Updated December 2019 to match BR version 1.6.6

CA's Self-Assessment of CP/CPS documents to CA/Browser Forum Baseline Requirements (BRs)

Introduction must include:

Introduction
1) CA's Legal Name
e-commerce monitoring GmbH

2) RootCA
CN:GLOBALTRUST 2020
Subject: CN=GLOBALTRUST 2020; O=e-commerce monitoring GmbH; C=AT
Issuer : CN=GLOBALTRUST 2020; O=e-commerce monitoring GmbH; C=AT
Valid From (GMT) 2/10/2020
Valid To (GMT) 6/10/2040
Certificate Serial Number: 5A4BBD5AFB4F8A5BFA65E5
SHA-1 Fingerprint: D067C11351010CAAD0C76A65373116264F5371A2
SHA-256 Fingerprint: 9A296A5182D1D451A2E37F439B74DAAFA267523329F90F9A0D2007C334E23C9A

3) Version(s) of the BRs that were used
Version v1.6.7

4) Policy
[GCP] GLOBALTRUST Certificate Policy V2.0g http://www.globaltrust.eu/certificate-policy.html
[GCPS] GLOBALTRUST Certificate Practice Statement V2.0g http://www.globaltrust.eu/static/globaltrust-practice-statement.pdf

BR Section Number	**List the specific documents and section numbers of those documents which meet the requirements of each BR section**	**Explain how the CA's listed documents meet the requirements of each BR section.**
1.2.1. Revisions Note the Effective Date for each item in the table. Certificates created after each Effective Date are expected to be in compliance with the item. Make sure your CA is in compliance with each of these items. After careful consideration, *indicate if your CA is fully compliant with all items in the table, or clearly indicate action that your CA is taking to improve compliance.*	[GCP] GLOBALTRUST® Certificate Policy Version 2.0g (OID: 1.2.40.0.36.1.1.8) [GCPS] GLOBALTRUST® Certificate Practice Statement Version 2.0g (OID: 1.2.40.0.36.1.2.3.1)	Issued certificates are fully compliant with the items listed below

1.2.2. Relevant Dates Note the Compliance date for each item in the table. Those are the dates by which your CP/CPS and practices are expected to be updated to comply with the item. Make sure your CA is in compliance with each of these items. After careful consideration, *indicate if your CA is fully compliant with all items in the table, or clearly indicate action that your CA is taking to improve compliance.*		GCP, GCPS and practices are fully compliant with the items listed below
1.3.2. Registration Authorities Indicate whether your CA allows for Delegated Third Parties, or not. *Indicate which sections of your CP/CPS specify such requirements, and how the CP/CPS meets the BR requirements for RAs.*	GCP Section 1.3.2. items "Registration authorities", "Certification partner" and "service provider" GCP Section 5.3.7. "Independent contractor requirements"	a partial delegation of RA functions is currently being planned with some providers, but not yet implemented
2.1. Repositories *Provide the direct URLs to the CA's repositories*	GCP Section 2.1 and 2.2	http://www.globaltrust.eu/certificate-policy.html
2.2 Publication of information - RFC 3647 "Effective as of 31 May 2018, the Certificate Policy and/or Certification Practice Statement **MUST be structured in accordance with RFC 3647**."	GCP 1.2 GCPS 1.2	CP and CPS are structured according to RFC 3647
2.2 Publication of information - CAA **Section 4.2 of a CA's Certificate Policy and/or Certification Practice Statement SHALL state the CA's policy or practice on processing CAA Records for Fully Qualified Domain Names; that policy shall be consistent with these Requirements.** **It shall clearly specify the set of Issuer Domain Names that the CA recognises in CAA "issue" or "issuewild" records as permitting it to issue. The CA SHALL log all actions taken, if any, consistent with its processing**	GCPS 4.2 Certificate application processing	The Domain Name globaltrust.eu in CAA „issue“ or „issuewild“ records is regognized as permission to issue.
2.2. Publication of information - BR text "The CA SHALL publicly give effect to these Requirements and represent that it will adhere to the latest published version." --> ***Copy the specific text that is used into the explanation in this row. (in English)***	GCP 8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS	"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: [...] - CA/Browser Forum: Baseline Requirements [CABROWSER-BASE] published at http://www.cabforum.org

2.2. Publication of information - test websites "The CA SHALL host test Web pages that allow Application Software Suppliers to test their software with Subscriber Certificates that chain up to each publicly trusted Root Certificate. At a minimum, the CA SHALL host separate Web pages using Subscriber Certificates that are (i) valid, (ii) revoked, and (iii) expired." --> ***List the URLs to the three test websites (valid, revoked, expired) for each root certificate under consideration. If you are requesting EV treatment, then the TLS cert for each test website must be EV.***	GCP 2.2 links to repository where test websites can be found	valid: https://www.testok-2020-server-ev-1.e-monitoring.at expired: https://www.testold-2020-server-ev-1.e-monitoring.at revoked: https://www.testrevoked-2020-server-ev-1.e-monitoring.at
2.3. Time or frequency of publication "The CA SHALL ... **annually** update a Certificate Policy and/or Certification Practice Statement that describes in detail how the CA implements the latest version of these Requirements. Section 3.3 of Mozilla's Root Store Policy states: "CPs and CPSes MUST be reviewed and updated as necessary at least once every year, as required by the Baseline Requirements. **CAs MUST indicate that this has happened by incrementing the version number and adding a dated changelog entry**, even if no other changes are made to the document." *Indicate your CA's policies/practices to ensure that the BRs are reviewed regularly, and that the CA's CP/CPS is updated annually.*	GCP Section 9.12.1 Procedure for amendment GCPS Section 5.4 Audit logging procedures GCP Section 8.1 Frequency or circumstances of assessment	GCP and GCPS are updated a least once a year (GCP 9.12) This is demonstrated by incrementing the version number and an entry in Section 1.2 "history of changes" Applicable requirements are continuously observed by review team. (not publicly documented) Self Assessment of issued certificates is conducted quarterly on at least 3%. of non SSL-certificates, 3% of OV certificates and 6% of EV certificates (GCPS 5.4) External Audit is conducted at least annualy (GCP 8.1)
2.4. Access controls on repositories *Acknowledge that all Audit, CP, CPS documents required by Mozilla's CA Certificate Policy and the BRs will continue to be made publicly available.*	GCP Section 2.2 + 2.4	http://www.globaltrust.eu/certificate-policy.html contains CP and CPS and audit history
3.2.2.1 Identity If the Subject Identity Information in certificates is to include the name or address of an organization, *indicate how your CP/CPS meets the requirements in this section of the BRs.*	GCP Section 3.2.2 Authentication of organization identity GCP Section 4.2 Certificate application processing	All sources that are used comply with the requirements for QIIS, QGIS and QTIS according the CA/Browser-Forum EV Guidelines
3.2.2.2 DBA/Tradename If the Subject Identity Information in certificates is to include a DBA or tradename, *indicate how your CP/CPS meets the requirements in this section of the BRs.*	see above	see above- DBA/Tradename must be treated the same as the Organizational Name

3.2.2.3 Verification of Country If the subject:countryName field is present in certificates, *indicate how your CP/CPS meets the requirements in this section of the BRs.*	GCP Section 7.1.4 Name formats GCP Section 4.2 Certificate application processing	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 value confirmed in the course of identity verification. The identification methods named in 4.2. and 3.2.2 can also be used to verify country information, i.e. QIIS, QGIS, QTIS
3.2.2.4 Validation of Domain Authorization or Control *Indicate which of the methods of domain validation your CA uses, and where this is described in your CP/CPS.* ***Section 2.2 of Mozilla's Root Store Policy states: "For a certificate capable of being used for SSL-enabled servers, the CA must ensure that the applicant has registered all domain(s) referenced in the certificate or has been authorized by the domain registrant to act on their behalf. This must be done using one or more of the methods documented in section 3.2.2.4 of the CA/Browser Forum Baseline Requirements. The CA's CP/CPS must clearly specify the procedure(s) that the CA employs, and each documented procedure should state which subsection of 3.2.2.4 it is complying with. CAs are not permitted to use 3.2.2.5 (4) ("any other method") to fulfill the requirements of method 3.2.2.4.8 (IP Address)."***	Make sure the CP/CPS states what the CA actually does, not what it could do. Such as which of the allowed domain validation methods the CA uses.	GCPS 4.2 list of validation methods with reference to the Baseline Requirements sections
3.2.2.4.1 Validating the Applicant as a Domain Contact For certificates issued on or after August 1, 2018, **this method SHALL NOT be used** for validation, and completed validations using this method SHALL NOT be used for the issuance of certificates.	**This method SHALL NOT be used.**	not used GCPS 4.2 method list is exhaustive
3.2.2.4.2 Email, Fax, SMS, or Postal Mail to Domain Contact If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.*	n.A.	
3.2.2.4.3 Phone Contact with Domain Contact **CAs SHALL NOT perform validations using this method after May 31, 2019**. Completed validations using this method SHALL continue to be valid for subsequent issuance per the applicable certificate data reuse periods.	**This method SHALL NOT be used after May 31, 2019.**	

3.2.2.4.4 Constructed Email to Domain Contact If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.*	GCPS 4.2 Certificate application processing	1. Constructed email to domain contact: The following restrictions apply: (a) the email address of the domain owner must be composed of "hostmaster", "postmaster", "admin", "administrator", "webmaster" followed by an "at" sign ("@ "), Followed by the domain name. (b) The control email sent by the CA shall contain a random, unique value. (c) The Applicant must return a confirmation that contains this random value before the expiration of 30 days. The method is also allowed for wildcard certificates. (According to [CABROWSER-BASE] 3.2.2.4.4)
3.2.2.4.5 Domain Authorization Document "For certificates issued on or after August 1, 2018, **this method SHALL NOT be used** for validation, and completed validations using this method SHALL NOT be used for the issuance of certificates."	**This method SHALL NOT be used.**	
3.2.2.4.6 Agreed-Upon Change to Website If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.*	GCPS 4.2 Certificate application processing	2. The applicant can practically demonstrate control over the domain, in particular using a pre-agreed change to the website. (According to [CABROWSER-BASE] 3.2.2.4.6) This method will not be used after 30th June 2020-
3.2.2.4.7 DNS Change If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.*	n.A.	
3.2.2.4.8 IP Address If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.*	n.A.	
3.2.2.4.9 Test Certificate **"This method has been retired and MUST NOT be used."**	**This method SHALL NOT be used.**	
3.2.2.4.10. TLS Using a Random Number If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.* *This subsection contains major vulnerabilities.* ***If the CA uses this method, then the CA should describe how they are mitigating those vulnerabilities. If not using this method, the CPS should say so.***	Further explanation is required if this method is used.	
3.2.2.4.11 Any Other Method **"This method has been retired and MUST NOT be used."**	This method SHALL NOT be used.	

3.2.2.4.12 Validating Applicant as a Domain Contact "This method may only be used if the CA is also the Domain Name Registrar, or an Affiliate of the Registrar, of the Base Domain Name." If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs*.	Use of this method is restricted, per the BRs.	
3.2.2.4.13 Email to DNS CAA Contact If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs*.		
3.2.2.4.14 Email to DNS TXT Contact If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.*		
3.2.2.4.15 Phone Contact with Domain Contact If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.*		
3.2.2.4.16 Phone Contact with DNS TXT Record Phone Contact If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.*		
3.2.2.4.17 Phone Contact with DNS CAA Phone Contact If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.*		

3.2.2.5 Authentication for an IP Address If your CA allows IP Addresss to be listed in certificates, ***indicate which methods your CA uses*** *and how your CA meets the requirements in this section of the BRs.* **Section 2.2 of Mozilla's root store policy says: "the CA must ensure that the applicant has control over all IP Address(es) referenced in the certificate. This must be done using one or more of the methods documented in section 3.2.2.5 of the CA/Browser Forum Baseline Requirements. The CA's CP/CPS must clearly specify the procedure(s) that the CA employs, and each documented procedure should state which subsection of 3.2.2.5 it is complying with."**	Method 3.2.2.5.4, Any Other Method, SHALL NOT be used. "After July 31, 2019, CAs SHALL maintain a record of which IP validation method, including the relevant BR version number, was used to validate every IP Address."	GCPS 4.2. 1. The applicant can practically demonstrate control over the ip address, in particular using a pre-agreed change to the website using the "/.well-known/pki-validation" directory or equivalent. (According to [CABROWSER-BASE] 3.2.2.5.1) 2. Direct communication with the validated IP-Contact via email. The control mail sent by the CA contains a random, unique value. The IP-Contact must return a confirmation that contains this random value before the expiration of 30 days. (According to [CABROWSER-BASE] 3.2.2.5.2) 3. The domain name whose IP address is investigated using reverse lookup has been verified in compliance with the conditions of this policy. (According to [CABROWSER-BASE] 3.2.2.5.3.) The CA maintains documentation that enables for each domain- or IP adress validation to check which validation method was used and which requirements including their version number was applicable.
3.2.2.6 Wildcard Domain Validation If your CA allows certificates with a wildcard character (*) in a CN or subjectAltName of type DNS-ID, then *indicate how your CA meets the requirements in this seciton of the BRs.*	GCPS 4.2	A domain validation method described in GCPS 4.2 for the entire space that is covered by the wildcard character
3.2.2.7 Data Source Accuracy *Indicate how your CA meets the requirements in this section of the BRs.*	e.g. GCP Section 3.2.2., GCP 3.2.5, GCPS Section 4.2	Only either governmental sources or equally reliable data sources are used; for example organizational data as per GCP Section 3.2.2. meeting BR requirements 3.2.2.1 ; Or: Applications on behalf of another person or organization have to meet the applicable commercial laws on authority to act, etc. Each specific data source is evaluated before it may be used.
3.2.2.8 CAs MUST check and process CAA records *Indicate how your CA meets the requirements in this section of the BRs.* *Section 2.2 of the BRs states: "**CA's Certificate Policy and/or Certification Practice Statement ... shall clearly specify the set of Issuer Domain Names that the CA recognises in CAA "issue" or "issuewild" records as permitting it to issue."***	GCPS 4.2 Certificate application processing	The Domain Name globaltrust.eu in CAA "issue" or "issuewild" records is regognized as permission to issue.
3.2.3. Authentication of Individual Identity	GCP Section 3.2.3	Individual identity is authenticated via official photo ID, either face-to-face or by obtaining a copy. Only passport, driving license or personal ID is accepted.

3.2.5. Validation of Authority	GCP Section 3.2.5	Authority can be demonstrated by: - the Applicant Representative is listed in a QIIS, QGIS, QTIS as a duly mandated official (for example, in the austrian commercial register) - express authority - reliable source of the applicants organization confirms the authority (e.g. HR departement)
3.2.6. Criteria for Interoperation or Certification Disclose all cross-certificates in the CA hierarchies under evaluation.	n.A.	none
4.1.1. Who Can Submit a Certificate Application Indicate how your CA identifies suspicious certificate requests.	GCPS Section 4.2 paragraph 3	We maintain internal databases for all previously for any reason revoked or rejected certificates, high profile domain names and domain names, that had been target of attacks in the past. We also use Google Safe Browsing.
4.1.2. Enrollment Process and Responsibilities	GCP 4.1.2	The applicant has to use a webform for the certificate request including CSR. The webform links to the policy and terms, and the applicant has to agree, otherwise the request cannot be completed. There is also some additional mandatory information required to complete the proces, e.g. full name and contact information.
4.2. Certificate application processing		
4.2.1. Performing Identification and Authentication Functions *Indicate how your CA identifies high risk certificate requests.* **Re-use of validation information is limited to 825 days**	For high risk applications please see above item 46 GCP Section 4.2, last item (825-days-limitation see)	For high risk applications please see above item 46 content will be verified for up-to-dateness and correctness at least every 825 days (397 days from 1. September 2020)
4.2.2. Approval or Rejection of Certificate Applications "Within 30 days after ICANN has approved a new gTLD for operation, as evidenced by publication of a contract with the gTLD operator on [www.ICANN.org] each CA MUST (1) compare the new gTLD against the CA's records of valid certificates and (2) cease issuing Certificates containing a Domain Name that includes the new gTLD until after the CA has first verified the Subscriber's control over or exclusive right to use the Domain Name in accordance with Section 3.2.2.4. Within 120 days after the publication of a contract for a new gTLD is published on [www.icann.org], CAs MUST revoke each Certificate containing a Domain Name that includes the new gTLD unless the Subscriber is either the Domain Name Registrant or can demonstrate control over the Domain Name."	documented internally	The exact procedure is documented internally. We do not issue certificates for gTLD under consideration. So far, it has not been necessary to revoke a certificate for an approved new gTLD according to this requirement.
4.3.1. CA Actions during Certificate Issuance	GCP Section 6.1.1	CA key generation mentioned in GCP 6.1.1, the details are documented in the Security Policy, which is not publicly disclosed

4.9.1.1 Reasons for Revoking a Subscriber Certificate *Indicate which section in your CA's CP/CPS contains the list of reasons for revoking certificates.*	GCP Section 4.9.1	
4.9.1.2 Reasons for Revoking a Subordinate CA Certificate *Indicate which section in your CA's CP/CPS contains the list of reasons for revoking subordinate CA certificates.*	GCP Section 4.9.1	
4.9.2. Who Can Request Revocation	GCP Section 4.9.2	
4.9.3. Procedure for Revocation Request **The CA SHALL publicly disclose the instructions through a readily accessible online means and in section 1.5.2 of their CPS.**	GCP Section 4.9.3	Any form of communication will be dealt with, a webinterface is available 24/7 at https://www.globaltrust.eu/revocation.html
4.9.5. Time within which CA Must Process the Revocation Request	GCP Section 4.9.5	less than 24 hours
4.9.7. CRL Issuance Frequency *Indicate if your CA publishes CRLs. If yes, then please test your CA's CRLs.*	GCP Section 4.9.7	Revocation and suspension lists for servercertificates are valid for a maximum of 10 days (and updated at least every 7 days). Currently, CRLs are renewed every 12 hours (or earlier, in case of revocation) CRL Check via https://certificate.revocationcheck.com/ was successful. Example CRL: http://service.globaltrust.eu/static/globaltrust-2020-server-ov-1.crl
4.9.9. On-line Revocation/Status Checking Availability	GCP Section 4.9.9	The registry for suspension and revocation lists is publically and internationally available. It is not possible to prevent the publication of revocations and suspensions.

4.9.10. On-line Revocation Checking Requirements *Indicate how your CA meets all of the requirements listed in this section,* ***including support of GET, update frequency, preventing errounious return of "good" status.***	GCP Section 7	OCSP Check via https://certificate.revocationcheck.com/ was successful. GCP Section 7: OCSP service as per [RFC2560] and the relevant standards, as per [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]). An OCSP responder never delivers a "good" status back to an unknown certificates. The OCSP responses have a version number as per [RFC6960]. The OSCP responses can contain extension as per [RFC6960]. GCP Section 4.9.7: Revocation and suspension lists for servercertificates are valid for a maximum of 10 days (and updated at least every 7 days). OCSP answers are valid for 10 days (the data for which is updated every 4 days).
4.9.11. Other Forms of Revocation Advertisements Available Indicate if your CA supports OCSP stapling.	GCP Section 4.9.11	Users can request the current status of an issued certificate from the operator, e.g. by telephone. For certificates that are publicated in LDAP (which is the applicant's choice) there is also information on the revocation status: ldap.globaltrust.eu, port:389, simple authentication, Anonymous connection, c=at, o=GLOBALTRUST OCSP Stapling is not supported.
4.10.1. Operational Characteristics	GCP Section 4.9.7	Information on revoked certificates is kept until at least the expiry of the certificate (this is 35 years due to austrian signature law)
4.10.2. Service Availability	GCP Section 4.10.2	All Certificate status services are available 24/7/365.
5. MANAGEMENT, OPERATIONAL, AND PHYSICAL CONTROLS		
5.2.2. Number of Individuals Required per Task	GCP Section 5.2.2.	Critical processes are subject to the four-eyes principle. The persons involved are documented.
5.3.1. Qualifications, Experience, and Clearance Requirements	GCP Section 5.3 + 5.3.1	The detailed requirements are described internally
5.3.3. Training Requirements and Procedures	GCP Section 5.3.3	Employees are entrusted with certification tasks only after sufficient training.

5.3.4. Retraining Frequency and Requirements	GCP Section 5.3.4	Operations personnel are continually trained in the use of monitoring tools and other tools necessary for certification services. 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.
5.3.7. Independent Contractor Controls	GCP Section 5.3.7	Third party operators are be contractually bound to the requirements applicable for their task. The CA retains responsibility for the proper performance of certification services. A third party can never validate IP addresses or domain names An annual audit of the operator according to the Baseline Requirements is carried out.
5.4.1. Types of Events Recorded *Indicate how your CA meets the requirements of this section.*	GCP Section 5.4, 5.5	Please see GCP Sections
5.4.3. Retention Period for Audit Logs	GCP Section 5.4.3	as long as legally necessary (this is 35 years due to Austrian Signature Law)
5.4.8. Vulnerability Assessments *Indicate how your CA meets the requirements of this section.*	GCP Section 5.4.8 GCP Section 6.5.1	A risk assessment is carried out once a year, the details are doucmented internally. Internal and external vulnerability and penetration tests are regularly conducted
5.5.2. Retention Period for Archive	GCP Section 5.5.2	35 years
5.7.1. Incident and Compromise Handling Procedures *Indicate how your CA meets the requirements of this section.*	GCP Section 5.7.1	We have a disaster plan that is described in the Security Policy (not publically available.) It is part of the annual audits and has been approved by the Austrian Supervisory Body. Disaster plan and failure procedures are revised/tested once a year.

6.1.1. Key Pair Generation	GCP Section 6.1.1	"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."
6.1.2. Private Key Delivery to Subscriber	Not applicable	Not applicable: For SSL/TLS certificates, the key has always to be generated by the applicant. (GCP Section 6.1.2 only deals with other certification services.)
6.1.5. Key Sizes	GCP Section 6.1.5 + 7.1	RootCA GLOBALTRUST 2020: SHA-256, RSA 4096 bit All Issuing CAs: SHA-256, RSA 4096bit All Enduser Certificates: SHA-256, RSA at least 2048bit (if validity period not longer than 2022) or at least RSA 4096bit if validitiy longer than 2022) or for eliptical curves minimum 256 bits, and parameters: FR, Brainpool or NIST, each with a hash algorithm of the SHA2 family (from SHA256).
6.1.6. Public Key Parameters Generation and Quality Checking	GCP Section 6.1.6	confirmed
6.1.7. Key Usage Purposes	GCP Section 1.6 item "Root-certificate"	Root key are only used to sign CA certificates and CA Revocation List
6.2. Private Key Protection and Cryptographic Module Engineering Controls	GCP Section 6.2.	Comply. This is in detail described in the GLOBALTRUST Security Policy (not publically disclosed)

6.2.5. Private Key Archival	GCP Section 6.2.5	"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." Please notice that the rest of this section is not applicable to SSL certificates. We do not generate or archive private keys for subcribers
6.2.6. Private Key Transfer into or from a Cryptographic Module	GCP Section 6.2.6.	It is not possible to transfer private keys for CA certificates belonging to the operator.
6.2.7. Private Key Storage on Cryptographic Module	GCP Section 6.2.7 + GCP Section 6	"All private keys are stored on appropriate signature creation devices." For CA Private keys we currently use HSMs with certification according to FIPS-2 level 3
6.3.2 Certificates issued after March 1, 2018, MUST have a Validity Period no greater than 825 days *Indicate how your CA meets the requirements of this section.*	GCP Sections 6.3.2. , 4.2 , 4.6.3	The standard offer for ssl certificates is 1 or 2 years. Issuance of certificates that exceed 825 days validitiy is prevented by the certification tool. As of 1 September 2020 the validty period is limited to 397 days
6.5.1. Specific Computer Security Technical Requirements **The CA SHALL enforce multi-factor authentication for all accounts capable of directly causing certificate issuance.** *Indicate how your CA meets the requirements of this section.*	GCP Section 5.2.3	Hardware token with a certificate issued from a dedicated CA + password
7.1. Certificate profile **CAs SHALL generate non-sequential Certificate serial numbers greater than 0 containing at least 64 bits of output from a CSPRNG.** *Indicate how your CA meets the requirements of this section.*	GCP Section 7.1 paragraph 5	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)
7.1.1. Version Number(s)	GCP Section 7.1.1	The version number 3 according to [RFC5280] (X509v3) is supported.
7.1.2. Certificate Content and Extensions; Application of RFC 5280	GCP Section 7 GCP Section 7.1 - 7.9 GCP Section 1.6 items "Root certificate", "CA-Certificate" , "simple certificate", "further information in the certificate"	please see GCP Sections
7.1.2.1 Root CA Certificate		
7.1.2.2 Subordinate CA Certificate		
7.1.2.3 Subscriber Certificate		
7.1.2.4 All Certificates		
7.1.2.5 Application of RFC 5280		
7.1.3. Algorithm Object Identifiers		
7.1.4. Name Forms		
7.1.4.1 Issuer Information	GCP Section 7	The issuer string is always equal to the subject DN of the issuing CA, example certificate: https://testok-2020-server-qualified-ev-1.e-monitoring.at/
7.1.4.2 Subject Information - Subscriber Certificates	GCP 7.1.4	Attribute fields always contain a substantial entry

7.1.4.2.1 Subject Alternative Name Extension **This extension MUST contain at least one entry. Each entry MUST be either a dNSName containing the Fully-Qualified Domain Name or an iPAddress containing the IP address of a server. The CA MUST confirm that the Applicant controls the Fully-Qualified Domain Name or IP address or has been granted the right to use it by the Domain Name Registrant or IP address assignee, as appropriate. Wildcard FQDNs are permitted.** **CAs SHALL NOT issue certificates with a subjectAlternativeName extension or Subject commonName field containing a Reserved IP Address or Internal Name.** **Entries in the dNSName MUST be in the "preferred name syntax", as specified in RFC 5280, and thus MUST NOT contain underscore characters ("_").**	GCP 7.1.2 Certificate extensions	Please see detailed GCP Sections
7.1.4.2.2 Subject Distinguished Name Fields If present, this field MUST contain a single IP address or Fully-Qualified Domain Name that is one of the values contained in the Certificate's subjectAltName extension (see Section 7.1.4.2.1).	GCP 7.1.2 Certificate extensions	Please see detailed GCP Sections
7.1.4.3 Subject Information - Root Certificates and Subordinate CA Certificates	GCP Section 1.6 item "CA-Certificate"	from February 1, 2020: 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.

7.1.5. Name Constraints ***Indicate your CA's understanding of section 5.3 of Mozilla's root store policy, and requirement to disclose in the CCADB all subordinate CA certificates that are not technically constrained as described in this section of the BRs.*** ***"All certificates that are capable of being used to issue new certificates, that are not technically constrained, and that directly or transitively chain to a certificate included in Mozilla's root program:*** ***MUST be audited in accordance with Mozilla's Root Store Policy. ...*** ***MUST be publicly disclosed in the CCADB by the CA that has their certificate included in Mozilla's root program. The CA with a certificate included in Mozilla's root program MUST disclose this information within a week of certificate creation, and before any such subordinate CA is allowed to issue certificates. ..."***	GCP 2.2 GCP 1.6 item "enduser-sub-certificate"	Comply
7.1.6. Certificate Policy Object Identifier		
7.1.6.1 Reserved Certificate Policy Identifiers	Policy extension: GCP Section 7.1.6 Subject DN: GCP 7.1.4 and for EV 7.1 "In addition, the following applies for EV and qualified server certificates:"	always: 1.2.40.0.36.1.1.8.1 (GLOBALTRUST Certificate Policy) additionally: 2.23.140.1.2.2 (OV) or 2.23.140.1.1.1 (EV) and/or 0.4.0.194112.1.4 (ETSI 319 411-2 QCP-w)
7.1.6.2 Root CA Certificates	GCP 7.1.6	Comply, no policy extension in RootCA: http://service.globaltrust.eu/static/globaltrust-2020.txt
7.1.6.3 Subordinate CA Certificates	GCP 7.1.6	For SSL Certificates the folowing applies:
7.1.6.4 Subscriber Certificates	GCP 7.1.6	
8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS	GCP Section 8. Compliance Audit and other assessments	

8.1. Frequency or circumstances of assessment **The period during which the CA issues Certificates SHALL be dividied into an unbroken sequence of audit periods. An audit period MUST NOT exceed one year in duration.** For new CA Certificates: The point-in-time readiness assessment SHAL be completed no earlier than twelve months prior to issuing Publicly-Trusted Certificates and SHALL be followed by a complete audit under such scheme within ninety (90) days of issuing the first Publicly-Trusted Certificate. *Indicate your CA's understanding of this requirement, and how your CA meets the requirements of this section.*	GCP Section 8.1	External audits are conducted at minimum once a year. As we have a currently valid audit report for OV, we do not need to have a pre-issuance assessment. For EV, a pre-issuance assessment was carried out.
8.2. Identity/qualifications of assessor *Indicate how your CA meets he requirements of this section.*	GCP Section 8.2, GCP Section 1.3.5 Item "competent independent auditor"	Please see GCP Sections
8.4. Topics covered by assessment	GCP Section 8.4.	"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 (p148)."
8.6. Communication of results	GCP Section 8.6	Audit report is being made publicly available within 3 months.

Also indicate your understanding and compliance with section 3 of Mozilla's Root Store Policy, which says: "Full-surveillance period-of-time audits MUST be conducted and updated audit information provided no less frequently than annually. Successive audits MUST be contiguous (no gaps). .... The publicly-available documentation relating to each audit MUST contain at least the following clearly-labelled information: - name of the company being audited; - name and address of the organization performing the audit; - Distinguished Name and SHA256 fingerprint of each root and intermediate certificate that was in scope; - audit criteria (with version number) that were used to audit each of the certificates; - a list of the CA policy documents (with version numbers) referenced during the audit; - whether the audit is for a period of time or a point in time; - the start date and end date of the period, for those that cover a period of time; - the point-in-time date, for those that are for a point in time; - the date the report was issued (which will necessarily be after the end date or point-in-time date); and - For ETSI, a statement to indicate if the audit was a full audit, and which parts of the criteria were applied, e.g. DVCP, OVCP, NCP, NCP+, LCP, EVCP, EVCP+, QCP-w, Part1 (General Requirements), and/or Part 2.		Yes, annual full-audits are carried out. (NO surveillance audits) For the required content of the audit report, the auditors use ETSI TS 119 403, 4.3 which matches the mozilla requirements
8.7. Self-Audits	GCPS Section 5.4	Self assessments are conducted quarterly Samples of issued certificates are taken: 3% of OV certificates 6% of EV certificates another 3% of OV and EV, if a third party was involved in identification 3% of technical constrained SubCAs

9.6.1. CA Representations and Warranties	GCP Section 9.6.1	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
9.6.3. Subscriber Representations and Warranties	GCP Section 9.6.3	The general terms and conditions, GCP and GCPS apply.
9.8. Limitations of liability	GCP Section 9.8	
9.9.1. Indemnification by CAs	GCP Section 9.9	
9.16.3. Severability		We confirm that there is no applicable Law in direct conflict with BR. We confirm that we have read and understood the obligations and will notify any relevant case immediately upon our awareness.
APPENDIX A - RFC 6844 ERRATA 5065 To prevent resource exhaustion attacks, CAs SHOULD limit the length of CNAME chains that are accepted. However CAs MUST process CNAME chains that contain 8 or fewer CNAME records.		Currently we process any CNAME chain
APPENDIX B – DNS CONTACT PROPERTIES These methods allow domain owners to publish contact information in DNS for the purpose of validating domain control.		