest einmal pro Stunde mit öffentlichen Zeitservern synchronisiert . Im übrigen erfolgt die Datensicherung gemäß GLOBALTRUST® Certificate Security Policy.

5.5.6 Archive collection system (internal or external) / Archivierung (intern/extern)

The integrity of all operational data, especially orders, log files and certification data is ensured through the use of non-rewritable data carriers and by electronically signing archived data, restricting access (authentication procedures), and reference documentation/hash procedures or a combination of these methods.

Die Integrität aller betriebsrelevanten Daten, wie insbesondere Bestellungen, Logdateien und Zertifizierungsdaten, wird durch Verwendung nicht überschreibbarer Datenträger, durch elektronische Signatur von archivierten Dateien, durch Zugriffsrestriktionen (Authentisierungsverfahren), durch Referenzdokumentationen/Hashverfahren oder durch eine Kombination der genannten Methoden gesichert.

5.5.7 Procedures to obtain and verify archive information / Verfahren zur Beschaffung und Verifikation von Aufzeichnungen

The restore mechanisms are constructed so that the certification system can be restored from backup copies.

Restore measures are initiated by the person responsible as per the role concept (⇨ GLOBALTRUST® Certificate Security Policy).

If it is necessary to restore data from a backup, all data necessary for this is restored in its own area, and after the data is checked for accuracy and necessity, only the data that is actually required is transferred into the production system.

Die Restoremechanismen sind so ausgelegt, dass das Zertifizierungssystem von Sicherungsbeständen wieder hergestellt werden kann.

Restoremaßnahmen werden durch eine verantwortliche Person gemäß Rollenkonzept (⇨ GLOBALTRUST® Certificate Security Policy) veranlasst.

Ist das Restore (die Wiederherstellung) von Daten aus einem Backup erforderlich, dann werden die dazu notwendigen Daten in einem eigenen Bereich wieder hergestellt und nach Kontrolle der Richtigkeit und Erforderlichkeit der Daten nur jene Daten in das Produktionssystem übernommen, die tatsächlich notwendig sind.

5.6 Key changeover / Schlüsselwechsel des Betreibers

The changeover of keys by the operator is planned in good time and is subject to all necessary audits. Third parties affected by a planned changeover are informed in a timely fashion.

Der Wechsel eines Schlüssels beim Betreiber wird zeitgerecht geplant und unterliegt allen erforderlichen Audits. Vom Wechsel betroffene Dritte werden zeitgerecht über einen geplanten Wechsel informiert.

5.7 Compromise and disaster recovery / Kompromittierung und Geschäftsweiterführung

The compromising of a CA key is considered a worst-case scenario. A compromise is the transfer of the CA private key to third parties in a form that makes use / exploitation possible.

In this event, the CA immediately briefs and informs the regulatory authority, the subscribers, persons who rely on the certification services, and if necessary other certification service providers and organisations with whom the CA has relevant agreements, that the revocation and certificate information can no longer be seen as reliable. If necessary, the public is

Als Katastrophenszenario ("worst case") wird die Kompromittierung eines Zertifizierungsschlüssels angesehen. Als Kompromitierung gilt die Weitergabe des CA-PrivatKey an Dritte in einer Form, die eine Nutzung/Verwertung möglich machen.

Für diesen Fall wird der VDA die Aufsichtsstelle, die Signatoren, die auf die Verlässlichkeit der Zertifizierungsdienste vertrauenden Personen und ggf. andere Zertifizierungsdiensteanbieter und Einrichtungen, mit denen einschlägige Vereinbarungen bestehen, unverzüglich davon unterrichten und mitteilen, dass die Widerrufs- und Zertifikatsinformationen nicht

informed via the website http://www.globaltrust.eu/limitation.html.

Certificates and revocation lists will immediately be marked as no longer valid. The subscriber will be issued with a new certificate with the aid of a newly generated secure CA key.

mehr als zuverlässig anzusehen sind. Sofern notwendig, erfolgt eine Information der Öffentlichkeit über die Website http://www.globaltrust.eu/limitation.html.

Zertifikate und Widerrufslisten werden unverzüglich als nicht mehr gültig gekennzeichnet. Den Signatoren werden mit Hilfe eines neu generierten sicheren Zertifizierungsschlüssels neue Zertifikate ausgestellt.

5.7.1 Incident and compromise handling procedures / Handlungsablauf bei Zwischenfällen und Kompromittierungen

The operator has taken precautions in case of the failure of individual operational components. Certification services will then be in failure operation (partial functionality is available) instead of normal operation (full functionality is available). Details are described in the GLOBALTRUST® Certificate Security Policy.

The transition from normal operation ("primary") to failure operation ("disaster recovery") is mostly automatic and takes five minutes including delays. The maximum permitted outage that still allows an automated transition from normal operation to failure operation is described in the internal GLOBALTRUST® Certificate Security Policy as a worst-case scenario. Additional failures require manual intervention by authorised staff. The response time for manual intervention is a maximum of 24 hours, but a response is made within the time requirements of the regulatory authority at least.

Where alternative services or systems are used, these comply with the same security requirements as the main system.

The transition from normal operation to failure operation and other failure procedures are tested at regular intervals to an extent that is reasonable and economically acceptable.

Der Betreiber hat Vorkehrungen für den Fall des Ausfalls einzelner Betriebskomponenten getroffen. Die Zertifizierungsdienste werden dann statt im Normalbetrieb (volle Funktionalität ist vorhanden) im Ausfallsbetrieb (Teilfunktionalitäten sind vorhanden) betrieben. Die Details sind in der GLOBALTRUST® Certificate Security Policy beschrieben.

Der Übergang von Normalbetrieb ("primary") auf Ausfallsbetrieb ("disaster recovery") erfolgt weitestgehend automatisiert und mit Verzögerungen unter fünf Minuten. Die maximal zulässigen Ausfälle, die noch einen automatisierten Übergang vom Normalbetrieb in den Ausfallsbetrieb erlauben sind in der internen GLOBALTRUST® Certificate Security Policy als "Worst Case Szenario" beschrieben. Darüber hinausgehende Ausfälle erfordern manuelle Eingriffe autorisierten Personals. Die Reaktionszeit dieser manuellen Eingriffe beträgt maximal 24 Stunden, erfolgen jedoch zumindest innerhalb der zeitlichen Vorgaben der Aufsichtstelle.

Soweit alternative Dienste oder Systeme verwendet werden, entsprechen diese denselben Sicherheitsanforderungen wie die Hauptsysteme.

Die Übergänge vom Normalbetrieb zu Ausfallsbetrieb und das sonstige Ausfallsverhalten wird in regelmäßigen Abständen in einem Umfang, der sinnvoll und wirtschaftlich vertretbar ist, getestet.

5.7.2 Computing resources, software, and/or data are corrupted / Wiederherstellung nach Kompromittierung von Ressourcen

There is a risk analysis for all central components of certification operations, which is described in the GLOBALTRUST® Certificate Security Policy. In this risk analysis, the procedures for restoring normal operation after resources have been compromised are also described.

Für alle zentralen Komponenten des Zertifizierungsbetriebes existiert eine Risikoanalyse die in der GLOBALTRUST® Certificate Security Policy beschrieben ist. Im Rahmen der Risikoanalyse sind auch die Verfahren zur Wiederherstellung des Normalbetriebs nach Kompromittierung von Ressourcen beschrieben.

5.7.3 Entity private key compromise procedures / Handlungsablauf Kompromittierung des privaten Schlüssels des VDA

Internal documentation exists on the applicable steps and measures in case of compromise of a private key belonging to a CA-certificate. The certificate is revoked in any case. The status information is disseminated via a CRL which is signed by the root certificate. Further, all end-user-certificates that have been issued under the comrpomised CA-certificate are revoked. The status information is disseminated via a CRL that is signed by another, non-compromised key.

Es besteht eine interne Dokumentation der zu setzenden Schritte und Maßnahmen bei Kompromittierung eines privaten Schlüssels des VDA. Es erfolgt zumindest unverzüglich der Widerruf des betroffenen CA-Zertfikats. Die Verbreitung des Widerrufstatus erfolgt durch eine mit dem Root-Schlüssel signierte CRL. Weiters werden alle unter dem betroffenen CA-Zertifikat ausgestellen Endnutzerzertifikate widerrufen. Die Verbreitung des Widerrufsstatus erfolgt durch eine CRL, die mit einem anderen, nicht-kompromittierten Schlüssel signiert ist.

5.7.4 Business continuity capabilities after a disaster / Möglichkeiten zur Geschäftsweiterführung im Katastrophenfall

Measures for business continuity in the event of a disaster are documented in the GLOBALTRUST® Certificate Security Policy.

Die Maßnahmen zur Geschäftsweiterführung im Katastrophenfall sind in der GLOBALTRUST® Certificate Security Policy dokumentiert.

5.8 CA or RA termination / Einstellung der Tätigkeit

The CA immediately announces the termination to the regulatory authority and other participants, if planned, and ensures that any resulting impairment of its services for subscribers as well as parties who rely upon the services is kept to a minimum. The detailed procedure (including takeover costs) is documented internaly and approved by the management.

Der VDA zeigt die Einstellung der Tätigkeit - sofern vorgesehen - unverzüglich der Aufsichtsstelle und weiteren Beteiligten an und stellt sicher, dass eine eventuelle Beeinträchtigung ihrer Dienstleistungen sowohl gegenüber Signatoren als auch gegenüber allen auf die Zuverlässigkeit der Dienste vertrauenden Parteien möglichst gering

Apart from this, all subscribers and any third parties with whom the CA has relevant agreements are informed. The authorization of service providers to perform certification-related tasks on behalf of the CA is revoked. All private keys available at the CA are destroyed or removed from circulation in a way, that they cannot be retrived.

Further efforts are made so that a minimal amount of services can be undertaken by a third party, in particular the distribution of revocation statuses and the further archiving of legally required documents.

If possible, arragements with supervisory bodies or other appropriate entities are made to continue the certification services.

The CA has an agreement to cover cost in case of transfer or termination of the certification services.

gehalten wird. Der detaillierte Ablauf (inklusive Kostenübernahme) ist intern dokumentiert und von der Geschäftsführung genehmigt.

Über die Einstellung werden außerdem alle Signatoren sowie etwaige Dritte, mit denen der VDA relevante Vereinbarungen geschlossen hat, informiert. Die Bevollmächtigung von Dienstleistern, im Namen des VDA zertifizierungsrelevante Aufgaben auszuführen, wird widerrufen. Alle beim VDA vorhandenen privaten Schlüssel werden zerstört oder so aus dem Verkehr gezogen, dass eine Rekonstruktion nicht stattfinden kann .

Weiters werden Anstrengungen unternommen, damit eine minimale Abwicklung der angebotetenen Dienste, insbesondere die Verbreitung des Widerrufsstaus, und die weitere Archivierung von gesetzlich notwendigen Unterlagen von einem Dritten vorgenommen werden kann.

Sofern möglich, werden Vereinbarungen mit Aufsichtsbehörden oder sonstigen geeigneten Einrichtungen zur Weiterführung der Zertifizierungsdienste getroffen.

Der VDA verfügt über eine Vereinbarung zur Kostenübernahme im Zusammenhang mit der Übertragung oder Einstellung der Zertifizierungsdienste.

6. TECHNICAL SECURITY CONTROLS / TECHNISCHE SICHERHEITSMAßNAHMEN

The operational infrastructure of the operator is checked and adjusted to changed requirements regularly. Changes that affect the extent to which security is achieved must be approved by the certification committee as per the role concept (⇨ GLOBALTRUST® Certificate Security Policy). In the event of a change of the GLOBALTRUST® Certificate Security Policy, the responsible regulatory authorities are informed.

Technical operations are conducted in the offices of the operator or a sufficiently qualified contractor. Current contractors are fully documented and can be disclosed to the regulatory authority at any time. All contractors are bound to protect data security in accordance with this policy, [DSG 2000], signature requirements and other relevant legal requirements and technical standards, as it concerns the activity assigned to them.

The operator uses signature and cryptographic keys to perform certification services and internal (administrative) business processes where technically possible, technically necessary for security and economically acceptable.

These keys are administered and made available in the following categories:

Category 1: Signature keys for certification services. This includes certification services that concern qualified, as well as non-qualified certificates.

Category 2: Infrastructure keys for protecting individual processes, devices or objects of certification services. In particular, these are keys for the secure transmission of data between the certification data centre and the

Die Betriebsinfrastruktur des Betreibers wird regelmäßig überprüft und an geänderte Anforderungen angepasst. Änderungen, die einen Einfluss auf das Ausmaß der erreichten Sicherheit haben, sind vom Zertifizierungsauschuss gemäß Rollenkonzept (⇨ GLOBALTRUST® Certificate Security Policy) zu genehmigen. Im Falle einer Änderung der GLOBALTRUST® Certificate Security Policy erfolgt eine Mitteilung an die zuständigen Aufsichtsstellen.

Der technische Betrieb erfolgt beim Betreiber oder in den Räumen ausreichend qualifizierter Vertragspartner. Die aktuellen Vertragspartner sind vollständig dokumentiert und können der Aufsichtsbehörde jederzeit bekannt gegeben werden. Alle Vertragspartner sind an die Wahrung der Datensicherheit im Sinne dieser Policy, des [DSG 2000], der Signaturbestimmungen und sonstiger zutreffender rechtlicher Bestimmungen und technischen Standards vertraglich insoweit gebunden, als es die ihnen übertragene Tägigkeit betrifft.

Der Betreiber verwendet zur Erbringung seiner Zertifizierungsdienste und zur Abwicklung der internen (administrativen) Geschäftsprozesse soweit technisch möglich, sicherheitstechnisch erforderlich und wirtschaftlich sinnvoll Signatur- und Kryptographieschlüssel.

Diese Schlüssel werden in folgenden Kategorien verwaltet und bereit gestellt:

Category/Kategorie 1: Signaturschlüssel zur Erbringung von Zertifizierungsdiensten. Umfasst sind Zertifizierungsdienste, die qualifizierte, also auch nicht-qualifizierte Zertifikate betreffen.

Category/Kategorie 2: Infrastrukturschlüssel, zur Absicherung einzelner Prozesse, Geräte oder Objekte der Zertifizierungsdienste. Insbesondere sind dies Schlüssel zur gesicherten Datenübertragung zwischen

office of the CA or mobile access devices, or for the signature (inc. timestamping) of log data, programmes or other data relevant to certification.

Category 3: Identification keys for protecting communication between technical systems and employees and for authenticating employees.

Category 4: Session keys, exclusively temporarily generated keys for protecting communication between technical systems.

The keys from categories 1 to 3 are issued according to the state of the art in consideration of national and international requirements, for example [ETSI TS 119 312]. Keys in category 1 comply with the legal requirements for certification services.

Category 1 keys (including neccesary random numbers) are generated on systems meeting the requirements of FIPS 140-2 level 3 or higher [FIPS-140-2], CMCSOB PP [CWA 14167-2], CMCKG PP [CWA 14167-3], CMCSO PP [CWA 14167-4], EAL 4 or higher in accordance with ISO / IEC 15408 [CC-ITSE], or is a system that, according to a risk analysis according to [ETSI EN 319 411-2], meets the safety objectives or safety profiles through physical and / or other non-physical measures.

Access to signature creation data is restricted as per the GLOBALTRUST® Certificate Security Policy. Access to signature creation data that is intended for certification services or serves as infrastructure or identification keys are subject to access controls.

Zertifizierungsrechenzentrum und Büro des VDAs oder mobiler Zugangsgeräte, oder zur Signatur (inkl. Zeitstempel) von Log-Dateien, Programmen oder anderer für die Zertifizierung relevanter Dateien.

Category/Kategorie 3: Identifikationsschlüssel, zur Absicherung der Kommunikation zwischen technischen Systemen und Mitarbeitern und der Authentifizierung der Mitarbeiter.

Category/Kategorie 4: Session Keys, ausschließlich temporär generierte Schlüssel zur Absicherung der Kommunikation zwischen technischen Systemen.

Die Schlüssel der Kategorien 1 bis 3 werden nach dem Stand der Technik erstellt, wobei nationale und internationale Anforderungen, etwa von [ETSI TS 119 312] beachtet werden. Schlüssel der Kategorie 1 entsprechen jedenfalls den gesetzlichen Anforderungen zur Erbringung der Signaturdienste.

Die Erzeugung von Schlüsseln der Kategorie 1 inklusive erforderlicher Zufallswerte erfolgen auf Systemen, die den Anforderungen von FIPS 140-2 level 3 oder höher [FIPS-140-2], CMCSOB PP [CWA 14167-2], CMCKG PP [CWA 14167-3], CMCSO PP [CWA 14167-4], EAL 4 oder höher in Übereinstimmung mit ISO/IEC 15408 [CC-ITSE] verfügen oder sind ein System, dass gemäß einer Risikoanalyse nach [ETSI EN 319 411-2] die Sicherheitsziele bzw. Sicherheitsprofile durch physikalische und/oder anderen nicht-physikalischen Maßnahmen erfüllt.

Der Zugriff auf Signaturerstellungsdaten wird gemäß GLOBALTRUST® Certificate Security Policy beschränkt. Der Zugriff auf Signaturerstellungseinheiten, die für Zertifizierungsdienste vorgesehen sind oder für Infrastruktur- oder Identifikationsschlüssel dienen unterliegt einer Zugangskontrolle.

6.1 Key pair generation and installation / Erzeugung und Installation von Schlüsselpaaren

The operator makes available signature creation devices as per legal

Der Betreiber stellt Signaturerstellungseinheiten gemäß den rechtlichen

requirements and current technical standards for qualified electronic signatures and qualified certificates as well as for advanced or other signatures.

In case of server certificates (EV and qualified server certificates included) the key generation has to be undertaken by the applicant.

For the issuance of signature creation devices suitable for electronic signatures, the following processes must be ensured:

(a) standard process
(b) producer process
(c) policy process

(a) Standard process

To issue signature creation devices that are secure and suitable for qualified electronic signatures, a suitable security certification of the operating system is necessary for the technical components. A security certification is particularly suitable if it complies with regulations as per [EG-REF] or [CWA-14169] or has been confirmed as suitable by the regulatory authority responsible.

Signature creation devices are issued in an environment secured by the CA according to the following mandatory steps:

(i) Delivery of the signature creation devices

is performed

(a) personally in the offices of the producer, an authorised reseller or the operator by a person authorised by the producer,

(b) by courier or post. The signature creation devices are transported in

Vorgaben und aktuellen technischen Standards sowohl für qualifizierte elektronische Signaturen und qualifizierte Zertifikate, als auch für fortgeschrittene und sonstige Signaturen zur Verfügung.

Im Fall von Serverzertifikaten (inklusive EV und qualifizierter Serverzertifikate) erfolgt die Erzeugung des Schlüsselpaare jedenfalls durch den Signator selbst.

Für die Ausstellung von Signaturerstellungseinheiten, die für elektronische Signaturen geeignet sind, muss einer der folgenden Abläufe gewährleistet sein:

(a) Standardvorgabe
(b) Herstellervorgabe
(c) Policyvorgabe

(a) Standardvorgabe

Zur Ausstellung sicherer, damit für qualifizierte elektronische Signaturen geeigneter, Signaturerstellungseinheiten ist für die technische Komponente zumindest eine geeignete Sicherheitszertifizierung des Betriebssystems erforderlich. Eine Sicherheitszertifizierung ist insbesondere geeignet, wenn sie den Vorgaben gemäß [EG-REF] oder [CWA-14169] entspricht oder von den zuständigen Aufsichtstellen als geeignet bestätigt wird.

Die Ausstellung der Signaturerstellungseinheit erfolgt in einer vom VDA gesicherten Umgebung und durchläuft folgende zwingende Schritte:

(i) Lieferung der Signaturerstellungseinheiten

Erfolgt durch

(a) persönliche Übergabe in den Geschäftsräumen des Herstellers, eines von ihm autorisierten Händlers oder in den Geschäftsräumen des Betreibers durch autorisierte Personen des Herstellers,
(b) durch Boten oder Postdienste, wobei die

packaging or a container which can be checked for integrity upon delivery,

(c) using another form of delivery, provided that it can be established beyond doubt that every single signature creation device has originated from the producer (for example using an origin or production certificate that clearly refers to the producer).

(d) in case of signature creation devices for non-qualified signatures, using another form of delivery according to this Policy.

(ii) Pre-personalisation

In the case of signature creation devices for qualified signatures, a pre-personalisation takes place. Information about a particular person cannot be deduced from a pre-personalised signature creation device.

Pre-personalisation is understood to be the advance determination of a data structure on the signature creation device. This data structure can have different structures according to individual requirements. For secure signature creation devices suitable for qualified signatures, this always contains a secure key as per this document (⇨ 6.1.2 Private key delivery to subscriber / Zustellung privater Schlüssel an den Signator, p132). If the signature creation device contains additional data, this should be stored separately from the secure key and qualified certificate so that the secure key and qualified certificate can be used independently of this data and does not interfere with it.

Pre-personalisation is performed
(a) either at the offices of the producer due to the requirements of the CA or

Signaturerstellungseinheiten in Verpackungen und/oder Behälter transportiert werden, bei denen die Unversehrtheit bei der Übergabe geprüft werden kann,
(c) durch sonstige Zustellung, sofern für jede einzelne Signaturerstellungeinheit die Herkunft vom Hersteller zweifelsfrei festgestellt werden kann (zum Beispiel mittels eines Herkunfts- oder Produktionszertifikates, das dem Hersteller eindeutig zugeordnet ist).
(d) Im Falle von Signaturerstellungseinheiten für nichtqualifizierte Signaturen durch sonstige Zustellung im Sinne dieser Policy.

(ii) Pre-Personalisierung

Im Falle von Signaturerstellungseinheiten für qualfizierte Signaturen erfolgt eine Pre-Personalisierung. Eine pre-personalisierte Signaturerstellungseinheit lässt keine Rückschlüsse auf eine bestimmte Person zu.

Unter Pre-Personalisierung wird die Festlegung der Datenstruktur auf der Signaturerstellungseinheit verstanden. Diese Datenstruktur kann auf Grund individueller Anforderungen unterschiedliche Struktur haben, enthält aber bei sicheren Signaturerstellungseinheiten die für qualifizierte Signaturen geeignet sind jedenfalls einen sicheren Schlüssel im Sinne dieses Dokuments (⇨ 6.1.2 Private key delivery to subscriber / Zustellung privater Schlüssel an den Signator, p132). Soweit die Signaturerstellungseinheit weitere Daten enthält, sind sie vom sicheren Schlüssel und qualifizierten Zertifikat so getrennt zu speichern, dass sicherer Schlüssel und qualifiziertes Zertifikat unabhängig von diesen Daten verwendet werden können und eine Beeinflussung ausgeschlossen ist.

Die Pre-Personalisierung erfolgt
(a) entweder beim Hersteller auf Grund der Vorgaben des VDA oder

(b) at the offices of the producer due to a security certification or approval from a regulatory authority or
(c) at the offices of the operator as per documented requirements. The requirements could be of a general nature (for example, because of product-specific definitions) or the individual wishes of the customer.

(iii) Key generation

In signature creation devices, end user keys suitable for electronic signatures are generated according to the state of the art (including run-time-recommandations), taking legal and technical requirements into account. The keys can be generated at the offices of the operator, the producer of the signature creation devices, the subscriber or a contractor of the operator.

In any event, the requirements of the applicable certificate policy should be observed.

If the end user key is not generated in the signature creation device, it is generated in a secure environment that has the following characteristics:

- the secure environment ensures the confidentiality and integrity of the end user key throughout the duration of the check,
- the secure environment ensures the confidential transfer of the end user key to the secure signature creation device,
- the secure environment ensures the integrity of the public end user key if it is going to be exported into another system or application,
- the secure environment is used only by identified and authorised users,
- access to the services is limited,
- the functionality of the secure environment can be checked and tested and returns to a defined original state if errors occur,

(b) beim Hersteller auf Grund einer Sicherheitszertifizierung bzw. Genehmigung durch eine Aufsichtstelle oder
(c) beim Betreiber gemäß dokumentierter Anforderungen, wobei die Anforderungen genereller Natur sein können (etwa auf Grund produktspezifischer Definitionen) oder auf Grund individueller Wünsche von Kunden.

(iii) Schlüsselerzeugung

In den Signaturerstellungseinheiten werden für elektronische Signaturen geeignete Endkundenschlüssel nach Stand der Technik erzeugt, wobei rechtliche und technische Vorgaben, inklusive Laufzeitempfehlungen beachtet werden. Die Erzeugung kann sowohl beim Betreiber, beim Hersteller der Signaturerstellungseinheit, beim Signator oder bei einem vom Betreiber beauftragten Dienstleister erfolgen.

In allen Fällen sind die Vorgaben der jeweils anzuwendenden Certificate Policy zu beachten.

Sofern der Endkundenschlüssel nicht in der Signaturerstellungseinheit selbst erzeugt wird, erfolgt die Erzeugung in einer gesicherten Umgebung, die jedenfalls folgende Eigenschaften aufweist:

- die gesicherte Umgebung stellt für die gesamte Dauer die Kontrolle über den Endkundenschlüssel dessen Vertraulichkeit und Integrität sicher,
- die gesicherte Umgebung gewährleistet den vertraulichen Transfer des Endkundenschlüssels in die sichere Signaturerstellungseinheit,
- die gesicherte Umgebung sichert die Integrität des öffentlichen Endkundenschlüssels, wenn er in ein anderes System oder eine andere Applikation exportiert wird,
- die gesicherte Umgebung wird nur von identifizierten und autorisierten Benutzern verwendet,
- der Zugang und Zugriff zu den Diensten ist limitiert,
- die Funktionalität der gesicherten Umgebung kann geprüft und getestet werden und geht in einen definierten Ausgangszustand bei

- the secure environment is secured against physical attacks (damages) and returns to a secure original state if such an attack is detected.

The evaluation of these requirements complies with the regulations [CWA-14167-3] or an equivalent legally and technically acceptable procedure. The end user key is transferred by secure means. After successful transfer the end user key is irreversibly deleted in the secure environment.

(iv) Storage

If signature creation devices are stored at the offices of the CA (kept in stock), they are stored in pre-personalised or earlier state and not personalised.

The keeping of personalised signature creation devices to be delivered or picked up by the subscriber does not count as storage.

In any event, signature creation devices intended for qualified certificates for electronic signatures are stored in locked facilities. Access to these facilities is restricted to authorised personnel who have been entrusted with issuing signature creation devices.

(v) Issuance of certificates

To issue a certificate, if asymmetric encryption of public end user keys is used, data is extracted from the signature creation device and signed by the operator with his key in the secure environment. Certificates are otherwise issued as per the requirements in ⇨ 4.3 Certificate issuance / Zertifikatsausstellung (p62) and ⇨ 7.1 Certificate profile / Zertifikatsprofile (p157) and the applicable GLOBALTRUST® Certificate Practice Statement.

Auftreten von Fehlern,
- die gesicherte Umgebung ist gegen physische Angriffe (Beschädigungen) gesichert und geht in einen gesicherten Ausgangszustand, wenn derartige Angriffe erkannt werden.

Die Evaluation dieser Anforderungen entspricht den Vorgaben [CWA-14167-3] oder einem anderen vergleichbaren rechtlich und technisch zulässigen Verfahren. Die Übertragung des Endkundenschlüssels erfolgt auf gesicherte Weise, nach erfolgter Übertragung wird der Endkundenschlüssel in der gesicherten Umgebung auf nicht rekonstruierbare Weise gelöscht.

(iv) Lagerung

Soweit Signaturerstellungseinheiten beim VDA gelagert werden (auf Vorrat gehalten werden), werden sie nur in einer Pre-personalisierten oder davor liegenden Form, nicht jedoch personalisiert gelagert.

Keine Lagerung ist die bloß kurzzeitige Aufbewahrung von personalisierten Signaturerstellungseinheiten zum Zwecke der Zustellung an den oder zur Abholung durch den Signator.

In allen Fällen werden Signaturerstellungseinheiten die für qualifizierte Zertifikate für elektronische Signaturen vorgesehen sind in versperrten Einrichtungen verwahrt, der Zugriff auf diese Einrichtungen ist auf autorisiertes Personal, dass mit der Ausstellung der Signaturerstellungseinheiten betraut ist, beschränkt.

(v) Zertifikat ausstellen

Zur Erstellung des Zertifikates wird bei asymetrischer Verschlüsselung der öffentliche Endkundenschlüssel aus der Signaturerstellungseinheit extrahiert und in der gesicherten Umgebung des Betreibers mit einem Schlüssel des Betreibers unterfertigt. Im Übrigen erfolgt die Ausstellung gemäß den Vorgaben ⇨ 4.3 Certificate issuance / Zertifikatsausstellung (p62) und ⇨ 7.1 Certificate profile / Zertifikatsprofile (p157) und dem jeweils anzuwendenden

The duration and content of the certificate, process of identity verification, contractual obligations of the subscriber, CA and operator are defined in the applicable certificate policy.

(vi) Input of additional signature generation data

Additional data can be entered into a signature creation device for reasons specific to the product, legal reasons or according to the customer's wishes.

The following data structures are permitted and do not interfere with signature creation devices intended for qualified signatures:

- The storage of references to secure keys (public and private components) deposited in the signature creation device, in particular in the format of a PKCS#15 container [PKCS15].
- Additional certificates and end user keys that can be used for other signatures or encrypting data.
- Additional (cross) certificates that refer to the secure keys of the signature creation device and do not contravene the requirements of the GLOBALTRUST® Certificate Practice Statement, the GLOBALTRUST® Certificate Security Policy, this GLOBALTRUST® Certificate Policy or compulsory legal or technical requirements.
- Data necessary for the use of a signature creation device as a citizen card as defined by the Austrian E-Government Law [BÜRGERKARTE].
- Every additional data structure that is seen as suitable by a regulatory authority, taking into account restrictions on permitted signature creation devices and uses where applicable.

GLOBALTRUST® Certificate Practice Statement.

Insbesondere Laufzeit und Inhalt eines Zertifikates, Ablauf der Identitätsprüfung, die vertraglichen Verpflichtungen des Signators, des VDA und des Betreibers werden in der jeweils anzuwendenden Certificate Policy festgelegt.

(vi) Zusätzliche Signaturerstellungsdaten ablegen

Aus produktspezifischen Gründen, aus gesetzlichen Gründen oder auf Grund von Kundenwünschen können auf der Signaturerstellungseinheit zusätzliche Daten abgelegt werden.

Zulässig und keine Beeinflussung der Signaturerstellungseinheit für Zwecke der qualifizierten Signatur sind folgende Datenstrukturen:

- Die Speicherung von Verweisen auf den in der Signaturerstellungseinheit abgelegten sicheren Schlüssel (öffentliche und private Komponente) insbesondere im Format eines PKCS#15 Containers [PKCS15].
- Zusätzliche Zertifikate und Endkundenschlüssel, die für sonstige Signaturen oder zur Verschlüsselung von Daten verwendet werden können.
- Zusätzliche (Cross-)Zertifikate, die auf den sicheren Schlüssel der Signaturerstellungseinheit verweisen und nicht im Widerspruch zu den Anforderungen des GLOBALTRUST® Certificate Practice Statements, der GLOBALTRUST® Certificate Security Policy, dieser GLOBALTRUST® Certificate Policy oder zwingenden rechtlichen oder technischen Bestimmungen stehen.
- Die für die Nutzung der Signaturerstellungseinheit als Bürgerkarte im Sinne des österreichischen eGovernment-Gesetzes [BÜRGERKARTE] erforderlichen Daten.
- Jede weitere Datenstruktur, die von einer Aufsichtstelle als geeignet angesehen wird. Dabei sind auch allfällige Beschränkungen bei den zulässigen Signaturerstellungseinheiten und Nutzungen zu

- Every additional data structure that does not allow a signature creation device for qualified signatures to be interfered with.

(vii) Protection from misuse

All information put into the signature creation device, in particular end user keys for qualified electronic signatures and qualified certificates, is put in in such a way that it is impossible to corrupt the data.

Protection from misuse does not prevent the subscriber from transferring additional information to the signature creation device, deleting individual information or re-initialising the entire signature creation device.

These changes can only be made to the extent that they are permitted by the applicable GLOBALTRUST® Certificate Practice Statement and do not lead to misleading information in the certificate or on the subscriber.

(viii) Transport protection

Signature creation devices for qualified signatures are provided with a confidential initialisation PIN. In addition, the signature creation device is provided with protection during transport. The security creation device can be used for the first time only by using the initialisation PIN or by breaking or removing the protection.

Suitable transport protection measures are
(a) technical containers, for which only the subscriber has the key

(b) packaging or containers, damage to which can be unfailingly detected by a third party
(c) protection of the subscriber key with a password or

beachten.
- Jede weitere Datenstruktur, bei der im Einzelfall eine Beeinflussung der Signaturerstellungseinheit für Zwecke der qualifizierten Signatur ausgeschlossen ist.

(vii) Missbrauchsschutz

Alle auf der Signaturerstellungseinheit aufgebrachten Informationen, insbesondere Endkundenschlüssel zur qualifizierten elektronischen Signatur und qualifiziertes Zertifikat sind so aufgebracht, dass eine Verfälschung der Daten ausgeschlossen ist.

Der Missbrauchsschutz schließt nicht aus, dass der Signator zusätzliche Informationen auf der Signaturerstellungseinheit aufbringen kann, einzelne Informationen löschen kann oder die gesamte Signaturerstellungseinheit neu initialisieren kann.

Diese Änderungen können aber nur im Umfang erfolgen, wie sie gemäß anzuwendendem GLOBALTRUST® Certificate Practice Statement zulässig sind und können in keinem Fall zu irreführenden Angaben über Zertifikate oder über den Signator führen.

(viii) Transportsicherung

Signaturerstellungseinheiten für qualifizerte Signaturen werden mit einem vertraulichen Initialisierungs-PIN versehen. Zusätzlich wird die Signaturerstellungseinheit mit einer Transportsicherung versehen. Die Signaturerstellungseinheit kann erstmalig nur durch Verwendung des Initialisierungs-PINs und Bruch/Beseitigung der Transportsicherung verwendet werden.

Geeignete Transportsicherungen sind
(a) technische Behältnisse, zu denen ausschließlich der Signator einen Schlüssel hat,
(b) Verpackungen oder Behälter, bei denen eine Beschädigung durch Dritte zuverlässig erkannt werden kann,
(c) Sicherung des Signaturschlüssels durch ein Passwort oder

(d) data transferred directly into the signature creation device, which must be removed by the subscriber before the signature creation device can be used for the first time.

An appropriate measure for the purpose of (c) is to attach a transport PIN that can only be used once and must be entered before the signature creation device is used for the first time. In case of qualified certificates for electronic signatures, (c) is a suitable method of securing during transport.

Transport protection can be omitted. The criteria for this are listed in ⇨ 6.1.2 Private key delivery to subscriber / Zustellung privater Schlüssel an den Signator.

If confidential information is used for transport protection (in particular a transport PIN), this will be delivered in a form that allows the recipient to determine if unauthorised persons have been able to access the confidential information. Suitable forms of delivery are, in particular, the use of closed envelopes and the protection of confidential information using high-security labels.

If the integrity of the signature creation device or transport unit during transfer cannot be established, the subscriber is obliged to inform the CA. The CA must then revoke the issued certificate. The subscriber is made aware of his responsibility to check integrity and report possible violations of integrity before the contract is signed in the applicable certificate policy.

(ix) General framework

If work is conducted at the offices of the producer or other contractor at the request of the CA for which a confirmation by the confirmation authority is not available, adequate supervision is agreed in accordance with this

(d) direkt auf der Signaturerstellungseinheit aufgebrachte Daten, die vor der ersten Verwendung der Signaturerstellungseinheit vom Signator entfernt werden müssen.

Eine geeignete Maßnahme im Sinne von (c) ist das Anbringen eines einmalig verwendbaren Transport-PINs der vor der erstmaligen Verwendung der Signaturerstellungseinheit zwingend eingegeben werden muss. Im Falle qualifizierter Zertifikate für elektronische Signaturen ist Fall (c) eine geeignete Transportsicherung.

Die Transportsicherung kann entfallen, die Kriterien dafür sind unter ⇨ 6.1.2 Private key delivery to subscriber / Zustellung privater Schlüssel an den Signator (p132) aufgelistet.

Werden im Rahmen der Transportsicherung vertrauliche Informationen (insbesondere Transport-PIN) verwendet, werden diese in einer Form zugestellt, die dem Empfänger erlaubt zu erkennen, ob Unberechtigte Kenntnisnahme der vertraulichen Informationen erlangen konnten. Geeignete Zustellformen sind insbesondere die Verwendung von verschlossenen Kuverts und die Absicherung der vertraulichen Informationen durch "High-Security-Labels".

Sofern bei Übergabe nicht die Unversehrtheit der Signaturerstellungseinheit beziehungsweise der Transporteinrichtung festgestellt werden kann, ist der Signator verpflichtet den VDA davon in Kennntis zu setzen. Dieser hat das ausgestellte Zertifikat zu widerrufen. Die Verantwortung des Signators zur Prüfung der Unversehrtheit und der Meldung von möglichen Verletzungen der Unversehrtheit wird dem Signator vor Vertragsabschluss im Rahmen der jeweils anzuwendenden Certificate Policy zur Kenntnis gebracht.

(ix) Rahmenbedingungen

Sofern Fertigungsschritte beim Hersteller oder bei sonstigen Dienstleistern auf Wunsch des VDA durchgeführt werden, die keine Zertifizierung einer Bestätigungsstelle aufweisen, wird im Einzelfall eine

GLOBALTRUST® Certificate Policy together with the applicable GLOBALTRUST® Certificate Practice Statement.

Adequate supervision is agreed if
(a) the producer names responsible supervisors who are appropriately qualified,
(b) qualified employees of the operator supervise the production process or

(c) the operator names a qualified third party to oversee the production process.

In any event, the production process must be supervised and documented by the supervising personnel.

Certificates can be issued by the operator, a contractor or the producer of the signature creation device at the request of the operator.

The entire process of initialising the signature creation devices is logged.

(b) Producer requirements

Signature creation devices for qualified signatures can be fully or partially issued using a process defined by the producer, if this process is recognised or approved by a regulatory authority responsible for the issuance of qualified certificates or generation of qualified electronic signatures.

(c) Policy requirements

The issuance of signature creation devices can be defined in the applicable

ausreichende Beaufsichtigung im Sinne dieser GLOBALTRUST® Certificate Policy in Verbindung mit der jeweils anzuwendenden GLOBALTRUST® Certificate Practice Statement vereinbart.

Eine ausreichende Beaufsichtigung ist vereinbart, wenn
(a) der Hersteller verantwortliche Aufsichtspersonen nennt, diese eine ausreichende Qualifikation aufweisen,
(b) der Betreiber die ordnungsgemäße Durchführung der Fertigungsschritte durch eigenes qualifiziertes Personal überwacht oder
(c) der Betreiber qualifizierte Dritte nennt, der die ordnungsgemäße Durchführung der Fertigungsschritte überwacht.

In allen Fällen ist die ordnungsgemäße Durchführung der Fertigungsschritte durch das überwachende Personal zu bestätigen.

Die Ausstellung des Zertifikats kann durch den Betreiber, einem beauftragten Dienstleister oder durch den Hersteller der Signaturerstellungseinheit im Auftrag des Betreibers erfolgen.

Der gesamte Ablauf der Initialisierung der Signaturerstellungseinheiten wird protokolliert.

(b) Herstellervorgabe

Die Ausstellung von Signaturerstellungseinheiten für qualifizierte Signaturen kann vollständig oder teilweise auch durch einen vom Hersteller der Signaturerstellungseinheit vorgegebenen Prozess erfolgen, wenn dieser Prozess von einer Aufsichtstelle für die Ausstellung qualifizierter Zertifikate bzw. Erstellung qualifizierter elektronischer Signaturen genehmigt bzw. anerkannt ist.

(c) Policyvorgabe

Die Ausstellung von Signaturerstellungseinheiten kann auch in der

GLOBALTRUST® Certificate Practice Statement. In this event, it should be made clear whether the devices are only issued according to these requirements or whether the requirements of the GLOBALTRUST® Certificate Practice Statement are to be applied alternatively (optionally) as per the GLOBALTRUST® Certificate Policy.

The issuing of signature creation devices based on CompanyCAs can also be regulated by supplementary, end-customer-specific issuing processes. These are reviewed by the operator and it is ensured that they do not conflict with the operator's security requirements. 169/5000

The issuing process is described in a publicly accessible document, which is entered in the certificate by an OID from the number range 1.2.40.0.36.1.1.999.***. *** means numbered consecutively and the number is internally attached an organisation.

jeweils anzuwenden GLOBALTRUST® Certificate Practice Statement vorgegeben werden. In diesem Fall ist klarzustellen, ob die Ausstellung ausschließlich nach diesen Vorgaben erfolgt oder ob die Vorgaben des GLOBALTRUST® Certificate Practice Statement alternativ (optional) zur Ausstellung gemäß diesem GLOBALTRUST® Certificate Policy anzuwenden sind.

Die Ausstellung von Signaturerstellungseinheiten auf Basis von Endkunden-Sub-Zertifikaten kann auch durch ergänzende endkundenspezifische Ausstellungsprozesse geregelt werden. Das Ausstellungskonzept wird vom Betreiber begutachtet und es wird sichergestellt, dass sie nicht in Widerspruch zu den Sicherheitsanforderungen des Betreibers stehen. Der Ausstellungsprozess ist in einem öffentlich zugänglichen Dokument beschrieben, das im Zertifikat mittels OID aus dem Nummernkreis 1.2.40.0.36.1.1.999.*** eingetragen ist. Mit *** eine fortlaufende Nummer die intern einer Organisation zugewiesen wird.

6.1.1 Key pair generation / Erzeugung von Schlüsselpaaren

Generation of private keys and certificates for CA certificates

The necessary keys for certification services as per this policy are generated in a dedicated system according to the four-eyes principle and documented, including the methods and formats applied. If these keys are used to issue qualified certificates or are necessary to issue qualified timestamps or for other services, they are generated in systems that comply with the requirements [ETSI TS 101 456] inclusive successor: [ETSI EN 319 401], [ETSI EN 319 411-1], [ETSI EN 319 411-2] that are in force at the time that the keys are generated, in particular [SVV]. The keys are generated according to the rules that apply at the time. In particular, be supervised by an independent person or recorded on video. The adherence of these rules is confirmed by an independent person.

The operator's signature keys used for certification services, in particular for the issuance of end user certificates, are generated on secure HSM hardware. They are not publicly available or given to a third party.

The technical requirements for security that must be fulfilled for HSM modules and the signature server system are specified in the GLOBALTRUST® Certificate Security Policy. In particular, the HSM modules for RootCAs are operated offline or airgapped in a high security zone.

Generation of the subscriber's private key

The subscriber's key is generated either by the subscriber or the operator

Erzeugung der privaten Schlüssel und des Zertifikates zu den CA-Zertifikaten

Die notwendigen Schlüssel zur Erbringung der Zertifizierungsdienste gemäß dieser Policy werden in einem dedizierten System nach dem Vier-Augen-Prinzip generiert und inklusive der verwendeten Methoden und Formate dokumentiert. Soweit diese Schlüssel zur Ausstellung von qualifizierten Zertifikaten verwendet werden, zur Ausstellung von qualifizierten Zeitstempeln oder für sonstige Diensterbringung erforderlich sind, werden sie in Systemen erstellt, die den Anforderungen [ETSI TS 101 456] inklusive Nachfolger: [ETSI EN 319 401], [ETSI EN 319 411-1], [ETSI EN 319 411-2] in der zum Zeitpunkt der Schlüsselerstellung gültigen Version insbesondere [SVV] entsprechen. Diese Erstellung erfolgt gemäß den zum Zeitpunkt der Erstellung gültigen Regeln, insbesondere wird sie von einer unabhängigen Person überwacht oder auf Video festgehalten..

Die Signaturschlüssel des Betreibers die für die Zertifizierungsdienste, insbesondere die zur Ausstellung von Endkundenzertifikaten dienen, werden auf sicherer HSM Hardware erstellt. Sie sind nicht öffentlich verfügbar, sind auch nicht bei Dritten hinterlegt.

Die sicherheitstechnischen Anforderungen, die die HSM Module und das Signaturserver-System erfüllen müssen, werden in der GLOBALTRUST® Certificate Security Policy spezifiziert. Insbesondere werden die HSM Module für RootCAs offline oder airgapped in einer Hochsicherheitszone betrieben.

Erzeugung der privaten Schlüssel des Signators

Die Schlüssel des Signators werden abhängig vom betriebenen

depending on the certification service.

In case of server certificates, the key generation has to be performed by the subscriber

If keys are generated for qualified certificates for electronic signatures, appropriate secure signature creation devices must be used. The names of appropriate signature creation devices can be requested from the CA or found on its website. The requirements and generation process are described in ⇨ 6.1 Key pair generation and installation / Erzeugung und Installation von Schlüsselpaaren (p121).

Zertifizierungsdienst entweder vom Signator oder vom Betreiber erzeugt.

Im Falle von Serverzertifikaten erfolgt die Schlüsselerzeugung jedenfalls durch den Signator.

Werden Schlüssel zu qualifizierten Zertifikaten für elektronische Signaturen erstellt, ist die Verwendung geeigneter sicherer Signaturerstellungseinheiten zwingend erforderlich. Geeignete Signaturerstellungseinheiten werden auf Anfrage vom VDA bekannt gegeben oder auf der Website des VDAs veröffentlicht. Deren Anforderung und der Prozess der Ausstellung ist in ⇨ 6.1 Key pair generation and installation / Erzeugung und Installation von Schlüsselpaaren (p121) beschrieben

6.1.2 Private key delivery to subscriber / Zustellung privater Schlüssel an den Signator

Private keys are never distributed in clear text format. They must be stored and distributed at least as encrypted data or they must be distributed over password-protected encrypted connections or using another transfer method compliant with the current state of the art.

Signature keys for qualified electronic signatures are only delivered to the applicant with the appropriate signature creation device. A signature creation device is delivered using the applicable processes. It is ensured that only the authorised subscriber receives the signature creation device.

In case of qualified certificates for electronic signatures, the receiving according to Art. 24/1 lit. a

[eIDAS regulation] takes place by checking the identity of the personally

present person or the representative of a legal person by an official ID or by

Private oder geheime Schlüssel werden in keinem Fall im Klartext-Format verteilt. Sie werden zumindest als verschlüsselte Datei gespeichert und verteilt oder ihre Verteilung erfolgt über passwort-gesicherte verschlüsselte Verbindungen oder einer sonstigen dem Stand der Technik entsprechenden gesicherten Übertragung.

Die Zustellung von Signaturschlüsseln zur qualifizierten elektronischen Signatur an den Antragsteller erfolgt nur in Verbindung mit einer geeigneten Signaturerstellungseinheit. Die Zustellung der Signaturerstellungseinheit erfolgt im Rahmen des anzuwendenden Prozesses. Dabei wird sicher gestellt, dass nur der berechtigte Signator die Signaturerstellungseinheit übernimmt.

Die Übernahme erfolgt im Falle qualifizierter Zertifikate für elektronische Signaturen gemäß Art. 24 Abs. 1 lit. a [eIDAS-VO] durch Prüfung der Identität der persönlich anwesenden natürlichen Person oder des Vertreters einer juristischen Person anhand eines amtlichen Lichtbildausweises oder durch einen anderen in seiner Zuverlässigkeit

another equivalent proof that must be documented:
[1] the VDA or one of its authorized employees
[2] a representative of the VDA
[3] other identification methods that provide an equivalent level of security as personal presence (Article 24 (1) (d) [eIDAS regulation]
In the case of [3] letters within Austria will be delivered by POST AG to adressee only („Ident.Brief").

- qualified certificates for electronic signatures can be delivered using the same methods as advanced signatures and official signatures, but with the restriction that the appropriate signature creation devices produced by the operator must be delivered using transport protection (⇨ (viii) Transport protection, p127). The necessity of transport protection can be anticipated if the signature creation device is given personally by an authorised person to a subscriber and if the signature creation device has been produced by the operator under the supervision of the subscriber. In this event, the subscriber is obligated to check the integrity of the signature creation device immediately (in the presence of the authorised person) and to secure it using an authorisation code known only to himself. The signature function can only be initiated using the authorisation code. The use of the authorisation code can be subject to additional restrictions, for example [eIDAS-VO] or the specific requirements of the regulatory authority.

Other keys (not intended for qualified certificates) are delivered using appropriate transport protection, in person or using secure (encrypted) data transfer paths. At no point during delivery can a private key be accessed

gleichwertigen, dokumentierten oder zu dokumentierenden Nachweis festzustellen durch
[1] den VDA bzw. einem seiner befugten Mitarbeiter
[2] einem vom VDA beauftragten Vertreter
[3] sonstige Identifizierungsmethoden, die eine gleichwertige Sicherheit hinsichtlich der Verlässlichkeit bei der persönlichen Anwesenheit bieten, angewendet werden (Art. 24 Abs. 1 lit. d [eIDAS-VO]
Im Fall [3] werden innerhalb Österreichs Poststücke durch die POST AG per Postidentverfahren („Ident.Brief") zugestellt. Bei Zustellung in anderen Ländern wird eine gleichwertige Zustellvariante verwendet.

- Bei qualifizierten Zertifikaten für elektronische Signaturen gilt zusätzlich, dass beim Betreiber erstellte geeignete Signaturerstellungseinheiten mit Transportsicherung (⇨ (viii) Transportsicherung, p127) ausgeliefert werden. Vom Erfordernis der Transportsicherung kann abgesehen werden, wenn die Signaturerstellungseinheit von einer autorisierten Personen persönlich an den Signator übergeben wird oder wenn die Signaturerstellungseinheit vom Betreiber unter Aufsicht des Signators erstellt wurde. In diesem Fall ist der Signator verpflichtet unverzüglich (im Beisein der autorisierten Person) die Unversehrtheit der Signaturerstellungseinheit zu prüfen und durch ein eigenen nur ihm bekannten Authorisierungscode zu sichern. Die Signaturfunktion kann nur durch Verwendung von diesen Authorisierungscodes ausgelöst werden. Die Verwendung der Authorisierungscodes kann zusätzlichen Beschränkungen, etwa der [eIDAS-VO] oder spezifischen Vorgaben der Aufsichtsstelle unterliegen.

Die Übergabe von sonstigen Schlüssels (die nicht zur für qualifizierte Zertifikate vorgesehen sind) erfolgt entweder mittels geeigneter Transportsicherungen, persönlich oder durch gesicherte (verschlüsselte)

without a password.

A certification confirmation is delivered to the subscriber befor the certificate has been issued. The confirmation contains, at a minimum, the name of the applicant, signatory of the contract and a reference to the requirements of the policy.

The certification confirmation contractually obligates the subscriber to adhere to the applicable policy and must be returned with the signature of an authorised person (⇨ 4.2 Certificate application processing / Bearbeitung von Zertifkatsanträgen, p59)

Depending on the application, delivery proceeds according to the following rules:

- certificates for advanced signatures and official signatures can be delivered by ordinary post (if possible also by electronic post, inc. email or fax), if identity verification for the application has been completed.
- advanced signatures and official signatures can be delivered by a courier that offers identity verification upon delivery (in Austria this is, in particular, POST AG), if the identity check has not yet been completed or only consists of a plausibility check. Items of post can be delivered by POST AG to addressee only ("Ident.Brief"). If delivered by other delivery services, equivalent procedures are used. The identity check is concluded when the delivered certification confirmation has been returned with a signature which matches the signature on previously submitted official documents. If the signature substantially differs, a signature sample sheet with the current signature of the applicant is requested.

Datenübertragungswege. Zu keinem Übergabezeitpunkt kann auf den privaten Schlüssel ohne Kenntnis eines Passwortes zugegriffen werden.

Dem Signator wird vor Erstellung des Zertifikats eine Zertifizierungsbestätigung zugestellt. Sie enthält zumindest den Namen des Antragstellers, des Vertragsunterzeichners und einen Hinweis auf die Bestimmungen der Policy.

Diese Zertifizierungsbestätigung bindet den Signator vertraglich an die anzuwendende Policy und ist von einer autorisierten Person (⇨ 4.2 Certificate application processing / Bearbeitung von Zertifkatsanträgen, p59) unterfertigt zu retournieren.

Abhängig von der Antragstellung erfolgt die Zustellung nach folgenden Regeln:

- Bei Zertifikaten für fortgeschrittene Signaturen und Amtssignaturen als gewöhnliche Post (soweit möglich auch als elektronische Post inkl. E-Mail oder Fax), sofern die Identitätsprüfung im Rahmen der Antragstellung schon abgeschlossen wurde.
- Bei Zertifikaten für fortgeschrittene Signaturen und Amtssignaturen über einen Zustelldienst, der eine Identitätsprüfung bei der Übergabe von Dokumenten anbietet (in Österreich ist das insbesondere die POST AG), sofern die Identitätsprüfung noch nicht vollständig abgeschlossen wurde und nur eine Plausibilitätsprüfung der Identitätsangaben vorliegt. In Fall der POST AG werden Poststücke per Postidentverfahren („Ident.Brief") zugestellt, bei anderen Zustelldiensten werden gleichwertige Verfahren verwendet. Die Identitätsprüfung gilt in diesem Fall als abgeschlossen, wenn die zugestellte Zertifizierungsbestätigung unterschrieben retourniert wird und die darin enthaltene Unterschrift mit der Unterschrift auf vorab vorgelegten amtlichen Dokumenten vergleichbar ist. Bei erheblichen Abweichungen wird über einen getrennten Weg ein Unterschriftsprobenblatt mit der aktuellen Unterschrift des Antragstellers angefordert.

- advanced signatures and official signatures can be picked up in person at the offices of the CA or another registration office, if the identity check has not yet been completed. The identity check is concluded when the submitted certification confirmation has been signed in front of an authorised person and the applicant has proved identity using an official document in original. The process must be confirmed by the authorised person.

- Certificates on signature creation devices that are intended for simple signatures are delivered by ordinary post, as long as there is no reasonable doubt as to the identity of the applicant. The CA reserves the right to apply the same delivery requirements as those for certificates for advanced signatures due to technical or legal requirements.

- Other certificates intended for simple signatures are delivered using a reliable and secure method (if appropriate, also as electronic post inc. email or fax). The CA reserves the right to apply the same delivery requirements as those for certificates for advanced signatures due to technical or legal requirements.

After the certification confirmation has been received and the subscriber's signature has been checked, access to the simple certificates and/or private keys is made available. If a private key is not delivered as signature creation device hardware, the key must be downloaded over a secure connection that fulfils the following minimum criteria:

- End-to-end encryption of the transfer path,
- Authentication of the applicant (at least with the activation password given by the applicant and the reference number given in the

- Bei Zertifikaten für fortgeschrittene Signaturen und Amtssignaturen durch persönliche Abholung beim VDA oder bei einer Registrierungsstelle, sofern die Identitätsprüfung noch nicht vollständig abgeschlossen wurde. Die Identitätsprüfung gilt als abgeschlossen, wenn die ausgehändigte Zertifizierungsbestätigung vor einer autorisierten Person unterschrieben wird und sich der Antragsteller durch ein amtliches Dokument (Original) ausweisen kann. Der Vorgang ist durch die autorisierte Person zu bestätigen.
- Bei Zertifikate auf Signaturerstellungseinheiten, die für einfache Signaturen vorgesehen sind, auch als gewöhnliche Post, sofern keine vernünftigen Zweifel zu den Identitätsangaben des Antragstellers existieren. Der VDA behält sich vor, auf Grund technischer oder rechtlicher Vorgaben auch für diese Zertifikate die Zustellanforderungen gemäß Zertifikate für fortgeschrittene Signaturen anzuwenden.
- Für sonstige Zertifikate, die für einfache Signaturen vorgesehen sind, erfolgt die Zustellung in einer Form, die die zuverlässige und sichere Kenntnisnahme durch den Signator erlaubt (sofern geeignet auch als elektronische Post inkl. E-Mail oder Fax). Der VDA behält sich vor, auf Grund technischer oder rechtlicher Vorgaben auch für diese Zertifikate die Zustellanforderungen gemäß Zertifikate für fortgeschrittene Signaturen anzuwenden.

Nach Erhalt und erfolgreicher Unterschriftsprüfung der vom Empfänger unterfertigten Zertifizierungsbestätigung wird der Zugang zu einfachen Zertifikaten und/oder privatem Schlüssel freigegeben. Sofern die Zustellung des privaten Schlüssels nicht in Form einer hardwarebasierten Signaturerstellungseinheit erfolgt, muss der Schlüssel über eine gesicherte Verbindung heruntergeladen werden, die folgende Mindestkriterien erfüllt:

- Ende-zu-Ende Verschlüsselung des Übertragungsweges,
- Authentifizierung des Antragstellers (zumindest mit dem vom Antragsteller selbst vergebenen Aktivierungspassworts und der in

certification confirmation ⇨
GLOBALTRUST® Certificate Practice Statement section 4.1 7.,
- Encryption of the key using a password given by the applicant.

der Zertifizierungsbestätigung genannten Referenznummer⇨
GLOBALTRUST® Certificate Practice Statement Abschnitt 4.1 7,
- Verschlüsselung des Schlüssel durch ein vom Antragsteller vergebenes Passwort.

6.1.3 Public key delivery to certificate issuer / Zustellung öffentlicher Schlüssel an den VDA

Certificate data generated in a registration office is signed and transferred to the operator's certification office in an encrypted form. Confidentiality and integrity of all data is ensured. Encryption and signature are not necessary if the data transmitted is only the basis of the application and will only be entered into the certificates after the content and format has been checked by the CA.

Non-certified public keys are not distributed and are administered in a secure certification environment only.

The integrity and authenticity of a public key during distribution is maintained using the following measures:
- transfer of the public root CA and sub CA key to be released to the regulatory authority through the submission of a signed PKCS#10 certificate request,
- issuance and publishing of root CA and sub CA certificates on the website or registry of the CA,
- voluntary certification using recognised (private or public) audit entities,
- publication and integration in the software of trustworthy third party companies. The current state of integration of the root certificate at a third party company can be accessed on the website of the CA.

For certificates for advanced and simple signatures, at least one method of publication must be used. For qualified certificates, publication through the

Die in einer Registrierungsstelle erzeugten Zertifikatsdaten werden signiert und verschlüsselt an die Zertifizierungsstelle des Betreibers übertragen. Vertraulichkeit und Integrität sämtlicher Daten sind sicher gestellt. Das Erfordernis der Verschlüsselung und Signatur besteht nicht, wenn die übermittelten Daten nur Antragsgrundlage sind und beim VDA erst nach inhaltlicher und formaler Prüfung in die Zertifikate übernommen werden.

Nicht zertifizierte öffentliche Schlüssel werden nicht verteilt und werden ausschließlich innerhalb der gesicherten Zertifizierungsumgebung verwaltet.

Die Integrität und Authentizität der öffentlichen Schlüssel anlässlich der Verteilung bleibt insbesondere durch folgende Maßnahmen gewahrt:
- durch Übergabe des öffentlichen Root-CA- und Sub-CA-Schlüssels zur Veröffentlichung an die Aufsichtsstelle durch Übermittlung eines signierten PKCS#10 Certificate Requests,
- durch Ausstellung und Veröffentlichung der Root-CA- und Sub-CA-Zertifikate auf der Website oder eines Verzeichnisdienstes des VDA,
- durch freiwillige Zertifizierungen durch anerkannte (private oder staatliche) Audit- und Prüfeinrichtungen,
- durch Publikation und Integration in Software vertrauenswürdiger Drittfirmen. Der aktuelle Stand der Integration des Root-Zertifikates bei Drittfirmen kann über die Website des VDAs abgerufen werden.

Im Zusammenhang mit Zertifikaten für fortgeschrittene und einfache Signaturen muss zumindest eine der Veröffentlichungsformen erfüllt sein.

designated regulatory authority is necessary.

Integrity is ensured in the transfer of the data described above to third parties, in particular through the use of signatures or check sums.

Im Zusammenhang mit qualifizierten Zertifikaten ist jedenfalls eine Veröffentlichung durch die vorgesehene Aufsichtsstelle erforderlich.

Bei der Übergabe der oben beschriebenen Daten an Dritte wird die Integrität gesichert, insbesondere durch den Einsatz von Signaturen oder Prüfsummen.

6.1.4 CA public key delivery to relying parties / Verteilung öffentliche CA-Schlüssel

Information relevant to certificates (items of information of any kind) is provided, accessed and distributed as per the requirements of this GLOBALTRUST® Certificate Policy, the applicable GLOBALTRUST® Certificate Practice Statement and the GLOBALTRUST® Certificate Security Policy.
It is ensured that authorised users can read the information provided and can edit it only in compliance with defined certification processes and distribution of roles as per the role concept (⇨ GLOBALTRUST® Certificate Security Policy).

Certificates are distributed to third parties as per the requirements of the applicant and the compulsory legal requirements. The CA uses the appropriate technical procedures.

Die Bereitstellung, der Zugriff und die Verbreitung von zertifikatsrelevanten Informationen (Informationsobjekten jeglicher Art) erfolgt ausschließlich gemäß den Vorgaben dieser GLOBALTRUST® Certificate Policy, dem anzuwendenden GLOBALTRUST® Certificate Practice Statement und der GLOBALTRUST® Certificate Security Policy.
Dabei ist sicher gestellt, dass nur berechtigte Benutzer lesenden Zugriff auf die bereitgestellten Informationen haben und dass ein schreibender Zugriff nur in Übereinstimmung mit den definierten Zertifizierungsprozessen und der vorgegebenen Rollenverteilung gemäß Rollenkonzept (⇨ GLOBALTRUST® Certificate Security Policy) erfolgt.

Die Verbreitung von Zertifikaten an Dritte erfolgt gemäß den Vorgaben des Antragstellers und den zwingenden rechtlichen Vorgaben. Der VDA bedient sich dabei geeigneter technischer Verfahren.

6.1.5 Key sizes / Schlüssellängen

At the time of their issuance, the standards, algorithms and key sizes used for certificates and keys comply - regarding the run-time - with the applicable technical recommendations of the relevant regulatory authority, national or international requirements, ETSI standards, requirements of those documents with which the certification service conforms (⇨ 8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS / Prüfung der Konformität und andere Beurteilungen, p168) or the requirements of other

Die verwendeten Standards, Algorithmen und Schlüssellängen für Zertifikate und Schlüssel entsprechen unter Beachtung der Laufzeit den zum Zeitpunkt der Erstellung gültigen technischen Empfehlungen der jeweils zutreffenden Aufsichtsbehörde, nationalen oder internationalen Bestimmungen, den ETSI-Standards, den Vorgaben jener Dokumente, zu denen der Zertifizierungsdienst konform ist (⇨ 8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS / Prüfung der Konformität und

(private or public) entities that are consulted on the examination of the certification services of the CA. If different recommendations describe differing requirements and security levels, the approach that complies with the minimum requirement of all relevant recommendations is selected.

andere Beurteilungen, p168) oder den Vorgaben anderer (privater oder staatlicher) Einrichtungen, die zur Prüfung der Zertifizierungsdienste des VDAs herangezogen werden. Soweit die verschiedenen Empfehlungen unterschiedliche Anforderungen und Sicherheitsniveaus beschreiben wird jene Variante gewählt die zumindest den Mindestanforderungen aller relevanten Empfehlungen entspricht.

If differing requirements for the use of certificates or keys at different times arise, for example because of new security requirements, the updated requirements are published on the website of the CA and made public according to the wishes of the regulatory authority, auditor or other partners of the CA.

Soweit bei der Erstellung von Zertifikaten oder Schlüsseln für verschiedene Zeitpunkte unterschiedliche Anforderungen zur Anwendung kommen, beispielsweise auf Grund neuer Sicherheitsanforderungen, werden die geänderten Anforderungen auf der Website des VDA veröffentlicht oder auf Wunsch Aufsichtsbehörden, Auditstellen oder sonstigen Partnern des VDA zugänglich gemacht.

6.1.6 Public key parameters generation and quality checking / Festlegung der Schlüsselparameter und Qualitätskontrolle

Key parameters are subject to the same procedures and measures as in ⇨ 6.1.5 Key sizes / Schlüssellängen (p137).

Die Festlegung der Schlüsselparameter folgt denselben Abläufen und Maßnahmen wie unter ⇨ 6.1.5 Key sizes / Schlüssellängen (p137) festgelegt.

The quality of keys generated is continually checked as per the current state of the art.

Die Qualität der erzeugten Schlüssel wird laufend gemäß Stand der Technik geprüft.

6.1.7 Key usage purposes (as per X.509 v3 key usage field) / Schlüsselverwendung

The only intended use of the key for electronic signature is to be made known in the certificate, where technically possible and reasonable. In any other event, this is made known using the appropriate reference to the applicable GLOBALTRUST® Certificate Practice Statement.

Die vorgesehene ausschließliche Verwendung des Schlüssels zur elektronischen Signatur ist - soweit technisch möglich und sinnvoll - im Zertifikat erkennbar zu machen, in den anderen Fällen durch einen entsprechenden Hinweis im anzuwendenden GLOBALTRUST® Certificate Practice Statement.

The private key of the CA is used only for the generation of certificates explicitly intended for this purpose and the signature of the corresponding revocation lists within the premises used for certification.

Der private Schlüssel der Zertifizierungsstelle wird nur für die Erstellung von den dafür ausdrücklich vorgesehenen Zertifikaten und für die Signatur der zugehörigen Widerrufslisten innerhalb der für die Zertifizierung bestimmten Räumlichkeiten verwendet.

6.2 Private Key Protection and Cryptographic Module Engineering Controls / Schutz des privaten Schlüssels und Anforderungen an Signaturerstellungseinheiten

All measures that concern signature keys, in particular the generation of the keys, export and import procedures where applicable, backup and restoration, are taken by authorised persons only and are logged according to the four-eyes principle. The log contains information on procedures, hardware used and persons responsible. Generation is logged according to internal documentation.

Alle Maßnahmen, die die Signaturschlüssel betreffen, insbesondere die Erzeugung der Schlüssel, allfällige Export- und Importvorgänge, Backup oder Wiederherstellung, erfolgen - soweit diese Maßnahmen rechtlich zulässig sind - nach dem Vier-Augen-Prinzip ausschließlich durch autorisierte Personen und werden protokolliert, wobei das Protokoll Angaben zum Vorgang, zur verwendeten Hardware und zu den verantwortlichen Personen enthält. Die Generierung erfolgt jedenfalls nach dem Vier-Augen-Prinzip. Zur Generierung wird ein Protokoll gemäß interner Dokumentation erstellt.

The operator can use signature creation devices for different certification services. Valid and expired signature creation data (inc. certificates and other signature creation data, in particular hash values) are published on the website of the operator without the private signature key. All issued certificates contain a link to corresponding signature creation data and the applicable certificate policy of the operator.

Der Betreiber kann für verschiedene Zertifizierungsdienste unterschiedliche Signaturerstellungsdaten verwenden. Die gültigen und abgelaufenen Signaturerstellungsdaten (inkl. Zertifikate und sonstige Signaturprüfdaten, insbesondere Hash-Werte) werden auf der Webseite des Betreibers veröffentlicht, nicht jedoch die geheimen Signaturschlüssel. Alle ausgestellten Zertifikate enthalten einen Verweis (Link) wo die entsprechenden Signaturerstellungsdaten und die anzuwendende Certificate Policy des Betreibers abrufbar sind.

Separate signature creation data must be generated to issue qualified certificates. This signature creation data is only used to issue and revoke qualified certificates.

Für die Ausstellung von qualifizierten Zertifikaten sind jedenfalls eigene Signaturerstellungsdaten zu erzeugen. Diese Signaturerstellungsdaten werden nur zur Ausgabe und dem Widerruf qualifizierter Zertifikate verwendet.

Depending on the category of the key, there are different risk assessments and security measures. There are rules for the following points for all keys:

- key generation and distribution
- key use

Abhängig von der Kategorie des Schlüssels erfolgen unterschiedliche Risikobewertungen und Sicherheitsmaßnahmen der Schlüssel. Jedenfalls werden für alle Schlüssel folgende Punkte geregelt:

- Schlüsselgenerierung und -verteilung
- Schlüsselverwendung

- change of keys
- key destruction if compromised or the end of life cycle is reached

- key storage, backup and restoration
- key archiving

The signature keys in ⇨ **Category/Kategorie 1** / Category 1 (p120) have the longest duration and the greatest risk. They undergo a specialised assessment as per the GLOBALTRUST® Certificate Security Policy and are subject to special security measures. The life cycle of these keys is documented

Where applicable, necessary additional security requirements for keys in ⇨ **Category/Kategorie 2** / Category 2 (p120, "infrastructure keys") are handled in the context of the security measures of the office where they are deployed, as per the GLOBALTRUST® Certificate Security Policy. If technically possible and organisationally reasonable, different infrastructure keys are used for different services/purposes. These keys are not identical to the signature keys in ⇨ **Category/Kategorie 1** / Category 1 (p120).

The keys in ⇨ **Category/Kategorie 3** / Category 3 (p121, "identification key") are issued to authorised personnel only and are used to support and simplify identification and authorisation processes.

All private keys are kept securely. The keys in ⇨ **Category/Kategorie 2** and 3 (p120) are generated and administered in hardware suitable for cryptography. If keys are issued by the CA, the same requirements apply to the issuance of certificates as those described in ⇨ 4.3 Certificate issuance / Zertifikatsausstellung (p62). If keys are used by a third party, they are equivalent to those issued by the CA. Keys are distributed according to the same criteria as those for issuing certificates intended for

- Schlüsseländerungen
- Schlüsselzerstörung bei Kompromittierung und/oder Ende seines Lebenszyklus
- Schlüsselspeicherung, -backup und -wiederherstellung
- Schlüsselarchivierung

Die Signaturschlüssel der ⇨ **Category/Kategorie 1** (p120) haben die längste Laufzeit und für sie besteht das höchste Risiko. Sie werden im Rahmen der GLOBALTRUST® Certificate Security Policy einer gesonderten Bewertung unterzogen und unterliegen besonderen Sicherheitsmaßnahmen. Der Lebenszyklus dieser Schlüssel wird dokumentiert.

Allfällig notwendige zusätzliche Sicherheitsanforderungen der Schlüssel der ⇨ **Category/Kategorie 2** (p120, "Infrastrukturschlüssel") werden in der GLOBALTRUST® Certificate Security Policy im Rahmen der Sicherheitsmaßnahmen jener Einrichtungen behandelt, in den sie eingesetzt sind. Soweit technisch möglich und organisatorisch sinnvoll werden für unterschiedliche Dienste/Zwecke unterschiedliche Infrastrukturschlüssel verwendet. Diese Schlüssel sind nicht ident mit Signaturschlüssel der ⇨ **Category/Kategorie 1** (p120).

Die Schlüssel der ⇨ **Category/Kategorie 3** (p121, "Identifikationsschlüssel") werden ausschließlich an autorisiertes Personal vergeben und dienen zur Unterstützung und Vereinfachung von Identifikations- und Authentisierungsprozessen.

Alle privaten und geheimen Schlüssel werden sicher aufbewahrt, die Schlüssel der ⇨ **Category/Kategorie 2** und 3 (p120) werden jedenfalls in für Kryptographie geeigneter Hardware erzeugt und verwaltet. Sofern die Schlüssel vom VDA ausgestellt werden, gelten für die Ausstellung der Zertifikate sinngemäß dieselben Anforderungen wie unter ⇨ 4.3 Certificate issuance / Zertifikatsausstellung (p62) beschrieben. Soweit Schlüssel durch Drittanbieter verwendet werden, werden jene

the advanced electronic signatures of applicant. When certificates are used based on keys in ⇨ **Category/Kategorie 2** and 3 (p120), it is ensured that they are still valid. This can be done by checking the relevant revocation status information or using other appropriate technical or organisational measures, in particular operation supervision measures. The keys in **Category/Kategorie 2** and 3 (p120) are changed using a secure method before they expire or if there is clear evidence that the algorithms used are no longer sufficiently secure or if the are being regenerated for other reasons.

herangezogen, die vergleichbar mit ausgestellten Schlüsseln des VDA sind. Die Verteilung erfolgt gemäß denselben Kritieren wie die Ausgabe von Zertifikaten, die für fortgeschrittene elektronische Signaturen von Antragstellern vorgesehen sind. Bei Verwendung der Zertifikate basierend auf den Schlüsseln der ⇨ **Category/Kategorie 2** und 3 (p120) wird sichergestellt, dass diese noch gültig sind. Dies kann durch Prüfung der zugehörigen Widerrufsstatusinformationen oder anderer geeigneter technischer oder organisatorischer Maßnahmen erfolgen, insbesondere durch Maßnahmen im Rahmen der Betriebsüberwachung. Die Schlüssel der ⇨ **Category/Kategorie 2** und 3 (p120) werden zeitgerecht vor Ablauf, wenn es objektive Hinweise darauf gibt, dass die verwendeten Algorithmen nicht mehr ausreichend sicher sind oder aus sonstigen Gründen erneuert werden, in sicherer Weise gewechselt.

The keys in ⇨ **Category/Kategorie 4** (p121) that are only used for a short time are not subject to specialised documentation or supervision.

Keiner gesonderten Dokumentation oder Überwachung unterliegen die Schlüssel der ⇨ **Category/Kategorie 4** (p121), die nur kurzzeitig in Verwendung sind.

6.2.1 Cryptographic module standards and controls / Standards und Sicherheitsmaßnahmen für Signaturerstellungseinheiten

Secure signature creation devices are made available for qualified electronic signatures.

Zur qualifizierten elektronischen Signatur werden sichere Signaturerstellungseinheiten zur Verfügung gestellt.

The CA provides a list of suitable signature creation products upon request and/or on its website.

Der VDA stellt eine Liste der geeigneten Signaturerstellungsprodukte auf Anfrage und/oder über seine Website zur Verfügung.

A part of this documentation is which algorithms and parameters are used to fulfil the requirements that comply with a secure signature creation device. These specifications are defined as per the credentials that come with the signature creation devices. Alternatively, a reference to publicly accessible credentials (certification) that contains the necessary information is permitted.

Teil dieser Dokumentation ist die Angabe gemäß welcher Algorithmen und Parameter den Anforderungen für eine sichere Signaturerstellungseinheit entsprochen wird. Diese Angaben erfolgen gemäß den zu den Signaturerstellungseinheiten vorliegenden Bescheinigung(en). Alternativ ist auch der Verweis auf eine öffentlich zugängliche Bescheinigung (Zertifizierung) zulässig, die die erforderlichen Angaben enthält.

Private keys are used to sign certificates as long as the algorithms used are seen as secure in the sense of the definition in ⇨ secure signature creation device, secure key (p40).

Private Schlüssel zur Signatur von Zertifikaten werden verwendet, solange die verwendeten Algorithmen als sicher im Sinne der Definition ⇨ Sichere Signaturerstellungseinheit, sicherer Schlüssel (p40) anzusehen sind.

The operator uses an HSM system with redundancy for certification services. Synchronization of data between individual hardware modules uses a secure format that is part of the security certification of the used hardware.

Für die Erbringung der Zertifizierungsdienste verwendet der Betreiber ein HSM-System das redundant ausgeführt ist, der Datenabgleich zwischen den einzelnen Hardwaremodulen erfolgt in einem gesicherten Format, das Teil der Sicherheitszertifizierung der eingesetzten Hardware ist.

The list of HSM products used by the operator is documented internally. Operation is initiated using a written protocol. The form and content of the protocol are internally documented.

Die Liste der vom Betreiber verwendeten HSM-Produkte ist intern dokumentiert. Die Inbetriebnahme erfolgt mittels eines schriftlichen Protokolls. Form und Inhalt des Protokolls sind intern dokumentiert.

For the signature creation devices and procedures, the certification statements and confirmation authority upon which the fulfilment of requirements for qualified electronic signature are based are documented.

Zu den Signaturerstellungseinheiten und -verfahren wird dokumentiert auf Basis welcher Bescheinigung und welcher Bestätigungsstelle die Voraussetzungen für qualifizierte elektronische Signatur erfüllt sind. Bescheinigungen der Aufsichtstellen sind gleichwertig.

If certifications only refer to individual technical components, these may only be used for qualified signatures in combinations of components that together fulfil the security requirements for qualified signatures. Appropriate combinations of technical components can be listed in ⇨ Appendix / Anhang A: 3 supported signature creation unitS / Unterstützte Signaturerstellungsprodukte (p211)

Soweit sich Bescheinigungen nur auf einzelne technische Komponenten beziehen dürfen diese für qualifizierte Signaturen nur in Kombinationen eingesetzt werden, die in ihrer Gesamtheit die Sicherheitsanforderungen für die qualifizierte Signatur erfüllen. Geeignete Kombinationen von technischen Komponenten können im ⇨ Appendix / Anhang A: 3 supported signature creation unitS / Unterstützte Signaturerstellungsprodukte (p211) gelistet werden.

Certifications from the regulatory authority can be kept in copy. Alternatively, the operator can keep a reference to where they are kept at the regulatory authority.

Bescheinigungen der Aufsichtstellen werden als Kopie oder als Verweis auf die Fundstellen der Aufsichtstellen vom Betreiber in Evidenz gehalten.

If only individual technical components fulfil these requirements, they can only be used in a secure environment. The specifications for this secure environment are given in the GLOBALTRUST® Certificate Security Policy.

Erfüllen nur einzelne technische Komponenten diese Anforderungen, dann können sie nur in einer gesicherten Umgebung eingesetzt werden. Die Anforderungen dieser gesicherten Umgebung werden in der GLOBALTRUST® Certificate Security Policy festgelegt.

6.2.2 Private key (n out of m) multi-person control / Mehrpersonen-Zugriffssicherung zu privaten Schlüsseln (n von m)

The operator's private keys for CA certificates are managed according to the four-eyes principle.	Die privaten Schlüssel der CA-Zertifikate des Betreibers werden gemäß 4-Augen-Prinzip verwaltet.

6.2.3 Private key escrow / Hinterlegung privater Schlüssel (key escrow)

Not applicable	Nicht zutreffend

6.2.4 Private key backup / Backup privater Schlüssel

The operator's private keys for CA certificates are stored redundantly in a system intended for certification services.	Die privaten Schlüssel der CA-Zertifikate des Betreibers bleiben im für die Durchführung der Zertifizierung vorgesehenen System redundant gespeichert.
Private keys for CA certificates belonging to the operator that no longer comply with security requirements, or can no longer be used for other reasons, are deleted. Keys that are no longer active are not archived.	Private Schlüssel der CA-Zertifikate des Betreibers, die den Sicherheitsanforderungen nicht mehr entsprechen oder aus anderen Gründen nicht mehr weiter betrieben werden, werden gelöscht. Es erfolgt keine Archivierung nicht mehr aktiver Schlüssel.
If the subscriber's private keys do not comply with security requirements fitting the purposes for which they were issued, the subscriber is informed immediately and requested to cease using and delete the key.	Entsprechen private Schlüssel der Signatoren nicht den Sicherheitsanforderungen gemäß den Zwecken, zu denen sie ausgegeben wurden, wird der Signator unverzüglich darüber informiert und aufgefordert den Schlüssel nicht weiter zu benutzen und zu löschen.

6.2.5 Private key archival / Archivierung privater Schlüssel

The operator's private keys for CA certificates are stored in a system intended for certification services. Nothing is archived outside of the certification system.	Die privaten Schlüssel der CA-Zertifikate des Betreibers bleiben im für die Durchführung der Zertifizierung vorgesehenen System gespeichert, es erfolgt keine Archivierung außerhalb des Zertifizierungssystems.
Where applicable, available archive copies of private keys belonging to the subscriber are securely stored so that it is not possible for them to be	Allfällig vorhandene Archiv-Kopien von privaten Schlüsseln der Signatoren werden beim Betreiber so gesichert aufbewahrt, dass eine

transferred to a productive system unobserved.

Copies of private keys belonging to the subscriber are deleted at the office of the operator after they have been transferred to the subscriber.

Never private keys are stored in a nonencrypted format, like text / "plain-text".

unbeabsichtigte Übernahme in produktive Systeme nicht möglich ist.

Kopien der privaten Schlüssels der Signatoren werden - sofern beim Betreiber vorhanden - nach Ende des Übergabeverfahrens beim Betreiber gelöscht.

In keinem Fall werden private Schlüssel in einem unverschlüsseltem Format, etwa als Text / "plain-text" gespeichert.

6.2.6 Private key transfer into or from a cryptographic module / Transfer privater Schlüssel in oder aus Signaturerstellungseinheiten

It is not possible to transfer private keys for CA certificates belonging to the operator or private keys for qualified signatures from signature creation devices.

Ein Transfer von privaten Schlüsseln der CA-Zertifikate des Betreibers oder von privaten Schlüsseln für qualifizierte Signaturen dienen aus Signaturerstellungseinheiten wird ausgeschlossen.

6.2.7 Private key storage on cryptographic module / Speicherung privater Schlüssel auf Signaturerstellungseinheiten

All private keys are stored on appropriate signature creation devices.

If keys in ⇨ categories 1 to 3 have to be stored outside of their intended secure systems ("key export"), their confidentiality is secured as per the current state of the art, for example, using cryptographic measures that fulfil the requirements of [ETSI TS 119 312] and accord with the security measures of the secure module.

To ensure the authenticity of publicly availalble verification data, keys in ⇨ **Category/Kategorie 1** (p120) can be cross-certified using the CA's other certificates of the same level of confidentiaity, certificates from the regulatory office, authorities and other trustworthy third parties. This applies particularly to protecting the continuity of the confidentiality of expired or new signature certificates belonging to the CA. A cross-certification only takes place if the specification is sufficently authenticated, integrity is

Alle privaten Schlüsseln werden auf geeigneten Signaturerstellungseinheiten gespeichert.

Soweit Schlüssel der ⇨ Kategorien 1 bis 3 außerhalb der vorgesehen sicheren Systeme gespeichert werden müssen ("Schlüsselexport") erfolgt dies nach einer dem Stand der Technik entsprechende Sicherung der Vertraulichkeit, etwa durch kryptographische Maßnahmen die die Anforderungen von [ETSI TS 119 312] erfüllen und im Einklang mit den Sicherheitsmaßnahmen des sicheren Moduls sind.

Zur Sicherung der Authentizität der öffentlich verfügbaren Prüfdaten können Schlüssel der ⇨ **Category/Kategorie 1** (p120) durch andere Zertifkate des VDAs in derselben Vertrauensstufe, durch Zertifikate von Aufsichtstelle, Behörden, sonstigen vertrauenswürdigen Dritten, Cross-Zertifiziert werden. Dies gilt insbesondere zur Sicherung der Kontinuität der Vertrauenswürdigkeit abgelaufener oder neuer Signaturzertifikate des VDA. Eine Cross-Zertifizierung erfolgt nur, wenn die Anforderung

protected and it is ensured that no specifications can be falsified, particularly through replay attacks. Specifications are checked as per ⇨ 4.1 Certificate Application / Antragstellung (p57).

ausreichend authentisiert ist, die Integrität gewahrt ist und sichergestellt ist, dass keine Verfälschung der Anforderungen, insbesondere durch Replay-Angriffe möglich ist. Im übrigen erfolgt die Prüfung der Anforderungen gemäß ⇨ 4.1 Certificate Application / Antragstellung (p57).

If private keys are available in clear text, their storage space can be rewritten with zeroes.

Sofern geheime oder private Schlüssel im Klartext vorliegen, besteht die Möglichkeit die entsprechenden Speicherbereiche mit Nullen zu überschreiben

6.2.8 Method of activating private key / Aktivierung privater Schlüssel

To issue qualified certificates, the keys for CA certificates necessary for certification services must be used by two authorised persons. In other cases, certificates can be issued by one authorised person.

Die Verwendung der Schüssel der CA-Zertifikate, die für die Erbringung der Zertifizierungsdienste erforderlich sind, ist im Falle der Ausgabe qualifizierter Zertifikate durch je zwei autorisierte Personen erlaubt, in den anderen Fällen können Zertifikate auch nur durch eine autorisierte Person erstellt werden.

6.2.9 Method of deactivating private key / Deaktivierung privater Schlüssel

The signature creation devices that contain the private keys of the operator's CA certificates are automatically deactivated when the certification system is terminated.

Die Signaturerstellungseinheiten die die privaten Schlüssel der CA-Zertifikate des Betreibers beinhalten, werden bei der Beendigung des Zertifizierungssystems automatisch deaktiviert.

6.2.10 Method of destroying private key / Zerstörung privater Schlüssel

Private keys for CA certificates that do not comply with the requirements of the operator are immediately deleted in such a way that it is not possible to reconstruct them with the current state of the art. The following measures are taken:

- signature creation devices that contain private keys are taken out of operation.

Private Schlüssel, von CA-Zertifikaten die den Anforderungen des Betreibers nicht entsprechen werden unverzüglich so gelöscht, dass eine Rekonstruktion nach Stand der Technik nicht möglich ist.. Dazu werden eine Reihe von Maßnahmen gesetzt:

- Signaturerstellungseinheiten die den privaten Schlüssel enthalten, werden außer Betrieb genommen.

- certificates that have been issued on the basis of a private key are revoked.
- technical and organisational measures are taken that prevent certifications from being issued by a deactivated private key.

If private keys on signature creation devices cannot be sufficiently securely deleted, the entire signature creation device is destroyed.

- Zertifikate, die auf Grundlage des privaten Schlüssels ausgestellt wurden, werden widerrufen.
- Es werden technische und organisatorische Maßnahmen gesetzt, die eine Neuausstellung von Zertifikaten zu einem deaktivierten privaten Schlüssel verhindern.

Können auf Signaturerstellungseinheiten private Schlüssel nicht mit ausreichender Sicherheit gelöscht werden, wird die gesamte Signaturerstellungseinheit zerstört.

6.2.11 Cryptographic Module Rating / Beurteilung Signaturerstellungseinheiten

Signature creation devices are rated as per ⇨ secure signature creation device, secure key (p40).

Die Signaturerstellungseinheiten werden gemäß ⇨ Sichere Signaturerstellungseinheit, sicherer Schlüssel (p40) bewertet.

6.3 Other aspects of key pair management / Andere Aspekte des Managements von Schlüsselpaaren

6.3.1 Public key archival / Archvierung eines öffentlichen Schlüssels

The CA's and subscriber's public keys are archived in such a way to ensure that they can be reconstructed and checked for the agreed duration of the certificate.

Öffentliche Schlüssel des VDA und der Signatoren werden so archiviert, dass die Rekonstruierbarkeit und Prüfbarkeit für die zugesagte Dauer der Zertifikate gesichert ist.

6.3.2 Certificate operational periods and key pair usage periods / Gültigkeitsdauer von Zertifikaten und Schlüsselpaaren

The signature key can be used for electronic signatures from the time that the transport protection is removed or the signature creation device is transfered to the subscriber, but not before the starting date of validity as given in the certificate. It can be used until the end date of validity as given in the certificate but not after the certificate has been revoked.

Die zulässige Verwendung eines Signaturschlüssels zur elektronischen Signatur beginnt mit Aufhebung der Transportsicherung bzw. mit Übergabe der Signaturerstellungsdaten an den Signator, jedoch nicht vor Beginn des im Zertifikat eingetragenen Gültigkeitsdatums und endet spätestens mit dem im Zertifikat eingetragenen Endedatum der Gültigkeit, geht jedoch keinesfalls über das Widerrufsdatum des Zertifikats hinaus.

The maximum permitted duration of validity for qualified certificates is determined by legal requirements and the requirements of regulatory authorities. For other certificates, this is determined by the product description and the individual requirements of the subscriber. For simple certificates, it is possible to have a different validity period than as stipulated in the policy: this must be agreed with the subscriber and cannot be longer than the maximum permitted validity period of the issuing CA certificate.

For server certificates with a validity starting date on or after 1.7.2012, the maximum validity period is 60 months. For server certificates with a validity starting date on or after 1.4.2015, the maximum validity period is 39 months. For server certificates with a validity starting date on or after 1.3.2018, the maximum validity period is 825 days. For server certificates with a validity starting date on or after 1st September 2020, the maximum validty period is 397 days.

An electronic signature issued within the validity period remains valid after the validity period has expired or the certificate has been suspended of revoked.

Der maximal zulässige Gültigkeitszeitraum richtet sich bei qualifizierten Zertifkaten nach den gesetzlichen Anforderungen und Vorgaben der Aufsichtsbehörden, in den anderen Fällen nach der jeweiligen Produktbeschreibung und den individuellen Anforderungen des Signators. Für einfache Zertifikate ist eine von der Policy abweichende Gültigkeitsdauer möglich, diese muss mit dem Signator vereinbart werden und kann nicht länger sein, als die maximal zulässige Gültigkeitsdauer des ausstellenden CA-Zertifikates.

Bei Serverzertifikaten mit einem Gültigkeitsbeginn nach dem 1.7.2012, beträgt die maximale Gültigkeitsdauer 60 Monate. Bei Serverzertifikaten mit einem Gültigkeitsbeginn nach dem 1.4.2015, beträgt die maximale Gültigkeitsdauer 39 Monate. Bei Serverzertifikaten mit einem Gültigkeitsbeginn nach dem 1.3.2018, beträgt die maximale Gültigkeitsdauer 825 Tage. Bei Serverzertifikaten mit einem Gültigkeitsbeginn nach dem 1.9.2020, beträgt die maximale Gültigkeitsdauer 397 Tage

Eine innerhalb des Gültigkeitszeitraums ausgestellte elektronische Signatur behält auch nach Ablauf der Gültigkeit, bei Sperre oder Widerruf des Zertifikates ihre Gültigkeit.

6.4 Activation data / Aktivierungsdaten

6.4.1 Activation data generation and installation / Generierung und Installation von Aktivierungsdaten

Advanced signatures or signatures that have been provided with a qualified certificate can only be created using activation data.

Fortgeschrittene Signaturen oder Signaturen, die mit einem qualifizierten Zertifikat versehen werden können nur mit Hilfe von Aktivierungsdaten ausgelöst werden.

6.4.2 Activation data protection / Schutz von Aktivierungsdaten

Activation data must be kept confidential and stored in such a way that illegitimate use to the current state of the art is not possible.

Aktivierungsdaten sind vertraulich zu halten und so aufzubewahren, dass eine unrechtmäßige Verwendung nach dem Stand der Technik nicht möglich ist.

6.4.3 Other aspects of activation data / Andere Aspekte von Aktivierungsdaten

The operator obligates the subscriber to handle the activation data confidentially and helps the subscriber to select the data, where legally permitted and explicitly desired.

Der Betreiber verpflichtet den Signator zur vertraulichen Behandlung seiner Aktivierungsdaten und unterstützt ihn- sofern rechtlich zulässig und ausdrücklich gewünscht- bei deren Auswahl.

6.5 Computer security controls / Sicherheitsmaßnahmen IT-System

Technical components necessary for the operation of certification services are separated from the operator's other (office) facilities in terms of hardware and software. Organisational and administrative measures necessary for certification services are documented. The steps taken can be reconstructed if required.

Die zum Betrieb der Zertifizierungsdienste erforderlichen technischen Komponenten sind von sonstigen (Büro-)Einrichtungen des Betreibers hard- oder softwaretechnisch getrennt. Die im Rahmen der Zertifizierungsdienste erforderlichen organisatorischen und administrativen Maßnahmen sind dokumentiert, die getätigten Schritte können bei Bedarf nachvollzogen werden.

If communication with a certification component installed in a data centre is necessary to issue signature creation data, this communication takes place as per the requirements of the GLOBALTRUST® Certificate Security Policy in a way that effectively prevents certification services from being compromised, in any case using a secure virtual private network (VPN). Alongside technical security, organisational measures are taken to restrict access to technical devices, such as restriction to authorised persons.

Soweit zur Ausstellung von Signaturerstellungsdaten eine Kommunikation mit den in einem Rechenzentrum installierten Zertifizierungskomponenten erforderlich ist, erfolgt sie gemäß den Vorgaben der GLOBALTRUST® Certificate Security Policy in einer Form, die die Kompromittierung der Zertifizierungsdienste wirksam verhindert, jedenfalls in Form eines gesicherten virtuellen privaten Netzes (VPN). Neben der technischen Absicherung werden dabei auch organisatorische Maßnahmen, wie Beschränkung der Zugriffsberechtigten, Beschränkung der zum Zugriff technisch geeigneten Geräten gesetzt.

The integrity of computer systems and information is protected against viruses and malicious or unauthorised software.

Die Integrität der Computersysteme und Informationen ist gegen Viren und böswillige oder unautorisierte Software geschützt.

Capacity needs are monitored and future developments predicted so that

Kapazitätserfordernisse werden beobachtet und künftige Entwicklungen

appropriate bandwidths, processing capacity and other IT resources are available.

Functions critical to security for certification and revocation services are separated from ordinary administrative functions. Functions critical to security can be seen as all IT measures that maintain the operational capability of certification services. This is in particular

- the planning and acceptance of security systems,
- protection from malicious software and attacks,
- active checking of log files and reports, analysis of incidents,

- general system maintenance activities,
- network administration,
- data management, data carrier administration and security,
- software updates.

prognostiziert, sodass stets angemessene Bandbreiten, Prozessorleistungen und sonstige IT-Ressourcen zur Verfügung stehen.

Die sicherheitskritischen Funktionen im Rahmen der Zertifizierungs- und Widerrufsdienste werden von den gewöhnlichen administrativen Funktionen getrennt. Als sicherheitskritische Funktionen werden alle IT-Maßnahmen angesehen, die zur Erhaltung der Betriebsfähigkeit des Zertifizierungsdienstes dienen. Insbesondere sind dies

- Planung und Abnahme von Sicherheitssystemen,
- Schutz vor böswilliger Software und Angriffen,
- Aktive Überprüfung von Log-Files und Prüfberichten, Analyse von Zwischenfällen,
- Allgemeine System-Wartungstätigkeiten,
- Netzwerkadministration,
- Datenmanagement, Datenträgerverwaltung und –sicherheit,
- Softwareupdates.

6.5.1 Specific computer security technical requirements / Spezifische technische Sicherheitsanforderungen an die IT-Systeme

The necessary security requirements are defined and implemented specific to each component and are documented in the GLOBALTRUST® Certificate Security Policy.

All technical components of the certification operation are operated in secure environments. Entrance and access are only available through authorized users. The networks of the VDA are physically and logically separated. The communication of the various segments is limited to what is necessary for operation. Critical systems are located in specially protected zones. Networks for system administration and operations are separated. Productive systems are separated from development and test systems. The communication between different trustworthy systems takes place exclusively through distinct protected connections. Where high availability is required, systems are redundant. The VDA regularly conducts vulnerability scans and penetration tests. Timetables are internaly documented.

Die erforderlichen Sicherheitsanforderungen werden komponentenspezifisch definiert und umgesetzt und sind in der GLOBALTRUST® Certificate Security Policy dokumentiert.

Alle technischen Komponenten des Zertifizierungsbetriebes werden in gesicherten Umgebungen betrieben. Zugang und Zugriff erfolgen nur durch berechtigte Benutzer. Die Netzwerke des VDA sind physisch und logisch getrennt. Die Kommunikation der verschiedenen Segmente ist auf das für den Betrieb notwendige Ausmaß beschränkt. Kritische Systeme sind in besonders geschützten Zonen untergebracht. Netzwerke für die Systemadministration und den operativen Betrieb sind voneinander getrennt. Produktivsysteme sind von Entwicklungs- und Testsystemen getrennt. Die Kommunikation zwischen verschiedenen vertrauenswürdigen Systemen erfolgt ausschließlich über eigene geschützte Verbindungen. Wo eine hohe Verfügbarkeit notwendig ist,

werden Systeme redundant ausgeführt. Der VDA führt regelmäßig Schwachstellenscans und Penetrationstests durch. Zeitpläne sind intern dokumentiert.

6.5.2 Computer security rating / Beurteilung der Computersicherheit

The security of the entire certification system has undergone risk analysis. The approch of the analysis, results and measures are internally documented, in particular in the GLOBALTRUST® Certificate Security Policy and are regularly evaluated during audits.

Die Sicherheit des gesamten Zertifizierungssystems wurde einer Risikoanalyse unterzogen. Die Vorgangsweise der Analyse, die Ergebnisse und Maßnahmen sind intern, insbesondere in der GLOBALTRUST® Certificate Security Policy dokumentiert und werden jedenfalls im Zuge der vorgesehenen Audits regelmäßig evaluiert.

6.6 Life cycle technical controls / Technische Maßnahmen während des Lebenszyklus

All technical components relevant to certification are subject to continual monitoring throughout their entire life cycle and documented throughout their entire life cycle.

Alle zertifizerungsrelevanten technischen Komponenten unterliegen während ihres gesamten Lebenszyklus einem laufenden Monitoring und sind über den gesamten Lebenszyklus dokumentiert.

6.6.1 System development controls / Sicherheitsmaßnahmen bei der Entwicklung

System developments are made in development systems separate from real operations.

Die Systementwicklung erfolgt in vom Echtbetrieb getrennten Entwicklungssystemen.

The processes necessary for certification services are continually developed and optimised. Optimisation of security as well as improvement of user friendliness determines system development.

Die für die Zertifizierungsdienste notwendigen Prozesse werden laufend weiterentwickelt und optimiert. Neben einer Optimierung der Sicherheit bestimmt auch die Verbesserung der Kundenfreundlichkeit die Systementwicklung.

Development will be based on security requirements in accordance with the GLOBALTRUST® Certificate Security Policy.

Bei der Entwicklung wird auf Sicherheitsvorgaben gemäß der GLOBALTRUST® Certificate Security Policy Bedacht genommen.

Software modules used in operations are electronically signed. The signatures are continually checked and unwanted changes can be

Die in Betrieb befindlichen Softwaremodule werden elektronisch signiert. Die Signaturen werden laufend geprüft, unerwünschte Änderungen

recognised.
There are transfer procedures for the installation of new software.

können erkannt werden.
Zur Installation neuer Softwaremodule existieren Übergabeverfahren.

6.6.2 Security management controls / Sicherheitsmaßnahmen beim Computermanagement

The necessary security controls are documented in the GLOBALTRUST® Certificate Security Policy.

Die erforderlichen Sicherheitsmaßnahmen sind in der GLOBALTRUST® Certificate Security Policy dokumentiert.

6.6.3 Life cycle security controls / Sicherheitsmaßnahmen während des Lebenszyklus

The appropriate publications, recommendations and manufacturer information regarding the cryptographic keys are continuously evaluated and implemented. This is done at least once a year, but in any case on an ad hoc basis, for example in case of changes in the procedures of the CA, notifications by the supervisory authorities or other qualified third parties. The necessary security controls are documented in the GLOBALTRUST® Certificate Security Policy.

Die geeigneten Publikationen, Empfehlungen und Herstellerangaben bezüglich der kryptographischen Schlüssel werden laufend evaluiert und umgesetzt. Dies erfolgt mindestens einmal jährlich, jedenfalls aber anlassbezogen, zum Beispiel bei einer Änderungen in den Verfahren des VDA, bei Mitteilungen der Aufsichtsbehörden oder sonstigen qualifizierten Dritten. Die erforderlichen Sicherheitsmaßnahmen sind in der GLOBALTRUST® Certificate Security Policy dokumentiert.

6.7 Network security controls / Sicherheitsmaßnahmen Netzwerke

The necessary security controls are documented in the GLOBALTRUST® Certificate Security Policy.

Die erforderlichen Sicherheitsmaßnahmen sind in der GLOBALTRUST® Certificate Security Policy dokumentiert.

6.8 Time-stamping / Zeitstempel

Qualified and non-qualified time-stamping is conducted as per the GLOBALTRUST® Certificate Practice Statement ⇨ 6.8 Time-stamping / Zeitstempel.

Qualified timestamps are issued using a certificate with the additional qualification " QUALIFIED TIMESTAMP " and a number to distinguish different versions.

Qualifizierte und nicht-qualifizierte Zeitstempel werden gemäß GLOBALTRUST® Certificate Practice Statement ⇨ 6.8 Time-stamping / Zeitstempel erbracht.

Qualifizierte Zeitstempel werden durch ein Zertifikat mit der Zusatzbezeichnung " QUALIFIED TIMESTAMP" und einer Ziffer zur Unterscheidung unterschiedlicher Versionen des Dienstes ausgestellt.

Time-stamping is performed on the basis of [eIDAS-VO]. The accuracy of time information (maximum deviation from the actual time) fulfils the legal requirements for qualified timestamp services and is specified in the GLOBALTRUST® Certificate Practice Statement.

Timestamp services are offered as server services, the technical facilities for which are subject to the same security and operational requirements as those for the issuance of certificates. The servers are operated in a secure environment and are physically, technically and organisationally secured against unauthorised changes. These requirements are described in the GLOBALTRUST® Certificate Security Policy.

The operator uses a timestamp to confirm the existence of a particular hash value at the time that is shown in the timestamp. Hash values are accepted that are generated with algorithms that comply with the current state of the art, taking into consideration national and international requirements, for example from [ETSI TS 119 312]. The hash procedures accepted are particularly SHA-256, SHA-512 and RIPEMD-160. Further procedures are published on the website http://www.globaltrust.eu/produkte.html, for which the CA explicitly reserves the right to exclude particular procedures (without giving reasons) and/or accept new, appropriate procedures.

Timestamps are confirmed using an electronic signature generated by mechanism that comply with legal requirements and current technical standards (in particular [ETSI TS 119 312]). Timestamps are generated using keys intended only for timestamp services which are generated and administered in hardware that is suitable for cryptography Products are used to administer the keys that are appropriate for issuing qualified certificates. These are operated in a way that allows them to issue mass signatures. These products are secured against unauthorised reading and

Die Erbringung von Zeitstempeldiensten erfolgt auf Basis der [eIDAS-VO]. Die Genauigkeit der Zeitangaben (maximale Abweichung von der tatsächlichen Zeit) erfüllt die rechtlichen Anforderungen für qualifizierte Zeitstempeldienste und wird im GLOBALTRUST® Certificate Practice Statement spezifiziert.

Zeitstempeldienste werden als Serverdienste angeboten, wobei die technischen Einrichtungen denselben Sicherheits- und Betriebsanforderungen wie für die Ausstellung von Zertifikaten unterliegt. Die Server werden in gesicherter Umgebung betrieben und sind baulich, technisch und organisatorisch gegen unbefugte Veränderungen gesichert. Diese Anforderungen sind in der GLOBALTRUST® Certificate Security Policy beschrieben.

Mit dem Zeitstempel bestätigt der Betreiber das Bestehen eines bestimmten Hashwertes zum im Zeitstempel ausgewiesenen Zeitpunkt. Akzeptiert werden Hashwerte, die mit Algorithmen erstellt werden, die dem Stand der Technik entsprechen, wobei nationale und internationale Anforderungen, etwa von [ETSI TS 119 312] beachtet werden. Die akzeptierten Hash-Verfahren sind insbesondere SHA-256, SHA-512 und RIPEMD-160. Weitere Verfahren werden auf der Website http://www.globaltrust.eu/produkte.html veröffentlicht, wobei sich der VDA ausdrücklich vorbehält, bestimmte Verfahren (auch ohne Angabe von Gründen) jederzeit auszuschließen bzw. neue, geeignete Verfahren zu akzeptieren.

Die Bestätigung des Zeitstempels erfolgt mittels elektronischer Signatur die durch Mechanismen erzeugt wird, die den gesetzlichen Anforderungen und aktuellen technischen Standards (insbesondere [ETSI TS 119 312]) entspricht. Insbesondere erfolgt die Generierung des Zeitstempels durch eigene nur für den Zeitstempeldienst vorgesehene Schlüssel, die in Hardware erzeugt und verwaltet werden, die zur Kryptographie geeignet ist. Zur Verwaltung des Schlüssels werden Produkte verwendet, die zur Ausstellung qualifizierter Zertifikate geeignet

changes of the keys.

The keys and certificates necessary for the timestamp service are generated in the same way as described for the issuance of end user keys for the subscriber (⇨4.1 Certificate Application / Antragstellung, p57). All relevant timestamping processes are documented, in particular with relation to key generation, key life cycle management and failures inc. deviations from the guaranteed time.

The timestamp service is available during the business hours of the CA and, at the least, during the legally stipulated minimum hours. Changes or exceptions to this availability, especially additional availability, is published on the website of the operator http://www.globaltrust.eu/auditreport.html or agreed individually with the users of the timestamp service.

The operator aims for 99% availability of the timestamp service (fewer than 88 hours of outage per year) and provides a report on the outage times for registered users of the timestamp service and regulatory authorities on an annual basis. However, the minimum availability time alone does not constitute a guarantee.

Every timestamp is provided with a distinctive serial number, the issuing certificate, an accuracy statement (or a reference to the relevant policy in which accuracy is defined) and the conditions of the timestamp allocation (or a reference to the relevant policy in which the conditions are described).

In addition, every timestamp contains information on which request (hash

sind. Sie werden in einer Form betrieben, die die Ausstellung von Massensignaturen erlauben. Diese Produkte sind gegen unbefugtes Auslesen und Veränderung der Schlüssel gesichert.

Die für den Zeitstempeldienst erforderlichen Schlüssel und Zertifikate werden in derselben Weise erzeugt, wie allgemein in der Ausstellung des Endkundenschlüssel für den Signator beschrieben (⇨4.1 Certificate Application / Antragstellung, p57). Alle relevanten Vorgänge des Zeitstempeldienstes, insbesondere im Zusammenhang mit der Schlüsselerzeugung, dem Schlüssel-Lebenszyklusmanagements und Fehlfunktionen des Zeitstempeldienstes inkl. Abweichungen von der zugesicherten Zeit werden dokumentiert.

Die Verfügbarkeit des Zeitstempeldienstes ist grundsätzlich in den Geschäftszeiten des VDA, jedenfalls jedoch zu den gesetzlich vorgegebene Mindestzeiten gegeben. Davon abweichende, insbesondere darüber hinausgehende Verfügungszeiten, werden auf der Website http://www.globaltrust.eu/auditreport.html des Betreibers bekannt gegeben oder mit Nutzern des Zeitstempeldienstes individuell vereinbart.

Der Betreiber strebt eine 99%ige Verfügbarkeit des Zeitstempeldienstes an (weniger als 88 Stunden Ausfall im Jahr) und wird jährlich einen Bericht über die Ausfallszeiten für registrierte Benutzer des Zeitstempeldienstes und Aufsichtstellen bereit stellen. Aus der Unterschreitung der Verfügbarkeitszeit allein kann jedoch keine Gewährleistung abgeleitet werden.

Jeder Zeitstempel wird mit einer eindeutigen Seriennummer, dem ausstellenden Zertifikat, einer Genauigkeitsangabe (bzw. mit einem Verweis auf die zugehörige Policy, in der die Genauigkeit definiert ist) und den Bedingungen der Zeitstempelvergabe (bzw. mit einem Verweis auf die zugehörige Policy, in der die Bedingungen beschrieben sind) versehen.

Weiters enthält jeder Zeitstempel die Angabe, auf welche Anforderung

value) it corresponds to. Every valid timestamp assigned is archived. The time information for which a hash value is signed and the hash tag itself are an integral part of the data structure signed by the timestamp service (⇨ Timestamp).

The current signature verification data necessary to establish a valid timestamp can be determined using the certificate that issues the timestamp. Timestamp certificates contain references to one or more CA certificates. In any event, the highest certificate is the GLOBALTRUST® root certificate, an earlier or succeeding root certificate, for which the operator is responsible. The certificate verification data for the timestamp (inc. the current timestamp procedure) is published on the website of the CA at http://www.globaltrust.eu/certificate-policy.html or in one of links listed in the applicable certificate policy. A timestamp issued by the CA can be verified using any software that conforms to the standard [RFC3161]. In addition, the CA makes verification software available for download free from its website http://www.globaltrust.eu/certificate-policy.html. If the correctness of the timestamp cannot be established beyond doubt by the user, the CA offers individual verification of timestamp data by the CA.

A timestamp is verified by comparing the hash values of an existing document with the signed hash value from the data structure of the time stamp. If the hash values are identical, the existence of the document at the time given in the time-stamp is confirmed.

Regarding timestamps that are generated according to procedure and can no longer be definitely seen as reliable as per the decision of the regulatory authority or recognized standardization committees (in particular as per the recommendations [ETSI TS 119 312]), the requester will be informed, if their identity is known and valid contact details are available.

(Hash-Wert) er sich bezieht. Jeder vergebene gültige Zeitstempel wird archiviert. Die Zeitangaben zu denen ein vorgelegter Hashwert signiert wird und der Hashwert selbst sind integraler Teil der durch den Zeitstempeldienst signierten Datenstruktur (⇨ Zeitstempel, Timestamp).

Die zur Feststellung eines gültigen Zeitstempels erforderlichen aktuellen Signaturprüfdaten können durch das Zertifikat, das den Zeitstempel ausstellt, festgestellt werden. Zeitstempelzertifikate enthalten Verweise auf ein oder mehrere CA-Zertifikate, das oberste Zertifikat ist in allen Fällen das GLOBALTRUST®-Root-Zertifikat, ein früheres oder ein nachfolgendes Root-Zertifikat, für das der Betreiber verantwortlich ist. Die Zertifikatsprüfdaten für die Zeitstempel (inkl. dem aktuellen Zeitstempelverfahren) sind auf der Website des VDA unter http://www.globaltrust.eu/certificate-policy.html oder in einem in der anzuwendenden Certificate Policy genannten Link veröffentlicht. Ein vom VDA ausgestellter Zeitstempel kann durch jede standardkonforme Software (Standard [RFC3161]) geprüft werden, darüber hinaus stellt der VDA eine Prüfsoftware zur Verfügung, die von der Website des VDA kostenfrei http://www.globaltrust.eu/certificate-policy.html geladen werden kann. Kann die Korrektheit eines Zeitstempels vom Nutzer nicht zweifelsfrei festgestellt werden, bietet der VDA eine individuelle Prüfung der Zeitstempeldaten durch den VDA an.

Die Prüfung eines Zeitstempels erfolgt durch Vergleich der Hashwerte eines bestehenden Dokuments mit dem signierten Hashwert aus der Datenstruktur des Zeitstempels. Sind die Hashwerte ident, wird damit die Existenz des Dokuments zum Zeitpunkt gemäß Zeitangaben im Zeitstempel bestätigt.

Bei Zeitstempel, die mit Verfahren erstellt werden, die gemäß [SVV] oder gemäß der Entscheidung der Aufsichtsstelle oder anerkannter Standardisierungsgremien (insbesondere gemäß den Empfehlungen [ETSI TS 119 312]) als nicht mehr sicher zuverlässig anzusehen sind, werden die Anforderer - sofern ihre Identität bekannt ist und gültige

The operator ensures the accuracy of the timestamp with a maximum deviation from the actual time of 1 second. If European legal requirements or international standards require greater accuracy, this will be ensured. Current information on time accuracy is made available on the website of the CA http://www.globaltrust.eu or upon request. The actual time is defined as UTC. Measures to ensure adherence to the actual time are described in the GLOBALTRUST® Certificate Practice Statement.

Kontaktdaten vorhanden sind - über die fehlende Zuverlässigkeit des Zeitstempels informiert.

Der Betreiber gewährleistet eine Genauigkeit des Zeitstempels mit einer maximalen Abweichung von einer Sekunde zur tatsächlichen Zeit. Sofern europarechtliche Vorgaben oder internationale Standards eine höhere Genauigkeit verlangen, wird diese gewährleistet. Aktuelle Informationen zur Zeitgenauigkeit werden auf der Website des VDA http://www.globaltrust.eu oder auf Anfrage bekannt gegeben. Als tatsächliche Zeit wird UTC definiert. Die Maßnahmen zur Einhaltung der tatsächlichen Zeit sind im GLOBALTRUST® Certificate Practice Statement beschrieben.

7. CERTIFICATE, CRL, AND OCSP PROFILES / PROFILE DER ZERTIFIKATE, WIDERRUFSLISTEN UND OCSP

The content and technical description of the certificate can be read from the respective announcements and notices on the website of the CA. For the use of standardised certificate formats(eg X509v3), a reference to the applicable standards, for example [RFC5280], is sufficient.

In addition, the following applies for server certificates (EV included):

- further information on the applicant is only admissable if it has been checked during an application review. If necessary because of missing information, fields in the subject string are left completely blank.

- the issuer string contains the same data as the issuing CA-certificate's Subject String data.

Essentially standardised directory and revocation services are provided for issued certificates as per the following technical standards and technical norms:

- directory service as LDAP service as per [RFC4511] and the relevant standards.
- revocation service as OCSP service as per [RFC2560] and the relevant standards.
- revocation service as CRL service as per [RFC5280] and the relevant standards distributed.

Inhalt und technische Beschreibung des Zertifikats sind der jeweiligen Anzeige bzw. den Ankündigungen auf der Website des VDA zu entnehmen. Bei der Verwendung von standardisierten Zertifikatsformaten (z.B. X509v3) genügt der Verweis auf die anzuwendenden Standards, wie z.B. [RFC5280].

Für alle Server-Zertifikate (inklusive EV) gilt darüber hinaus folgendes:

- Weitere Informationen zum Antragsteller sind nur dann zulässig, wenn diese im Rahmen der Antragsprüfung überprüft wurden. Sofern es aufgrund mangelnder Information notwendig ist, werden Felder im Subject String komplett leer gelassen.
- Der Issuer String enthält enthält dieselben Einträge wie der Subject String des ausstellenden CA-Zertifikats..

Zu den ausgestellten Zertifikaten werden grundsätzlich standardisierte Verzeichnis- und Widerrufsdienste gemäß folgender technischer Standards und technischer Normen bereitgestellt:

- Verzeichnisdienst als LDAP-Dienst gemäß [RFC4511] und den dazugehörigen Standards.
- Widerrufsdienst als OCSP-Dienst gemäß [RFC2560] und den dazugehörigen Standards.
- Widerrufsdienst als CRL-Service gemäß [RFC5280] und den dazugehörigen Standards verbreitet.

The scope and technique of the registry and revocation services provided come from the individual entries in the certificate, the applicable certificate policy, the legal requirements and individual agreements.

Umfang und Technik der bereitgestellten Verzeichnis- und Widerrufsdienste ergibt sich aus den individuellen Eintragungen im Zertifikat, der jeweils anzuwendenden Certificate Policy, den gesetzlichen Vorgaben und individuellen Vereinbarungen.

7.1 Certificate profile / Zertifikatsprofile

All certificate formats described in the respective GLOBALTRUST® Certificate Practice Statement are supported, at least certificates as per X.509v3. The procedures and algorithms used for X.509v3 certificates are documented in [ITU-X509v3] and [RFC5280]. In addition, restrictions and the requirements of standards and documents that conform to the certification service are observed, in particular requirements that come from the requirements of the regulatory authority [CABROWSER-BASE] or [CABROWSER-EV].

Qualified certificates contain information as per [ETSI EN 319 412]. Additional information is possible in the certificates, if they are not misleading, are factually correct and do not breach any compulsory legal requirements.

Qualified certificates for electronic signatures are issued so as to comply with the requirements in [eIDAS-VO] Appendix I, [ETSI EN 319 412]. In countries where [eIDAS-VO] is not in effect, they are issued as per the national regulations of the country where the applicant has domicile.

Qualified server certificates are issued so as to comply with the requirements in [eIDAS-VO] Appendix IV, [ETSI EN 319 412] and [CABROWSER-EV]. In countries where [eIDAS-VO] is not in effect, they are issued as per the national regulations of the country where the applicant has domicile.

Unterstützt werden alle Zertifikatsformate die im jeweiligen GLOBALTRUST® Certificate Practice Statement beschrieben sind, jedenfalls jedoch Zertifikate gemäß X.509v3. Die zu X.509v3-Zertifikaten verwendeten Verfahren und Algorithmen sind in [ITU-X509v3] und [RFC5280] dokumentiert. Zusätzlich werden Einschränkungen und Vorgaben jener Standards und Dokumente beachtet, zu denen der Zertifizierungsdienst konform ist, insbesondere Vorgaben, die sich insbesondere aus Empfehlungen der Aufsichtsstelle, [CABROWSER-BASE] oder [CABROWSER-EV] ergeben.

Qualifizierte Zertifikate enthalten jedenfalls die Angaben gemäß [ETSI EN 319 412]. Zusätzliche Angaben in den Zertifikaten sind möglich, sofern sie nicht irreführend, sachlich richtig und nicht gegen zwingende rechtliche Bestimmungen verstoßen.

Qualifizierte Zertifikate für elektronische Signaturen werden so ausgegeben, dass sie jedenfalls den Anforderungen der [eIDAS-VO] Anhang I, [ETSI EN 319 412] entsprechen. In Ländern in denen die [eIDAS-VO] keine Wirksamkeit hat, gemäß jenen nationalen Bestimmungen, in denen der Antragsteller seinen Sitz hat.

Qualifizierte Serverzertifikate werden so ausgegeben, dass sie jedenfalls den Anforderungen der [eIDAS-VO] Anhang IV, [ETSI EN 319 412] sowie [CABROWSER-EV] entsprechen. In Ländern in denen die [eIDAS-VO] keine Wirksamkeit hat, gemäß jenen nationalen Bestimmungen, in denen der Antragsteller seinen Sitz hat.

In addition to this, a permissible qualified certificate can contain information (additional or optional) that is admissable on the basis of other regulations.

Every certificate is issued with a distinct serial number.

The serial number of a server certificate contains an entropy of at least 64 bits and is generated by a cryptographically secure pseudo-random number generator (CSPRNG)

For all issuance of certificates, including re-certification und re-key, certificates are issued with a new distinct number. An exchange of certificates with the same number is not anticipated and is prevented with technical and organisational measures. The requirements for the issuance of certificates for re-certification and re-key are the same as those for the original issuance.

The certificates contain at least the following information:

- name or identifier of the subscriber. Identifiers are selected so as not to be confused with the name of a third party,
- where applicable, pseudonyms are specially marked so that they are not confused with first names or surnames, or official company or organisation names.
- the public key that is assigned to the private key of the subscriber,
- the advanced signature of the CA,
- the distinct identifier and serial number of the certification service,
- the start date of the validity of the certificate,
- the end date of the validity of the certificate, which cannot be before the start date,
- the signature algorithm (in case of elipitic curves, including Curve

Dazu ergänzend kann ein zulässiges qualifiziertes Zertifikat auch jene Angaben (ergänzend oder alternativ) enthalten, die auf Grundlage anderer Bestimmungen zulässig sind.

Jedes Zertifikat wird mit einer eindeutigen Seriennummer ausgestellt.

Die Seriennummer eines Serverzertifikates enthält zumindest 64 bit Entropie und wird von einem kryptographisch sicheren Zufallszahlengenerator (CSPRNG) erzeugt.

In allen Fällen der Zertifikatserstellung, inklusive von "Re-Certification" und "Re-Key" werden die Zertifikate mit neuer eindeutiger Nummer ausgestellt. Ein Austausch von Zertifikaten mit derselben Nummer ist nicht vorgesehen und wird durch technische und organisatorische Maßnahmen verhindert. Die Anforderungen für die Zertifikatserstellung entsprechen in beiden Varianten "Re-Certification" und "Re-Key" zumindest den Anforderungen der Originalausstellung.

Die Zertifikate enthalten zumindest folgende Angaben:

- Name oder Bezeichnung des Signators, wobei Bezeichnungen so zu wählen sind, dass sie nicht mit Namen Dritter verwechselt werden können,
- allfällige Pseudonyme sind so gesondert gekennzeichnet eingetragen, dass sie nicht mit Vor- bzw. Familiennamen, offiziellen Firmen- oder Organisationsbezeichnungen verwechselt werden können,
- den öffentlichen Schlüssel, der dem privaten Schlüssel des Signators zugeordnet ist,
- die fortgeschrittene Signatur des VDA,
- eindeutige Bezeichnung und Seriennummer des Zertifizierungsdienstes,
- ein Beginndatum der Gültigkeit des Zertifikates,
- ein Endedatum der Gültigkeit des Zertifikates, das nicht vor dem Beginndatum liegt,
- der im Zertifikat mittels OID eingetragene verwendete

Parameters) used is described in the certificate via an OID entry. It must comply with the current state of the art. It must comply with national and international requirements. In the case of RSA keys the minimum length is 2048 bits. For ecliptical curves (EC) the minimum length is 256 bits, and one of the following Curve Parameters has to be used: FR, Brainpool or NIST, each with a hash algorithm of the SHA2 family (from SHA256).

- a reference to the applicable certificate policy.
- If a certificate is issued to a person who belongs to an organization, the personal and organizational data are entered in the fields provided, so that the subject identifier identify person and organization correctly.

In addition, the following applies for EV and qualified server certificates:

- the certificate contains a verified organisation name.
- wild card entries are not allowed in subjectAltName or in commonName.
- the subject string contains the field businessCategory with the content "Private Organization", "Government Entity" or "Non-Commercial Entity", depending on the categorisation of the organisation of the applicant (⇨ 3.2.5 Validation of authority / Nachweis der Vertretungsbefugnis, p54).
- the subject string contains a selection of fields jurisdictionOfIncorporationLocalityName, jurisdictionOfIncorporationStateOrProvinceName, jurisdictionOfIncorporationCountryName. The selection is defined by the jurisdiction of the organisation registration.
- the subject string contains the field serialNumber which contains the

Signaturalgorithmus (bei eliptischen Kurven inklusive Curve Parameter) muss dem Stand der Technik entsprechen, jedenfalls jedoch nationalen und internationalen Vorgaben entsprechen. Im Falle von RSA-Schlüsseln muss die Mindestlänge 2048 bit betragen. Bei eliptischen Kurven (EC) muss die Mindestlänge 256 bit betragen ECDSA und einer der folgenden Curve Parameter verwendet werden: FR, Brainpool oder NIST, jeweils mit einem Hash-Algorithmus der SHA2-Familie (ab SHA256) ,

- einen Verweis auf die anzuwendende Certificate Policy.
- Wird ein Zertifikat einer Person ausgestellt, die einem Unternehmen zugehörig ist, werden die Personen- und Unternehmensdaten in die dafür vorgesehenen Felder eingetragen, sodass das Zertifikat im Subject Identifier Person und Unternehmen korrekt ausweisen.

Für EV und qualifizierte Serverzertifikate gilt darüber hinaus folgendes:

- Das Zertifikat enthält jedenfalls einen geprüften Organisationsnamen.
- Wildcard Einträge sind weder im subjectAltName noch im commonName erlaubt.
- Der Subject String enthält das Feld businessCategory mit dem Inhalt "Private Organization", "Government Entity" oder "Non-Commercial Entity", je nach Kategorisierung der Organisation des Antragstellers (⇨ 3.2.5 Validation of authority / Nachweis der Vertretungsbefugnis, p54).
- Der Subject String enthält jedenfalls eine Auswahl der Felder jurisdictionOfIncorporationLocalityName, jurisdictionOfIncorporationStateOrProvinceName, jurisdictionOfIncorporationCountryName.
  Die Auswahl wird durch den rechtlichen Gültigkeitsbereich der Organisationsregistrierung bestimmt (z.B. im Falle einer landesweiten Registrierungsbehörde wird nur das Land eingetragen, gemäß .
- Der Subject String enthält das Feld serialNumber welches die

verified registration number of the organisation. If this is not available, the data of registration can also be entered.

- the verified address of the organisation is shown in the subject string in the fields countryName, stateOrProvincename (if applicable for that country) and localityName. The fields postalCode and streetAddress are optional.
- If an organizationIdentifier (OID: 2.5.4.97) containing a registration number according to [ETSI 319 412-4] is present, also a cabfOrganizationIdentifier (OID: 2.23.140.3.1) entry according to [CABROWSER-EV] is used.

The root certificates of the issuer and user (applicant) have identical information. They can be verified on the basis of the information in the certificate, in particular on the basis of the policy reference.

The private key of the root certificate is generated for use using RSA and with a minimum length of 4096 bits. The hash algorithm used is for the root certificate SHA1. For root certificates that have been created since 1 October 2014, this is at least SHA256.

The private keys of any CA certificates are generated using RSA and with a minimum length of 4096 bits. The hash algorithm used is at least SHA256.

geprüfte Registrierungsnummer der Organisation enthält. Sofern eine solche nicht vorliegt, kann auch das Datum der Registrierung eingetragen werden.

- Die geprüfte Adresse der Organisation wird im Subject String jedenfalls in den Feldern countryName, stateOrProvincename (sofern für das Land zutreffend) und localityName abgebildet. Optional können auch die Felder postalCode und streetAddress eingetragen werden.
- Die Registrierungsnummer einer Organisation kann gemäß [ETSI 319 412-4] zusätzlich im Feld organizationIdentifier (OID: 2.5.4.97) eingetragen werden, in diesem Fall wird auch das Feld cabfOrganizationIdentifier (OID: 2.23.140.3.1) gemäß [CABROWSER-EV] gesetzt. .

Die Root-Zertifikate sind in den Angaben von Herausgeber und Anwender (Antragsteller) ident und Root-Zertifikate weisen im Herausgeber- und Subject-Feld idente Angaben auf. Sie können auf Grund der Angaben im Zertifikat, insbesondere des Policy-Verweises verifiziert werden.

Der private Schlüssel von Root-Zertifikaten wird für die Verwendung mittels RSA und mit einer Mindestlänge von 4096 bit generiert, der verwendete Hash-Algorithmus ist für Root-Zertifikate SHA1, für Root-Zertifikate, die nach dem 1. Oktober 2014 erstellt werden zumindest SHA256.

Der private Schlüssel von CA-Zertifikaten wird für die Verwendung mittels RSA mit einer Mindestlänge von 4096 bit generiert, der verwendete Hash-Algorithmus ist zumindest SHA256.

7.1.1 Version number(s) / Versionsnummern

The version number 3 according to [RFC5280] (X509v3) is supported.

Es wird jedenfalls die Versionsnummer 3 laut [RFC5280] (X509v3) unterstützt.

7.1.2 Certificate extensions / Zertifikatserweiterungen

Certificates in X.509 format can contain arbitrary technically and legal permitted extensions that do not contradict the purpose of the certificate and are not misleading. The applicant or the CA can initiate the adding of extensions. Care is taken to sufficiently document the identifiers and content of the extensions and to ensure that conditions and restrictions on use are observed.

If server certificates are issued in X.509v3 format, they always contain the extension subjectAltName [RFC5280]. This contains entries of the dNSName (in the preferred syntax according to [RFC 5280]) or iPAddress type only. If the subject contains the field commonName, its content is always an entry (domain name or IP address) from subjectAltName.

The commonName or subjectAltName extension field of a server certificate never contains an IP adress that the IANA has marked as reserved, or a Domain name that can not be seen as globallly unique because it does not end with a Top Level Domain that has been registered with the IANA Root Zone Database.

For the distribution of revocation status information, all certificates contain the following extensions:

1. a crlDistributionPoint extension that is not marked as critical and that contains a HTTP URL for the relevant revocation list
2. an authorityInformationAccess extension that is not marked as critical and that contains a HTTP URL to the relevant OCSP responder

Zertifikate im X.509 Format können beliebige technisch und rechtlich zulässige Erweiterungen enthalten die nicht dem Zertifikatszweck widersprechen und nicht irreführend sind. Die Aufnahme der Erweiterungen kann sowohl vom Antragsteller als auch vom VDA initiiert werden. Dabei wird darauf geachtet, dass die Kennung und der Inhalt der Erweiterung ausreichend dokumentiert ist und die Bedingungen und Einschränkungen zur Verwendung erfüllt werden.

Soweit Serverzertifikate im Format X.509v3 ausgestellt werden enthalten sie in jedem Fall die Erweiterung subjectAltName [RFC5280]. Diese enthält ausschließlich Einträge des Typs dNSName (in der bevorzugten Syntax gemäß [RFC 5280]) oder iPAddress. Sofern der Subject das Feld commonName enthält, ist dessen Inhalt jedenfalls ein Eintrag (Domainname oder IP-Adresse) aus dem subjectAltName.

Serverzertifikate enthalten in den Feldern commonName oder subjectAltName niemals eine IP-Adresse, die die IANA als reserviert gekennzeichnet hat[9] oder einen Domainnamen, der nicht als eindeutig angesehen werden kann, weil er nicht mit einer nicht in der IANA Root Zone Database registrierten Top Level Domain endet.

Zur Verbreitung der Widerrufsstatusinformationen enthalten alleZertifikate folgende Erweiterungen

1. Eine crlDistributionPoint Erweiterung, die als nicht kritisch markiert ist und eine HTTP URL zur entsprechenden Widerrufsliste enthält
2. Eine authorityInformationAccess Erweiterung, die als nicht kritisch markiert ist und eine HTTP URL zum entsprechenden OCSP Responder enthält.

[9] http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml
http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xml

Point 2 is not necessary if "OCSP stapling"(as per [RFC4366]) is deployed and is either technically examined or contractually required by the operator.

Similarly, all other CA, sub- and end user certificates contain these extensions if they do not contradict technical or legal reasons.

The CA can issue enduser-sub-certificates especially for a subscriber. The private key can remain in the sole control of the CA or be administered by the user.

A enduser-sub-certificate is technically restricted as far as is possible. This means that:

- A enduser-sub-certificate in X.509v3 format contains an ExtendedKeyUsage extension that contains possible EKU values of end user certificates. The extension never contains the value anExtendedKeyUsage.
- If a enduser-sub-certificate in X.509v3 format is allowed the EKU id-kp-serverAuth, the option to issue dNSName entries must be restricted to confirmed domains (⇨ 7. CERTIFICATE, CRL, AND OCSP PROFILES / Profile der Zertifikate, Widerrufslisten und OCSP, p156) using a NameConstraints extension or entries of the dNSName type must be completely prohibited.
- If a enduser-sub-certificate in X.509v3 format is allowed, the EKU id-kp-serverAuth, the option to issue iPAddress entries must be restricted to confirmed address ranges (⇨ 7. CERTIFICATE, CRL, AND OCSP PROFILES / Profile der Zertifikate, Widerrufslisten und OCSP, p156) using a NameConstraints extension or entries of the iPAddress type must be completely prohibited (IPv4 as well as IPv6 addresses).
- If a enduser-sub-certificate in X.509v3 format is allowed the EKU id-

Punkt 2 ist nicht erforderlich , wenn "OCSP Stapling" (laut [RFC4366]) eingesetzt wird und dies vom Betreiber entweder technisch geprüft oder vertraglich festgelegt wird.

Alle anderen CA-, Sub- und Endkunden-Zertifikate enthalten ebenfalls diese Erweiterungen, sofern nicht technische oder rechtliche Gründe dem entgegenstehen

Der VDA kann Endkunden-Sub-Zertifikate speziell für einen Signator erstellen. Dabei kann der private Schlüssel unter der alleinigen Kontrolle des VDA verbleiben oder vom Nutzer verwaltet werden.

Ein Endkunden-Sub-Zertifikat wird nach Möglichkeit technisch eingeschränkt. Das bedeutet jedenfalls:

- Ein Endkunden-Sub-Zertifikat im Format X.509v3 enthält eine ExtendedKeyUsage Erweiterung, die die möglichen EKU Einstellungen von Endzertifikaten enthält. Diese Erweiterung enthält niemals den Wert anyExtendedKeyUsage.
- Wenn einem Endkunden-Sub-Zertifikat im Format X.509v3 die EKU id-kp-serverAuth erlaubt ist, so muss die Möglichkeit dNSName Einträge zu erstellen durch den Einsatz einer NameConstraints Erweiterung auf bestätigte Domains (⇨ 7. CERTIFICATE, CRL, AND OCSP PROFILES / Profile der Zertifikate, Widerrufslisten und OCSP, p156) beschränkt werden oder Einträge vom Typ dNSName allgemein unterbunden werden.
- Wenn einem Endkunden-Sub-Zertifikat im Format X.509v3 die EKU id-kp-serverAuth erlaubt ist, so muss die Möglichkeit IPAddress Einträge zu erstellen durch den Einsatz einer NameConstraints Erweiterung auf bestätigte Addressbereiche (⇨ 7. CERTIFICATE, CRL, AND OCSP PROFILES / Profile der Zertifikate, Widerrufslisten und OCSP, p156) beschränkt werden, oder Einträge vom Typ iPAddress allgemein unterbunden werden (sowohl IPv4 als auch IPv6 Adressen).
- Wenn einem Endkunden-Sub-Zertifikat im Format X.509v3 die EKU

kp-emailProtection, the option to issue email address entries must be restricted to confirmed address ranges (⇨ 7. CERTIFICATE, CRL, AND OCSP PROFILES / Profile der Zertifikate, Widerrufslisten und OCSP, p156).
- If a enduser-sub-certificate in X.509v3 format is allowed the EKU id-kp-codeSigning, the possible directoryName must be restricted to a verified organizationName and countryName as well as an optional localityName and stateOrProvinceName entries using the NameConstraints extension.

If the enduser-sub-certificate is not restricted due to the above criteria, the following organisational requirements are fulfilled together:

- The certificate in X.509v3 format is published in the DER format before the user can issue certificates with it.
- The Certificate Policy and the Certificate Practice Statement of the enduser-sub-certificate is published if available. At least one of the documents must exist.
- The certifcate policy/certificate practice statement of the enduser-sub-certificate fulfils the criteria of [MOZILLA-CAPOL].

- The certificate policy of the enduser-sub-certificate is audited at least once a year by a competent independent auditor. The audit must at a minimum comply with the criteria [CABROWSER-BASE]. The audit report is published.

All publications named above are available on the website of the CA and are available without restriction.

id-kp-emailProtection erlaubt ist, so muss die Möglichkeit E-Mail Adressen Einträge zu erstellen auf bestätigte Addressbereiche (⇨ 7. CERTIFICATE, CRL, AND OCSP PROFILES / Profile der Zertifikate, Widerrufslisten und OCSP, p156) beschränkt werden.
- Wenn einem Endkunden-Sub-Zertifikat im Format X.509v3 die EKU id-kp-codeSigning erlaubt ist, so muss der mögliche directoryName mittels NameConstraints Erweiterung auf geprüfte organizationName und countryName sowie optional localityName und stateOrProvinceName Einträge beschränkt werden.

Sofern das Endkunden-Sub-Zertifikat nicht anhand der obigen Kriterien eingeschränkt ist, werden jedenfalls folgende organisatorische Bedingungen gemeinsam erfüllt:
- Das Zertifikat im Format X.509v3 wird im DER Format veröffentlicht bevor der Nutzer damit Zertifikate ausstellen kann.
- Die Certificate Policy und das Certificate Practice Statement des Endkunden-Sub-Zertifikates werden veröffentlicht. Es muss jedoch zumindest eines der Dokumente existieren.
- Die Certificate Policy/das Certificate Practice Statement des Endkunden-Sub-Zertifikates erfüllen jedenfalls die Kriterien von [MOZILLA-CAPOL].
- Es erfolgt zumindest einmal jährlich eine Auditierung der Certificate Policy des Endkunden-Sub-Zertifikates durch eine kompetente unabhängige Auditstelle. Die Auditierung muss zumindest den Kriterien [CABROWSER-BASE] entsprechen. Der Report dieser Auditierung wird veröffentlicht .

Alle oben angegebenen Veröffentlichungen erfolgen auf der Webseite des VDA und sind ohne Einschränkungen verfügbar.

7.1.3 Algorithm object identifiers / Algorithmen OIDs

Certificates contain a reference to the algorithm of the public key and the method with which it was signed by the CA certificate. All methods specified

Zertifikate enthalten einen Hinweis auf den Algorithmus des öffentlichen Schlüssels und des Verfahrens mit dem es vom CA-Zertifikat

or referenced in [RFC5280] and other compatible algorithms that satisfy the technical requirements of the respective certification service are permitted.

unterschrieben wurde. Zulässig sind alle in [RFC5280] spezifizierten bzw. referenzierten Verfahren sowie andere kompatible Algorithmen, die den technischen Ansprüchen des jeweiligen Zertifizierungsdienstes genügen.

7.1.4 Name formats / Namensformate

Certificates always identify the subscriber (subject) and the respective CA (issuer).

Zertifikate enthalten jedenfalls eine Identifikation des Signators (Subject) und der jeweiligen CA (Issuer).

If an attribute field is present in a certificate, it always contains a substantial entry, but never a mere indication of absence or inapplicability.

Soweit Attributfelder in einem Zertifikat präsent sind, enthalten immer einen inhaltlichen Eintrag, niemals aber einen bloßen Hinweis auf Abwesenheit oder Nichtanwendbarkeit.

If the identity of the applicant has been verified for a server certificate, the certificate contains the organisation name according to registration documents. If server certificates in X.509v3 format are issued, the subject contains the entries: organizationName and also a countryName, a localityName and/or a stateOrProvince Name. In this event, an organizationalUnit entry can also exist, as long as this does not contain misleading or unverified information. The country in countryName refers to the IP address of the applicant, the IP address of their website, the country code of the contained domain or a valueconfirmed in the course of identity verification.

Wurde bei einem Serverzertifikat die Identität des Antragstellers geprüft, so enthält das Zertifikat den Organisationsnamen laut offiziellen Registrierungsunterlagen. Soweit Serverzertifikate im Format X.509v3 ausgestellt werden beinhaltet das Subject einen organizationName Eintrag und zusätzlich einen countryName sowie einen localityName und/oder einen stateOrProvinceName Eintrag. In diesem Fall kann auch ein organizationalUnit Eintrag vorhanden sein, sofern dieser keine irreführenden oder ungeprüften Informationen enthält. Das Land in countryName bezieht sich dabei entweder auf die IP-Adresse des Antragstellers, die IP-Adresse seiner Webseite, den Ländercode der eingetragenen Domain oder auf eine im Zuge der Identitätprüfung erhaltene Bestätigung.

If the addresses entered were only technically verified and identification verification was not carried out, the subject of the certification does not contain any of the following fields: organizationName, localityName, stateOrProvinceName, postcalCode. If the subject has a domainComponent entry, this contains all sorted parts of the domain name entered in the certificate in reverse order.

Wurde bei einem Serverzertifikat lediglich eine technische Prüfung der einzutragenden Adressen und keine Identifikationsprüfung vorgenommen, so enthält der Subject des Zertifikates keines der folgenden Felder: organizationName, localityName, stateOrProvinceName, postalCode. Sofern das Subject einen domainComponent Eintrag besitzt, enthält dieses alle geordneten Teile eines im Zertifikat eingetragenen Domainnamen in umgekehrter Reihenfolge.

7.1.5 Name constraints / Namensbeschränkungen

For all certificates, the same name (eg. distinguishedName) is never used for two different applicants within the same respective CA-certificate or enduser-sub certificate.

Für alle Zertifikate gilt, dass derselbe Name (z.B. distinguishedName) innerhalb des jeweiligen CA-Zertifikats oder Endkunden-Sub-Zertifikats niemals für zwei unterschiedliche Antragsteller verwendet wird.

7.1.6 Certificate policy object identifier / Certificate Policy Object Identifier

Certificates with the exception of root certificates from 2015, contain a reference to the applicable Certificate Policy under which they were issued. For this GLOBALTRUST® Certificate Policy, there is the OID-Number 1.2.40.0.36.1.1.8.1 In addition, certificates can contain a reference to the specifications of a third party that are observed when subscriber certificates are issued, in particular those given in [CABROWSER-BASE] and [CABROWSER-EV]. Server certificates contain the additional OID entry 2.23.140.1.2.2 (OV) or 2.23.140.1.1 (EV)

Zertifikate (ausgenommen Root-Zertifikate ab 2015) enthalten jedenfalls einen Verweis auf die anzuwendende Certificate Policy, nach der sie ausgestellt wurden. Für die vorliegende GLOBALTRUST® Certificate Policy wird die OID-Nummer 1.2.40.0.36.1.1.8.1 eingetragen. Darüberhinaus können an dieser Stelle ein Verweis auf Spezifikationen von Dritten enthalten sein, die bei der Erstellung des Signatorzertifikates beachtet wurden, insbesondere die in [CABROWSER-BASE] und [CABROWSER-EV] angegebenen. Serverzertifikate enthalten, den zusätzlichen OID Eintrag 2.23.140.1.2.2 (OV) oder 2.23.140.1.1.1 (EV)

Certificates that were issued between 1.7.2014 and 1.1.2020 and whose keys have not been generated in a signature creation device that complies with at least FIPS-140 2 L2 or CC Protection Profile CWA 14169 can contain the policy OID entry 1.2.40.0.36.4.1.10. This OID is not in use anymore and has no impact on the validity of the respective certificates.

Zertifikate die zwischen 1.7.2014 und 1.1.2020 ausgestellt wurden und deren Schlüssel nicht in einer Signaturerstellungseinheit erzeugt wurden, die zumindest FIPS-140 2 L2 oder CC Protection Profile CWA 14169 entspricht können den zusätzlichen Policy-OID-Eintrag 1.2.40.0.36.4.1.10 enthalten. Dieser OID wird nicht mehr verwendet und hat keinen Einfluss auf die Gültigkeit der betroffenen Zertifikate

7.1.7 Usage of Policy Constraints extension / Nutzung der Erweiterung „PolicyConstraints“

This extension can be used according to the specifications of [RFC5280] if required.

Diese Erweiterung kann bei Bedarf gemäß den Spezifikation von [RFC5280] eingesetzt werden.

7.1.8 Policy qualifiers syntax and semantics / Syntax und Semantik von „PolicyQualifiers“

This extension can be used according to the specifications of [RFC5280] if required.

Diese Erweiterung kann bei Bedarf gemäß den Spezifikation von [RFC5280] eingesetzt werden.

7.1.9 Processing semantics for the critical Certificate Policies extension / Verarbeitung der Semantik der kritischen Erweiterung CertificatePolicies

Critical and non-critical extensions are used according to the specifications of [RFC5280].

Kritische und nicht-kritische Erweiterung werden gemäß den Spezifikation von [RFC5280] eingesetzt.

7.2 CRL profile / Sperrlistenprofile

The content of the revocation list for certificates suitable for qualified signature, official signature or advanced signature complies with [RFC5280].

Der Inhalt der Widerrufsliste entspricht bei Zertifikaten die zur qualifizierten Signatur, zur Amtssignatur oder zur fortgeschrittenen Signatur geeignet sind [RFC5280].

The issued certificate states which revocation and suspension service may be used. The subscriber's individual technical requirements can be considered if they do not contradict the standards used, legal requirements or applicable GLOBALTRUST® Certificate Practice Statement.

Welche Widerrufs- und Sperrdienste verwendet werden, sind im ausgegebenen Zertifikat festgelegt. Dabei können individuelle technische Anforderungen der Signatoren berücksichtigt werden, soweit sie nicht im Widerspruch zu den verwendeten Standards, rechtlichen Vorgaben und dem anzuwendenden GLOBALTRUST® Certificate Practice Statement stehen.

The scope of the revocation and/or suspension list can be found in the certification service's notices at the regulatory authority or in the documentation on the website of the CA.

Der Umfang der Widerrufs- bzw. Sperrliste ist - sofern anzeigepflichtig - der Anzeige des jeweiligen Zertifizierungsdienstes bei der Aufsichtsbehörde bzw. den Dokumentationen auf der Website des VDA zu entnehmen.

7.2.1 Version number(s) / Versionsnummern

Each CRL is provided with a version number.

Jede CRL ist mit einer Versionsnummer versehen.

7.2.2 CRL and CRL entry extensions / Erweiterungen von Widerrufslisten und Widerrufslisteneinträgen

Revocation lists can contain extensions that are specified in [RFC5280] or are compatible with [RFC5280].	Widerrufslisten können in [RFC5280] spezifizierte oder mit [RFC5280] kompatible Erweiterungen enthalten

7.3 OCSP profile / Profile des Statusabfragedienstes (OCSP)

The operator's OCSP service is operated as per [RFC6960].	Der OCSP Dienst des Betreibers erfolgt gemäß [RFC6960].
OCSP responses for CAs that issue server certificates in X.509v3 format are signed by either the CA certificate itself or by a dedicated OCSP responder certificate that contains the extension id-pkix-oCA-nocheck (according to [RFC2560]).	OCSP Antworten für CAs die Serverzertifikate im Format X.509v3 ausstellen werden entweder vom CA Zertifikat selbst oder von einem dedizierten OCSP Responder-Zertifikat signiert, dass die Erweiterung id-pkix-oCA-nocheck (laut [RFC2560]) enthält .
An OCSP responder never delivers a "good" status back to an unknown certificates.	Ein OCSP-Responder liefert niemals den Status "good" für ein unbekanntes Zertifikat zurück.

7.3.1 Version number(s) / Versionsnummern

The OCSP responses have a version number as per [RFC6960].	Die OCSP Antworten enthalten eine Versionsnummer gemäß [RFC6960].

7.3.2 OCSP extensions / OCSP-Erweiterungen

The OSCP responses can contain extension as per [RFC6960].	Die OCSP Antworten können Erweiterung gemäß [RFC6960] enthalten.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS / PRÜFUNG DER KONFORMITÄT UND ANDERE BEURTEILUNGEN

The operator declares that this document, together with the GLOBALTRUST® Certificate Practice Statement (OID: 1.2.40.0.36.1.2.3.1) and the GLOBALTRUST® Certificate Security Policy (OID: 1.2.40.0.36.1.2.2.1), fulfils the requirements of the following regulations in their current version:

- REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [eIDAS-VO]
- Austrian Signature Law [SVG] together with the Signature Act [SVV]
- ETSI Policy and security requirements for Trust Service Providers issuing certificates EN 319 411 (Part 1: General Requirements and Part 2: Requirements for trust service providers issuing EU qualified certificates)
- Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements [CWA-14167-1]
- Microsoft Root Certificate Program [MS-CA]
- CA/Browser Forum: Baseline Requirements [CABROWSER-BASE] published at https://www.cabforum.org
- [CABROWSER-EV] Guidelines For The Issuance And Management Of Extended Validation Certificates published at https://cabforum.org/extended-validation/

Der Betreiber erklärt, dass dieses Dokument gemeinsam mit dem GLOBALTRUST® Certificate Practice Statement (OID-Nummer: 1.2.40.0.36.1.2.3.1) und der GLOBALTRUST® Certificate Security Policy (OID-Nummer: 1.2.40.0.36.1.2.2.1) die Anforderungen gemäß der jeweils gültigen Fassung folgender Bestimmungen erfüllen:

- VERORDNUNG (EU) Nr. 910/2014 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG [eIDAS-VO]
- österreichisches Signatur- und Vertrauensdienstegesetz [SVG] in Verbindung mit der Signatur- und Vertrauensdiensteverordnung [SVV]
- ETSI Policy and security requirements for Trust Service Providers issuing certificates EN 319 411 (Part 1: General Requirements and Part 2: Requirements for trust service providers issuing EU qualified certificates)
- Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements [CWA-14167-1]
- Microsoft Root Certificate Program [MS-CA]
- CA/Browser Forum: Baseline Requirements [CABROWSER-BASE] veröffentlicht unter https://www.cabforum.org
- [CABROWSER-EV] Guidelines For The Issuance And Management Of Extended Validation Certificates veröffentlicht unter https://cabforum.org/extended-validation/

- Mozilla CA Certificate Inclusion Policy [MOZILLA-CAPOL]
- Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework [RFC3647]
- Trust Service Principles and Criteria for Certification Authorities [WEBTRUST-CA]
- Conformity with [MOZILLA-CAMAINT]
- Conformity with [APPLE-CA]
- Conformity with [ENISA-ALG]

Regular audits that comply with the conformity requirements of the documents cited ensure that the requirements are observed.

In the event of inconsistencies between the certification service's documents and the documents which the certification services comply with, the following rules apply:

a) legal requirements are immediately effective over the requirements of the documents of the certification service,
b) inconsistencies without a direct effect on the policy of the certification service are interpretively clarified on the website of the CA,
c) inconsistencies that directly affect the policy of the certification service, if they concern qualified certificates, lead to adjustments of the documents concerned to establish consistency,
d) in all other cases, the requirements of the conformity documents have priority.

- Mozilla CA Certificate Inclusion Policy [MOZILLA-CAPOL]
- Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework [RFC3647]
- Trust Service Principles and Criteria for Certification Authorities [WEBTRUST-CA]
- Konformität mit [MOZILLA-CAMAINT]
- Konformität mit [APPLE-CA]
- Konformität mit [ENISA-ALG]

Die Einhaltung der Anforderungen wird durch regelmäßige Audits sichergestellt, die den Konformitätsanforderungen der angebenen Dokumente entsprechen.

Im Fall von Inkonsistenzen zwischen den Dokumenten des Zertifizierungsdienstes und den Dokumenten, zu denen die Zertifizierungsdienste konform sind, gelten folgende Regeln:

a) gesetzliche Anforderungen sind unmittelbar vor den Anforderungen der Dokumente des Zertifizierungsdienstes wirksam,
b) Inkonsistenzen ohne direkten Einfluss auf die Policy des Zertifizierungsdienste werden auf der Website des VDAinterpretativ klargestellt,
c) Inkonsistenzen mit direkten Einfluß auf die Policy des Zertifizierungsdienste - sofern davon qualifizierte Zertifikate betroffen sind, führen zu Anpassungen der betroffenen Dokumente des Zertifizierungsdienstes, um die Konsistenzen herzustellen,
d) in allen anderen Fällen haben die Anforderungen der Konformitätsdokumente Vorrang.

8.1 Frequency or circumstances of assessment / Häufigkeit und Umstände für Beurteilungen

Audits are conducted on principle once a year or as frequently as legally provided for or as provided for on the basis of the documents named in ⇨ 8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS / Prüfung der

Audits erfolgen grundsätzlich einmal jährlich, jedenfalls so häufig, wie gesetzlich oder auf Grund der in ⇨ 8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS / Prüfung der Konformität und andere

Konformität und andere Beurteilungen with which this GLOBALTRUST® Certificate Policy conforms.

Beurteilungen genannten Dokumenten zu denen diese GLOBALTRUST® Certificate Policy konform ist, vorgesehen ist.

8.2 Identity/qualifications of assessor / Identifikation/Qualifikation des Gutachters

External assessors are only consulted if they have an acceptable qualification in the sense of the definition of a ⇨ competent independent auditor (p25). For internal assessors, in particular for self-assessments, the operator ensures they have the acceptable qualification and are reponsible for their activity.

In each case, it is documented which person is actually active as the assessor.

Externe Gutachter werden nur herangezogen, wenn Sie eine ausreichende Qualifikation im Sinne der Definition von ⇨ kompetente unabhängige Auditstelle (p25) aufweisen. Bei internen Gutachtern, insbesondere im Rahmen von Self-Assessments, stellt der Betreiber die ausreichende Qualifikation sicher und haftet für die Tätigkeit.

In jedem Fall wird dokumentiert, welche Personen tatsächlich als Gutachter tätig wurden.

8.3 Assessor's relationship to assessed entity / Beziehung des Gutachters zur geprüften Einrichtung

In the case of an internal assessor, an employee of the operator is nominated as per the role concept (⇨ GLOBALTRUST® Certificate Security Policy). This person is independent in their audit activity and is not bound to any instructions.

Im Falle interner Gutachter wird ein Mitarbeiter des Betreibers gemäß Rollenkonzept (⇨ GLOBALTRUST® Certificate Security Policy) nominiert. Er ist für die Audittätigkeit unabhängig und an keine Weisungen gebunden.

8.4 Topics covered by assessment / Behandelte Themen der Begutachtung

The topics covered are documented in the assessment, in particular the standards or requirements under which an audit has been conducted, in the sense of the documents listed in ⇨ 8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS / Prüfung der Konformität und andere Beurteilungen (p168).

Die im Rahmen einer Begutachtung behandelten Themen, insbesondere nach welchen Standards bzw. Vorgaben im Sinne ⇨ 8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS / Prüfung der Konformität und andere Beurteilungen (p168) gelisteten Dokumenten eine Prüfung erfolgte, wird im Gutachten dokumentiert.

8.5 Actions taken as a result of a deficiency / Handlungsablauf bei negativem Ergebnis

If a particular attribute or quality of certification services in the sense of this

Kann auf Grund eines Gutachten eine bestimmte Eigenschaft oder

GLOBALTRUST® Certificate Policy cannot be confirmed by an assessment, adjustments will be immediately made to technical and organizational procedures in order to achieve the necessary attribute or quality.

If a particular attribute or quality of certification services cannot be achieved even after adjustment of technical and organizational procedures, it will be assessed as to whether an equivalent attribute or quality of certification services can be achieved. In this event, and if necessary, affected documents are adjusted, in particular the GLOBALTRUST® Certificate Policy or the GLOBALTRUST® Certificate Practice Statement.

If there are no alternatives available, the attribute or quality concerned is removed from the applicable documents.

Qualität der Zertifizierungsdienste im Sinne dieser GLOBALTRUST® Certificate Policy nicht bestätigt werden, dann erfolgt eine unverzügliche Anpassung der technischen und organisatorischen Abläufe um die erforderliche Eigenschaft oder Qualität zu erreichen.

Kann eine bestimmte Eigenschaft oder Qualität der Zertifizierungsdienste auch nach Änderung der technischen und organisatorischen Abläufe nicht erreicht werden, wird geprüft ob eine gleichwertige Eigenschaft oder Qualität der Zertifizierungsdienste möglich ist. Sofern erforderlich erfolgt in diesem Fall eine Anpassung der betroffenen Dokumente, insbesondere der GLOBALTRUST® Certificate Policy bzw. des GLOBALTRUST® Certificate Practice Statement.

Stehen keine Alternativen zur Verfügung wird die betroffene Eigenschaft oder Qualität der Zertifizierungsdienste aus den entsprechenden Dokumenten entfernt.

8.6 Communication of results / Mitteilung des Ergebnisses

Audit Attestation are published on the operator's website within a maximum of three months.

If necessary because of a negative result, all ⇨ affected parties are informed of the relevant results and measures in an appropriate fashion.

Gutachten auf Grundlage von Audits werden innerhalb von drei Monaten auf der Webseite des Betreibers veröffentlicht. Sofern auf Grund des negativen Ergebnisses erforderlich, erfolgt in geeigneter Form eine Verständigung aller Beteiligten über die sie betreffenden Ergebnisse und getroffenen Maßnahmen.

9. OTHER BUSINESS AND LEGAL MATTERS / REGELUNGEN FÜR SONSTIGE FINANZIELLE UND GESCHÄFTLICHE ANGELEGENHEITEN

9.1 Fees / Kosten

Certificates are issued and certification services are performed subject to a fee.

The operator reserves the right to offer individual services for free, particularly for testing purposes.

Time-stamping services are offered both at a cost and free of charge. Timestamps can be retrieved with authentication or anonymously. In all cases, timestamping fulfils the same technical security requirements. In the case of authenticated retrieval, it is noted which office has made the request.

Die Ausstellung von Zertifikaten und Erbringung von Zertifikatsdiensten erfolgt grundsätzlich kostenpflichtig.

Der Betreiber behält sich jedoch vor einzelne Dienste, insbesondere zu Testzwecken, kostenfrei anzubieten.

Zeitstempeldienste werden sowohl kostenpflichtig, als auch kostenfrei angeboten. Abfragen von Zeitstempel können sowohl authentisiert, als auch anonym erfolgen. In allen Fällen erfüllt der Zeitstempel dieselben technischen Sicherheitsanforderungen. Im Falle authentisierter Abfragen erfolgt die Aufzeichnung der abfragenden Stelle.

9.1.1 Certificate issuance or renewal fees / Kosten für Zertifikatsaustellung und -erneuerung

The applicable costs and conditions for each situation are published on the website of the CA or provided upon request.

Die jeweils gültigen Kosten und Konditionen werden auf der Website des VDA publiziert oder auf Anfrage beauskunftet.

9.1.2 Certificate access fees / Kosten für den Zugriff auf Zertifikate

Access to public certificates on the website of the operator is free-of-charge and not subject to non-technical restrictions.

Der Zugriff auf öffentliche Zertifikate ist im Rahmen der Website des Betreibers kostenfrei und unterliegt keinen unsachlichen Beschränkungen.

Reimbursement can be requested for individual information disclosures and confirmations, in particular about certificates that are no longer in use and no longer available online. The reimbursement is at most the actual cost of

Für individuelle Auskünfte und Bestätigungen, insbesondere über Zertifikate die nicht mehr in Verwendung sind und nicht mehr Online abrufbar sind, kann ein Kostenersatz eingehoben werden. Dieser

this activity.

Kostenersatz hat maximal die Höhe der tatsächlich anfallenden Kosten.

9.1.3 Revocation or status information access fees / Kosten für Widerruf oder Statusinformationen

The applicable costs and conditions for each situation are published on the website of the CA or provided upon request.

Die jeweils gültigen Kosten und Konditionen werden auf der Website des VDA publiziert oder auf Anfrage beauskunftet.

9.1.4 Fees for other services / Kosten für andere Dienstleistungen

The applicable costs and conditions for each situation are published on the website of the CA or provided upon request.

Die jeweils gültigen Kosten und Konditionen werden auf der Website des VDA publiziert oder auf Anfrage beauskunftet.

9.1.5 Refund policy / Kostenrückerstattung

The CA refunds costs for errors caused by the activities for which it is responsible.

In addition, the CA offers to replace products that no longer comply with the current state of the art free of charge, regardless of the cause. Reimbursement of costs and effort beyond this, in particular costs resulting from the installation or operation of certificates, are not possible.

Der VDA refundiert Kosten, die auf Grund von Fehlern seiner Tätigkeit verursacht wurden, die er zu verantworten hat.

Weiters bietet der VDA kostenlosen Ersatz bei Produkten an, die nicht mehr den aktuellen technischen Standards entsprechen, unabhängig davon, was die Ursache ist. Ein weitergehender Ersatz von Kosten und Aufwändungen, insbesondere Folgekosten, die sich aus Installation oder Betrieb von Zertifikaten ergeben ist in diesem Fall ausdrücklich ausgeschlossen.

9.2 Financial responsibility / Finanzielle Verantwortung

The CA is aware of its responsibility to have sufficient financial means available and ensures that the financing of certification services is secure over the long term using appropriate operational activities and financial resources.

Der VDA ist sich seiner Verantwortung über ausreichende finanzielle Mittel zu verfügen bewusst und stellt durch entsprechende betriebliche Tätigkeit und finanzielle Ausstattung sicher, dass die Finanzierung der Zertifizierungsdienste langfristig gesichert ist.

9.2.1 Insurance coverage / Versicherungsdeckung

The CA has arranged indemnity insurance with an insurance company of sufficient solvency that complies with legal requirements. The insurance arranged is documented internally.

Der VDA hat eine Haftpflichtversicherung bei einem Versicherungsunternehmen mit ausreichender Bonität, die den gesetzlichen Anforderungen entspricht abgeschlossen. Die abgeschlossene Versicherung ist intern dokumentiert.

9.2.2 Other assets / Andere Ressourcen für Betriebserhaltung und Schadensdeckung

The CA conducts an intensive exchange of experiences with equivalent entities to minimise and recognise (technical) threats early.

Der VDA betreibt zur Minimierung und zum frühzeitigen Erkennen neuer (technischer) Bedrohungen einen intensiven Erfahrungsaustausch mit vergleichbaren Einrichtungen.

9.2.3 Insurance or warranty coverage for end users / Versicherung oder Gewährleistung für Endnutzer

The CA does not provide insurance for end users. The warranty covers the features promised in the GLOBALTRUST® Certificate Policy. This does not affect or restrict warranties based on legal regulations.

Der VDA stellt keine Versicherung für Endnutzer zur Verfügung, die Gewährleistung erstreckt sich auf den in die GLOBALTRUST® Certificate Policy zugesicherten Eigenschaften. Davon nicht berührt oder beschränkt sind Gewährleistung aufgrund gesetzlicher Bestimmungen.

9.3 Confidentiality of business information / Vertraulichkeit von Geschäftsdaten

9.3.1 Scope of confidential information / Definition vertrauliche Geschäftsdaten

Four security levels are applied to all information for the governance of operations. These levels lead to different appropriate security controls.

- "Public" level: includes all data that is intended or suitable to be published. Access to this data is not restricted, but controls are used to

Zur Steuerung des Betriebs wurden für alle Informationen vier Sicherheitsstufen eingeführt, die zu entsprechend unterschiedlichen betrieblichen Sicherheitsmaßnahmen führen.

- "Public" level / **Stufe "öffentlich"**: Umfasst alle Daten, die zur Veröffentlichung bestimmt oder geeignet sind. Der Zugriff auf diese

ensure availability and maintain data integrity .

All further levels include data that is not suitable for publication. Access is restricted to the intended users of the data. The levels result from the scope of technical controls to maintain availability and data integrity.

- "Internal" level (administration, "restricted access"): includes all data used for orderly operations in a commercial sense, inc. documentation, accounting, administration of customers and potential customers, offers and billing. Access to this data is regulated with instructions and/or activity descriptions and restricted to employees and persons authorised by the operator.

- "Confidential" level (system administration, "confidential information"): includes all data used to maintain and continue operations. Access is restricted using instructions and/or activity descriptions and technical restrictions (eg. passwords).

- "Secure" level ("private information"): includes all data subject to special certification processes, in particular data that is directly connected to key and certificate generation. Access is restricted using instructions and/or activitiy descriptions, increased technical access restrictions (eg. password + token) and specific secure hardware components.

Daten ist nicht beschränkt, es werden jedoch Maßnahmen zum Erhalt der Verfügbarkeit und der Datenintegrität ergriffen.

Alle weiteren Stufen enthalten Daten, die nicht zur Veröffentlichung geeignet sind. Der Zugriff ist jeweils auf die für die Verwendung der Daten vorgesehenen Personen beschränkt. Abstufungen ergeben sich weiters im Umfang der technischen Maßnahmen zum Erhalt der Verfügbarkeit und der Datenintegrität.

- "Internal" level / **Stufe "intern" (administration, "eingeschränkte Zugänglichkeit")**: Umfasst alle Daten, die zur ordnungsgemäßen Betriebsführung im kaufmännischen Sinn dienen, inkl. interne Dokumentationen, Buchhaltung, Kunden- und Interessentenadministration, Angebots- und Rechnungslegung. Der Zugriff auf diese Daten wird durch Dienstanweisung bzw. Tätigkeitsbeschreibung geregelt und ist auf Mitarbeiter und Bevollmächtigte des Betreibers beschränkt.
- "Confidential" level / **Stufe "vertraulich" (systemadministration, "Vertrauliche Informationen")**: Umfasst alle Daten, die zur Aufrechterhaltung und Weiterführung des Zertifizierungsbetriebs dienen. Der Zugriff ist durch Dienstanweisung bzw. Tätigkeitsbeschreibung und durch technische Zugangsbeschränkungen (z.B. Passwörter) beschränkt.
- **"Secure" level / Stufe "geheim" ("Geheime Informationen")**: Umfasst alle Daten, die besonderen Zertifizierungsprozessen unterworfen sind, insbesondere sind dies die Daten die im unmittelbaren Zusammenhang mit Schlüsselerstellung und Zertifikatsgenerierung stehen. Der Zugriff ist durch Dienstanweisung bzw. Tätigkeitsbeschreibung, durch erhöhte technische Zugangsbeschränkungen (z.B. Passwörter+Token) und durch spezifische sichere Hardwarekomponenten beschränkt.

9.3.2 Information not within the scope of confidential information / Geschäftsdaten, die nicht vertraulich behandelt werden

Non-confidential business data is handled as per ⇨ "Public" level / **Stufe "öffentlich"**.

Nicht vertrauliche Geschäftsdaten werden im Sinne der ⇨ "Public" level / **Stufe "öffentlich"** behandelt.

9.3.3 Responsibility to protect confidential information / Zuständigkeiten für den Schutz vertraulicher Geschäftsdaten

The protection of confidential business data is seen as a part of the comprehensive information security concept (⇨ Management-Statement p12) and is conceptually governed in security goals and guidelines as per the GLOBALTRUST® Certificate Practice Statement and technically as per the GLOBALTRUST® Certificate Security Policy. The responsibilities come from the role concept (⇨ GLOBALTRUST® Certificate Security Policy).

Der Schutz vertraulicher Geschäftsdaten wird als Teil des umfassenden Informationssicherheitskonzepts angesehen (⇨ Management-Statement p12) und ist in den Sicherheitszielen und -leitlinien gemäß GLOBALTRUST® Certificate Practice Statement konzeptionell und gemäß GLOBALTRUST® Certificate Security Policy technisch geregelt. Die Zuständigkeiten ergeben sich aus dem Rollenkonzept (⇨ GLOBALTRUST® Certificate Security Policy).

9.4 Privacy of personal information / Datenschutz von Personendaten

All information kept on persons in the context of certification services is handled as confidential and is only used for the purposes of the certification service and for communication purposes in connection with the certification services of the CA.

Alle im Rahmen der Zertifizierungsdienste erhaltenen personenbezogenen Informationen werden vertraulich behandelt und nur für Zwecke des Zertifizierungsdienstes und für Verständigungszwecke im Zusammenhang mit den Zertifizierungsdienstleistungen des VDAs verwendet.

Legal obligations to store and transfer data remain unaffected. Data is never transmitted to a commercial data seller (address publishers, list brokers,...)

Gesetzliche Aufbewahrungs- und Übermittlungsverpflichtungen bleiben unberührt. Eine Datenweitergabe an kommerzielle Datenhändler (Adressenverlage, Listbroker, ...) wird ausdrücklich ausgeschlossen.

Certification data, that is personal in the sense of the General Data Protection Regulation 2016/679, is being deleted after the expiry of the legal retention obligation.

Zertifizierungsdaten werden, soweit sie personenbezogen im Sinne der Datenschutzgrundverordnung (DSGVO) 2016/679 sind, nach Ablauf der gesetzlichen Aufbewahrungspflicht gelöscht.

Service providers have no direct access to personally identifiable information but only receive data previously released by the management

Dienstleister haben keinen direkten Zugriff auf personenbezogene Daten, sondern erhalten nur Daten übermittelt, auf die sie rechtmäßigen

and the service provider have the right to dispose about them.

Anspruch haben und die vorher von der Geschäftsführung freigegeben wurden.

9.4.1 Privacy plan / Datenschutzkonzept

The CA fulfils all requirements as per the applicable Austrian and European data protection laws. If not otherwise regulated, the regulations of the Austrian data protection law applies in its current version on the basis of the data protection guidelines of the General Data Protection Regulation 2016/679 of the European Union or successor regulation of the European Union.

Der VDA erfüllt alle Auflagen nach den jeweils geltenden österreichischen und europäischen Datenschutzbestimmungen. Sofern nicht anders geregelt gelten die Bestimmungen des österreichischen Datenschutzgesetzes in der geltenden Fassung auf Basis der Datenschutzgrundverordnung (DSGVO) 2016/679 der Europäischen Union oder der ihr nachfolgenden Regelung der Europäischen Union.

9.4.2 Information treated as private / Definition von Personendaten

The CA understands private data as data on persons as per the current applicable European data protection law. If Austrian laws provide an extended scope, these data categories are also included in the scope of definition of private data.

Der VDA versteht unter Personaldaten personenbezogen Daten im Sinne der jeweils geltenden europäischen Datenschutzbestimmung. Soweit österreichische Bestimmungen eine erweiterten Umfang vorsehen, fallen auch diese Datenkategorien unter den Definitionsumfang von Personendaten.

9.4.3 Information not deemed private / Daten, die nicht vertraulich behandelt werden

The data of the subscriber is published only as necessary for the respective certification service (directory service, revocation service), for legal or other acceptable juridical reasons or at the explicit wish of the subscriber.

Veröffentlicht werden Daten des Signators ausschließlich auf Grund der Erfordernisse des jeweiligen Zertifizierungsdienstes (Verzeichnisdienst, Widerrufsdienst), aus gesetzlichen oder sonstigen zulässigen rechtlichen Gründen oder auf ausdrücklichen Wunsch des Signators.

9.4.4 Responsibility to protect private information / Zuständigkeiten für den Datenschutz

Data protection laws are observed on the basis of the role concept (⇨ GLOBALTRUST® Certificate Security Policy).

Die Einhaltung der Datenschutzbestimmungen erfolgt auf Grundlage des Rollenkonzepts (⇨ GLOBALTRUST® Certificate Security Policy).

9.4.5 Notice and consent to use private information / Hinweis und Einwilligung zur Nutzung persönlicher Daten

The CA meets all necessary information, declaration and consent obligations of the applicable data protection regulations.

Der VDA kommt allen erforderlichen Informations-, Aufklärungs- und Zustimmungspflichten der anzuwendenden Datenschutzbestimmungen nach.

9.4.6 Disclosure pursuant to judicial or administrative process / Auskunft gemäß rechtlicher oder staatlicher Vorschriften

The CA guarantees the fulfillment of information obligations towards ⇨ affected parties and in the context of obligations towards authorities and third parties, if they can prove a legitimate legal interest.

Der VDA garantiert die Erfüllung der Auskunftspflichten gegenüber dem ⇨ Betroffenen und im Rahmen der gesetzlichen Verpflichtungen gegenüber Behörden und Dritten, sofern diese ein berechtigtes rechtliches Interesse nachweisen.

9.4.7 Other information disclosure circumstances / Andere Bedingungen für Auskünfte

The CA does not pass on data on persons if it is not explicitly obligated or is not explicitly authorised by an ⇨ affected party to do so.

Der VDA gibt keine personenbezogene Daten weiter, wenn er dazu nicht ausdrücklich verpflichtet ist oder vom ⇨ Betroffenen ausdrücklich ermächtigt ist.

9.5 Intellectual property rights / Schutz-und Urheberrechte

The operator observes all necessary copyright laws and ensures in particular that it only uses or offers products or services for which it has the necessary copyright or license.

Der Betreiber beachtet alle erforderlichen urheberrechtlichen Bestimmungen und stellt insbesondere sicher, dass er nur Produkte oder Dienste verwendet bzw. anbietet, zu denen er die erforderlichen Urheberrechte bzw. Lizenzen besitzt.

9.6 Representations and warranties / Zusicherungen und Garantien

9.6.1 CA representations and warranties / Leistungsumfang des VDA

The scope of services of the CA is fully described in this GLOBALTRUST® Certificate Policy, the applicable GLOBALTRUST® Certificate Practice Statement and on the website of the operator

Der Leistungsumfang des VDA ist in dieser GLOBALTRUST® Certificate Policy, dem anzuwendenden GLOBALTRUST® Certificate Practice Statement und der Website des Betreibers vollständig beschrieben.

9.6.2 RA representations and warranties / Leistungsumfang der Registrierungsstellen

The current scope of services of the registration offices is described on the website of the operator and in no event exceeds the GLOBALTRUST® Certificate Policy.

Der aktuelle Leistungsumfang der Registrierungsstellen ist auf der Website des Betreibers beschrieben und geht in keinem Fall über die GLOBALTRUST® Certificate Policy hinaus.

9.6.3 Subscriber representations and warranties / Zusicherungen und Garantien des Signators

The general terms and conditions of the operator, this policy and the GLOBALTRUST Certificate Practice Statement apply.

Es gelten die Allgemeinen Geschäftsbedingungen des Betreibers, diese Policy sowie das GLOBALTRUST Certificate Practice Statement.

9.6.4 Relying party representations and warranties / Zusicherungen und Garantien für Nutzer

Because there is no contractual relationship, there are no warranties or guarantees for the user.

Es bestehen mangels eines Vertragsverhältnisses keine Zusicherungen und Garantien für Nutzer.

9.6.5 Relying party representations and warranties of other participants / Zusicherungen und Garantien anderer Teilnehmer

Because there is no contractual relationship, there are no warranties or guarantees for other parties.

Es bestehen mangels eines Vertragsverhältnisses keine Zusicherungen und Garantien für andere Teilnehmer.

9.7 Disclaimer of warranties / Haftungsausschlüsse

The CA is not liable if it can demonstrate that it is not responsible for breaching the obligations detailed above and has not acted negligently. This applies particularly if

- applicants or subscribers use issued certificates contrary to the applicable policy or
- users of signatures, certificates and public keys neglect to observe validity periods, existing suspensions, revocations or other restrictions on a signature confirmed by a certificate from the CA or
- the applicant submits falsified or otherwise manipulated documents and this manipulation or falsification is not conspicuous.

Der VDA haftet nicht, falls er nachweisen kann, dass ihn an der Verletzung der oben angeführten Verpflichtungen keine Schuld trifft und er nicht fahrlässig gehandelt hat. Dies trifft insbesondere zu, wenn

- Antragsteller oder Signatoren ausgegebene Zertifikate entgegen der gültigen Policy verwenden oder
- Nutzer von Signaturen, Zertifikaten und öffentliche Schlüssel es unterlassen Gültigkeitszeitraum, bestehende Sperren, Widerrufe oder sonstige Beschränkungen einer durch ein Zertifikat des VDAs bestätigten Unterschrift zu beachten oder
- der Antragsteller gefälschte oder sonstwie manipulierte Unterlagen vorliegt und deren Manipulation bzw. Fälschung nicht offensichtlich erkennbar ist.

Anbieter von Browsern haften nicht für Tätigkeiten des VDA oder seiner ausgestellten Zertifikate.

9.8 Limitations on liability / Haftungsbeschränkungen

The CA is responsible

- for observing this policy in its own realm of responsibility, in particular for the measures contained within for the prompt publication of suspension and revocation lists and for the maintenance of suspension and revocation standards named in this policy.
- for informing applicants, subscribers and users of signatures, certificates and public keys of their obligations to observe the policy. It is proved that this has been communicated if the certificates issued by the CA contain clear reference to the location of documentation for the applicable policy.

Der VDA haftet

- in seinem Verantwortungsbereich für die Einhaltung dieser Policy, insbesondere für die darin festgelegten Maßnahmen zur prompten Veröffentlichung von Sperr- und Widerrufslisten und die Einhaltung der in der Policy genannten Sperr- und Widerruf-Standards.
- dafür, dass Antragsteller, Signatoren und Nutzer von Signaturen, Zertifikaten und öffentlicher Schlüssel über ihre Verpflichtungen zur Beachtung der Policy in Kenntnis gesetzt wurden. Der Nachweis der Kenntnisnahme ist jedenfalls erbracht, wenn die vom VDA ausgegebenen Zertifikate eindeutige Verweise auf die Dokumentationsstellen für die anzuwendende Policy enthalten.

- for ensuring that the applicant data contained in a certificate is verified at the time that the certificate is issued and that the data does not differ from the data in registries used for verification or from documents submitted. Verification measures are documented in this policy. The registries used for verification depend on the kind of applicant and can include technically or regionally different sources. Which sources are used for which applicant is documented in detail in CA internal process documentation.

- for following up on evidence that a registration office or other persons or organisations authorised by the CA have established a deficiency in verification of identity and ensuring that certificates are not issued without sufficient identification of the subscriber and that certificates are immediately revoked if there is reason to doubt that an identity verification has not been conducted properly.
- that a qualified certificate for electronic signatures matches the signature creation data in a signature creation device, if this has been issued by the CA. Otherwise that the subscriber was in the possession of the SSCD at the time that the qualified certificate for electronic signatures was issued.

This responsibility applies similarly for all certificates that have been issued using enduser-sub-certificates.

Software producers that distribute the root certificates of the CA are not responsible for the content of the certificates. They are held harmless by the CA where this is legally permitted and does not affect procedures for which the software producer is responsible. The software producer is responsible for ensuring that validity status is displayed correctly in the certificates of the CA.

- dafür, dass die im Zertifikat enthaltenen Daten des Antragstellers zum Zeitpunkt der Ausstellung des Zertifikats überprüft wurden und keine Abweichungen der Daten gegenüber den Prüfverzeichnissen und den vorgelegten Dokumenten festgestellt wurden. Die Prüfmaßnahmen sind in dieser Policy dokumentiert, die verwendeten Prüfverzeichnisse ergeben sich aus der Art des Antragstellers und können sachlich und regional unterschiedliche Quellen umfassen. Welche Quellen für welche Antragsteller verwendet werden, wird im Detail im Rahmen der VDA-internen Prozessdokumentation geregelt.
- dafür, dass Hinweisen einer fehlerhaften Identitätsprüfung durch eine Registrierungsstelle oder anderen von der VDA autorisierten Personen und Stellen in jedem Fall nachgegangen wird und Zertifikate ohne ausreichende Identifikation des Signators nicht freigegeben oder bei Zweifel einer ordnungsgemäßen Identitätsprüfung unverzüglich widerrufen werden.
- dafür, dass ein qualifiziertes Zertifikat für elektronische Signaturen zu den Signaturerstellungsdaten der Signaturerstellungseinheit passt, sofern diese vom VDA erstellt wurde. Andernfalls dafür, dass der Signator zum Zeitpunkt der Ausstellung eines qualifizierten Zertifikates für elektronische Signaturen im Besitz des SSCD war.

Diese Haftung gilt in gleicher Weise für alle Zertifikate, die mittels Endkunden-Sub-Zertifikate ausgestellt wurden.

Softwarehersteller, die die Root-Zertifikate des VDA vertreiben, haften nicht für den Inhalt der Zertifikate. Sie werden vom VDA, soweit dies rechtlich zulässig ist und keine Vorgänge betrifft, die der Softwarehersteller zu verantworten hat, klag und schadlos gehalten. Jedenfalls zu verantworten hat der Softwarehersteller die korrekte Anzeige des Gültigkeitsstatus eines Zertifikates des VDA.

9.9 Indemnities / Schadensersatz / Indemnities

The CA guarantees indemnities for proven damages for which it is responsible.

Der VDA gewährleistet Schadenersatz für nachgewiesene Schäden, die er zu verantworten hat.

9.10 Term and termination / Gültigkeitsdauer der CP und Beendigung der Gültigkeit / Term and termination

9.10.1 Term / Gültigkeitsdauer der CP / Term

The GLOBALTRUST® Certificate Policy is valid until revoked.

Die GLOBALTRUST® Certificate Policy ist bis auf Widerruf gültig.

9.10.2 Termination / Beendigung der Gültigkeit / Termination

The validity of the GLOBALTRUST® Certificate Policy is terminated by
- revocation or
- notice of termination of the activity of the CA at the regulatory authority or
- the issuance of a new GLOBALTRUST® Certificate Policy

In all cases, ⇨ affected parties are informed in an appropriate fashion and the information is published on the website of the operator.

Die Gültigkeit der GLOBALTRUST® Certificate Policy endet durch
- Widerruf oder
- Anzeige der Einstellung der Tätigkeit des VDA bei der Aufsichtsbehörde oder
- Ausgabe einer neuen GLOBALTRUST® Certificate Policy

In allen Fällen erfolgt eine Verständigung der ⇨ Beteiligten in geeigneter Form, jedenfalls eine Veröffentlichung auf der Website des Betreibers.

9.10.3 Effect of termination and survival / Auswirkung der Beendigung

Consequences of termination depend on the kind of termination and are stated in the communication to ⇨ affected parties and the publication on the website of the operator.

Die Auswirkungen der Beendigung ergeben sich aus der Art der Beendigung und werden jedenfalls in der Verständigung der ⇨ Beteiligten und derVeröffentlichung auf der Website des Betreibers dargestellt.

9.11 Individual notices and communications with participants / Individuelle Mitteilungen und Absprachen mit Beteiligten

Individual communications will not be exchanged and agreements will not

Es erfolgen keine individuellen Mitteilungen und Absprachen mit ⇨

be made with ⇨ involved parties who contravene the GLOBALTRUST® Certificate Policy, the GLOBALTRUST® Certificate Practice Statement or other conditions necessary for certification services.

Beteiligten, die der GLOBALTRUST® Certificate Policy, dem GLOBALTRUST® Certificate Practice Statement oder sonstigen für die Erbringung der Zertifizierungsdienste wesentlichen Bestimmungen widersprechen.

9.12 Amendments / Änderungen

9.12.1 Procedure for amendment / Verfahren bei Änderungen

Amendments are assigned, planned and implemented as per the role concept (⇨ GLOBALTRUST® Certificate Security Policy).

Changes, revisions and updates to the GLOBALTRUST® Certificate Policy, the GLOBALTRUST® Certificate Practice Statement, and the GLOBALTRUST® Certificate Security Policy are approved by the Board. The review take place at least once a year.

Änderungen werden im Rahmen des Rollenkonzepts (⇨ GLOBALTRUST® Certificate Security Policy) beauftragt, geplant und durchgeführt..

Änderungen, Revisionen und Aktualisierungen an GLOBALTRUST® Certificate Policy, dem GLOBALTRUST® Certificate Practice Statement und der GLOBALTRUST® Certificate Security Policy werden von der Geschäftsführung genehmigt. Der Review erfolgt mindestens einmal jährlich.

9.12.2 Notification mechanism and period / Benachrichtigungsmechanismen und –fristen

Changes are communicated electronically, where permitted and technically possible. If the changes affected many ⇨ parties, the changes are published on the website of the operator.

If it is not possible or not permitted to communicate the change electronically and the information on the website of the operator is not sufficient, other suitable methods of communicate are used, in particular post or courier services.

Die Benachrichtigung über Änderungen erfolgt - soweit zulässig und technisch möglich - auf elektronischen Wege. Betreffen Änderungen eine größer Zahl an ⇨ Beteiligten werden Änderungen auf der Website des Betreibers veröffentlicht.

Ist eine Benachrichtigung auf elektronischen Wege nicht möglich oder nicht zulässig und die Information auf der Wesite des Betreibers nicht ausreichend, werden andere geeignete Wege der Verständigung benutzt, insbesondere die Zustellung der Informationen durch Postdienste oder Boten.

Changes are communicated to ⇨ parties as early as possible. It is likewise communicated to the ⇨ parties how they can respond.

Änderungen werden den ⇨ Beteiligten so frühzeitig wie möglich mitgeteilt. Ebenso welche Reaktionsmöglichkeiten die ⇨ Beteiligten haben.

9.12.3 Circumstances under which OID must be changed / Bedingungen für OID-Änderungen

Changes of OID, in particular changes in meaning, are only anticipated in the event of compulsory legal requirements or the requirements of the responsible standardisation committee.

Änderungen von OID-Kennzeichen insbesondere Änderungen der Bedeutung sind nur im Falle zwingender gesetzlicher Vorgaben oder durch Vorgaben der zuständigen Standardisierungsgremien vorgesehen.

9.13 Dispute resolution provisions / Bestimmungen zur Schlichtung von Streitfällen

The CA reserves the right to suggest arbitration services out of court. These arbitration services are published on the website of the operator.

Der VDA behält sich vor außergerichtliche Schlichtungsstellen vorzuschlagen. Diese Schlichtungsstellen werden auf der Website des Betreibers veröffentlicht (⇨ http://www.globaltrust.eu/impressum.html).

Complaints can be submitted in any way communicated by the TSP (including telefon and email). They are documented internally, checked by responsible positions, observed and used to improve services.

Beschwerden können auf jedem vom VDA bekannt gegebenen Kommunikationsweg (inklusive Telefon und eMail) übermittelt werden. Sie werden intern dokumentiert, von den zuständigen Stellen geprüft, beachtet und zur Verbesserung der Dienste herangezogen.

In case of questions about interpretation or implementation of this GLOBALTRUST® Certificate Policy, all parties have the right to consult experts or institutions. The VDA will answer to their proposals and include them in its decisions.

Im Fall von Fragen zur Interpretation oder Umsetzung dieser GLOBALTRUST® Certificate Policy können alle Beteiligte geeignete Sachverständige oder Einrichtungen zur außergerichtlichen Klärung von Streitfragen beiziehen. Der VDA wird auf Vorschläge dieser Sachverständigen bzw. Einrichtungen eingehen und in seinen Entscheidungen berücksichtigen.

Attention is invited to the fact that all parties at any time have the right to call the RTR GmbH, which is the inspecting authority, to clarify open questions. The VDA will consider the opinions and proposals of the RTR GmbH

Ausdrücklich wird darauf hingewiesen, dass alle Beteiligte jederzeit die Aufsichtsstelle des VDA, die RTR GmbH zur Klärung offener Fragen anrufen können. Der VDA wird die Stellungnahmen und Vorschläge der Aufsichtsstelle beachten.

9.14 Governing law / Gerichtsstand

The operator is a company registered in the Austrian commercial register.

Its place of jurisdiction is in Vienna. Austrian law applies.

The CA is subordinate to the regulatory authorities responsible as per the following regulations:

- REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC in its current version or a succeeding (superseding or additional) regulation of the European Union
- the Signature Law [SVG] together with the Signature Act [SVV] in the respectively current versions

  technical standards and legal requirerments as per ⇨ 8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS / Prüfung der Konformität und andere Beurteilungen (p168)

The contact data of the regulatory authorities responsible and the registration information of the CA are published on the website of the CA.

Der Betreiber ist ein im österreichischen Firmenbuch protokolliertes Unternehmen.

Gerichtsstand ist Wien. Es gilt österreichisches Recht.

Der VDA untersteht den zuständigen Aufsichtsbehörden gemäß folgender Bestimmungen:

- VERORDNUNG (EU) Nr. 910/2014 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG [eIDAS-VO] in der geltenden Fassung oder einer nachfolgenden (ersetzenden oder ergänzenden) Regelung der Europäischen Union
- Signatur- und Vertrauensdienstegesetz [SVG] in Verbindung mit der Signatur- und Vertrauensdiensteverordnung [SVV] in der jeweils gültigen Fassung
- den technischen Standards und rechtlichen Vorgaben gemäß ⇨ 8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS / Prüfung der Konformität und andere Beurteilungen (p168)

Die Kontaktdaten der zuständigen Aufsichtsbehörden und die erforderlichen Registerinformationen des VDA werden auf der Website des VDA veröffentlicht.

9.15 Compliance with applicable law / Einhaltung geltenden Rechts

All certification services described in this document are performed as per the Austrian Signature Law, including the Signature Act [SVG] + [SVV] or the EU signature regulation [eIDAS-VO] or a national law of another state of the European Union or another state with an agreement with the

Alle in diesem Dokument beschriebenen Zertifizierungsdienste werden gemäß österreichischem Signatur- und Vertrauensdienstegesetz inkl. Signatur- und Vertrauensdiensteverordnung [SVG] + [SVV] oder der EU Signaturverordnung [eIDAS-VO] oder nach einem nationalen Gesetz

European Economic Area, so that the assessment of security requirements for secure signature creation devices is appropriate as per the EU signature regulation [eIDAS-VO] or another law equivalent to the EU signature regulation [eIDAS-VO].

eines anderen Mitgliedstaaten der Europäischen Union oder von anderen Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum erlassen wurde, dass zur Beurteilung der Sicherheitsanforderungen für sichere Signaturerstellungseinheiten nach der EU Signaturverordnung [eIDAS-VO] geeignet ist oder sonstiger gesetzlicher Bestimmungen, die der EU Signaturverordnung [eIDAS-VO] gleichwertig sind, erbracht.

Technical implementation is performed as per ETSI standard [ETSI TS 101 456] including successors: [ETSI EN 319 401], [ETSI EN 319 411-1], [ETSI EN 319 411-2]. Extensions for the issuance of qualified certificates are performed as per [ETSI EN 319 412] or equivalent standards. In addition, the [CWA-14167-1] requirements for the operation of certification services and the [EG-REF] requirements for issuing secure signature creation devices are fulfilled.

Die technische Umsetzung erfolgt gemäß ETSI-Standard [ETSI TS 101 456] inklusive Nachfolger: [ETSI EN 319 401], [ETSI EN 319 411-1], [ETSI EN 319 411-2], die Erweiterungen für die Ausgabe qualifizierter Zertifikate gemäß [ETSI EN 319 412] oder vergleichbarer gleichwertiger Standards. Weiters werden die Anforderungen [CWA-14167-1] für den Betrieb des Zertifizierungsdienstes und [EG-REF] zur Ausstellung sicherer Signaturerstellungseinheiten erfüllt.

The security concept fulfils the requirements of the EU signature regulation [eIDAS-VO], [SVG], [ETSI TS 101 456] including successors: [ETSI EN 319 401], [ETSI EN 319 411-1], [ETSI EN 319 411-2] and [CWA-14167-1] and is declared in the GLOBALTRUST® Certificate Security Policy. It applies for all certification services run by the operator, including the timestamping service, mobile signatures and server-based signature services.

Das Sicherheitskonzept erfüllt jedenfalls die Anforderungen der EU Signaturverordnung [eIDAS-VO], [SVG], [ETSI TS 101 456] inklusive Nachfolger: [ETSI EN 319 401], [ETSI EN 319 411-1], [ETSI EN 319 411-2] und [CWA-14167-1] und ist im Dokument GLOBALTRUST® Certificate Security Policy dargestellt. Sie gilt für alle vom Betreiber betriebenen Zertifizierungsdienste, einschließlich Zeitstempeldienste, mobiler Signaturen und serverbasierte Signaturdienste.

All certification services described in this GLOBALTRUST® Certificate Policy are performed as per the requirements of the EU signature regulation [eIDAS-VO], the Austrian Signature Law [SVG], the Austrian Signature Act [SVV], the [ETSI TS 101 456] including successors: [ETSI EN 319 401], [ETSI EN 319 411-1] and (QCP Public + SSCD) policy requirements relating to the performance of certification services and [ETSI EN 319 411-2] relating to other certificate services and the [CWA-14167-1] security requirements, as well as the [ETSI EN 319 412] requirements for issuing qualified certificates. If individual regulations contradict one another, the regulation

Alle in dieser GLOBALTRUST® Certificate Policy beschriebenen Zertifizierungsdienste werden gemäß den Anforderungen der EU Signaturverordnung [eIDAS-VO], dem österreichischen Signatur- und Vertrauensdienstegesetz [SVG], der österreichischen Signatur- und Vertrauensdiensteverordnung [SVV], den Policy-Anforderungen [ETSI TS 101 456] inklusive Nachfolger: [ETSI EN 319 401], [ETSI EN 319 411-1] (QCP Public + SSCD) im Zusammenhang mit der Erbringung qualifizierter Zertifizierungsdienste und [ETSI EN 319 411-2] im Zusammenhang sonstiger Zertifizierungsdienste und den

that comes closest to the technical and legal requirements of a secure certification service will be adopted.

Sicherheitsanforderungen [CWA-14167-1] erbracht. Weiters [ETSI EN 319 412] für die Erstellung qualifizierter Zertifikate. Sofern einzelne Bestimmungen in Konflikt stehen, wird die jeweils aktuellere Bestimmung, die den technischen und rechtlichen Anforderungen sicherer Zertifzierungsdienste am nächsten kommt, herangezogen.

This policy has been drafted in compliance with signature regulations and constitutes the basis of the subscriber's usage of GLOBALTRUST® certificates together with applicable agreements and the notices of the regulatory authority, as necessary according to [eIDAS-VO], [SVG] or other laws.

Diese Policy wurde in Übereinstimmung mit den Signaturbestimmungen verfasst und bildet gemeinsam mit allfälligen individuellen Vereinbarungen und der - soweit gemäß [eIDAS-VO], [SVG] oder anderer Bestimmungen erforderlichen - Anzeige bei der Aufsichtsbehörde die Grundlage für die Verwendung von GLOBALTRUST® Zertifikaten durch den Signator.

Certification services are operated as per [CWA-14167-1] for all certificates and services governed by this policy. The operational technical details are documented in the GLOBALTRUST® Certificate Practice Statement. If specific precautions relevant to security must be met, these are documented in the GLOBALTRUST® Certificate Security Policy.

Der Betrieb des Zertifizierungsdienstes erfolgt für alle in dieser Policy geregelten Zertifikate und Dienste gemäß [CWA-14167-1]. Die betriebstechnischen Details sind in einem eigenen GLOBALTRUST® Certificate Practice Statement dokumentiert. Soweit spezifische sicherheitsrelevante Vorkehrungen zu treffen sind, sind diese in der GLOBALTRUST® Certificate Security Policy dokumentiert.

9.16 Miscellaneous provisions / Sonstige Bestimmungen

9.16.1 Entire agreement/ Vollständigkeitserklärung

The CA is obligated to ensure that all requirements that arise from certification services are documented and the requirements stated in ⇨ 4.5.1 Subscriber private key and certificate usage / Nutzung des privaten Schlüssels und des Zertifikates durch den Signator (p66) are brought to the attention of the subscriber and that it is contractually agreed that these requirements will be fulfilled.

The CA is responsible for observing all business processes for certification services.

Der VDA verpflichtet sich sicherzustellen, dass alle Anforderungen, die sich aus den Zertifizierungsdiensten ergeben dokumentiert sind und die in ⇨ 4.5.1 Subscriber private key and certificate usage / Nutzung des privaten Schlüssels und des Zertifikates durch den Signator (p66) dargelegt sind, dem Signator zur Kenntnis gebracht wird und die Erfüllung vertraglich vereinbart wird.

Der VDA ist verantwortlich für die Einhaltung aller Geschäftsprozesse zu den Zertifizierungsdiensten.

9.16.2 Assignment / Abgrenzungen

The GLOBALTRUST® Certificate Security Policy, the GLOBALTRUST® Certificate Practice Statement and the GLOBALTRUST® Certificate Security Policy are together the basis of the business concept submitted to the regulatory authority for approval. Other conditions not described in this document do not apply.

Die GLOBALTRUST® Certificate Security Policy, das GLOBALTRUST® Certificate Practice Statement und die GLOBALTRUST® Certificate Security Policy gemeinsam sind Grundlage des der Aufsichtsbehörde zur Genehmigung vorgelegten Betriebskonzepts, sonstige - nicht in diesen Dokumenten beschriebenen - Bestimmungen kommen nicht zur Anwendung.

9.16.3 Severability / Salvatorische Klausel

If parts of this agreement are void and legal requirements change, this affects only those parts of this agreement. Other parts of the agreement remain in force.

Sollten Bestandteile dieser Vereinbarung unwirksam sein und sich gesetzliche Bestimmungen ändern, die die sachlichen Bestandteile dieser Vereinbarung berühren, bleiben die anderen Teile der Vereinbarung in Kraft.

9.16.4 Enforcement (attorneys' fees and waiver of rights) / Vollstreckung (Anwaltsgebühren und Rechtsmittelverzicht)

Certification services based on this GLOBALTRUST® Certificate Policy are undertaken only after approval by the responsible regulatory authority.

Der Zertifizierungsbetrieb auf Basis dieser GLOBALTRUST® Certificate Policy wird erst nach Genehmigung durch die zuständigen Aufsichtsstellen vorgenommen.

9.16.5 Force Majeure / Höhere Gewalt

The CA and the operator are not liable in the event of force majeure.

Keine Haftung des VDA und des Betreibers im Falle höherer Gewalt.

9.17 Other provisions / Other provisions

No change is made to this GLOBALTRUST® Certificate Security Policy if

- it is an editorial correction only (correction of spelling, numbering,

Es liegt keine Änderung dieser GLOBALTRUST® Certificate Security Policy vor, wenn

- ausschließlich redaktionelle Korrekturen (Korrektur von

reference, link or grammar mistakes)

- individual fragments of text are moved to other sections or chapters, or explanatory subheadings or comments are inserted.

Changes of this kind will be noted on the website.

Schreibfehlern, Nummerierungsfehlern, Verweis- und Linkfehlern, Grammatik) vorgenommen werden oder

- einzelne Textteile in andere Abschnitte oder Kapitel verlegt werden, erläuternde Zwischenüberschriften oder Kommentare eingefügt werden.

Auf derartige Änderungen wird auf der Website des Betreibers hingewiesen.

SCHEDULE / VERZEICHNISSE

Author(s) and validity / Autor(en) und Gültigkeitshistorie

Previous versions of this document are available on the website of the operator.

Each document is valid between the date it becomes valid and the date the successor document becomes valid. If not otherwise marked, the validity of the old document ends the day before the new document becomes valid.

Die historischen Versionen dieses Dokuments sind über die Website des Betreibers abrufbar.

Die Gültigkeit der jeweiligen Dokumente ergibt sich aus dem Beginndatum der Gültigkeit und dem Beginndatum der Gültigkeit des nächstfolgenden Dokuments. Sofern nicht anders vermerkt endet die Gültigkeit des alten Dokuments am Vortag der Gültigkeit des neuen Dokuments.

Name	Version	Date / Stand	File / Datei	Comment / Kommentar
	Version 1.0 bis Version 1.4			internal only / interne Fassungen, die nicht in Kraft traten
Hans G. Zeger	Version 1.5	10.08.2006	http://www.globaltrust.eu/static/globaltrust-certificate-policy.20060810.pdf	Stammfassung
Hans G. Zeger	Version 1.6	12.04.2007	http://www.globaltrust.eu/static/globaltrust-certificate-policy.20070412.pdf	Ergänzungen lt. Änderungshistorie Version 1.6 Änderungen I 12. April 2007
Hans G. Zeger	Version 1.7	1th April 2014		internal only / interne Fassungen, die nicht in Kraft trat (Versicherungsversion) Ergänzungen lt. Änderungshistorie Version 1.7 Änderungen II 1. April 2014
Hans G. Zeger	Version 1.8	1th Juni 2014		internal only / interne Fassungen, die nicht in Kraft trat (Antragsversion) Ergänzungen lt. Änderungshistorie Version 1.8 Änderungen III 1. Juni 2014
Hans G. Zeger	Version 1.8a	1th Oktober 2014		internal only / interne Fassungen, die nicht in Kraft trat Ergänzungen lt. Änderungshistorie Version 1.8a Änderungen IV 1. Oktober 2014
Hans G. Zeger	Version 1.8b	1th Februar 2015	http://www.globaltrust.eu/static/globaltrust-certificate-policy.20150201.pdf	Ergänzungen lt. Änderungshistorie Version 1.8b Änderungen V 1. Februar 2015
Hans G. Zeger	Version 1.8c	1th Juni 2015	http://www.globaltrust.eu/static/globaltrust-certificate-policy.20150601.pdf	Ergänzungen lt. Änderungshistorie Version 1.8c Änderungen VI 1. Juni 2015

Hans G. Zeger	Version 1.8d	1th Juni 2016		Vorbereitungsversion für Änderungen gemäß eIDAS-VO, wurde nicht in Kraft gesetzt.
Hans G. Zeger	Version 2.0	22th June 2017	http://www.globaltrust.eu/static/globaltrust-certificate-policy.20170622.pdf	Ergänzungen lt. Änderungshistorie Version 2.0 Änderungen VII 1. Juni 2017
Hans G. Zeger	Version 2.0b	13th August 2018	http://www.globaltrust.eu/static/globaltrust-certificate-policy.20180813.pdf	Ergänzungen lt. Änderungshistorie Version 2.0b Änderungen VIII 13. August 2018
Hans G. Zeger	Version 2.0c	15th January 2019	http://www.globaltrust.eu/static/globaltrust-certificate-policy.20190115.pdf	Ergänzungen lt. Änderungshistorie Version 2.0c Änderungen IX 15. Jänner 2019
Hans G. Zeger	Version 2.0d	19th April2019		Vorbereitungsversion für EV- und qualifizierte Serverzertifikate, wurde nicht in Kraft gesetzt
Hans G. Zeger	Version 2.0e	15th June 2019	http://www.globaltrust.eu/static/globaltrust-certificate-policy.20190625.pdf	Ergänzungen lt. Änderungshistorie Version 2.0e Änderungen 25. Juni 2019
Hans G. Zeger	Version 2.0f	13th December 2019	http://www.globaltrust.eu/static/globaltrust-certificate-policy.20191213pdf	Ergänzungen lt. Änderungshistorie Version 2.0f Änderungen 13. Dezember 2019
Hans G. Zeger	Version 2.0g	3rd April 2020	http://www.globaltrust.eu/static/globaltrust-certificate-policy.pdf	Ergänzungen lt. Änderungshistorie Version 2.0g Änderungen 3. April 2020

APPENDIX / ANHANG

APPENDIX / ANHANG A: DOCUMANTATION / DOKUMENTATION

1 BIBLIOGRAPHY / BIBLIOGRAPHIE

Die Listung der Dokumente erfolgt mit Stand 3rd April 2020. Zur Anwendung kommt die jeweils gültige Fassung bzw. der entsprechende zutreffende Folgestandard. Die eingesetzten Dokumente und Standards sind intern dokumentiert und werden laufend aktualisiert.

The documents are listed as of 3rd April 2020. The applicable version or the corresponding applicable follow-up standard is used. The documents and standards used are documented internally and are continuously updated.

1 [ADOBE-TRUST] Adobe Approved Trust List Technical Requirements Version 2.0 Stand: 2017/06/28
Original-Site: https://helpx.adobe.com/acrobat/kb/approved-trust-list2.html
Adobe Systems Inc. (Corporate headquarters), USA-95110-2704 San Jose, CA, 345 Park Avenue

2 [APPLE-CA] Program Requirements, Submission Process & Root Acceptance Stand: 2018/03/14
Original-Site: https://www.apple.com/certificateauthority/ca_program.html

3 [ASIG-EXT] Hollosi A., X.509 Zertifikatserweiterungen für die Verwaltung, X509ext - v1.0.3 Stand: 2005/02/21
Original-Site: http://www.cio.gv.at/it-infrastructure/pki/X509ext-1.0.3-20050221.pdf
Stabsstelle IKT-Strategie des Bundes (CIO Chief Information Officer), A-1010 Wien, Ballhausplatz 2

4 [ASIG-LAY] Layout Amtssignatur v2.0.1 Stand: 2014/12/31
Original-Site: http://www.ref.gv.at/AG-RS-Amtssignatur-las-2-0-1.3100.0.html
Stabsstelle IKT-Strategie des Bundes (CIO Chief Information Officer), A-1010 Wien, Ballhausplatz 2

5 [ASIG-LTF] Leitfaden Amtssignatur v1.0.0 Stand: 2009/01/13
Original-Site: http://www.ref.gv.at/AG-RS-Amtssignatur-las-1-4-0.2195.0.html
Bundeskanzleramt (BKA), A-1014 Wien, Ballhausplatz 2

6 [ASIG-MOA] MOA-Amtssignaturen - MOA-AS Spezifikation Version 1.0.1 Stand: 2008/02/11
Original-Site: https://demo.egiz.gv.at/plain/content/download/454/2634/file/Spezifikation-MOA-AS.pdf
EGIZ E-Government Innovationszentrum, A-8010 Graz, Inffeldgasse 16a

7 [ASR] Richtlinien der Österreichischen Notariatskammer vom 19.10.2006 für die Ausstellung und die Ausgabe von Ausweisen und Signaturkarten für die elektronische Notarsignatur, elektronische Kandidatensignatur und elektronische Beurkundungssignatur idF 21. Stand: 2016/10/21

8 [ASZ] Karlinger G., Amtssignaturzertifikate (ASZ) - Allgemeine Richtlinien für Amtssignaturzertifikate in der Verwaltung, Version 1.0.0 Stand: 2005/04/06
Original-Site: http://reference.e-government.gv.at/Amtssignaturzertifikate-erarb.1095.0.html
Stabsstelle IKT-Strategie des Bundes (CIO Chief Information Officer), A-1010 Wien, Ballhausplatz 2

9 [BMI-SZR] SZR 2.0 Anwendungsdokumentation extern Version 2.0 Stand: 2014/12/05
IT-Service - BM für Inneres (BMI), A-1090 WIEN, Berggasse 43

10 [BNA-IDV] Bestätigte Identifizierungsverfahren nach Art 24 Abs 1 litera d) eIDAS Stand: 2019/05/06
Original-Site: bundesnetzagentur.de

11 [BSI-100-1] BSI-Standard 100-1: Managementsysteme für Informationssicherheit (ISMS) v1.5 Stand: 2008/05/01
Original-Site:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/standar

d_1001_pdf.pdf?__blob=publicationFile
Bundesamt für Sicherheit in der Informationstechnik (BSI), D-53175 BONN, Godesberger Allee 185-189

12 [BSI-100-2] BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise v2.0 Stand: 2008/05/01
Original-Site:
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/Standard201/ITGStandard201_node.html
Bundesamt für Sicherheit in der Informationstechnik (BSI), D-53175 BONN, Godesberger Allee 185-189

13 [BSI-100-3] BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz v2.5 Stand: 2008/05/01
Original-Site:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/standard_1003_pdf.pdf?__blob=publicationFile
Bundesamt für Sicherheit in der Informationstechnik (BSI), D-53175 BONN, Godesberger Allee 185-189

14 [BSI-100-4] BSI-Standard 100-4 Notfallmanagement v1.0 Stand: 2008/11/01
Original-Site:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/standard_1004_pdf.pdf?__blob=publicationFile
Bundesamt für Sicherheit in der Informationstechnik (BSI), D-53175 BONN, Godesberger Allee 185-189

15 [BSI-GRUND] BSI - IT Grundschutz - Beschreibung Stand: 2010/04/07
Original-Site:
https://www.bsi.bund.de/cln_174/DE/Themen/ITGrundschutz/StartseiteITGrundschutz/startseiteitgrundschutz_node.html
Bundesamt für Sicherheit in der Informationstechnik (BSI), D-53175 BONN, Godesberger Allee 185-189

16 [BSI-TR-02102-2] BSI TR-02102-2 Technische Richtlinie - Kryptographische Verfahren: Empfehlungen und Schlüssellängen Version: 2019-01 Stand: 2019/02/22
Original-Site:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2.html
Bundesamt für Sicherheit in der Informationstechnik (BSI), D-53175 BONN, Godesberger Allee 185-189

17 [BSI-TR-03116] Technische Richtlinie BSI TR-03116 Kryptographische Vorgaben für Projekte der Bundesregierung Stand: 2019/05/02

18 [BSI-TR-03125] BSI TR-03125 Beweiswerterhaltung kryptographisch signierter Dokumente Stand: 2008/05/01
Original-Site: https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03125/index_htm.html
Bundesamt für Sicherheit in der Informationstechnik (BSI), D-53175 BONN, Godesberger Allee 185-189

19 [BSI-TR-03147-ANFORDERUNGEN] Anforderungskatalog zur Prüfung von Identifikationsverfahren gemäß TR-03147 in Version 1.0 Stand: 2018/12/11

20 [BSI-TR-03147-PRÜFBERICHT] Prüfberichtsvorlage zur Prüfung von Identifikationsverfahren gemäß TR-03147 in Version 1.0 Stand: 2018/12/11

21 [BSI-TR-03147] Technische Richtlinie TR-03147 Vertrauensniveaubewertung von Verfahren zur Identitätsprüfung natürlicher Personen Version 1.0.5 Stand: 2018/12/05
Original-Site: https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03147/index_htm.html

22 [BSI-TR-CRYPTO] Kryptographische Verfahren - Empfehlungen und Schlüssellängen, Version 2019 02 Stand: 2019/02/01
Original-Site:
https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/technischerichtlinien_node.html
Bundesamt für Sicherheit in der Informationstechnik (BSI), D-53175 BONN, Godesberger Allee 185-189

23 [BÜRGERKARTE-STD] Standardisierte Key- und Infoboxen der österreichischen Bürgerkarte Stand: 2005/03/01
Original-Site:
http://www.buergerkarte.at/konzept/securitylayer/spezifikation/20140114/infoboxes/infoboxes.html
IT-Service - BM für Inneres (BMI), A-1090 WIEN, Berggasse 43

24 [BÜRGERKARTE] Die österreichische Bürgerkarte - Dokumentation und Spezifikation Version 1.2.0 Stand: 2014/01/14
Original-Site: http://www.buergerkarte.at/konzept/securitylayer/spezifikation/aktuell/

25 [CABROWSER-BASE] CA/Browser Forum: Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates v1.6.8 Stand: 2020/03/01

Original-Site: https://cabforum.org/baseline-requirements-documents/
CA/Browser Forum, UUU keine aktuelle Adresse verfügbar

26 [CABROWSER-EV] Guidelines For The Issuance And Management Of Extended Validation Certificates v1.7.1 Stand: 2020/01/31
Original-Site: https://cabforum.org/extended-validation/
CA/Browser Forum, UUU keine aktuelle Adresse verfügbar

27 [CABROWSER-NETSEC] CABForum Network Security Controls v1.1 Stand: 2017/10/31
Original-Site: https://cabforum.org/documents/#Network-and-Certificate-System-Security
CA/Browser Forum, UUU keine aktuelle Adresse verfügbar

28 [CARDOS53-ASIT-QES] Bestätigung A-SIT-1.108 Sichere Signaturerstellungseinheit CardOS V5.3 QES, V1.0 Stand: 2016/06/24
Original-Site: http://www.a-sit.at/de/bestaetigungsstelle/bescheinigungen_sigg/veroeffentlichungen.php
Atos IT Solutions and Services GmbH, D-81739 München, Otto-Hahn-Ring 6

29 [CARDOS53-CC-CR] Certification Report "CardOS V5.3 QES, V1.0" (BSI-DSZ-CC-0921-2014) Stand: 2014/08/06
Original-Site: https://www.bsi.bund.de/SharedDocs/Zertifikate_CC/CC/Digitale_Signatur-Sichere_Signaturerstellungseinheiten/0921.html
Atos IT Solutions and Services GmbH, D-81739 München, Otto-Hahn-Ring 6

30 [CARDOS53-CC-ST] Security Target 'CardOS V5.3 QES, V1.0', Rev. 1.61, Edition 07/2014 Stand: 2014/07/23
Original-Site: https://www.bsi.bund.de/SharedDocs/Zertifikate_CC/CC/Digitale_Signatur-Sichere_Signaturerstellungseinheiten/0921.html
Atos IT Solutions and Services GmbH, D-81739 München, Otto-Hahn-Ring 6

31 [CC-ITSE] Common Criteria for Information Technology Security Evaluation v3.1 - Revision 3 (ISO 15408) Stand: 2009/07/01
Original-Site: http://www.commoncriteriaportal.org/cc/
Common Criteria - Management c/o GCHQ - Government Communications Headquarters, GB-GL51 0EX Cheltenham, Gloucestershire, Room A2b, Hubble Road

32 [CEM-ITSE] Common Methodology for Information Technology Security Evaluation v3.1 - Revision 3 (ISO 15408) Stand: 2009/07/01
Original-Site: http://www.commoncriteriaportal.org/cc/
Common Criteria - Management c/o GCHQ - Government Communications Headquarters, GB-GL51 0EX Cheltenham, Gloucestershire, Room A2b, Hubble Road

33 [CWA 15579] CWA 15579 - E-invoices and digital signatures (Dezember 2007) Stand: 2007/12/01
Original-Site: https://www.cen.eu/work/areas/ICT/eBusiness/Pages/eInvoicing.aspx
CEN-CENELEC Management Centre, B-1000 Brussels, Avenue Marnix 17

34 [CWA-14167-1] CWA 14167-1 - Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements Stand: 2004/02/13
Original-Site: ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/
CEN-CENELEC Management Centre, B-1000 Brussels, Avenue Marnix 17

35 [CWA-14167-2] CWA 14167-2 - Cryptographic module for CSP signing operations with backup - Protection profile - CMCSOB PP Stand: 2004/05/28
Original-Site: ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/
CEN-CENELEC Management Centre, B-1000 Brussels, Avenue Marnix 17

36 [CWA-14167-3] CWA 14167-3 - Cryptographic module for CSP key generation services protection profile - CMCKG PP Stand: 2004/05/28
Original-Site: ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/
CEN-CENELEC Management Centre, B-1000 Brussels, Avenue Marnix 17

37 [CWA-14167-4] CWA 14167-4 - Cryptographic module for CSP signing operations - Protection profile - CMCSO PP Stand: 2004/05/28
Original-Site: ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/
CEN-CENELEC Management Centre, B-1000 Brussels, Avenue Marnix 17

38 [CWA-14169] CWA 14169 - Secure signature-creation devices "EAL 4+" Stand: 2004/05/28
Original-Site: ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/
CEN-CENELEC Management Centre, B-1000 Brussels, Avenue Marnix 17

39 [DSG-2018] Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz - DSG) - RIS-Zusammenstellung Stand: 2018/05/25

Original-Site:
http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10001597&FassungVom=2018-05-25
Bundeskanzleramt (BKA), A-1014 Wien, Ballhausplatz 2

40 [E-GOVG] Bundesgesetz über Regelungen zur Erleichterung des elektronischen Verkehrs mit öffentlichen Stellen (E-Government-Gesetz - E-GovG) - StF: BGBl. I Nr. 10/2004 Stand: 2013/05/23
Original-Site:
http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20003230
Bundeskanzleramt (BKA), A-1014 Wien, Ballhausplatz 2

41 [EBA-OP] EBA Opinion on the use of eIDAS certificates under the RTS on SCACSC Stand: 2019/05/02

42 [eBillVO] Verordnung der Bundesministerin für Finanzen, mit der die Anforderungen an eine elektronische Rechnung bestimmt werden (E-Rechnung-UStV) - RIS-Version Stand: 2012/12/28
Original-Site: http://ftp.freenet.at/privacy/gesetze/ebilling-verordnung-2013.pdf
BM für Finanzen (BMF), A-1010 Wien, Johannesgasse 5

43 [EG-REF] 2003/511/EG: Entscheidung der Kommission vom 14. Juli 2003 über die Veröffentlichung von Referenznummern für allgemein anerkannte Normen für Produkte für elektronische Signaturen gemäß der Richtlinie 1999/93/EG Stand: 2003/07/14
Original-Site: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32003D0511:DE:HTML
EUROPÄISCHE KOMMISSION (COMMISSION OF THE EUROPEAN COMMUNITIES), B-1049 BRUXELLES, Rue de la Loi 200

44 [EG-SSCD] 2009/767/EG Maßnahmen zur Erleichterung der Nutzung elektronischer Verfahren über „einheitliche Ansprechpartner" gemäß der Richtlinie 2006/123/EG Stand: 2009/12/28
Original-Site: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:299:0018:01_DEC_2009_767_54:DE:HTML
EUROPÄISCHE KOMMISSION (COMMISSION OF THE EUROPEAN COMMUNITIES), B-1049 BRUXELLES, Rue de la Loi 200

45 [EGOV-DOK] Übersicht E-Government-Dokumente Stand: 2015/12/31
Original-Site: https://www.ref.gv.at/KONVENTIONEN.1116.0.html
Bundeskanzleramt (BKA), A-1014 Wien, Ballhausplatz 2

46 [eIDAS-IMPL] Abl. L 235/37 Durchführungsbeschluss (EU) 2015/1506 zur Festlegung von Spezifikationen für Formate fortgeschrittener elektronischer Signaturen und fortgeschrittener Siegel, die von öffentlichen Stellen gemäß Artikel 27 Absatz 5 und Artikel 37 Stand: 2015/09/08
Original-Site: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOL_2015_235_R_0006
EUROPÄISCHE KOMMISSION (COMMISSION OF THE EUROPEAN COMMUNITIES), B-1049 BRUXELLES, Rue de la Loi 200

47 [eIDAS-SEC] DURCHFÜHRUNGSVERORDNUNG (EU) 2015/1502 DER KOMMISSION vom 8. September 2015 zur Festlegung von Mindestanforderungen an technische Spezifikationen und Verfahren für Sicherheitsniveaus elektronischer Identifizierungsmittel gemäß Artikel 8 Absatz Stand: 2015/11/08

48 [eIDAS-VO] Abl. L 257/73 VERORDNUNG (EU) 910/2014 elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt ("eIDAS-Verordnung") Stand: 2014/08/28
Original-Site: http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32014R0910
EUROPÄISCHE KOMMISSION (COMMISSION OF THE EUROPEAN COMMUNITIES), B-1049 BRUXELLES, Rue de la Loi 200

49 [ENISA-ALG] Algorithms- key size and parameters report - 2014.pdf Stand: 2014/01/01
Original-Site: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014
European Network and Information Security Agency (ENISA), GR-700 13 Heraklion, Vassilika Vouton (P.O. Box 1309)

50 [EREGV-2009] Ergänzungsregisterverordnung 2009 - ERegV 2009 - RIS-Version Stand: 2015/08/26
Original-Site:
http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20006490
Stammzahlenregisterbehörde, A-1010 Wien, Hohenstaufengasse 3

51 [ETOKEN-CC-CR] CC EAL4+ Certification Report: SafeNet eToken - Athena IDProtect/OS755 Java Card on Atmel AT90SC25672RCT-USB Microcontroller embedding IDSign applet Stand: 2011/03/04
Original-Site: http://www.commoncriteriaportal.org/files/epfiles/ANSSI-CC_2011-03fr.pdf
SafeNet, Inc., USA-MD 21017 Belcamp, 4690 Millennium Drive

52 [ETOKEN-CC-ST] CC EAL4+ Security Target: SafeNet eToken - Athena IDProtect/OS755 Java Card on Atmel AT90SC25672RCT-USB Microcontroller embedding IDSign applet v1.2 Stand: 2011/02/16
Original-Site: http://www.commoncriteriaportal.org/files/epfiles/ANSSI-CC-cible_2011-03en.pdf
SafeNet, Inc., USA-MD 21017 Belcamp, 4690 Millennium Drive

53 [ETOKEN-FIPS-L2-CERT] FIPS 140-2 L2 Zertifikat #1135 Aladdin eToken PRO (Java), Aladdin eToken Anywhere and Aladdin eToken PRO (Java) SC Stand: 2011/10/26
Original-Site: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-historical.htm#1135
SafeNet, Inc., USA-MD 21017 Belcamp, 4690 Millennium Drive

54 [ETOKEN-FIPS-L3-CERT] FIPS 140-2 L3 Zertifikat #1136 "Aladdin eToken PRO (java) HD" Stand: 2011/10/26
Original-Site: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140crt/140crt1136.pdf
SafeNet, Inc., USA-MD 21017 Belcamp, 4690 Millennium Drive

55 [ETOKEN-FIPS-L3-SP] FIPS 140-2 L3 Security Policy #1136 "Aladdin eToken PRO (java) HD" Stand: 2011/10/18
Original-Site: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1136.pdf
SafeNet, Inc., USA-MD 21017 Belcamp, 4690 Millennium Drive

56 [ETSI EN 301 549] ETSI EN 301 549 - V2.1.2 Accessibility requirements for ICT products and services Stand: 2018/08/28
Original-Site: https://portal.etsi.org/webapp/workProgram/Report_WorkItem.asp?wki_id=50127
European Telecommunications Standards Institute (ETSI), F-06921 Sophia-Antipolis Cedex, 650, route des Lucioles

57 [ETSI EN 319 122-1] ETSI EN 319 122-1 V1.1.1 CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures Stand: 2016/04/08
Original-Site: https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=39473

58 [ETSI EN 319 122-2] ETSI EN 319 122-2 V1.1.1 CAdES digital signatures; Part 2: Extended CAdES signatures Stand: 2016/04/01
Original-Site: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/e-Signature+standards
European Telecommunications Standards Institute (ETSI), F-06921 Sophia-Antipolis Cedex, 650, route des Lucioles

59 [ETSI EN 319 132-1] ETSI EN 319 132-1 V1.1.1 XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures Stand: 2016/04/29
Original-Site: https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=39476

60 [ETSI EN 319 132-2] ETSI EN 319 132-2 V1.1.1 XAdES digital signatures; Part 2: Extended XAdES signatures Stand: 2016/04/29
Original-Site: https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=39477
European Telecommunications Standards Institute (ETSI), F-06921 Sophia-Antipolis Cedex, 650, route des Lucioles

61 [ETSI EN 319 142-1] EN 319 142-1 V1.1.1 PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures Stand: 2016/04/12
Original-Site: https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=39485

62 [ETSI EN 319 142-2] ETSI EN 319 142-2 V1.1.1 PAdES digital signatures; Part 2: Additional PAdES signatures profiles Stand: 2016/04/12
Original-Site: https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=39479

63 [ETSI EN 319 401] ETSI EN 319 401 - V2.2.1 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers Stand: 2018/04/01
Original-Site:
http://www.etsi.org/deliver/etsi_en/319400_319499/319401/02.02.01_60/en_319401v020201p.pdf
European Telecommunications Standards Institute (ETSI), F-06921 Sophia-Antipolis Cedex, 650, route des Lucioles

64 [ETSI EN 319 403] ETSI EN 319 403 V2.2.2 Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers Conformity Assessment of Trust Service Stand: 2015/08/27
Original-Site: https://portal.etsi.org/webapp/workProgram/Report_WorkItem.asp?wki_id=39371
European Telecommunications Standards Institute (ETSI), F-06921 Sophia-Antipolis Cedex, 650, route des Lucioles

65 [ETSI EN 319 411-1] ETSI EN 319 411-1 v1.2.2 Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General Requirements Stand: 2018/04/01

Original-Site: https://portal.etsi.org/tbsitemap/esi/trustserviceproviders.aspx
European Telecommunications Standards Institute (ETSI), F-06921 Sophia-Antipolis Cedex, 650, route des Lucioles

66 [ETSI EN 319 411-2] ETSI EN 319 411-2 V2.2.2 (2018-04) Electronic Signatures and Infrastructures (ESI) Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified Stand: 2018/04/01
Original-Site: https://portal.etsi.org/tbsitemap/esi/trustserviceproviders.aspx
European Telecommunications Standards Institute (ETSI), F-06921 Sophia-Antipolis Cedex, 650, route des Lucioles

67 [ETSI EN 319 412-1] ETSI EN 319 412-1 V1.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI);Certificate Profiles; Part 1: Overview and common data structures Stand: 2016/02/26
Original-Site: https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=39367
European Telecommunications Standards Institute (ETSI), F-06921 Sophia-Antipolis Cedex, 650, route des Lucioles

68 [ETSI EN 319 412-2] ETSI EN 319 412-2 V2.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI);Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons Stand: 2016/02/01
European Telecommunications Standards Institute (ETSI), F-06921 Sophia-Antipolis Cedex, 650, route des Lucioles

69 [ETSI EN 319 412-3] ETSI EN 319 412-3 V1.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons Stand: 2016/02/01
Original-Site:
http://www.etsi.org/deliver/etsi_en/319400_319499/31941203/01.01.01_60/en_31941203v010101p.pdf

70 [ETSI EN 319 412-4] ETSI EN 319 412-4 - V1.1.1 - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4 Stand: 2016/02/01
European Telecommunications Standards Institute (ETSI), F-06921 Sophia-Antipolis Cedex, 650, route des Lucioles

71 [ETSI EN 319 412-5] V2.2.1 Part 5: QCStatements Stand: 2017/11/01
Original-Site: https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=51426

72 [ETSI EN 319 421] ETSI EN 319 421 V1.1.1 (2016-03) Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps Stand: 2016/03/01
Original-Site: https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=39366

73 [ETSI EN 319 422] ETSI EN 319 422 V1.1.1 - Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles Stand: 2016/03/01
Original-Site: https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=39370
European Telecommunications Standards Institute (ETSI), F-06921 Sophia-Antipolis Cedex, 650, route des Lucioles

74 [ETSI TS 102 778-1] ETSI TS 102 778-1 V1.1.1 Part 1: PAdES Overview - a framework document for PAdES Stand: 2009/07/31
Original-Site: https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=31003

75 [ETSI TS 103 123] ETSI TR 103 123 V1.1.1 Electronic Signatures and Infrastructures (ESI); Guidance for Auditors and CSPs on ETSI TS 102 042 for Issuing Publicly-Trusted TLS/SSL Certificates Stand: 2012/11/16
Original-Site: http://webapp.etsi.org/WorkProgram/Report_WorkItem.asp?wki_id=38245
European Telecommunications Standards Institute (ETSI), F-06921 Sophia-Antipolis Cedex, 650, route des Lucioles

76 [ETSI TS 119 312] ETSI TS 119 312 1.2.2 Electronic Signatures and Infrastructures (ESI); Cryptographic Suites Stand: 2018/09/20
Original-Site: https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=56375
European Telecommunications Standards Institute (ETSI), F-06921 Sophia-Antipolis Cedex, 650, route des Lucioles

77 [ETSI TS 119 312] ETSI TS 119 312 1.3.1 Electronic Signatures and Infrastructures (ESI); Cryptographic Suites Stand: 2019/02/01
Original-Site: https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=56375
European Telecommunications Standards Institute (ETSI), F-06921 Sophia-Antipolis Cedex, 650, route des Lucioles

78 [ETSI TS 119 403] ETSI TS 119 403 V2.1.1 (2014-11) Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers Stand: 2014/09/16
Original-Site: http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=44560
European Telecommunications Standards Institute (ETSI), F-06921 Sophia-Antipolis Cedex, 650, route des Lucioles

79 [ETSI TS 119 431-1] ETSI TS 119 431-1 V1.1.1 (2018-12) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev Stand: 2018/12/01
Original-Site: https://portal.etsi.org/webapp/workprogram/Report_WorkItem.asp?WKI_ID=47242
European Telecommunications Standards Institute (ETSI), F-06921 Sophia-Antipolis Cedex, 650, route des Lucioles

80 [ETSI TS 119 431-2] ETSI TS 119 431-2 V1.1.1 (2018-12) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 2: TSP service components supporting AdES digital signature creation Stand: 2018/12/01
Original-Site: https://portal.etsi.org/webapp/workprogram/Report_WorkItem.asp?WKI_ID=52778
European Telecommunications Standards Institute (ETSI), F-06921 Sophia-Antipolis Cedex, 650, route des Lucioles

81 [ETSI TS 119 432] ETSI TS 119 432 V1.1.1 (2019-03) Electronic Signatures and Infrastructures (ESI); Protocols for remote digital signature creation Stand: 2019/03/01
Original-Site:
https://www.etsi.org/standards#page=2&search=&title=1&etsiNumber=1&content=0&version=0&onApproval=1&published=1&historical=1&startDate=2015-01-15&endDate=2019-08-06&harmonized=0&keyword=&TB=607&stdType=&frequency=&mandate=&collection=&sort=2
European Telecommunications Standards Institute (ETSI), F-06921 Sophia-Antipolis Cedex, 650, route des Lucioles

82 [ETSI TS 119 495] V1.3.2 Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive (EU) 2015/2366 Stand: 2019/06/01
Original-Site: https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=58043

83 [EU-QSCD-LIST] Qualified Signature Creation Devices under Article 31(1)-(2), and Certified Qualified Seal Creation Devices under Article 39(3) of Regulation 910/2014 Stand: 2019/05/08
Original-Site: https://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-and-qscds
EUROPÄISCHE KOMMISSION (COMMISSION OF THE EUROPEAN COMMUNITIES), B-1049 BRUXELLES, Rue de la Loi 200

84 [EU-RICHT-ZAHL] Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinien 2002/65/EG, 2009/110/EG und 2013/36/EU und der Verordnung (EU) Nr. 1093/2010 Stand: 2015/11/25
Original-Site: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex:32015L2366

85 [FIPS-140-2] FIPS 140-2 Security Requirements for Cryptographic Modules inkl. Annex A-D Stand: 2002/03/12
Original-Site: http://csrc.nist.gov/publications/PubsFIPS.html
NIST - National Institute of Standards and Technology, USA-MD 20899-107 Gaithersburg, 100 Bureau Drive, Stop 1070

86 [FMA-IDV] Online-Identifikationsverordnung - Online-IDV Stand: 2019/04/01
Original-Site:
https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20009774

87 [FORTIOS-CC-CR] Certification Report: EAL 4+ evaluation of Fortinet FortiGate Unified Threat Management Solutions and FortiOS 4.0 CC compliant firmware v1.0 Stand: 2012/01/23
Original-Site: http://www.commoncriteriaportal.org/files/epfiles/383-4-133%20CR%20v1.0e.pdf
Fortinet Inc, USA-CA 94086 Sunnyvale, 1090 Kifer Road

88 [FORTIOS-CC-ST] Fortinet FortiGate Unified Threat Management Solutions and FortiOS 4.0 CC Compliant Firmware Stand: 2011/12/06
Original-Site: http://www.commoncriteriaportal.org/files/epfiles/383-4-133%20ST%20v1.2.pdf
Fortinet Inc, USA-CA 94086 Sunnyvale, 1090 Kifer Road

89 [FORTIOS-FIPS-CERT] Fips 140-2 (Level 1) Certificate #1754: FortiOS v4.0MR3 Stand: 2012/07/17
Original-Site: http://csrc.nist.gov/groups/STM/cmvp/documents/140-

1/140crt/FIPS140ConsolidatedCertList0019.pdf
Fortinet Inc, USA-CA 94086 Sunnyvale, 1090 Kifer Road

90 [FORTIOS-FIPS-SP] Fips 140-2 (Level 1) Security Policy #1754: FortiOS 4.0 MR3 Stand: 2012/04/13
Original-Site: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1754.pdf
Fortinet Inc, USA-CA 94086 Sunnyvale, 1090 Kifer Road

91 [HB-SICHERHEIT] Österreichisches Informationssicherheitshandbuch - Version 4.0.0 (Hrsg. Bundeskanzleramt) Stand: 2014/09/23
Original-Site: https://www.sicherheitshandbuch.gv.at/2013/index.php
Bundeskanzleramt (BKA), A-1014 Wien, Ballhausplatz 2

92 [ISO-7816-10] ISO/IEC 7816-10:1999: Identification cards -- Integrated circuit(s) cards with contacts -- Part 10: Electronic signals and answer to reset for synchronous cards Stand: 1999/11/01
Original-Site:
http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?ics1=35&ics2=240&ics3=15&csnumber=30558
International Organization for Standardization (ISO), CH-1211 Geneva 20, 1, ch. de la Voie-Creuse CP 56

93 [ISO-7816-11] ISO/IEC 7816-11:2004: Identification cards -- Integrated circuit cards -- Part 11: Personal verification through biometric methods Stand: 2004/04/01
Original-Site:
http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?ics1=35&ics2=240&ics3=15&csnumber=31419
International Organization for Standardization (ISO), CH-1211 Geneva 20, 1, ch. de la Voie-Creuse CP 56

94 [ISO-7816-12] ISO/IEC 7816-12:2005: Identification cards - Integrated circuit cards -- Part 12: Cards with contacts -- USB electrical interface and operating procedures Stand: 2005/10/01
Original-Site:
http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?ics1=35&ics2=240&ics3=15&csnumber=40604
International Organization for Standardization (ISO), CH-1211 Geneva 20, 1, ch. de la Voie-Creuse CP 56

95 [ISO-7816-13] ISO/IEC 7816-13:2007: Identification cards -- Integrated circuit cards -- Part 13: Commands for application management in a multi-application environment Stand: 2007/03/15
Original-Site:
http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?ics1=35&ics2=240&ics3=15&csnumber=40605
International Organization for Standardization (ISO), CH-1211 Geneva 20, 1, ch. de la Voie-Creuse CP 56

96 [ISO-7816-15] ISO/IEC 7816-15:2004: Identification cards -- Integrated circuit cards -- Part 15: Cryptographic information application inkl. Ergänzung Stand: 2008/12/15
International Organization for Standardization (ISO), CH-1211 Geneva 20, 1, ch. de la Voie-Creuse CP 56

97 [ISO-7816-1] ISO/IEC 7816-1:2011 Identification cards -- Integrated circuit(s) cards with contacts -- Physical Charcteristics of Integrated Circuit Cards ISO Stand: 2011/02/15
International Organization for Standardization (ISO), CH-1211 Geneva 20, 1, ch. de la Voie-Creuse CP 56

98 [ISO-7816-2] ISO/IEC 7816-2:2007 Identification cards -- Integrated circuit cards -- Dimensions and Location of the Contacts ISO Stand: 2007/10/15
International Organization for Standardization (ISO), CH-1211 Geneva 20, 1, ch. de la Voie-Creuse CP 56

99 [ISO-7816-3] ISO/IEC 7816-3:2006 Identification cards -- Integrated circuit cards -- Electronic Signals and Transmission Protocols ISO Stand: 2006/11/01
International Organization for Standardization (ISO), CH-1211 Geneva 20, 1, ch. de la Voie-Creuse CP 56

100 [ISO-7816-4] ISO/IEC 7816-4:2005 Interindustry Commands for Interchange + Korrektur Stand: 2013/04/15
International Organization for Standardization (ISO), CH-1211 Geneva 20, 1, ch. de la Voie-Creuse CP 56

101 [ISO-7816-5] ISO/IEC 7816-5:2004: Identification cards -- Integrated circuit cards -- Part 5: Registration of application providers Stand: 2004/12/01
International Organization for Standardization (ISO), CH-1211 Geneva 20, 1, ch. de la Voie-Creuse CP 56

102 [ISO-7816-6] ISO/IEC 7816-6:2004: Identification cards -- Integrated circuit cards -- Part 6: Interindustry data elements for interchange inkl. Korrektur Stand: 2004/05/15
International Organization for Standardization (ISO), CH-1211 Geneva 20, 1, ch. de la Voie-Creuse CP 56

103 [ISO-7816-7] ISO/IEC 7816-7:1999: Identification cards -- Integrated circuit(s) cards with contacts -- Part 7: Interindustry commands for Structured Card Query Language (SCQL) Stand: 1999/03/01
Original-Site:
http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?ics1=35&ics2=240&ics3=15&csnumber=28869
International Organization for Standardization (ISO), CH-1211 Geneva 20, 1, ch. de la Voie-Creuse CP 56

104 [ISO-7816-8] ISO/IEC 7816-8:2004: Identification cards -- Integrated circuit cards -- Part 8: Commands for security operations Stand: 2004/06/01
Original-Site:
http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?ics1=35&ics2=240&ics3=15&csnumber=37989
International Organization for Standardization (ISO), CH-1211 Geneva 20, 1, ch. de la Voie-Creuse CP 56

105 [ISO-7816-9] ISO/IEC 7816-9:2004: Identification cards -- Integrated circuit cards -- Part 9: Commands for card management Stand: 2004/06/01
International Organization for Standardization (ISO), CH-1211 Geneva 20, 1, ch. de la Voie-Creuse CP 56

106 [ISO27-A1TEL] A1 Telekom Austria - ISO 27001 Zertifikat 15/0 ISO/IEC 27001:2005 - pdf-Version deutsch + englisch Stand: 2012/11/28
A1 Telekom Austria AG, A-1020 Wien, Lassallestraße 9

107 [ITSEM] Handbuch für die Bewertung der Sicherheit von Systemen der Informationstechnik Stand: 2003/09/01
Original-Site:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/ITSicherheitskriterien/itsem-dt_pdf.html
Bundesamt für Sicherheit in der Informationstechnik (BSI), D-53175 BONN, Godesberger Allee 185-189

108 [ITU-509] ITU-T Recommendation X.509 : Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks Stand: 2019/08/02
Original-Site: https://www.itu.int/rec/T-REC-X.509-201610-I/en
International Telecommunication Union (ITU), CH-1211 Geneva 20, Place des Nations

109 [ITU-X501] ITU-T Recommendation X.501: Information technology - Open Systems Interconnection - The Directory: Models Stand: 2016/10/14
Original-Site: https://www.itu.int/rec/T-REC-X.501/en
International Telecommunication Union (ITU), CH-1211 Geneva 20, Place des Nations

110 [ITU-X509v3-ERR] ITU-T Recommendation X.509v3 Fehlerbehebung Stand: 2011/02/01
Original-Site: http://handle.itu.int/11.1002/1000/11735
International Telecommunication Union (ITU), CH-1211 Geneva 20, Place des Nations

111 [ITU-X509v3] ITU-T Recommendation X.509v3 - Open systems interconnection - The Directory: Public-key and attribute certificate frameworks Stand: 2016/10/01
Original-Site: https://www.itu.int/rec/T-REC-X.509/en
International Telecommunication Union (ITU), CH-1211 Geneva 20, Place des Nations

112 [ITU-X520] ITU-T Recommendation X.520: Information technology - Open Systems Interconnection - The Directory: Selected attribute types Stand: 2016/10/14
Original-Site: https://www.itu.int/rec/T-REC-X.520/en
International Telecommunication Union (ITU), CH-1211 Geneva 20, Place des Nations

113 [ITU-X660] ITU-T Recommendation X.660: Information technology - Procedures for the operation of object identifier registration authorities: General procedures and top arcs of the international object identifier tree Stand: 2011/07/29

Original-Site: https://www.itu.int/rec/T-REC-X.660/en
International Telecommunication Union (ITU), CH-1211 Geneva 20, Place des Nations

114 [ITU-X680] ITU-T X.680 (08/2015), Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation Stand: 2015/08/13
Original-Site: https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=x.680
International Telecommunication Union (ITU), CH-1211 Geneva 20, Place des Nations

115 [ITU-X681] ITU-T X.681 (08/2015), Information technology - Abstract Syntax Notation One (ASN.1): Information object specification Stand: 2015/08/13
Original-Site: https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=x.681
International Telecommunication Union (ITU), CH-1211 Geneva 20, Place des Nations

116 [ITU-X682] ITU-T X.682 (08/2015), Information technology - Abstract Syntax Notation One (ASN.1): Constraint specification Stand: 2015/08/13
Original-Site: https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=x.682
International Telecommunication Union (ITU), CH-1211 Geneva 20, Place des Nations

117 [ITU-X683] ITU-T X.683 (08/2015), Information technology - Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 specifications Stand: 2015/08/13
Original-Site: https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=x.683
International Telecommunication Union (ITU), CH-1211 Geneva 20, Place des Nations

118 [ITU-X690] ITU-T X.690 (08/2015), Information technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER) Stand: 2015/08/13
Original-Site: https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=x.690
International Telecommunication Union (ITU), CH-1211 Geneva 20, Place des Nations

119 [ITU-X691] ITU-T X.691 (08/2015), Information technology - ASN.1 encoding rules: Specification of Packed Encoding Rules (PER) Stand: 2015/08/13
Original-Site: https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=x.691
International Telecommunication Union (ITU), CH-1211 Geneva 20, Place des Nations

120 [ITU-X692] ITU-T X.692 (08/2015), Information technology - ASN.1 encoding rules: Specification of Encoding Control Notation (ECN) Stand: 2015/08/13
Original-Site: https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=x.692
International Telecommunication Union (ITU), CH-1211 Geneva 20, Place des Nations

121 [ITU-X693] ITU-T X.693 (08/2015), Information technology - ASN.1 encoding rules: XML Encoding Rules (XER) Stand: 2015/08/13
Original-Site: https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=x.693
International Telecommunication Union (ITU), CH-1211 Geneva 20, Place des Nations

122 [JAVA-CRYPTO] Class SecureRandom + Java Cryptography Architecture (JCA) Reference Guide Stand: 2018/01/01
Original-Site: https://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html

123 [KEY-RECO] Key Length Recommendations https://www.keylength.com/en/compare/ Stand: 2018/03/20
Original-Site: https://www.keylength.com/en/compare/

124 [LUNAK3-FIPS-CERT] FIPS 140-2 (L3) Zertifikat #685 "Luna PCI Cryptographic Module V2" (Hardware Version: VBD-01-0104; Firmware Version: 4.5.3) Stand: 2006/07/14
Original-Site: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-historical.htm#685
SafeNet, Inc., USA-MD 21017 Belcamp, 4690 Millennium Drive

125 [LUNAK3-FIPS-SP] FIPS 140-2 (L3) Security Policy #685 "Luna PCI Cryptographic Module V2" (Hardware Version: VBD-01-0104; Firmware Version: 4.5.3) Revision 8 Stand: 2006/06/09
Original-Site: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-historical.htm#685
SafeNet, Inc., USA-MD 21017 Belcamp, 4690 Millennium Drive

126 [LUNAK5-FIPS-CERT] FIPS 140-2 (L3) Zertifikat #2486 + #2487 12/15/2015 Luna® Backup HSM Cryptographic Module (Firmware Versions: 6.10.7 and 6.10.9) Stand: 2016/01/04
Original-Site: https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/2489
SafeNet, Inc., USA-MD 21017 Belcamp, 4690 Millennium Drive

127 [LUNAK5-FIPS-SECURITY-POLICY] FIPS 140-2 (L3) SECURITY POLICY #2489 Luna® PCI-E Cryptographic Module for Luna® SA (Firmware Versions: 6.10.7 and 6.10.9) Stand: 2016/01/04
Original-Site: https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/2489
SafeNet, Inc., USA-MD 21017 Belcamp, 4690 Millennium Drive

128 [MOBILE] Grundsatzpapier Mobile Signatur - Schwerpunktthema Bürgerkarte und eID - Version 1.0, 22.04.2008 Stand: 2008/04/22
Original-Site: https://demo.egiz.gv.at/plain/content/download/583/3362/file/Grundsatzpapier-Mobile-Signatur.pdf
EGIZ E-Government Innovationszentrum, A-8010 Graz, Inffeldgasse 16a

129 [MOZILLA-CAPOL] Mozilla Root Store Policy Version 2.7 Stand: 2019/12/19
Original-Site: https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/
Mozilla Foundation, USA-CA 94041-112 Mountain View, 1350 Villa Street, Suite C

130 [MOZILLA-CHECK] CA/Subordinate CA Checklist Stand: 2020/01/08
Original-Site: https://wiki.mozilla.org/CA/Subordinate_CA_Checklist
Mozilla Foundation, USA-CA 94041-112 Mountain View, 1350 Villa Street, Suite C

131 [MOZILLA-PROB] CA/Forbidden or Problematic Practices Stand: 2019/12/11
Original-Site: https://wiki.mozilla.org/CA/Forbidden_or_Problematic_Practices
Mozilla Foundation, USA-CA 94041-112 Mountain View, 1350 Villa Street, Suite C

132 [MOZILLA-REC] CA/Required or Recommended Practices Stand: 2020/03/09
Original-Site: https://wiki.mozilla.org/CA/Required_or_Recommended_Practices
Mozilla Foundation, USA-CA 94041-112 Mountain View, 1350 Villa Street, Suite C

133 [MS-CA-201604] Microsoft Trusted Root Certificate: Program Requirements - Ergänzung Re: April 2016 Stand: 2016/04/05
Microsoft Corporation, USA-WA 98052-639 Redmond, One Microsoft Way

134 [MS-CA-AUDITREQ] Microsoft Trusted Root Certificate Program Audit Requirements Stand: 2019/02/20
Original-Site: https://social.technet.microsoft.com/wiki/contents/articles/31635.microsoft-trusted-root-certificate-program-audit-requirements.aspx
Microsoft Corporation, USA-WA 98052-639 Redmond, One Microsoft Way

135 [MS-CA] Microsoft Trusted Root Certificate: Program Requirements Stand: 2020/01/01
Original-Site: https://docs.microsoft.com/en-us/previous-versions//cc751157(v=technet.10)?redirectedfrom=MSDN
Microsoft Corporation, USA-WA 98052-639 Redmond, One Microsoft Way

136 [MS-OID] Object IDs associated with Microsoft cryptography Stand: 2017/03/20
Original-Site: https://support.microsoft.com/en-us/help/287547/object-ids-associated-with-microsoft-cryptography
Microsoft Corporation, USA-WA 98052-639 Redmond, One Microsoft Way

137 [NIST-RANDOM] NIST Special Publication 800-90A Revision 1 Recommendation for Random Number Generation Using Deterministic Random Bit Generators Stand: 2015/06/01
Original-Site: http://dx.doi.org/10.6028/NIST.SP.800-90Ar1
SafeNet, Inc., USA-MD 21017 Belcamp, 4690 Millennium Drive

138 [NO] Notariatsordnung (NO) idF 18.7.2019 StF: RGBl. Nr. 75/1871 Stand: 2019/07/18
Original-Site: https://www.ris.bka.gv.at/

139 [OID-T1] Object Identifier der öffentlichen Verwaltung (Teil 1 - Allgemeine Beschreibung) V1.0.0 Stand: 2009/02/27
Original-Site: http://www.ref.gv.at/AG-II-BK-OID-T1_OID-T2-1-0-0.2230.0.html
Stabsstelle IKT-Strategie des Bundes (CIO Chief Information Officer), A-1010 Wien, Ballhausplatz 2

140 [OID-T2] Object Identifier der öffentlichen Verwaltung (Teil 2 - Taxative Definition) - Version 1.0.3 Stand: 2015/07/28
Original-Site: http://www.ref.gv.at/AG-II-BK-OID-T1_OID-T2-1-0-0.2230.0.html
Bundeskanzleramt (BKA), A-1014 Wien, Ballhausplatz 2

141 [OSSL-FIPS-CERT] FIPS 140-2 certificate #1747 for OpenSSL FIPS Object Module Stand: 2012/07/16
Original-Site: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140crt/FIPS140ConsolidatedCertList0018.pdf
OpenSSL Software Foundation, Inc., USA-MD 21710 Adamstown, 1829 Mount Ephraim Road

142 [OSSL-FIPS-DOC] User Guide 2.0 for the OpenSSL FIPS Object Module v2.0 Stand: 2017/03/14
Original-Site: https://www.openssl.org/docs/fips.html
OpenSSL Software Foundation, Inc., USA-MD 21710 Adamstown, 1829 Mount Ephraim Road

143 [OSSL-FIPS-SP] OpenSSL FIPS 140-2 Security Policy Version 2.0.1 Stand: 2012/07/09
Original-Site: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1747.pdf
OpenSSL Software Foundation, Inc., USA-MD 21710 Adamstown, 1829 Mount Ephraim Road

144 [PERSBIND-XML] XML-Spezifikation der Personenbindung v1.2.2 - pdf-Version Stand: 2005/02/14
Original-Site: http://www.buergerkarte.at/konzept/personenbindung/spezifikation/20050214/

145 [PKCS01] PKCS #1: RSA Cryptography Standard v2.1 Stand: 2002/06/14
Original-Site: ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-1/pkcs-1v2-1.pdf
RSA The Security Division of EMC, USA-MA 01730 Bedford, 174 Middlesex Turnpike

146 [PKCS08] PKCS #8: Private-Key Information Syntax Standard Stand: 1993/11/01
Original-Site: http://www.rsa.com/rsalabs/node.asp?id=2130
RSA The Security Division of EMC, USA-MA 01730 Bedford, 174 Middlesex Turnpike

147 [PKCS10] PKCS #10: Certification Request Syntax Standard Stand: 2000/05/26
Original-Site: ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-10/pkcs-10v1_7.pdf
RSA The Security Division of EMC, USA-MA 01730 Bedford, 174 Middlesex Turnpike

148 [PKCS11] PKCS #11 v2.20: Cryptographic Token Interface Standard - pdf-Version Stand: 2004/06/28
Original-Site: ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-11/v2-20/pkcs-11v2-20.pdf
RSA The Security Division of EMC, USA-MA 01730 Bedford, 174 Middlesex Turnpike

149 [PKCS12] PKCS #12: Personal Information Exchange Syntax Standard Stand: 1999/06/24
Original-Site: ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-12/pkcs-12v1.pdf
RSA The Security Division of EMC, USA-MA 01730 Bedford, 174 Middlesex Turnpike

150 [PKCS15] PKCS #15: Cryptographic Token Information Format Standard (v1.1) Stand: 2000/06/06
Original-Site: ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-15/pkcs-15v1_1.pdf
RSA The Security Division of EMC, USA-MA 01730 Bedford, 174 Middlesex Turnpike

151 [RFC2595] rfc2595 - Using TLS with IMAP, POP3 and ACAP Stand: 1999/06/01
Original-Site: https://www.rfc-editor.org/info/rfc2595
IETF - The Internet Engineering Task Force, USA-VA 20191-543 Reston, 1895 Preston White Drive, Suite 100

152 [RFC2818] rfc2818 - HTTP Over TLS Stand: 2000/05/01
Original-Site: https://www.rfc-editor.org/info/rfc2818
IETF - The Internet Engineering Task Force, USA-VA 20191-543 Reston, 1895 Preston White Drive, Suite 100

153 [RFC2986] rfc2986 - PKCS #10: Certification Request Syntax Specification Version 1.7 Stand: 2000/11/01
Original-Site: https://www.rfc-editor.org/info/rfc2986
IETF - The Internet Engineering Task Force, USA-VA 20191-543 Reston, 1895 Preston White Drive, Suite 100

154 [RFC3161] rfc3161 - Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP) Stand: 2001/08/01
Original-Site: https://www.rfc-editor.org/info/rfc3161
IETF - The Internet Engineering Task Force, USA-VA 20191-543 Reston, 1895 Preston White Drive, Suite 100

155 [RFC3279] rfc3279 - Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile Stand: 2002/04/01
Original-Site: https://www.rfc-editor.org/info/rfc3279
IETF - The Internet Engineering Task Force, USA-VA 20191-543 Reston, 1895 Preston White Drive, Suite 100

156 [RFC3447] rfc3447 - Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1 Stand: 2003/02/01
Original-Site: https://www.rfc-editor.org/info/rfc3447
IETF - The Internet Engineering Task Force, USA-VA 20191-543 Reston, 1895 Preston White Drive, Suite 100

157 [RFC3647] rfc3647 - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework Stand: 2003/11/01
Original-Site: https://www.rfc-editor.org/info/rfc3647
IETF - The Internet Engineering Task Force, USA-VA 20191-543 Reston, 1895 Preston White Drive, Suite 100

158 [RFC3739] rfc3739 - Internet X.509 Public Key Infrastructure: Qualified Certificates Profile Stand: 2004/03/01
Original-Site: https://www.rfc-editor.org/info/rfc3739

IETF - The Internet Engineering Task Force, USA-VA 20191-543 Reston, 1895 Preston White Drive, Suite 100

159 [RFC4511] rfc4511 - Lightweight Directory Access Protocol (LDAP): The Protocol Stand: 2006/06/01
Original-Site: https://www.rfc-editor.org/info/rfc4511
IETF - The Internet Engineering Task Force, USA-VA 20191-543 Reston, 1895 Preston White Drive, Suite 100

160 [RFC4517] rfc4517 - Lightweight Directory Access Protocol (LDAP): Syntaxes and Matching Rules Stand: 2006/06/01
Original-Site: https://www.rfc-editor.org/info/rfc4517
IETF - The Internet Engineering Task Force, USA-VA 20191-543 Reston, 1895 Preston White Drive, Suite 100

161 [RFC4519] rfc4519 - Lightweight Directory Access Protocol (LDAP): Schema for User Applications Stand: 2006/06/01
Original-Site: https://www.rfc-editor.org/info/rfc4519
IETF - The Internet Engineering Task Force, USA-VA 20191-543 Reston, 1895 Preston White Drive, Suite 100

162 [RFC4524] rfc4524 - COSINE LDAP/X.500 Schema Stand: 2006/06/01
Original-Site: https://www.rfc-editor.org/info/rfc4524
IETF - The Internet Engineering Task Force, USA-VA 20191-543 Reston, 1895 Preston White Drive, Suite 100

163 [RFC5246] rfc5246 - The Transport Layer Security (TLS) Protocol Version 1.2 Stand: 2019/12/27
Original-Site: https://www.rfc-editor.org/info/rfc5246

164 [RFC5280] rfc5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile Stand: 2008/05/01
Original-Site: https://www.rfc-editor.org/info/rfc5280
IETF - The Internet Engineering Task Force, USA-VA 20191-543 Reston, 1895 Preston White Drive, Suite 100

165 [RFC5288] rfc5288 - AES Galois Counter Mode (GCM) Cipher Suites for TLS Stand: 2019/12/27
Original-Site: https://www.rfc-editor.org/info/rfc5288

166 [RFC5289] rfc5289 - TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM) Stand: 2019/12/27
Original-Site: https://www.rfc-editor.org/info/rfc5289

167 [RFC5424] rfc5424 - The Syslog Protocol Stand: 2009/03/01
Original-Site: https://www.rfc-editor.org/info/rfc5424
IETF - The Internet Engineering Task Force, USA-VA 20191-543 Reston, 1895 Preston White Drive, Suite 100

168 [RFC5652] rfc5652 - Cryptographic Message Syntax (CMS) Stand: 2009/09/01
Original-Site: https://www.rfc-editor.org/info/rfc5652
IETF - The Internet Engineering Task Force, USA-VA 20191-543 Reston, 1895 Preston White Drive, Suite 100

169 [RFC5758] rfc5758 Internet X.509 Public Key Infrastructure: Additional Algorithms and Identifiers for DSA and ECDSA Stand: 2010/01/01
Original-Site: https://www.rfc-editor.org/info/rfc5758
IETF - The Internet Engineering Task Force, USA-VA 20191-543 Reston, 1895 Preston White Drive, Suite 100

170 [RFC5816] rfc5816 - ESSCertIDv2 Update for RFC 3161 ("Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)") Stand: 2010/04/01
Original-Site: https://www.rfc-editor.org/info/rfc5816
IETF - The Internet Engineering Task Force, USA-VA 20191-543 Reston, 1895 Preston White Drive, Suite 100

171 [RFC5905] rfc5905 - Network Time Protocol Version 4: Protocol and Algorithms Specification Stand: 2010/06/01
Original-Site: https://www.rfc-editor.org/info/rfc5905
IETF - The Internet Engineering Task Force, USA-VA 20191-543 Reston, 1895 Preston White Drive, Suite 100

172 [RFC6066] rfc6066 - Transport Layer Security (TLS) Extensions: Extension Definitions Stand: 2011/01/01
Original-Site: https://www.rfc-editor.org/info/rfc6066

IETF - The Internet Engineering Task Force, USA-VA 20191-543 Reston, 1895 Preston White Drive, Suite 100

173 [RFC6655] rfc6655 - AES-CCM Cipher Suites for Transport Layer Security (TLS) Stand: 2019/12/27
Original-Site: https://www.rfc-editor.org/info/rfc6655

174 [RFC6818] rfc6818 - Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile Stand: 2013/01/01
Original-Site: https://www.rfc-editor.org/info/rfc6818
IETF - The Internet Engineering Task Force, USA-VA 20191-543 Reston, 1895 Preston White Drive, Suite 100

175 [RFC6960] rfc6960 - X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP Stand: 2013/06/01
Original-Site: https://www.rfc-editor.org/info/rfc6960
IETF - The Internet Engineering Task Force, USA-VA 20191-543 Reston, 1895 Preston White Drive, Suite 100

176 [RFC6962] rfc6962 - Certificate Transparency Stand: 2013/06/01
Original-Site: https://www.rfc-editor.org/info/rfc6962
IETF - The Internet Engineering Task Force, USA-VA 20191-543 Reston, 1895 Preston White Drive, Suite 100

177 [RFC7159] rfc7159 - The JavaScript Object Notation (JSON) Data Interchange Format Stand: 2014/03/01
Original-Site: https://www.rfc-editor.org/info/rfc7159
IETF - The Internet Engineering Task Force, USA-VA 20191-543 Reston, 1895 Preston White Drive, Suite 100

178 [RFC7230] rfc7230 - Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing Stand: 2014/06/01
Original-Site: https://www.rfc-editor.org/info/rfc7230
IETF - The Internet Engineering Task Force, USA-VA 20191-543 Reston, 1895 Preston White Drive, Suite 100

179 [RFC7235] rfc7235 - Hypertext Transfer Protocol (HTTP/1.1): Authentication Stand: 2014/06/01
Original-Site: https://www.rfc-editor.org/info/rfc7235
IETF - The Internet Engineering Task Force, USA-VA 20191-543 Reston, 1895 Preston White Drive, Suite 100

180 [RFC7251] rfc7251 - AES-CCM Elliptic Curve Cryptography (ECC) Cipher Suites for TLS Stand: 2019/12/27
Original-Site: https://www.rfc-editor.org/info/rfc7251

181 [RFC7515] rfc7517 - The JavaScript Object Notation (JSON) Data Interchange Format Stand: 2015/05/01
Original-Site: https://www.rfc-editor.org/info/rfc7517
IETF - The Internet Engineering Task Force, USA-VA 20191-543 Reston, 1895 Preston White Drive, Suite 100

182 [RFC7518] rfc7518 - JSON Web Algorithms (JWA) Stand: 2015/05/01
Original-Site: https://www.rfc-editor.org/info/rfc7518
IETF - The Internet Engineering Task Force, USA-VA 20191-543 Reston, 1895 Preston White Drive, Suite 100

183 [RFC8398] rfc6818 - Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile Stand: 2013/01/01
Original-Site: https://www.rfc-editor.org/info/rfc6818
IETF - The Internet Engineering Task Force, USA-VA 20191-543 Reston, 1895 Preston White Drive, Suite 100

184 [RFC8398] rfc8398 - Internationalized Email Addresses in X.509 Certificates Stand: 2018/05/01
Original-Site: https://www.rfc-editor.org/info/rfc8398
IETF - The Internet Engineering Task Force, USA-VA 20191-543 Reston, 1895 Preston White Drive, Suite 100

185 [RKS-V] Registrierkassensicherheitsverordnung, RKSV - konsolidiert RIS inkl Anlagen Stand: 2015/08/04
Original-Site:
http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20009390
BM für Finanzen (BMF), A-1010 Wien, Johannesgasse 5

186 [RTS] Regulatory Technical Standards - EU-Verordnung technische Regulierungsstandards für die Authentifizierung und Kommunikation Stand: 2018/03/13

187 [SIGVO-DB-NOTIF-DE] Abl. L 289/18 Durchführungsbeschluss (EU) 2015/1984 Umstände, Formate und Verfahren der Notifizierung Stand: 2015/11/05
Original-Site: http://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1460296362627&uri=CELEX:32015D1984
EUROPÄISCHE KOMMISSION (COMMISSION OF THE EUROPEAN COMMUNITIES), B-1049 BRUXELLES, Rue de la Loi 200

188 [SIGVO-DB-NOTIF-EN] Abl. L 289/18 Commission Implementing Decision (EU) 2015/1984 circumstances, formats and procedures of notification Stand: 2015/11/05
Original-Site: http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1460296362627&uri=CELEX:32015D1984
EUROPÄISCHE KOMMISSION (COMMISSION OF THE EUROPEAN COMMUNITIES), B-1049 BRUXELLES, Rue de la Loi 200

189 [SIGVO-DB-SPEZF-DE] Abl. L 235/37 Durchführungsbeschluss (EU) 2015/1506 Spezifikation Formate fortgeschrittene Signaturen/Siegel Stand: 2015/09/09
Original-Site: http://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1445168928138&uri=CELEX:32015D1506
EUROPÄISCHE KOMMISSION (COMMISSION OF THE EUROPEAN COMMUNITIES), B-1049 BRUXELLES, Rue de la Loi 200

190 [SIGVO-DB-SPEZF-EN] Abl. L 235/37 COMMISSION IMPLEMENTING DECISION (EU) 2015/1506 specifications relating to formats of advanced electronic signatures Stand: 2015/09/09
Original-Site: http://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1445168928138&uri=CELEX:32015D1506
EUROPÄISCHE KOMMISSION (COMMISSION OF THE EUROPEAN COMMUNITIES), B-1049 BRUXELLES, Rue de la Loi 200

191 [SIGVO-DB-TRUST-DE] Abl. L 235/26 Durchführungsbeschluss (EU) 2015/1505 Vertrauenslisten Stand: 2015/09/09
Original-Site: http://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1445168928138&uri=CELEX:32015D1505
EUROPÄISCHE KOMMISSION (COMMISSION OF THE EUROPEAN COMMUNITIES), B-1049 BRUXELLES, Rue de la Loi 200

192 [SIGVO-DB-TRUST-EN] Abl. L 235/26 COMMISSION IMPLEMENTING DECISION (EU) 2015/1505 trusted lists Stand: 2015/09/09
Original-Site: http://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1445168928138&uri=CELEX:32015D1505
EUROPÄISCHE KOMMISSION (COMMISSION OF THE EUROPEAN COMMUNITIES), B-1049 BRUXELLES, Rue de la Loi 200

193 [SIGVO-DB-TRUST-EN] Abl. L 235/26 Durchführungsbeschluss (EU) 2015/1505 Vertrauenslisten http://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1445168928138&uri=CELEX:32015D1505 Stand: 2015/09/09
Original-Site: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015D1505&from=DE
RAT DER EUROPÄISCHEN UNION, B-1048 BRÜSSEL, Rue de la Loi 175

194 [SIGVO-DB-ZUSAMMMEN-DE] Abl. L 53/14 Durchführungsbeschluss (EU) 2015/296 Verfahrensmodalitäten Zusammenarbeit Mitgliedstaaten auf Gebiet elektronische Identifizierung Stand: 2015/02/25
Original-Site: http://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1445168928138&uri=CELEX:32015D0296
EUROPÄISCHE KOMMISSION (COMMISSION OF THE EUROPEAN COMMUNITIES), B-1049 BRUXELLES, Rue de la Loi 200

195 [SIGVO-DV-INTER-DE] Abl. L 235/1 Durchführungsverordnung (EU) 2015/1501 Interoperabilitätsrahmen Stand: 2015/09/09
Original-Site: http://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1445168928138&uri=CELEX:32015R1501
EUROPÄISCHE KOMMISSION (COMMISSION OF THE EUROPEAN COMMUNITIES), B-1049 BRUXELLES, Rue de la Loi 200

196 [SIGVO-DV-INTER-EN] Abl. L 235/1 COMMISSION IMPLEMENTING REGULATION (EU) 2015/1501 interoperability framework Stand: 2015/09/09
Original-Site: http://eur-lex.europa.eu/legal-

content/DE/TXT/?qid=1445168928138&uri=CELEX:32015R1501
EUROPÄISCHE KOMMISSION (COMMISSION OF THE EUROPEAN COMMUNITIES), B-1049 BRUXELLES, Rue de la Loi 200

197 [SIGVO-DV-MINIMUM-DE] Abl. L 235/7 Durchführungsverordnung (EU) 2015/1502 Mindestanforderungen an technische Spezifikationen und Verfahren Stand: 2015/09/09
Original-Site: http://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1445168928138&uri=CELEX:32015R1502
EUROPÄISCHE KOMMISSION (COMMISSION OF THE EUROPEAN COMMUNITIES), B-1049 BRUXELLES, Rue de la Loi 200

198 [SIGVO-DV-MINIMUM-EN] Abl. L 235/7 COMMISSION IMPLEMENTING REGULATION (EU) 2015/1502 minimum technical specifications and procedures Stand: 2015/09/09
Original-Site: http://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1445168928138&uri=CELEX:32015R1502
EUROPÄISCHE KOMMISSION (COMMISSION OF THE EUROPEAN COMMUNITIES), B-1049 BRUXELLES, Rue de la Loi 200

199 [SIGVO-DV-TRUSTQ-DE] Abl. L 128/13 Durchführungsverordnung (EU) 2015/806 Spezifikationen EU-Vertrauenssiegels qualifizierte Vertrauensdienste Stand: 2015/05/23
Original-Site: http://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1445168928138&uri=CELEX:32015R0806
EUROPÄISCHE KOMMISSION (COMMISSION OF THE EUROPEAN COMMUNITIES), B-1049 BRUXELLES, Rue de la Loi 200

200 [SIGVO-DV-TRUSTQ-EN] Abl. L 128/13 COMMISSION IMPLEMENTING REGULATION (EU) 2015/806 EU specifications trust mark for qualified trust services Stand: 2015/05/23
Original-Site: http://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1445168928138&uri=CELEX:32015R0806
EUROPÄISCHE KOMMISSION (COMMISSION OF THE EUROPEAN COMMUNITIES), B-1049 BRUXELLES, Rue de la Loi 200

201 [SOAP] SOAP Version 1.2 Stand: 2007/04/27
Original-Site: https://www.w3.org/TR/soap/
W3C - World Wide Web Consortium, F-06902 Sophia Antipolis Cedex, 2004, route des Lucioles

202 [SOG-IS] Crypto Evaluation Scheme Agreed Cryptographic Mechanisms v1.1 Stand: 2018/06/01
Original-Site: https://www.sogis.org/uk/supporting_doc_en.html

203 [STZREGBEHV-2009] Stammzahlenregisterbehördenverordnung 2009 - StZRegBehV 2009 - RIS-Version Stand: 2015/08/26
Original-Site: http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20006487
Stammzahlenregisterbehörde, A-1010 Wien, Hohenstaufengasse 3

204 [SVG] BGBl. I Nr.50/2016 Signatur- und Vertrauensdienstegesetz (SVG) Stand: 2016/07/01
Original-Site: http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20009585

205 [SVR] Richtlinien der Österreichischen Notariatskammer vom 19.10.2006 für das elektronische Verzeichnis für die Beurkundungs- und Notarsignaturen (Signaturverzeichnisrichtlinien, SVR 2006) Stand: 2018/02/01
Original-Site: notar.at

206 [SVV] BGBl. II Nr. 208/2016 Signatur- und Vertrauensdiensteverordnung - SVV sowie Verordnung über die Feststellung der Eignung des Vereins „Zentrum für sichere Informationstechnologie - Austria (A-SIT)" als Bestätigungsstelle Stand: 2016/08/01
Original-Site: https://www.ris.bka.gv.at/eli/bgbl/II/2016/208/20160801
Bundeskanzleramt (BKA), A-1014 Wien, Ballhausplatz 2

207 [VKZ-EB] Ebenen- und Bereichskennungen für das VKZ v1.2.13 Stand: 2016/02/02
Original-Site: https://www.ref.gv.at/EP-VV-VKZ-Bereichskennungen.673.0.html
Stabsstelle IKT-Strategie des Bundes (CIO Chief Information Officer), A-1010 Wien, Ballhausplatz 2

208 [VKZ] Empfehlung Verwaltungskennzeichen (VKZ) 1.2.0 Stand: 2007/03/25
Original-Site: http://reference.e-government.gv.at/Veroeffentlichte-Informationen.203.0.html
Stabsstelle IKT-Strategie des Bundes (CIO Chief Information Officer), A-1010 Wien, Ballhausplatz 2

209 [WEBTRUST-CA] Principles and Criteria for Certification Authorities 2.2 Stand: 2019/06/01
Original-Site: https://www.cpacanada.ca/en/business-and-accounting-resources/audit-and-assurance/overview-of-webtrust-services/principles-and-criteria

THE CANADIAN INSTITUTE OF CHARTERED ACCOUNTANTS, CDN-ON M5V 3H2 West Toronto, 277 Wellington Street

210 [WEBTRUST-EV] WebTrust Principles and Criteria for Certification Authorities - Extended Validation SSL - Version 1.6.8 Stand: 2019/05/01
Original-Site: https://www.cpacanada.ca/en/business-and-accounting-resources/audit-and-assurance/overview-of-webtrust-services/principles-and-criteria
THE CANADIAN INSTITUTE OF CHARTERED ACCOUNTANTS, CDN-ON M5V 3H2 West Toronto, 277 Wellington Street

211 [XMLSIG-XAdES] XML Advanced Electronic Signatures (XAdES) Stand: 2003/02/20
Original-Site: https://www.w3.org/TR/XAdES/
W3C - World Wide Web Consortium, F-06902 Sophia Antipolis Cedex, 2004, route des Lucioles

212 [XMLSIG] XML Signature Syntax and Processing (Second Edition) Stand: 2008/06/10
Original-Site: http://www.w3.org/TR/xmldsig-core/
W3C - World Wide Web Consortium, F-06902 Sophia Antipolis Cedex, 2004, route des Lucioles

213 [ZADIG] BGBl. I Nr. 17/2018 Bundesgesetz über die Erbringung von Zahlungsdiensten 2018 (Zahlungsdienstegesetz 2018, ZaDiG 2018) Stand: 2018/06/01

2 CONTENT CERTIFICATION-PROTOCOLS / INHALT AUSSTELLUNGS-, SPERR-, ENTSPERR- UND WIDERRUFS-PROTOKOLL FÜR ZERTIFIKATE

Protokoll zu Ausstellung Endkunden-Zertifikate

* Die Namen der Personen, die die Zertifizierung durchgeführt haben
* Zertifizierungszeitpunkt
* Eingesetztes Zertifizierungsprodukt (z.B. openssl)
* Bezeichnung des Zertifizierungsdienstes inkl. Name der verwendeten CA (z.B. GLOBALTRUST ADVANCED 3)
* Name und Organisation des Antragstellers
* Prüfung des Zertifikates (Unterschrift des CA Zertifikates)
* Seriennummer des Zertifikates
* Fingerprint(s) des Zertifikates
* Textversion des Zertifikates
* PEM kodiertes Zertifikat
* Fingerprint(s) CA Zertifikat
* PEM kodiertes CA Zertifikat
* Verwendete Konfigurationsdatei
* tatsächlich eingesetzte Hardware des privaten Schlüssels des CA-Zertifkates
* Tatsächlich eingesetzte Hardware des privaten Endkundenschlüssels (sofern Schlüssel von VDA oder autorisierter Stelle erzeugt)
* Standort der Durchführung des Zertifizierungsdienstes
* Identifikationsdaten des Zertifizierungsrechners
* Versionsnummer des Zertifizierungstools

Protocol for issuing end user certificates:

* Names of the persons who have executed the certification
* Certification date
* Installed certification product (e.g. openssl)
* Name of the certification service including the name of the used CA (e.g. GLOBALTRUST ADVANCED 3)
* Name and organisation of the applicant
* Check of the certificate (signature of the CA certificate)
* Serial number of the certificate
* Fingerprint (s) of the certificate
* Text version of the certificate
* PEM encoded certificate
* Fingerprint (s) of the CA certificate
* PEM encoded CA certificate
* Configuration files
* Used hardware of the private key of the CA certificate
* Used hardware of the private end user key (if key generated by VDA or authorized authority)
* Location of the certification service
* Identification data of the certification computer
* Version number of the certification tool

Protokoll zu Sperrung, Entsperrung und Widerruf Endkunden-Zertifikate

* Die Namen der Personen, die den Widerruf durchgeführt haben
* Durchführungsszeitpunkt
* Eingesetztes Zertifzierungsprodukt (z.B. openssl)
* Name der verwendeten CA (z.B. A-CERT ADVANCED 3)
* Seriennummer des widerrufenen Zertifikates
* Angaben zu den Sperr- und Widerrufsgründen
* Fingerprint(s) des widerrufenen-Zertifikates
* PEM kodiertes widerrufenen Zertifikates
* Textversion des widerrufenen Zertifikates
* Fingerprint(s) des CA-Zertifikates
* PEM kodiertes CA-Zertifikat
* Verwendete Konfiguration
* PEM kodierte CRL
* Signaturprüfung der CRL
* tatsächlich eingesetzte Hardware des privaten Schlüssels des CA-Zertifkates
* Standort der Durchführung des Zertifizierungsdienstes
* Identifikationsdaten des Zertifizierungsrechners
* Versionsnummer des Zertifizierungstools

Protocol for locking, unlocking and revocation of end user certificates

* Names of the persons who executed the revocation
* Revocation date
* used certification product (e.g. openssl)
* Name of the CA used (e.g. A-CERT ADVANCED 3)
* Serial number of the revocated certificate
* Information on the reasons for the revocation
* Fingerprint (s) of the revocated certificate
* PEM encoded revocated certificate
* Text version of the revocated certificate
* Fingerprint (s) of the CA certificate
* PEM encoded CA certificate
* configuration used
* PEM encoded CRL
* CRL signature verification
* Used hardware of the private key of the CA certificate
* Location of the certification service
* Identification data of the certification computer
* Version number of the certification tool

3 SUPPORTED SIGNATURE CREATION UNITS / UNTERSTÜTZTE SIGNATURERSTELLUNGSPRODUKTE

Die Aufzählung hat demonstrativen Charakter, weitere Produkte werden laufend auf der Website des VDA (⇨ http://www.globaltrust.eu/produkte.html) veröffentlicht.

This list has demonstrative character, other products will regularly be published on the website of the VDA (⇨ http://www.globaltrust.eu/produkte.html).

Produkte, die als sichere Signaturerstellungseinheiten geeignet sind:
- Smartcard mit Betriebssystem CardOS V5.0 [CARDOS50-BSI-QES] mit Application for QES, zertifiziert gemäß CC EAL4+ (⇨ Certification Report [CARDOS50-CC-CR])
- Smartcard mit Betriebssystem CardOS V5.3 [CARDOS53-ASIT-QES] mit Application for QES, sicherheitszertifiziert (⇨ Certification Report [CARDOS53-CC-CR])
- HSM inkl. Smartcards zu dem eine Bescheinigung gemäß [CWA-14169] vorgelegt werden kann

Products which are suitable as secure signature creation devices:
- Smartcard with CardOS V5.3 [CARDOS53-ASIT-QES] with application for QES, security certified (⇨ Certification Report [CARDOS53-CC-CR])
- HSM including smartcards to which a certificate according to [CWA-14169] can be submitted

Weitere Produkte für Signaturerstellungseinheiten, die zur Ausstellung fortgeschrittener Signaturen geeignet sind:
- Safenet eToken PRO 72k zertifiziert gemäß FIPS 140-2 L2 Zertifikat #1135 [ETOKEN-FIPS-CERT] sofern gemäß Policy [ETOKEN-FIPS-SP] verwendet wird.
- alle Produkte, die zumindest eine Zertifizierung gemäß [CC-ITSE] EAL4+ oder gemäß [FIPS-140-2] L1 aufweisen

Other products for signature creation suitable for issuing advanced signatures:
- Safenet eToken PRO 72k certified according to FIPS 140-2 L2 Certificate #1135 [ETOKEN-FIPS-CERT], if used according to Policy [ETOKEN-FIPS-SP].
- all products which have at least a certification according to [CC-ITSE] EAL4 + or [FIPS-140-2] L1

Produkte, die für mobile Signaturdienste geeignet sind:
- alle Produkte die gemäß Grundsatzpapier von E-GIZ zur mobilen Signatur ([MOBILE] in der aktuellen Version) als geeignet bezeichnet werden.
- alle Produkte, die zumindest eine Zertifizierung nach CC EAL4+ oder FIPS 140-2 L2 aufweisen

Products suitable for mobile signature:
- all products which are considered to be suitable according to the principle paper of E-GIZ for the mobile signature ([MOBILE] in the current version).
- all products that have at least a certification according to CC EAL4 + or FIPS 140-2 L2

Produkte, die als serverseitige Signaturerstellungseinheit für qualifizierte Signaturen geeignet sind:

- HSM zu dem eine Bescheinigung gemäß [CWA-14169] vorgelegt werden kann

Products which are suitable as a server signature creation device for qualified signatures:

- HSM to which a certificate according to [CWA-14169] can be submitted

Produkte, die als mobile technische Einheiten für serverbasierte mobile Signaturdienste geeignet sind:

- alle Mobiltelefone, zu denen der Signator eine Erklärung abgibt, ausschließlich darüber zu verfügen

Products suitable as mobile technical devices for server based mobile signature:

- all mobile telephones, to which the subscriber makes a declaration that he has the sole power about it