Certificate Policy of the E.ON SE PKI

Version 12th October 2015

Version	Date	Description
1.1 EN	01.02.2014	Initial version – based on D-TRUST Root PKI v. 1.8
1.1	01.11.2014	- Editorial changes - Specification of the revocation process via the EIDM - Specification of the process for job changes within the E.ON Group
1.3	22.06.2015	Addition of handover procedures during organisational changes for encryption keys with revoked encryption certificates
1.4	12.10.2015	Concretion of certificate usage on mobile devices

This is a translation of the Certificate Policy published in German language to be found here: www.eon.com/pki.

Should the English translation differ from the German original, the German version is binding.

D-TRUST GMBH
Kommandantenstr. 15
10969 Berlin, Germany
Tel: +49 (0)30 259391 0
E-Mail: info@d-trust.net

F60DE179W02

Table of contents

1. Introduction

1.1 Summary

This document describes the certificate policy (CP) of the E.ON SE PKI operated by D-TRUST GMBH.

The E.ON SE PKI is referenced by a Sub-CA below the “D-TRUST Root CA 3 2013”.

1.1.1 Certification service provider

The trust service provider (TSP) is

D-TRUST GMBH
Kommandantenstr. 15
10969 Berlin.

The TSP can outsource sub-tasks to partners or external providers with which the TSP maintains a properly documented agreement and an established contractual relationship at the time the services are provided.

The responsibility for compliance with this CP is borne by the head or the management of the TSP.

1.1.2 About this document

This CP sets parameters and requirements for the Root-PKI and thus regulates the certification process during the entire life of the end entity certificates (EE certificates) as well as the co-operation, rights and duties of the PKI participants[1].

This CP is part of the extIDENT agreement between the TSP and E.ON SE and is thus legally binding so far as permitted under German legislation. It contains statements on the duties, warranty and liability of PKI participants. Unless expressly stated, no warranties or guarantees in the legal sense can be derived on the basis of this CP.

The legally binding nature as well as the processes involving points a) provision of the CA, b) production of certificates on key material provided, c) provision of certificate revocation lists

[1] In the interests of making this document easier to read, the feminine form of PKI participant and of other specified groups of people is omitted. Users are kindly requested to regard the feminine form as included.

and d) provision of the OCSP service are defined conclusively by the CP and CPS documents. They are not subject to the German *Signaturgesetz* (Digital Signature Act) or other statutory regulations that pertain to an electronic signature of whatever kind. Any use of terms that are similar to or the same as those in the German Digital Signature Act is not to be regarded as a reference to the German Digital Signature Act.

Knowledge of the certification processes and rules described in this CP and of the general legal framework allows certificate users to develop trust in the components and PKI participants and to make decisions on to what extent the confidence and security level granted by the PKI is suitable for applications.

The structure of this document is based closely on the Internet standard RFC 3647 *Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework* in order to make it easy to read and to compare with other CPs.

1.1.3 Attributes of the PKI

The E.ON SE PKI has a multi-tiered hierarchy. Figure 1 shows one possible configuration of the E.ON SE PKI.

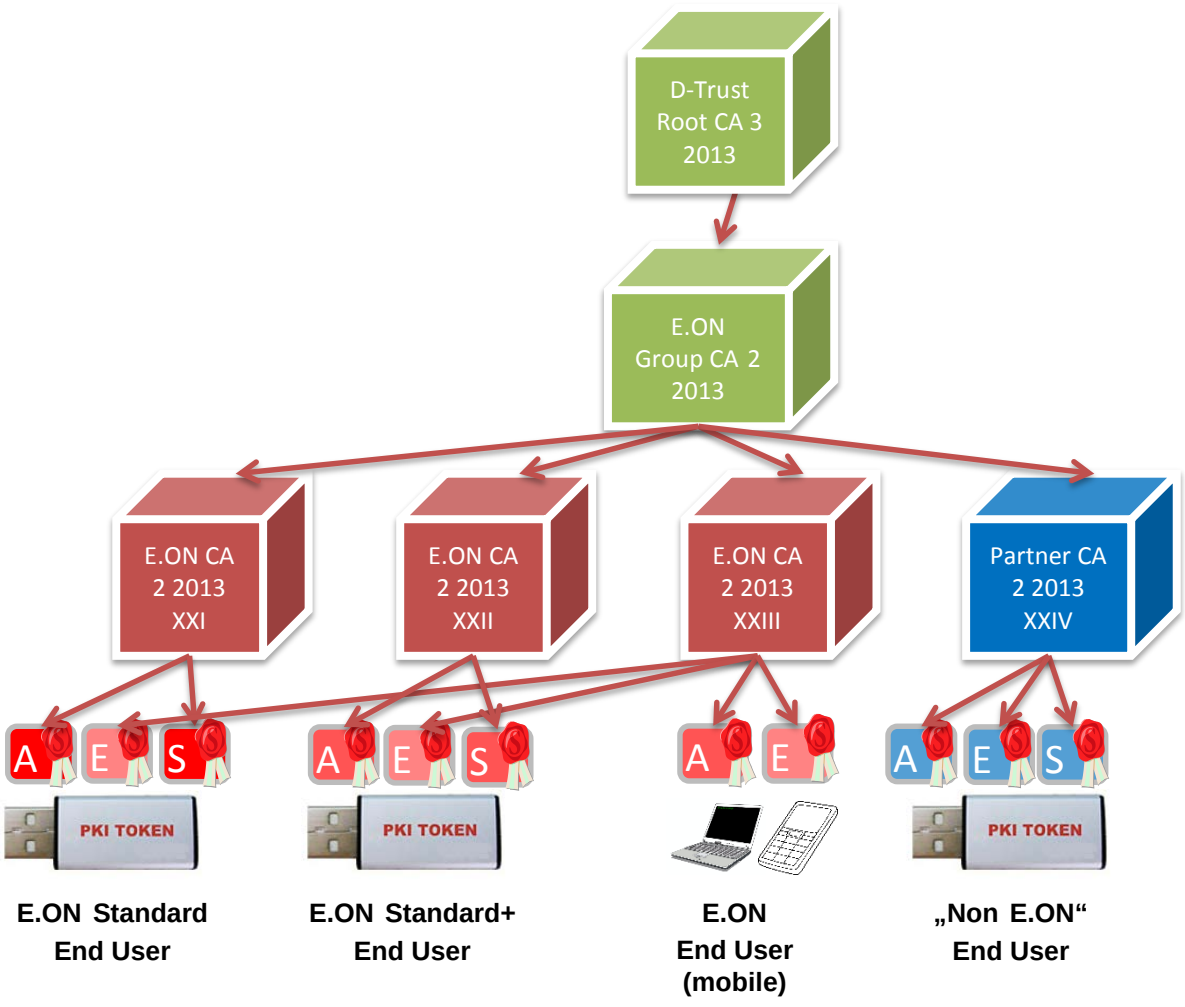


Figure 1 Structure of the issuing CAs and end user certificates

The EE and CA certificates are subject to the LCP security level. LCP certificates are high-quality, but unqualified certificates that fulfil the requirements of [ETSI-F] LCP. E.ON SE uses an E.ON SE Group CA under the D-Trust Root CA and under that the E.ON SE issuing CAs that issue the end user certificates.
Authentication, signature and encryption certificates are issued.

1.2 Document name and identification

Document name:	Certificate policy of the E.ON SE PKI
Object identification (OID):	This document is assigned the policy OID: 1.3.6.1.4.1.4788.2.210.1
Version	1.4

1.3 PKI participants

1.3.1 Certification authorities

The certification authorities (CAs) issue certificates and certificate revocation lists. The following types of certificates are possible:

- personal certificates for individuals (EE certificate);
- group certificates for groups of people, functions and IT processes (EE certificate);
- certification authority certificates (subordinate CA certificates of the TSP).

The root certification authorities issue certificates exclusively with the extension *basicConstraints: cA=TRUE* (CA certificate) pursuant to [X.509]. Subordinate CAs issue EE certificates and/or other CA certificates. The certification authority is named in the field *issuer* in the issued certificates or CRLs.

The employees in charge of issuing certificates are free from commercial, financial and other influences of the organisation.

1.3.2 Registration authorities (RA)

As an RA, E.ON SE identifies and authenticates end users using defined processes (see section 4), records and verifies applications for various certification services.

1.3.3 Subscribers

The subscriber is E.ON SE, which applies for and owns the EE certificate. The subscriber can be different from the *subject* named in the certificate. The duties of the subscriber are subject to separate contractual agreements.

The subscriber bears the responsibility for the key and content of the certificate. Other duties are additionally produced according to [ETSI-F]. The subscriber will indicate these duties to the end user no later than at the time of the application.

1.3.4 End entity (EE)

End users (subject; end entity (EE)) use the private end entity key (EE key). The identity of the end user is linked to the certificate and the related key pair. Permitted end users are individuals or groups of persons who have a Group ID administered by means of the E.ON SE identity management (EIDM) (e.g. E.ON employees or contractual partners and service providers with an active IT account) as well as functions and IT processes.

1.3.5 Relying party

Relying parties are individuals or legal persons who use the certificates of this E.ON SE PKI (e.g. to verify signed documents) and have access to the services of the TSP.

1.4 Certificate usage

1.4.1 Permitted certificate uses

CA certificates are used exclusively and in accordance with their extension (*BasicConstraints*) pursuant to [X.509] for issuing CA or EE certificates and CRLs.

EE certificates may be used for applications that are consistent with the types of usage indicated in the certificate.

Relying parties act under their own responsibility. It is the responsibility of the relying party to assess whether this CP meets the requirements of an application and whether the use of the certificate in question is suitable for a specific purpose.

1.4.2 Prohibited certificate uses

Uses other than those defined in the certificate are not permitted.

1.5 Maintenance of the CP/CPS

1.5.1 Document administrator

This CP is maintained by D-TRUST GMBH in co-operation with E.ON Business Service GmbH. The head of the TSP of D-TRUST GMBH is responsible for approving the document.

1.5.2 Contact person/secretariat

The following address can be contacted:

D-TRUST GMBH
Redaktion CP und CPS
Kommandantenstr. 15
10969 Berlin, Germany

Tel.: +49 (0)30 259391 0
E-mail: info@d-trust.net

E.ON SE as the subscriber is represented by:

E.ON Business Services GmbH
Information Security
Humboldtstraße 33,
30169 Hanover, Germany

E-mail: pki@eon.com

1.5.3 Compatibility of CPs of other CAs with this CP

This CP describes minimum requirements that have to be fulfilled by all PKI participants.

Other CPs that do not conflict with this CP can be referenced both in CA and in EE certificates through policy OIDs. The reference to a policy OID in the certificate extensions is confirmation by the CA of the compatibility of the certification practices with the referenced CP (LCP (0.4.0.2042.1.3) pursuant to [ETSI-F]).

1.6 Definitions and abbreviations

1.6.1 German definitions and names (translated)

Authentication certificate	Certificate with which an end user can identify themselves to an IT system.

Confirmer	Employee or manager who confirms the identity of colleagues for the certificate applications in the standard and standard+ process.
CA certificate	The certificate issued for a certification authority for the signature key of the certification authority.
D-TRUST Root CA	Root certification authority.
D-TRUST Root-PKI	PKI operated by D-TRUST GMBH.
E.ON SE PKI	PKI operated by D-TRUST GMBH for E.ON SE.
EE key	Also end entity (user) key, private key of the EE certificates.
EE certificate	Also end entity (user) certificate, see end entity certificate.
End user	Also *subject*, the identity of the end user is linked to the certificate and the related key pair, see also section 1.3.4.
End entity certificate	Certificate that may not be used to certify other certificates or CRLs. This includes signature, authentication and encryption certificates EE certificates may be used only for applications that are consistent with the types of usage indicated in the certificate.
Global Service Desk	Global Service Desk of HP for the end users of the E.ON SE PKI (GSD).
History certificates	Expired encryption certificates, the keys of which can be stored for later decryption of data and recreated by authorised end users.
KID (Group ID)	IT identifier that is unique, but not one-to-one and that cannot be reused, of each IT end user in the E.ON SE global directory Only individuals are given primary Group IDs and can thus receive end user certificates, as long as they are active. Secondary Group IDs (e.g. for e-mail, group mailboxes) are also always to be assigned to an individual as the owner, a responsible individual can thus always be clearly identified. Attributes that can be assigned to a Group ID are applied and managed using audited processes from HR and contract management systems.
LCP certificate	EE certificate that has been created according to ETSI TS 102 042 Lightweight Certificate Policy (LCP).

PKI supervisors	PKI supervisors form the central interface between E.ON SE and D-TRUST GMBH in all process issues of the extIDENT contract including CP and CPS for the E.ON SE PKI. This group answers questions on all PKI processes of the E.ON SE PKI and decides on all internal E.ON enquiries for the E.ON SE PKI in accordance with the extIDENT contract including CP and CPS.
PKI token	For the E.ON PKI, various form factors of smartcards that are managed using a smartcard management system are used under the designation PKI token. The PKI tokens currently include ISO-conformant smartcards as well as smartcard in the form of a USB token and a micro SD card. PKI token, USB PKI token, smartcard and PKI medium are used synonymously in instructions and documentation.
Q environment	Quality assurance systems that are used to test configuration changes and upgrades.
Registration authority	Also RA, PKI facility that conducts participant identification, see section 1.3.2.
Revocation authority (third party)	An individual or legal person that is authorised to revoke a certificate.
Signature card / smartcard	Processor chip card that can be used to generate electronic signatures as well as for other PKI applications. They are used in various form factors, such as ISO-conformant smartcards, USB tokens and even in micro SD format.
Signature certificate	Certificate that is used to generate electronic signatures.
Status request service	PKI service for online querying of the status of a certificate (OCSP).
Declaration of commitment	Instruction of the end user on its duties when handling EE keys and certificates.
Encryption certificate	Certificate that is used to encrypt electronic data.
Directory service	PKI service for the online retrieval of information, such as certificates and certificate revocation lists, generally operated using the LDAP protocol.
Subscriber	An individual or legal person who applies for and owns EE certificates, see section 1.3.3.
Relying party	An individual or legal person who uses certificates, see section 1.3.5.

Certificate policy	CP, see section 1.1.
Trust service provider	Provider of certification re trust services (former CSP).
Certification authority	CA, authority of the Root PKI, see section 1.3.1.

1.6.2 English definitions

CP, see section 1.1.	Certificate policy.
Certification Authority (CA)	Authority of the Root PKI, see section 1.3.1.
Distinguished Name	A technical name consisting of several name elements that clearly describes in certificates the issuing CA and/or the subscriber within the Root PKI. The Distinguished Name is defined in the standard [X.501].
Registration authorities (RA)	RA, PKI facility that conducts participant identification, see section 1.3.2.
Soft-PSE	Software Personal Security Environment, also called software token, contains the EE key pair, the EE certificate and the certificate of the issuing CA.
Token	Carrier medium for certificates and key material.
Trustcenter	The secure area on the premises of D-TRUST GMBH.
Certificate Policy (CP)	Certificate policy.
Certification Authority (CA)	Authority of the Root PKI, see section 1.3.1.
Distinguished Name	A technical name consisting of several name elements that clearly describes in certificates the issuing CA and/or the subscriber within the Root PKI. The Distinguished Name is defined in the standard [X.501].
Registration Authority (RA)	PKI facility that conducts participant identification, see section 1.3.2.
Soft-PSE	Software Personal Security Environment, also called software token, contains the EE key pair, the EE certificate and the certificate of the issuing CA.
Token	Carrier medium for certificates and key material.
Trustcenter	The secure area on the premises of D-TRUST GMBH.

1.6.3 Abbreviations

BRG	Baseline Requirements Guidelines
CA	Certification Authority

CN	Common Name
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DN	Distinguished Name
EAL	Evaluation Assurance Level
EIDM	E.ON Identity Management-System
FIPS	Federal Information Processing Standard
FQDN	Fully qualified domain name
GSD	Global Service Desk
HSM	Hardware Security Module
ISO	International Organization for Standardization
KID	E.ON SE Groupwide Account
LCP	Lightweight Certificate Policy
LDAP	Lightweight Directory Access Protocol
NetSec-CAB	Network Security Requirements- CA/Browser Forum
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PUK	Personal Unblocking Key
RA	Registration Authority
RFC	Request for Comment
SCM	Smartcard Management System
SSCD	Secure Signature Creation Device
SUD	Secure User Device
TSP	Trust Service Provider
URL	Uniform Resource Locator
UTF8	Unicode Transformation Format-8

1.6.4 References

[AGB]	Allgemeine Geschäftsbedingungen der Bundesdruckerei GmbH für den Verkauf von Zertifizierungsdiensten der D-TRUST, aktuelle Version
[BRG]	Baseline Requirements des CA/Browser Form, CA/Browser Forum, Version 1.3.0, 16. April 2015
[CP]	Zertifikatsrichtlinie der E.ON SE PKI, D-TRUST GMBH, aktuelle Version
[CPS]	Certification Practice Statement der E.ON SE PKI, D-TRUST GMBH, aktuelle Version
[Co-PKI]	Common PKI Specification, Version 2.0 vom 20. Januar 2009
[ETSI-F]	ETSI, Technical Specification Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates, ETSI TS 102 042 V2.4.1, Feb. 2013
[GL-BRO]	Guidelines for Issuance and Maintenance of Extended Validation Certificates, CA/Browser Forum, Version 1.5.5, 16. April 2015
[ISO 3166]	ISO 3166-1:1997: Codes for the representation of names of countries and their subdivisions - Part 1: Country codes
[NetSec-CAB]	CA / Browser Forum Network and Certificate System Security Requirements, Version 1.0, 1.1.2013
[RFC 2247]	Using Domains in LDAP/X.500 Distinguished Names, January 1998
[RFC 2560]	X.509 Internet Public Key Infrastructure – Online Certificate Status Protocol – OCSP, June 1999
[RFC 3647]	Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework, November 2003
[RFC 5280]	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, Mai 2008
[SigG]	Signaturgesetz (Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz – SigG) vom 16. Mai 2001 (BGBl. I S. 876), zuletzt geändert durch Artikel 4 des Gesetzes vom 17. Juli 2009 (BGBl. I S. 2091)
[SigV]	Verordnung zur elektronischen Signatur vom 16. November 2001 (BGBl. I., S. 3074), zuletzt geändert durch die Verordnung vom 5. November 2010 (BGBl. I S. 1542))

[SiKo-DTR]	Sicherheitskonzept des signaturgesetzkonformen Zertifizierungsdiensteanbieters D-TRUST GMBH
[X.501]	ITU-T RECOMMENDATION X.501, Information technology – Open Systems Interconnection – The Directory: Models, Version August 2005
[X.509]	ITU-T Recommendation X.509 (1997 E): Information Technology – Open Systems Interconnection – The Directory: Authentication Framework, June 1997

2. Repository and publication responsibilities

2.1 Repositories

The TSP publishes CRLs and CA certificates in the LDAP directory at: ldap://directory.d-trust.net (Internet) or ldap://cdp-ldap.intranet.eon.com (internal E.ON).

The full links specific to each certificate can be found in the certificates themselves.

The CA certificates can additionally be accessed using the following http path: http://pki.intranet.eon.com/cacerts/ (internal E.ON)

The CRLs certificates can additionally be accessed using the following http path: http://pki.intranet.eon.com/crls/ (internal E.ON)

The TSP provides an online service (OCSP) to enquire about the revocation status of certificates of the E.ON SE PKI. The status of the certificates can be accessed using this service for a minimum of one year after the validity of the certificates has expired.

This CP and the declaration of commitment (subscriber's obligations) are provided to requesters during the request process. Additionally they can be downloaded as a pdf file from the E.ON SE website (http://www.eon.com/pki).

Other information and terms and conditions of use not included in this CP will be provided to the end user during the registration process.

2.2 Publication of certificate information

The TSP publishes the following information on the E.ON SE PKI:

- CA certificates (trust anchor);
- certificate revocation lists (CRLs) and status information;
- this CP.

Where there is a legitimate interest, extracts of the CPS can be obtained both from D-TRUST GMBH and from E.ON SE.
EE certificates are not published by the TSP in the E.ON SE PKI.

2.3 Frequency of publications

CA certificates are published after they are issued and are retained for at least 1 year and up to the end of the year after the validity of the CA has expired.

Certificate revocation lists are issued on a regular basis and until the validity of the issuing CA certificate has ended. Certificate revocation lists will be issued and published immediately after a certificate is revoked. Even if there have been no revocations, the TSP will ensure that certificate revocation lists are issued at least every 72 hours. The certificate revocation lists are retained for a minimum of one year after the validity of the CA has expired.

As stated in section 2.1, this CP will be published and remain accessible for at least as long as certificates that have been issued on the basis of this CP are valid.

2.4 Repository access controls

CA certificates, certificate revocation lists and CPs are publicly accessible free of charge. There are no restrictions on read-only access. Changes to the directory and web content are carried out exclusively by the TSP.

Where there is a legitimate interest, the relevant parts of other documents that are not public can be issued upon request.

3. Identification and authentication

3.1 Naming conventions

3.1.1 Types of names

CA and EE certificates basically contain information on the issuer and subscriber or end user (*subject*). These names are assigned in accordance with the standard [X.501] as *DistinguishedName*.

Alternative names can be registered and recorded in the *subjectAltName* extension of the certificates.

3.1.2 Need for names to be meaningful

The Distinguished Name used is unique within the E.ON SE PKI. A unique assignment of the certificate to the end user is given by the use of the E.ON Group ID.

In the case of alternative names (*subjectAltName* in accordance with [X.509]), there is no need for names to be meaningful.

This information may not contain any references to the certificate itself. IP addresses are not permitted.

3.1.3 Subscriber anonymity or pseudonymity

Pseudonyms are used exclusively for individuals. Group IDs that are used at pseudonyms in the CN in authentication certificates consist exclusively of a Latin letter followed by at least four Arabic numerals. These Group IDs are not marked separately as pseudonyms (personal and unique Group ID of E.ON SE).

3.1.4 Rules for interpreting various name forms

The procedure for recording and interpreting names is defined in the [CPS].

The attributes of the *DistinguishedName* (DN elements) of EE certificates are interpreted as follows:

DN element	Interpretation
CN	*Common name*: The following variants are used: - Individuals with no pseudonym: "(optional)academic title<space>given name<space>family name". - Individuals with pseudonym: "Pseudonym:PN" or "Pseudonym" if this consists exclusively of a Latin letter followed by at least four Arabic numerals (personal and unique Group ID within E.ON SE). - Function or group of persons: Team designation formed from e-mail prefix and "team certificate".
serialNumber	*Serial number*: Name affix that guarantees the unique character of the DN (personal and unique Group ID within the E.ON Group).
O	Official designation of the *organisation*, of the related PKI structure (E.ON SE or eon).
OU *(optional)*	OU fields are filled in exclusively for technical purposes.
C	The country to be listed is noted in accordance with [ISO 3166] and is produced as follows: if an organisation O is listed in the Distinguished Name, then the registered office of the organisation determines the country C.

The way names are spelled in the certificate is determined by the EIDM management processes. In cases of doubt, the persons can be clearly identified by the subscriber using the Group ID.

Not all of the above-mentioned DN elements have to be used.
Others can be added.

Additional DN elements must comply with [RFC 5280] and [Co-PKI].

3.1.5 Uniqueness of names

The TSP ensures that a name (Distinguished Name) of the subscriber or of the end user (*subject* field) used in EE certificates is always unique within the E.ON SE PKI and after the lifecycle of the certificate has ended and is always assigned to the same subscriber or end user. The uniqueness is achieved using the Group ID. As a result, the unique identification[2] of the subscriber is guaranteed by the name used in the EE certificate (*subject*). It is possible for several Group IDs to be assigned to one end user.

[2] Identification here means the naming of the subscriber and their current data at the time the first application is submitted (not subsequent applications). It does not mean the elicitation of current data or the location of the subscriber at a later date.

In the context of the E.ON SE PKI, the uniqueness of user certificates is permanently achieved (also when names are changed, e.g. as a result of marriage) by indication of the Group ID in the certificate subject.

The TSP ensures the uniqueness of Distinguished Names in CA certificates.

3.1.6 Recognition, authentication and the role of trademarks

The subscriber is responsible for ensuring that they comply with intellectual property rights in their application and certificate data (see section 9.4).

3.2 Initial identity validation

3.2.1 Proof of ownership of the private key

Key pairs are produced within the scope of responsibility of the subscriber. Technical proof of possession of the private key must be furnished or possession must be verifiably confirmed by the subscriber.

3.2.2 Identification and authentication of organisations

Certificates for legal persons are not offered. Organisations that are named in the certificate are subsidiaries and partner companies of E.ON SE or companies in which E.ON SE holds an equity interest. As the RA, E.ON SE takes on the authentication of the organisations that are named in the certificate.

3.2.3 Identification and authentication of individuals

Individuals who apply for the certificates and who are named in the certificate must authenticate their identity without a doubt and furnish proof of their right to submit an application through the organisation. As the RA commissioned by the TSP, E.ON SE takes on the authentication of end users that are named in the certificate.

The requirements of section 3.2.2 and 4.1.3 shall apply.

3.2.4 Unverified subscriber information

The information of the subscriber is validated or not validated in accordance with sections 3.2.2 and 4.2.1.

3.2.5 Validation of authority to make an application

Applications may be made by individuals. The procedures are defined in the CPS.

3.2.6 Criteria for interoperability

See section 1.5.3.

3.3 Identification and authentication of applications for rekeying

Rekeying is not performed.

3.4 Identification and authentication of revocation applications

The TSP validates the authority of the revocation applicant to make the application before it revokes an EE certificate.

The revocation authority is validated as follows:

In the case of an application for revocation that is received in a *signed e-mail*, the revocation applicant must himself be the subscriber or have been named as a revocation authority of a third party, whose signature certificate used in the revocation e-mail must be provided to the TSP.

If a revocation takes place on the *online interface*, the transmission is secured on one side by an SSL certificate and the revocation application itself with a technical signature. Additionally, the revocation application will be sent along with the revocation password to the TSP.

Revocation applications via the online interface can also be submitted for third parties within E.ON SE PKI. For this, the party requesting the revocation must be logged on to the request with his personal token in the smartcard management system and authenticated.

Other procedures to authenticate revocation applications can be agreed with the subscriber.

Revocation procedures are defined in section 4.9.

4. Operating requirements

4.1 Certificate application and registration

4.1.1 Eligibility to apply for a certificate

Applications may be initiated by certain end users at E.ON SE who have been given this authority by the company (Group ID) and who can authenticate their identity to the RA.

When an employee or service provider commences a contract at E.ON SE, a dataset is created in a defined and trustworthy source system by the competent personnel or contract management department. An identity is generated from this once a day in E.ON's central secure Enterprise Directory. This directory is an essential part of the E.ON Identity Management System (EIDM). Changes to these programs/processes are subject to a strict change management system and are co-ordinated with the TSP.

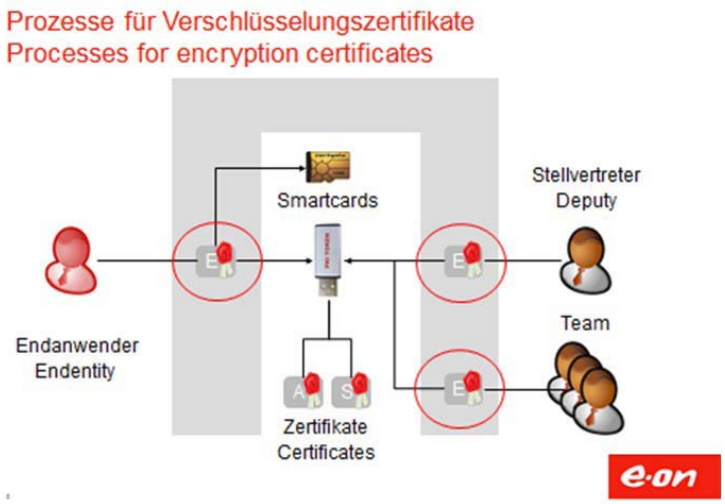
Unauthorised changes to EIDM data are not provided for, but may be carried out only in leading data sources by a restricted group of people on a request basis (in writing, traceable for audit compliance) and are individually logged there.

All EE keys (signature, encryption and authentication) are generated in the subscriber's control area.

Private EE keys that are not signature keys[3] can be securely escrowed in accordance with the specifications of the [CPS] for later reuse (key escrow, reuse in a new token) in data storages authorised by the TSP.

The escrowed encryption keys of an end user from SubCA XXIII can initially be accessed only by the authenticated end user herself, who can transfer these as history certificates to her PKI medium in order to access data encrypted for previously valid public keys.

[3] A signature key is a key for which a certificate is issued that contains the public key of the key pair and where the key use includes either "digital signature" or "contentCommitment" or "nonRepudiation".



An end user can define deputies through a workflow, who thus receive access to the end user's private decryption keys and can additionally transfer these to their PKI media in order to be able to access encrypted e-mails in the mailbox of the user in the context of the tasks of a deputy or assistant.

Team certificates differ in that the team leader can act as the owner of the certificate using a function Group ID and establish his primary Group ID and the Group IDs of the team members as deputies.

Deputies are thereby also given the option of obtaining the private keys of these certificates, if these certificates can be used exclusively for decryption.

Because of the need to protect this application, the SCM is administered only by a small group of people using the dual control principle, and will explicitly clear changes by PKI supervisors of E.ON SE.

CA certificates of the E.ON SE PKI are assigned exclusively to E.ON SE.

The TSP is entitled to reject applications (see section 4.2.2).

4.1.2 Registration process and responsibilities

The CP and a declaration of commitment (subscriber's agreement) as well as other documents are already provided to the subscriber and the end user at the beginning of the registration process in order to enable them to inform themselves of the conditions governing the use of the certificated being applied for.

Two registration processes are provided for in the E.ON SE PKI (Standard and Standard Plus); they are based on preregistered data from the identity management system and its audited data management processes.

The focal point of the standard process is to relocate the user identification into the co-operative environment, where the effectiveness and efficiency of the secure identification should be increased by the personal knowledge between end user and confirmer.

Authentication by the confirmer and confirmations with advanced signatures represent a deterrent to misuse. These features and the accurate audit task are made clear to the confirmers before confirmation. Attention is to be paid there that the confirmer must indicate the identifier (identity card, passport or personal relationship as a colleague) that has been used to identify the end user.

Applied consistently in the checking process, the dual control principle makes it difficult for the individual to come into possession of others' key pairs without being noticed.

4.1.3 Standard and Standard Plus process

The Standard process is the normal process used to identify end users.

The Standard Plus process is provided for specific locations in the E.ON SE Group that have extended process requirements. Here, only confirmers from an explicitly named group of confirmers may carry out the confirmation task. The two processes issue certificates of the same kind: authentication and signature certificates, where certificates based on the Standard Plus process are issued by a separate sub-CA.

Encryption certificates are also issued by a separate sub-CA that can issue authentication certificates as well; their assignment is permitted outside certified PKI media so that they can be used on mobile devices or in applications that cannot access smartcards and similar tokens.

The process is run on the software side by a process engine. The process has been modelled on the special requirements of E.ON SE and consequently safeguards the whole sequence of the process and the data flow between end user, confirmer and the TSP.

4.1.4 Standard process

The standard process can be used only by individuals who possess an active IT account at E.ON SE that has a unique designation from a primary Group ID. The standard process consists of the following steps:

1. An end user accesses the application URL in the E.ON SE intranet using a standard browser. He signs in with his Group ID and Windows password (if he does not yet have a token) or using an existing certificate.
2. When requested, the end user inserts a PKI medium pre-initialised for E.ON (smartcard or USB PKI token) in his computer and starts the end user-specific card initialisation.
   The applicant confirms that he has read and accepts the terms and conditions of use as well as the subscriber's obligations.
   In this process, keys for authentication and signature are generated for the end user on the card. Only the public key is transmitted to the SCM. The key pair for the encryption certificates is generated centrally by the SCM. By inputting an individual PIN, the end user takes possession of the card. The corresponding certificate requests are now generated by the E.ON SE smartcard management system (SCM); they have to be approved by one or two confirmers.
3. The end user has to propose two confirmers from the EIDM; they must already be in possession of a valid EE certificate.
4. If the applicant has already been authenticated with a legitimate certificate, only one confirmer is required, as the validation of the identity has already been performed once.
5. Concluding this step of the process, the end user receives an e-mail with which he can access the status of this process at any time and, if necessary, cancel it and start again.
6. The first confirmer receives an e-mail with a link to the confirmation process step in the standard process. This can only be conducted in an authenticated way with a legitimate authentication and signature certificate. The consent is signed here with the token of the confirmer and filed with the request in the database.
7. The first confirmer answers the displayed questions whether he knows the end user personally, how he has identified the application, whether the application data displayed is correct, and then signs the confirmation, if appropriate, with his signature certificate.
8. The second confirmer carries out the same steps as the first confirmer. The second confirmer may be omitted if the applicant signed into SCM using a valid E.ON PKI authentication certificate.
9. If the conditions for the issue of EE certificates are met after successful confirmation, the certificate applications are transmitted to the CA. After the certificates arrive, the end user receives an e-mail message with a URL that he can use download the certificates and install them on the smartcard.
10. To carry out the installation process for the certificates on the token, the end user has to authenticate his identity again using an existing token or user name/password. In addition to his token, he also needs the PIN that he has assigned.

The end user confirms again that he has read and accepts the terms and conditions of use and the subscriber's obligations.
After installation, the end user acknowledges receipt of the certificates by signing the confirmation of receipt using the newly issued card.
Exception: If no signature certificate does exist user will confirm receipt of ordered certificates manually.

4.1.5 Standard Plus process

The Standard Plus registration process is required in order to fulfil particular registration requirements in certain organisational units. This makes it possible for appropriately configured applications and portals to identify and verify certificates that have been issued following this slightly stricter registration process.

In contrast to the Standard registration process, the first confirmation is conducted on site by a local confirmer specified by the system (employee with defined role).

4.1.6 Variante des Prozesses für alle E.ON Endanwender für mobile Endgeräte

For users of processes described above authentication and encryption certificates are granted from CA XXIII as software certificates as well.
Transport of these towards applications must be encrypted.
Application must grant exclusive control for usage of private keys to user.
Users can order their recent encryption certificate, an encryption key or a similar authentication key from scratch at known self-service portal as software certificate.
Order will be verified and approved analogue to standard process.
Creation and handover of certificates is realized in a multi-step approach:

1. An end user retrieves the application URL in the E.ON SE intranet using a standard browser. He authenticates with his Group ID and Windows password (if he does not yet have a token) or using an existing certificate either from Standard CA (CA XXI) or from Standard+ CA (CA XXII). Certificates from CA XXXIII are excluded.
2. The applicant confirms that he has read and accepts the terms and conditions of use as well as the subscriber's obligations.
3. The key pair for authentication or encryption certificate (if new) is generated centrally by the SCM. A key pair for the current encryption certificate has both been generated and stored by HSM already and will be recovered or is generated during process if valid encryption key is missing. The corresponding certificate requests are now generated for all new keypairs by the E.ON SE smartcard management system (SCM); they have to be approved by one or two confirmer, according to the earlier authentication level, who must possess valid certificates (authentication for access SCM, access to encrypted p12-file in case of two confirmers).

4. User can decide whether she wants to receive the PIN per encrypted e-mail or alternatively in case of missing encryption certificate selects two users, who will receive one half of 12 digit random generated PIN each per encrypted e-Mail.
5. If the conditions for the issue of EE certificates are met after successful confirmation, the certificate applications are transmitted to the CA. After the certificates arrive, the end user receives an e-mail message with a URL where she can download the certificates and install the keys in an E.ON approved application. Download of certificates can be initiated by approved applications as well.
6. If user has already encryption keys on a smartcard, she will be asked during issuing process to synchronize her media self-dependent.
7. During download of certificates via office computer the end user confirms again that she has read and accepts the terms and conditions of use and the subscriber's obligations.
8. During installation procedure the user must enter the complete PIN from step 4.
9. The installation process itself starts based on p12 file. After successful installation user will confirm receipt of certificates to self-service portal either directly or via application which was used during installation.

4.2 Processing of certificate applications

4.2.1 Implementation of identification and authentication

The identification and registration process described must be completed in full and all necessary supporting documents must be furnished.

The authentication of individuals or organisations as well as the verification of other data relevant for the certificate can be made before or after the application is submitted, but must be concluded before the certificate application is handed in to the CA.

Individuals must be clearly identified. If legal persons are subscribers, the full name and the legal status as well as any relevant registry information must be verified.

Identification is carried out in accordance with section 3.2.3. The applicable procedures are defined in the CPS.

4.2.2 Approval or rejection of certificate applications

If the request for a certificate using the agreed online interface contains technical errors or the contents is incorrect, the application will be rejected. The corresponding online interface here transmits the reasons why the application has been rejected. The application is to be corrected accordingly and resubmitted.

Other reasons for rejecting an application can include:

- suspicion of an infringement of third-party name rights;
- failure to observe the time limits for verifying the data;
- circumstances that give rise to the suspicion that the issue of a certificate will discredit the operator of the CA.

Only after the TSP has completed a positive verification of the certificate application and the certificate applied for has been handed over (cf. section 4.4) is the application approved as unconditional.

4.2.3 Time limits for processing certificate applications

Not applicable

4.3 Issuance of certificates

4.3.1 Procedure of the TSP when issuing certificates

After the application has been verified with a positive result, the corresponding certificate is produced in the high security area of the Trustcenter. The application datasets and supporting documents are archived in a tamper-proof manner.

The TSP ensures that the correct time is used when the certificate is issued.

4.3.2 Notification to the subscriber of the issuance of the certificate

A separate message is not sent to the subscriber by the TSP after the certificate has been produced.

End users will be informed by the subscriber.

4.4 Delivery of the certificate

4.4.1 Conduct during the delivery of the certificate

If a certificate is issued for a subscriber's existing key pair, the certificate is either made available for download (e.g. published in the directory service) or sent electronically.

Different, customer-specific procedures can be agreed. If the subscriber discovers errors in his certificates or in the functions of the key or token, he has to notify these to the TSP immediately. The certificates will be revoked.

Further details can be found in the CPS.

Incorrect information in the certificates are regarded as contractual defects within the meaning of the contract only in so far as the TSP had to perform a check of the information affected by the error.

No acceptance procedure is carried out by the customer, as the process involves the performance of services, not the performance of work.

4.4.2 Publication of the certificate by the TSP

EE certificates are not published by the TSP. The subscriber undertakes the publication.

The status can be accessed using CRLs and the OCSP after the certificate has been produced (See section 2.1)[4].

4.4.3 Notification to other PKI participants of the issue of the certificate

Certificates of the E.ON SE PKI and their revocation information are stored fully automatically in a smartcard management system. Revocations can be arranged and commissioned in accordance with defined processes on the basis of this data. See also section 4.9.3 on this.

4.5 Key pair and certificate usage

4.5.1 Use of the private key and of the certificate by the subscriber

End users may use their private keys exclusively for the applications that are consistent with the types of usage indicated in the certificate.

[4] If in addition to the advanced certificates of the Root-PKI there are other end user certificates (qualified or qualified with provider accreditation) on the token, the status can be accessed using CRLs and the OCSP after the confirmation of receipt has been received by the TSP.

Key material for signature and authentication certificates from the XXI, XXII and XXIV sub-CAs is generated exclusively on certified PKI media.

Key material for authentication and encryption certificates from the SubCA XXIII are generated in a secured server environment by the subscriber.

The provisions of section 1.4 apply for subscribers.

4.5.2 Use of the public key and of the certificate by relying parties

The certificates of the E.ON SE PKI can be used by all relying parties. **They can, however, only be trusted** if

- the certificates are used in accordance with the types of usage noted on them (key usage, extended key usage, restricting certificate extensions if appropriate),
- the certificate chain can be successfully verified up to a trustworthy root certificate[5],
- the status of the certificates has been positively verified using a CRL or the status query service (OCSP),
- all other precautionary measures indicated in agreements or elsewhere have been taken and possible restrictions in the certificate and any application-specific precautions have been taken into consideration by the relying party and identified as compatible.

4.6 Certificate renewal

Certificate renewal is not offered.

4.7 Certificate renewal with rekeying

Rekeying is not offered.

4.8 Certificate amendments

Certificate amendments are not offered.

[5] The verification of the certificate chain should be carried out in line with the PKIX model (also known as the shell model) in accordance with [RFC 5280], section 6. A formal description of the algorithm for verifying the certificate chain can be found in [Co-PKI], Part 5.

4.9 Revocation and suspension of certificates

4.9.1 Conditions for a revocation

The revocation of a certificate is one of the contractual obligations to the subscriber and affected third parties that the TSP undertakes to perform. The TSP's procedures meet the conditions arising from [ETSI-F and [GL-BRO].

- Subscribers and affected third parties are requested to apply for the revocation immediately if the suspicion arises that private keys have been compromised or data contained in the certificate is no longer correct (e.g. the end user ceases to be a member of the organisation).

- Revocations indicate the time of the revocation and are not issued with retroactive effect.

Revocation authorities must authenticate their identity in accordance with section 3.4.

4.9.2 Eligibility to revoke certificates

- The TSP is authorised to revoke certificates. The TSP must carry out revocations in accordance with [GL-BRO] section 11.2.2 or 13.1.5.

- The subscriber always has the authority to revoke his own certificates.

In all other respects, any person who gives the correct revocation password is regarded as a revocation authority with regard to the TSP.

4.9.3 Revocation request procedure

The end user can revoke his certificates via the Global Service Desk of the subscriber within the E.ON SE infrastructure or directly in his personal area of the smartcard management system using the online interface.

Revocations via the Global Service Desk will be sent to the TSP.

E-mail address: eon.servicedesk@hp.com

Other revocation procedures can be agreed.

An application to revoke a certificate using an online interface should include the following information:

- the issuer of the certificate;
- the agreed revocation password;
- certificate serial number (if possible as a decimal number), so that the certificate can be clearly identified.

Via the personal area of the smartcard management system, revocation applications can also be submitted for third parties within E.ON SE PKI. For this, the party requesting the revocation must be logged on to the request with his personal token in the smartcard management system and authenticated.

Revocations take place within the scope of responsibility of the TSP and can be carried out with authorisation exclusively by employees eligible to do this.

The revocation of a certificate is final. A certificate cannot be reactivated after it has been revoked.

All revocation information will be appropriately documented. The end user will be informed that his certificates have been revoked by e-mail.

4.9.4 Revocation request time limits

The end user or subscriber must himself take responsibility for ensuring that he or a person with revocation authority for him applies for the revocation immediately reasons for the revocation become known.
For processing the revocation request the procedure likely to be fastest is to be used.

4.9.5 Time frame for the TSP to process the revocation request

Revocation requests are processed by the TSP from 08:00 to 17:00 on national working days. Revocation requests received by e-mail will be processed at the latest on the following working day.

In accordance with ETSI LCP, a revocation will be implemented within 72 hours.

4.9.6 Available methods for validating revocation information

Up-to-date revocation information is maintained in certificate revocation lists, which can be accessed using the LDAP protocol or the link indicated in section 2.1. An OCSP service is also available. URLs in the certificates indicate how these services can be accessed. Furthermore, revocation information can be obtained through the EIDM.
Delta CRLs are not offered.

The integrity and authenticity of the revocation information is guaranteed by a signature.

4.9.7 Frequency of publication of certificate revocation lists

See section 2.3.

4.9.8 Maximum latency period for certificate revocation lists

Certificate revocation lists are published immediately after they are generated.

4.9.9 Online availability of revocation information

An OCSP service is available for online verification. A URL in the certificates indicates how this service can be accessed.

4.9.10 Need to check revocation information online

There is no obligation to check revocation information online. However, section 4.5.2 applies.

4.9.11 Other displays of revocation information

None.

4.9.12 Special requirements in the event the private key is compromised

None.

4.9.13 Conditions for suspension

Suspensions of certificates are not offered.

4.10 Certificate status query service

4.10.1 How the status query service works

The status query service is available using the OCSP protocol. A URL in the certificates indicates how the service can be accessed.

4.10.2 Availability of the status query service

The status query service is permanently available (24 hours a day, 7 days a week).

4.10.3 Optional services

This regulation is recorded in the CPS.

4.11 Withdrawal from the certification service

The validity of a certificate ends on the expiry date marked in the certificate. A request to revoke a certificate by the subscriber or third-party revocation authority triggers the revocation by the TSP. The primary contractual obligations of the TSP are thereby fulfilled in their entirety.

4.12 Key escrow and recovery

Applications for the escrow of private EE keys can be submitted and will be implemented by the subscriber. Signature and authentication keys of EE certificates are not escrowed.

4.12.1 Conditions and procedures for the escrow and recovery of private keys

The TSP does not offer the escrow of private keys.

The subscriber (E.ON SE) escrows keys for encryption certificates in his own scope of responsibility in accordance with the following regulations:

The SCM offers a delimited and specially secured database area in which the master keys of the cards and personal decryption keys are escrowed symmetrically in encrypted form. All private decryption keys are generated using an HSM module and are available in encrypted form in a database.

Only the authenticated end user may access the decryption keys and transfer these as history certificates to his token or his mobile device (see 4.1.3). Access to currently and formerly valid certificates and related private keys for the decryption of older data is thus guaranteed.

Group IDs of employees who leave the company are deactivated and archived in an internal process. That does not, however, result in the private keys and certificates of the employee being removed from the SCM repository.

By registering on the central portal of the smartcard management system, an end user can configure deputies, who thus receive access to the end user's decryption keys and can additionally transfer these to their tokens in order to be able to access all encrypted e-mails of the end user in the context of the tasks of a deputy or assistant.

This confirmation of the deputies is made on an authenticated basis only via the portal of the smartcard management system, on which representation requests can be confirmed and the representatives currently set up can be displayed and deactivated again as required.

Before using new representative keys, the representatives must also register on the portal of the smartcard management system and are offered representative keys available to them for adding or deleting their own PKI medium or mobile device.

When adding or deleting a representative authorisation and when installing and uninstalling a representative key on the PKI medium, representatives and the persons represented[6] are informed automatically by e-mail, so that the persons represented have the opportunity to request representatives who are no longer required to remove the keys. This is also the case if the representative changes his PKI medium or mobile device, thereby requiring the new installation of the represented party's decryption key.

Representatives will still be able to use the private keys after the representation has been revoked until the PKI token of the representative has been reconfigured on the portal of the smartcard management system.

[6] If end users are inactive, the PKI supervisors and the head of EBS Security are informed by e-mail in their place.

On the basis of applicable law, the competent head of IT security can, while observing the dual control principle, authorise representatives by way of exception to use encryption certificates of other end users in order to enable access to encrypted e-mails. He is responsible for incorporating the relevant control bodies, verifying the documentation and, if appropriate, informing the end users in question.

In the case of team certificates, the team leader can act as the owner of the certificate using a function Group ID and establish his primary Group ID and the Group IDs of the team members as deputies. They thus also have the possibility of obtaining the private keys of these certificates.

4.12.2 Conditions and procedures for the escrow and recovery of session keys

Session keys are not offered.

5. Non-technical security measures

The TSP establishes non-technical security measures that meet the requirements arising from [ETSI-F].

6. Technical security measures

The TSP establishes technical security measures that meet the requirements arising from [ETSI-F]. Up-to-date information on signature and encryption algorithms can be found in the CPS. Subscribers and end users must use trustworthy computers and software; this condition is fulfilled in particular in accordance with the policies defined by E.ON SE.

The procedures are defined in the CPS.

7. Profiles of certificates, certificate revocation lists and OCSP

7.1 Certificate profiles

The certificates issued by sub-CAs of the E.ON SE PKI fulfil the requirements of the ITU [X.509] and IETF [RFC 5280] standards as well as the Common PKI 2.0 [Co-PKI] profiling: deviations are described in a reference document if necessary.
The profiles are defined in the CPS.

7.2 Certificate revocation list profiles

The certificate revocations lists that are issued fulfil the requirements of the ITU [X.509] and IETF [RFC 5280] standards as well as the Common PKI 2.0 [Co-PKI] profiling.

7.3 Profiles of the status query service (OCSP)

The status query service conforms with the [RFC 2560] standard and fulfils the requirements of the Common PKI 2.0 [Co-PKI] profiling.

8. Audits and other assessments

The sub-CAs of the E.ON SE PKI are operated by the TSP in the same premises as the CA of D-TRUST GMBH for the issue of qualified certificates with provider accreditation in accordance with the German Digital Signature Act. Audits, items subject to audit and processes are described in detail in the security concept [SiKo-DTR] of the certification services provider D-TRUST GMBH, which operates in conformity with the Digital Signature Act. The role concept section of this security concept [SiKo-DTR] documents the qualification and the position of the auditor.

The security concept has been audited by TÜV Informationstechnik GmbH. The relevant parts of these documents can be inspected when there is a legitimate interest.

Furthermore, controls are regularly conducted by external auditors of the test and confirmation agency TÜV Informationstechnik GmbH every three years in the course of the approval procedure for the voluntary accreditation of the TSP in accordance with section 15 SigG and section 11 SigV.
The TSP conducts reviews and audits of the technical and organisational processes that are used in the application procedure and in the identification of the end users at regular intervals. These include an annual document audit (provision of all documentation and manuals valid at the time of the review that describe the technical and organisational processes involved in the application and identification procedures) as well as an audit of all amended documentation and manual after each significant process change.

Furthermore, a regular interim audit at intervals of three years is conducted, if necessary on the premises of E.ON SE.

In addition, internal audits regularly take place that the TSP and E.ON SE conduct and document independently.

9. Other financial and legal regulations

9.1 Financial responsibilities

9.1.1 Insurance cover

The D-TRUST GMBH TSP has sufficient insurance cover to be able to satisfy the compensation of damages that are incurred as a result of the TSP breaching the duties or not implementing the requirements as they arise for it from this policy pursuant to section 12 SigG.

9.1.2 Other resources for maintaining operations and covering damages

Not specified.

9.1.3 Insurance or warranty for end users.

Not specified.

9.2 Confidentiality of business data

9.2.1 Definition of confidential business data

The confidentiality of information can be agreed if it is not already defined by applicable law.

9.2.2 Business data that is not treated as confidential

All information in certificates that have been issued and published as well as the data specified in section 2.2 is regarded as public information.

9.2.3 Responsibilities for protecting confidential business data

The TSP undertakes to protect the data designated to it as confidential business data against disclosure and espionage through appropriate technical and organisational measures and to

refrain from using this data for purposes for which it is not intended, or to disclose it to third parties, if such an obligation does not breach the law. As part of the organisational measures, the employees deployed by the TSP are obligated within the framework permitted by law not to disclose the confidential data.

9.3 Protection of personal data

9.3.1 Data protection concept

The TSP works on the basis of an auditable security concept that regulates the protection of confidential personal data (personal data for short). The TSP fulfils the requirements of sections 4a and b, 9 and 27 ff. of the *Bundesdatenschutzgesetz* (BDSG – German Federal Data Protection Act).

9.3.2 Definition of personal data

Section 3(1) of the BDSG applies.

9.3.3 Data that is not treated as confidential

Data that is explicitly contain in certificates, certificate revocation lists and status information is not included in the data that is treated as confidential.

9.3.4 Data protection responsibilities

The TSP ensures data protection compliance. All employees of the TSP are obligated to comply with the data protection requirements. Internal controls are carried out by the company data protection officer, external controls by the Berliner Beauftragter für Datenschutz und Informationsfreiheit (Berlin Commissioner for Data Protection and Freedom of Information).

9.3.5 Notice and consent to the use of personal data

The subscriber will be notified at the latest at the time of his application which personal data will be contained in the certificate.

All personal data that is no longer required is deleted immediately. The time limits of the CPS apply to personal data that is required for certificate verification.

9.3.6 Information pursuant to legal or government regulations

As a company under private law, the TSP is subject to the BDSG as well as the laws of the Federal Republic of Germany. Information is provided in accordance with these laws.

9.3.7 Other disclosure conditions

Information of any kind other than that described in section 9.3.6 is not provided.

9.4 Intellectual property rights and copyrights

9.4.1 TSP

The existence and content of copyrights and other intellectual property rights are governed by the general statutory regulations.

9.4.2 Subscriber

The subscriber undertakes to observe with intellectual property rights in the application and certificate data.

9.5 Warranties and guarantees

9.5.1 Scope of performance of the TSP

Unless expressly stated, the TSP does not grant any guarantees or warranties in the legal sense.

LCP certificates
The TSP ensures that the subscriber is clearly identified. The subscriber ensures that the public key can be assigned to the end user.

The TSP ensures that the procedures described in the CPS are complied with.

The TSP ensures that a name (*Distinguished Name* in the (*subject* field) used in certificates is always unique within the E.ON SE PKI and after the lifecycle of the certificate has ended and is always assigned to the same subscriber. As a result, the unique identification[7] of the subscriber is guaranteed by the name used in the certificate (*subject*).

The TSP maintains the operation of the CAs, the directory service and the provision of revocation information.

The TSP can outsource sub-tasks to partners or to external providers. The TSP ensures that the provisions of the CP and CPS are complied with in this event.

9.5.2 Warranties and guarantees of the subscriber

LCP certificate
The subscriber agrees to the declaration of commitment (subscriber agreement), which contains warranties and guarantees of the subscriber. The declaration of commitment complies with the requirements of [ETSI-F].

9.5.3 Warranties and guarantees of the relying party

Warranties and guarantees of the relying party are not regulated by this CP. No contractual relationship is established between the TSP and the relying party.

9.6 Limitations of liability

The liability of the TSP is limited to the scope insured within the meaning of section 9.1.1.

9.7 Compensation of damages

9.7.1 Claims of the TSP against subscribers

Claims for compensation of damages are regulated by a separate contract between the TSP and the subscribers.

[7] See footnote 2 on page 17.

9.8 Validity of the CP and end of validity

9.8.1 Validity of the CP

This CP is valid from the time that it is published and remains valid as long as certificates that have been issued on the basis of this CP are valid.

9.8.2 End of validity

See section 9.8.1.

9.9 Individual notices and agreements with PKI participants

Notices of the TSP to subscribers are sent to the last address registered in the documents of D-TRUST GMBH or to the corresponding e-mail address taken from the application (electronically signed).

9.10 Addenda

9.10.1 Procedure for addenda

Addenda to this CP are incorporated in this document and published under the same OID. Editorial amendments are marked.

9.10.2 Notification mechanisms and deadlines

E.ON SE will be informed of changes to the CP as regulated in more detail in the extIDENT contract.

9.11 Dispute resolution provisions

Complaints concerning compliance with or implementation of this CP are to be submitted in writing to the TSP (D-TRUST GMBH, Kommandantenstr. 15, 10969 Berlin, Germany). If the complaint has not been remedied within a period of 4 weeks of its submission, the following applies: All persons enjoy recourse to the courts in accordance with German law in all disputes.

9.12 Compliance with applicable law

This CP is subject to the law of the Federal Republic of Germany

9.12.1 Severability clause

Should individual provisions of this CP be invalid or unenforceable or become invalid or unenforceable after the contract has been concluded, this shall not affect the validity of the CP in any other respect. The valid and enforceable regulation, the effects of which most closely approximate to the economic objective that the parties to the contract pursued with the invalid or unenforceable provision shall replace the invalid or unenforceable provision. The above provisions also apply in the event that the CP proves to have any gaps or omissions.

9.12.2 Force majeure

The TSP is not liable for damages as a result of force majeure.

9.13 Other provisions

9.13.1 Compliance with export laws and regulations

The export of certain software that is employed in connection with the public certification services of D-TRUST GMBH can depend on the approval of the competent authorities. The parties shall comply with the relevant export laws and regulations.

The use of the public certification services of D-TRUST GMBH is subject to various laws of the Federal Republic of Germany. In any event of an infringement of the public certification services of D-TRUST GMBH, D-TRUST GMBH reserves the right to institute criminal proceedings.