Certification Practice Statement of the Uniper PKI

ENGLISH

DEUTSCH

Teil der Bundesdruckerei-Gruppe

Certification Practice Statement of the Uniper PKI

Version 2.6

Teil der Bundesdruckerei-Gruppe

COPYRIGHT NOTICE AND USE LICENSE

Certification Practice Statement of the Uniper PKI
©2022 D-Trust GmbH

This work is licensed under the Creative Commons Attribution-NoDerivatives 4.0 International License.

Requests for any other use of this CPS of D-Trust GmbH not contained in the aforementioned license are to be sent to:

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

Document history

Version	Date	Description
1.0	2014-02-01	▪ Initial version – based on D-TRUST Root PKI v. 1.9
1.1	2016-10-10	▪ Change to EN 319 411-1
1.2	2017-10-01	▪ Adaptation of the use license to "Creative Commons Attribution ▪ Editorial changes
2.0	2018-03-28	▪ In future, this CPS will be fully included in the Certificate Policy of D-Trust GmbH.
2.1	2018-07-05	▪ Section 4.2.1: Domain validation methods changed ▪ Editorial changes
2.2	2018-11-30	▪ Archiving times changed in sections 5.5.1 and 5.5.2 ▪ This CPS complies with the requirements of the Mozilla Policy 2.6.1 ▪ Annual review of the entire CPS ▪ Editorial changes
2.3	2020-03-19	▪ This CPS complies with the requirements of Mozilla Policy 2.7 ▪ Annual review of the entire CPS ▪ Update according to the CAB's observation report ▪ Editorial changes
2.4	2020-04-27	▪ Rollover CAs added, see section 1.1.3 ▪ Amendments to certificate chain verification in section 4.5.2. ▪ Amendments in section 5.5.2 and 5.3.7
2.5	2021-08-18	▪ Annual review of the entire CPS ▪ Editorial changes in sections 3.1.4, 7.1.2, 7.2.2, 7.3.2 ▪ Amendments in sections 1.1.3, 4.2.1, 4.9.1, 4.9.12, 7.1.1, 8
2.6	2022-11-18	▪ Informative introduction of the NCP policy level ▪ Amendments in sections 1.1.3, 1.4.2, 1.6.2, 2.4, 4.9.1, 4.10.1, 4.10.2, 5.5.1, 5.5.2, 6.3.2, 8 ▪ Annual review of the entire CPS

Contents

1. Introduction ... 6
1.1 Overview ... 6
1.2 Document Name and Identification ... 9
1.3 PKI Participants ... 10
1.4 Certificate Usage ... 10
1.5 Policy Administration ... 11
1.6 Definitions and Acronyms ... 12
2. Publication and Repository Responsibilities ... 13
2.1 Repositories ... 13
2.2 Publication of information concerning certificates ... 14
2.3 Publication frequency ... 14
2.4 Directory access control ... 14
2.5 Access to and use of services ... 14
3. Identification and Authentication (I&A) ... 14
3.1 Naming ... 14
3.2 Initial Identity Validation ... 16
3.3 I&A for Re-key Requests ... 17
3.4 I&A for Revocation Requests ... 17
4. Certificate Life-Cycle Operational Requirements ... 18
4.1 Certificate Application ... 18
4.2 Certificate Application Processing ... 22
4.3 Certificate Issuance ... 23
4.4 Certificate Acceptance ... 24
4.5 Key Pair and Certificate Usage ... 24
4.6 Certificate Renewal ... 25
4.7 Certificate Re-key ... 25
4.8 Certificate Modification ... 25
4.9 Certificate Revocation and Suspension ... 25
4.10 Certificate Status Services ... 29
4.11 End of Subscription ... 29
4.12 Key Escrow and Recovery ... 29
5. Facility, Management, and Operational Controls ... 30
5.1 Physical Security Controls ... 31
5.2 Procedural Controls ... 31
5.3 Personnel Controls ... 32
5.4 Audit Logging Procedures ... 33
5.5 Records Archival ... 34
5.6 Key Changeover ... 34
5.7 Compromise and Disaster Recovery ... 35
5.8 CA or RA Termination ... 35
6. Technical Security Controls ... 36
6.1 Key Pair Generation and Installation ... 36
6.2 Private Key Protection and Cryptographic Module Engineering Controls ... 37
6.3 Other Aspects of Key Pair Management ... 39
6.4 Activation Data ... 39
6.5 Computer Security Controls ... 40
6.6 Life Cycle Security Controls ... 40
6.7 Network Security Controls ... 42
6.8 Timestamping ... 42
7. Certificate, CRL, and OCSP Profiles ... 42
7.1 Certificate Profile ... 42
7.2 CRL Profiles ... 45

7.3 OCSP Profile 45
8. Compliance Audit and Other Assessment 46
9. Other Business and Legal Matters 46

1. Introduction

1.1 Overview

This document is the Certification Practice Statement (CPS) of the Uniper PKI operated by D-Trust GmbH.

The Uniper PKI is referenced by a SubCA structure below the "D-TRUST Root CA 3 2013".

1.1.1 Trust service provider

These rules are laid down in the CP of D-Trust GmbH.

1.1.2 About this document

This CPS defines processes and procedures within the scope of the trust services throughout the entire life of the CA and end-entity certificates (EE certificates). It determines the minimum measures that all PKI participants must fulfil.

This CPS refers to the CP (certificate policy) of D-Trust GmbH with OID 1.3.6.1.4.1.4788.2.200.1 and to [EN 319 411-1], respectively. It describes the implementation of the resultant requirements for the PKI of Uniper.

This CPS is part of the extIDENT agreement between the TSP and Uniper and is therefore legally binding in as far as this is permitted under German and European law.

The CP and CPS documents contain an exhaustive definition of the legally binding effect as well as the processes concerning the following aspects: a) provision of the CA, b) production of certificates for the key material made available, c) provision of revocation lists and d) provision of the OCSP service. They constitute a non-qualified trust service within the meaning of the eIDAS Regulation.

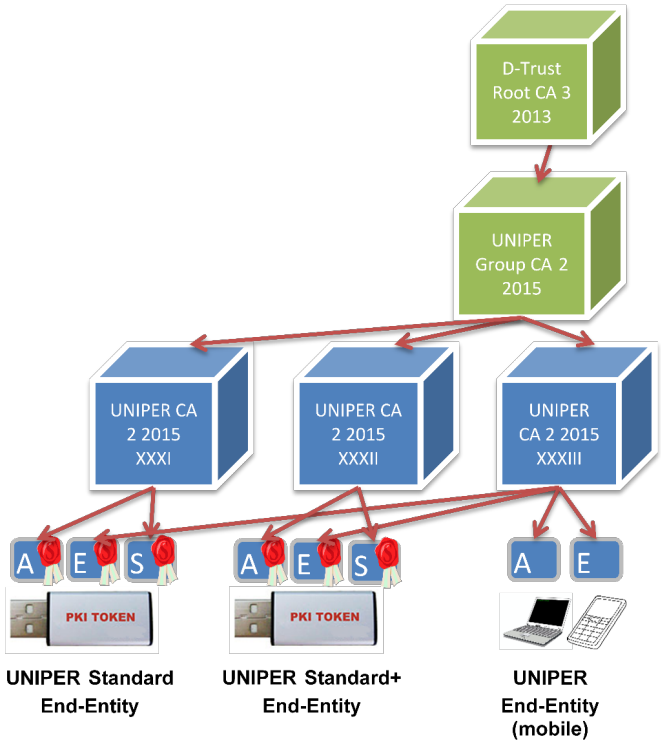
Knowledge of the certification procedures and rules described in this CPS and of the legal framework enables relying parties to build trust in components of this PKI and PKI participants and to decide to what extent the trust and security level established by the PKI is appropriate.

The structure of this document complies with the RFC 3647 Internet standard "*Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework".*

1.1.3 Properties of the PKI

The PKI described here features a multi-level hierarchy. Fig. 1 shows the configuration of the Uniper PKI.

The new 2020 PKI hierarchy will replace the 2015 PKI hierarchy in future. Until further notice, both can be operated and used parallel.



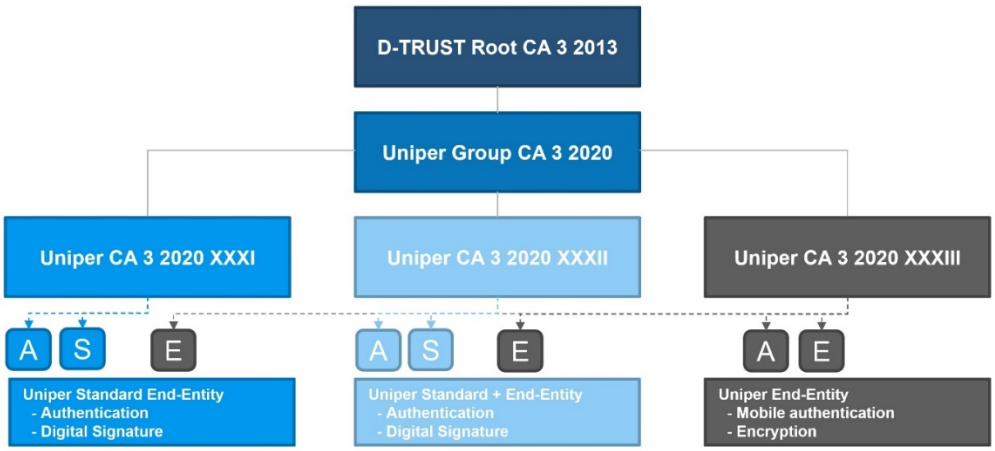


Fig. 1 Structure of the issuing CAs and end-entity/subject certificates

Requirements of the PKI

The EE and CA certificates are subject to security level NCP or LCP. NCP or LCP certificates have a high quality, however, they are not qualified certificates which meet the requirements of EN 319 411-1 NCP or LCP and [BRG]. Certificates of successful audits can be found in the Audit Attestation Letter. The conformity assessment body TÜViT publishes these certificates at:

https://www.tuvit.de/en/services/certification/audit-attestations-according-to-cabrowser-forum-requirements

Under the D-Trust Root CA, Uniper uses a Uniper Group CA and, below this, the Uniper issuing CAs that issue the end-entity certificates.

Authentication, signature and encryption certificates are issued. These include the OID 1.3.6.1.4.1.4788.2.212.1 for LCP and the OID 1.3.6.1.4.1.4788.2.212.2 for NCP.

CA Certificates

The complete overview of all root CAs and sub-CAs with certification levels QCP-w, EVCP, OVCP, DVCP, NCP and LCP, showing which CPS applies to each CA, can be found in the repository:

https://www.d-trust.net/files/dokumente/pdf/pki_structure_and_applicable_documents.pdf

The following table provides an overview of all root CAs and the associated sub-CAs to which this CPS applies.

D-TRUST Root CA 3 2013 http://www.d-trust.net/cgi-bin/D-TRUST_Root_CA_3_2013.crt SHA256 Fingerprint: A1A86D04121EB87F027C66F53303C28E5739F943FC84B38AD6AF009035DD9457
Uniper Group CA 2 2015 http://www.d-trust.net/cgi-bin/Uniper_Group_CA_2_2015.crt SHA256: B4B2810E787B8E6DBB8B0EA9242D8E195AD5BF4201FD98A09AEDAC8B5F23FAFE OID: 1.3.6.1.4.1.4788.2.212
Uniper CA 2 2015 XXXI http://www.d-trust.net/cgi-bin/Uniper_CA_2_2015_XXXI.crt SHA256: F471920D5679EE48219F51CBF44F0F22A7305332B869025E26050C5BED762F72 OID: 1.3.6.1.4.1.4788.2.212.1
Uniper CA 2 2015 XXXII http://www.d-trust.net/cgi-bin/Uniper_CA_2_2015_XXXII.crt SHA256: EFA0A2F29EABB43EAD97AD067297656088679C0B2E297C2D898C4F12C9759805 OID: 1.3.6.1.4.1.4788.2.212.1

Uniper CA 2 2015 XXXIII http://www.d-trust.net/cgi-bin/Uniper_CA_2_2015_XXXIII.crt SHA256: 79B9D31504B604293570ECCDC8A92553F937FD823380E560793987037C8B181D OID: 1.3.6.1.4.1.4788.2.212.1
Uniper Group CA 3 2020 http://www.d-trust.net/cgi-bin/Uniper_Group_CA_3_2020.crt SHA256: A502172DEAF811DD7FA9BC3329AEA72589F2FAEC9401CB7348819C75F2E705B9 SHA1: F6B7B49CC413C27D69BD7EFC12E4638D1B98BEEC OID: 1.3.6.1.4.1.4788.2.212.1
Uniper CA 3 2020 XXXI http://www.d-trust.net/cgi-bin/Uniper_CA_3_2020_XXXI.crt SHA256: 19D99B7FDD7EC707AC3023D72F50D4AB5199AF1FDD3013A96815CBC99B63BFD6 SHA1: 70997F9622B0341A9E3AE1EFF739714C10DBB643 OID: 1.3.6.1.4.1.4788.2.212.1
Uniper CA 3 2020 XXXII http://www.d-trust.net/cgi-bin/Uniper_CA_3_2020_XXXII.crt SHA256: B576C4A703CB973079F8374EF359E4FD8788584B4E9FB4BC90A7E9F8C3838791 SHA1: 15222F266E381B983A6B83CE705F4AADA8944B7A OID: 1.3.6.1.4.1.4788.2.212.1
Uniper CA 3 2020 XXXIII http://www.d-trust.net/cgi-bin/Uniper_CA_3_2020_XXXIII.crt SHA256: 364ED83755EA3EA8533856EFF72DE38271B54FF44905785EBF735BFFC29B6636 SHA1: 1e2c28405eeb2ef22567d8155e685d656ea0a12f OID: 1.3.6.1.4.1.4788.2.212.1

Both CA and EE certificates can contain references to CPs or OIDs which define detailed requirements and restrictions.

1.2 Document Name and Identification

Document name:	Certification Practice Statement of the Uniper PKI
Version	2.6

1.3 PKI Participants

1.3.1 Certification authorities (CAs)

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

- Certificates for natural persons (EE certificate)
- Group certificates for groups of natural persons, functions and IT processes (EE certificate)
- Certification authorities (lower-level CA certificates of the TSP)

Root authorities issue certificates exclusively with the extension basicConstraints: cA=TRUE (CA certificate) according to [X.509]. Lower-level CAs issue EE certificates and/or further CA certificates. The name of the certification authority is shown in the issuer field of the certificates issued and in the CRLs.
Personnel who create certificates are not subject to any commercial, financial or other influence by the organization.

1.3.2 Registration authorities (RAs)

Uniper as a RA uses defined processes (see section 4) in order to identify and authenticate end entities, and to receive and check requests for different certification services.

1.3.3 Subscribers

The subscriber is Uniper which has its place of business in Germany and which requests and holds the EE certificates. The subscriber is not identical to the subject whose name appears in the certificate. The subscriber's obligations are subject to separate contractual agreements.

Other subscribers are not foreseen in the Uniper PKI.

The subscriber is responsible for keys and certificate contents. Moreover, additional obligations exist under EN 319 411 1. The subscriber will communicate these obligations to the end-entity at the latest when the request is submitted.

1.3.4 End-entity (EE)

Subjects (end entities (EEs)) use the private end-entity keys (EE keys). The subject's identity is linked to the certificate and the related key pair. Permitted end entities are natural persons or groups of natural persons who have a KID (GroupID) that is managed by the identity management system of Uniper (EIDM) (e.g. Uniper employees or contract partners and service providers with an active IT account) as well as functions and IT processes.

1.3.5 Relying parties

Relying parties are natural persons or legal entities who use the certificates of this Uniper PKI (for instance, in order to verify signed documents) and who have access to the services of the TSP.

1.4 Certificate Usage

1.4.1 Permitted uses of certificates

These rules are laid down in the CP of the D-Trust GmbH.

1.4.2 Forbidden uses of certificates

Types of use (keyUsage) not laid down in the certificate are not permitted.

The rules of the CP of D-Trust GmbH also apply.

1.4.3 Service certificate usage

These rules are laid down in the CP of the D-Trust GmbH.

1.5 Policy Administration

1.5.1 Responsibility for the document

This CPS is updated by D-Trust GmbH in co-operation with Uniper. The representative of D-Trust GmbH's management is responsible for acceptance of the document.

This CPS is checked and, when necessary, updated annually by the TSP. A change is indicated by a new version number of this document.

1.5.2 Contact partner/contact person/secretariat

The following contact addresses are available:

D-Trust GmbH

CP und CPS editorial unit

Kommandantenstr. 15.

10969 Berlin, Germany

Tel.: +49 (0)30 259391 0

E-mail: info@d-trust.net

Uniper as the subscriber is represented by:

Uniper

Information Security

E.ON-Platz 1

40479 Düsseldorf, Germany

E-Mail: pki@uniper.energy

If you have any questions regarding the validity of concrete certificates from the Uniper PKI at a particular point in time, please send an e mail to: pki@uniper.energy

1.6 Definitions and Acronyms

1.6.1 Definitions and names

These rules are laid down in the CP of the D-Trust GmbH.

The following definitions are additionally used within the Uniper PKI:

Authentication certificate	A certificate that an end-entity can use in order to authenticate himself in relation to an IT system
Confirmer	Employees or superiors who confirm the colleagues' identity for certificate requests.
Uniper PKI	PKI operated by D-Trust GmbH for Uniper
Global service desk	Global service desk for the end entities of Uniper PKI (GSD)
History certificates	Expired encryption certificates whose keys are stored for the subsequent decryption of data and which can be recovered by authorized end entities.
KID (GroupID)	A unique, but not biunique and not reusable IT identifier for each IT end-entity in the global repository of Uniper. Primary KIDs (GroupIDs) are issued exclusively to natural persons who can thereby receive end-entity certificates as long as they are active. Secondary KIDs (GroupIDs) (for instance, for e-mail group inboxes) can also always be assigned to a natural person as their owner so that it is also always possible to unambiguously identify a responsible natural person. Attributes that can be assigned to a KID (GroupID) are created and updated via audited processes from the HR and contract management systems.
PKI supervisors	PKI supervisors are the central interfaces between Uniper and D-Trust GmbH in all process issues related to the extIDENT contract, including CP and CPS for the Uniper PKI. This group answers questions related to all PKI processes of the Uniper PKI and decides on all Uniper-internal queries for the Uniper PKI in conformity with the extIDENT contract, including CP and CPS.
PKI token	Various form factors of smartcards, called PKI tokens, are used for the Uniper PKI which are all managed by a smartcard management system. PKI tokens currently include both ISO-compliant smartcards, smartcards in the form of a USB token and a microSD card as well as TPM 2.0-based virtual smartcards (VSCs). The terms PKI token, USB PKI token, smartcard, PKI medium and VSC are used synonymously in manuals and documentations.
Q environment	Quality assurance systems used to test configuration changes and upgrades.
Trusted platform module	The trusted platform module (TPM) is a chip according to the TCG specification, Family 2, that adds basic security functions to a computer or similar devices.

Virtual smartcard	Virtual smartcards (VSCs) map the generally accessible functionalities of a customary smartcard in software. Sensitive data is protected by a TPM 2.0.

1.6.2 Acronyms

These rules are laid down in the CP of D-Trust GmbH.

The following definitions are additionally used within the Uniper PKI:

CP	Certificate Policy
EIDM	Uniper identity management system
GSD	Global service desk
KID	Uniper GroupID
LCP	Leightweight Certificate Policy
NCP	Normalized Certificate Policy
SCM	Smartcard management system
TPM	Trusted platform module
TSP	Trust service provider (previously CSP)
VSC	Virtual smartcard

1.6.3 References

These rules are laid down in the CP of D-Trust GmbH.

2. Publication and Repository Responsibilities

2.1 Repositories

The TSP publishes CRLs and certificates in the LDAP repository at: ldap://directory.d-trust.net and ldap://cdp-ldap.intranet.uniper.energy, respectively. Alternative http access to the CRLs is also possible at: http://crl.d-trust.net/crl/. The complete certificate-specific links can be found directly on the certificates. CA certificates are additionally published as described in section 1.1.3.

The TSP provides an online service (OCSP) that can be used to request the revocation status of certificates of the Uniper PKI. The status of the certificates will remain available there for up to at least one year after they have expired.

This CPS and the subscribers‘ obligations are made available to the applicant in PDF format on the request pages of Uniper during the request process. These documents can also be downloaded from the Internet at the following address;

https://www.d-trust.net/en/support/repository

The latest versions of the above-mentioned documents are published at this address.

2.2 Publication of information concerning certificates

The TSP publishes the following information regarding the Uniper PKI:

- CA certificates,
- the CP of D-Trust GmbH,
- this CPS,
- certificate revocation lists (CRLs) and status information.

The repositories and addresses where this information is available are described in section 2.1.

In the Uniper PKI, EE certificates are generally not published by the TSP.

2.3 Publication frequency

CA certificates are published after their creation and kept for a minimum period of one year following expiration of the validity of the CA.

Certificate revocation lists are issued regularly and until the end of validity of the issuing CA certificate. Certificate revocation lists are issued and published immediately following revocations. Even if no certificates were revoked, the TSP ensures that new certificate revocation lists are created at least every 24 hours. The certificate revocation lists are retained and kept for a minimum period of one year following expiration of the validity of the CA.

CA revocation lists that are issued by root CAs are issued and published at least every 12 months even if no revocations took place.

As described in section 2.1, this CPS is published and available for retrieval for a minimum period which is at least equal to the period of validity of the certificates that were issued on the basis of this CP.

2.4 Directory access control

Certificates, certificate revocation lists and this CPS can be publicly retrieved 24/7 at no cost. The repository service offers at least 98.5% availability. The TSP ensures that in the event of a malfunction, downtime is limited to a maximum of four hours.

Read access is unrestricted. Changes in repository and web contents are carried out exclusively by the TSP.

The relevant parts of other non-public documents can be issued on request against proof of a legitimate interest.

2.5 Access to and use of services

These rules are laid down in the CP of D-Trust GmbH.

3. Identification and Authentication (I&A)

3.1 Naming

3.1.1 Types of names

CA and EE certificates generally contain information regarding the issuer and the subscriber and/or subject. In line with the [X.501] standard, these names are given as DistinguishedName.

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

3.1.2 Need for telling names

The DistinguishedName used is unambiguous within the Uniper PKI. The unambiguous assignment of the certificate to the end-entity is ensured by the use of the Uniper GroupID (KID).

In the case of alternative names (subjectAltName according to [X.509]), there is no need for telling names.

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

3.1.3 Anonymity or pseudonyms of subscribers

Pseudonyms are used exclusively for natural persons.

KIDs (GroupIDs) that were used with authentication certificates as a pseudonym in the CN consist exclusively of a Latin letter followed by at least four Arabic numerals. These KIDs (GroupIDs) are not specifically identified as a pseudonym (personal and unambiguous KID (GroupID) of Uniper).

3.1.4 Rules for the interpretation of different name forms

The attributes of the distinguished name (DN components) of EE certificates are interpreted as follows:

DN component	Interpretation
CN (commonName)	*Common name*: The following variants are used: ▪ Natural persons without a pseudonym: "(optional) academic title<blank>first name<blank>family name". ▪ Natural persons with a pseudonym: "Pseudonym" if this consists exclusively of a Latin letter, followed by at least four Arabic numerals (personal and unambiguous KID (GroupID) within Uniper). ▪ Function or group of natural persons: Team name, made up of an e mail prefix and "team certificate".
serialNumber	*Serial number*: Name suffix that ensures unambiguity of the DN (personal and unambiguous KID (GroupID) within the Uniper).
O (organizationName)	Official name of the *organization*, of the pertinent PKI structure (Uniper, respectively).
OU (organizationalUnitName)	*Organization unit:* fields are filled exclusively for technical purposes.
C (countryName)	The notation of the *country* to be stated corresponds to [ISO 3166] and is set up as follows: If an organization O is listed in the DistinguishedName, the organization's place of business determines the country C.

The notation of names in the certificate is determined by the EIDM updating and management processes. When in doubt, the natural persons can be unambiguously identified by the subscriber via the KID (GroupID).
It is not necessary to use all of the above-mentioned DN components. Further components can be added.

Additional DN components must comply with [RFC 5280], [RFC 6818] and [EN 319 412].

3.1.5 Unambiguity of names

The TSP ensures that the name (DistinguishedName) of the subscriber and/or end-entity (subject field) (DistinguishedName) used in EE certificates is always unambiguous within the Uniper PKI and beyond the life cycle of the certificate and that it is always assigned to the same subscriber or end-entity, respectively. This unambiguity is achieved via the KID (GroupID). This ensures the unambiguous identification[1] of the subscriber on the basis of the name (subject) used in the EE certificate. Several KIDs (GroupIDs) can be assigned to one end-entity.

Within the scope of the Uniper PKI, the unambiguity of user certificates is permanently achieved by stating the KID (GroupID) in the certificate subject (even after changes in name, for instance, after marriage, etc.).

The TSP ensures the unambiguity of DistinguishedNames in CA certificates.

3.1.6 Recognition, authentication and the role of brand names

The subscriber is liable for compliance with intellectual property rights in the request and certificate data (see chapter 9 of the CP of D-Trust GmbH, section 9.5).

3.2 Initial Identity Validation

3.2.1 Proof of ownership of the private key

Key pairs are produced in the subscriber's sphere of responsibility. Ownership of the private keys must be either technically proven or plausibly confirmed by the subscriber.

See also section 6.1.3.

3.2.2 Identification and authentication of organizations

Certificates are not issued for legal entities.

Organizations named in the certificate are subsidiaries and affiliated companies of Uniper and/or companies of which Uniper is a shareholder. Uniper acts as the RA and authenticates the organizations that are named in the certificate.

This means that the only organization entry permitted in the DN field "O" is "Uniper" for the CAs of the Uniper PKI. The entries and the corresponding organization are automatically checked by the TSP.

Since the registered office of the organization ("Uniper") is relevant for the DN field "C", the only value permitted for this entry is "DE". The entry is automatically checked by the TSP.

3.2.3 Identification and authentication (I&A) of natural persons

Natural persons must provide unambiguous proof of their identity and, when necessary, also that their organization has authorized them to submit the request.

Natural persons are identified and authenticated in the control sphere of the subscriber as the RA with support by a technical service provider (see also section 4.2.1).

---

[1] "Identification" as used herein means the identification of the subscriber and the subscriber's up-to-date details at the time of the first-time request (not at the time of a subsequent/follow-up request). It does not mean the investigation of up-to-date details or the finding of he subscriber at a later point in time.

In the case of identification according to the standard process, the end-entity appoints two confirmers of the RA via their e mail address who must already have a valid and permitted EE certificate. The only permitted certificates in this case are EE certificates from the Uniper PKI of D-Trust GmbH.

If the applicant himself has already been authenticated with a valid authentication and signature certificate from the Uniper PKI of D-Trust GmbH, this certificate then replaces one of the two confirmers of the RA because the identity was already checked once.

If the preconditions for issuing a certificate are fulfilled after two successful confirmations by the RA, the certificate request is then automatically sent to the TSP. After the certificates have been received, the end-entity receives an e mail with a URL to download the certificates and install them on the smartcard.

3.2.4 Non-verified information concerning the subscriber

Verification of the subscriber's information is carried out or skipped according to sections 3.2.2, 3.2.3 and 4.2.1. In the case of alternative names, only the e-mail addresses or their domain components are generally verified. Other certificate contents, e.g. LDAP directories, etc. as well as certificate extensions (AdditionalInformation, monetaryLimit, etc.), if any, are not checked for correctness.

3.2.5 Verification of authority to apply

The provisions in section 3.2.3 apply.

Certificate requests are forwarded by Uniper via an agreed online interface.

Following successful identification in relation to the online interface, the request data is technically signed by the communication process. The requests are thus transmitted via an encrypted channel and additionally with an electronic signature.

Furthermore, only released article numbers that correspond to the products of the TSP are available via the interface.

This ensures that only the intended subscriber can receive the certificates requested..

3.2.6 Criteria for interoperability

See chapter 1 of the CP of D-Trust GmbH, section 1.5.3.

3.3 I&A for Re-key Requests

Re-keying is not offered.

3.4 I&A for Revocation Requests

Before revoking an EE certificate, the TSP checks whether the party requesting revocation is authorized to do so.

Revocation authorization is verified as follows:

If a revocation request is received in a signed e mail, revocation must be requested by the subscriber himself, or the party requesting revocation must have been named as a third party authorized to revoke and whose signature certificate used in the revocation e mail must be available to the TSP.

In the case of revocation via the online interface, transmission must be protected by an SSL certificate and a technical signature must be attached to the revocation request itself. Furthermore, the revocation password is sent to the TSP together with the revocation request.

Revocation requests via the online interface can also be submitted for third parties within the Uniper PKI. For this purpose, the party requesting revocation must, in his request, log in to the smartcard management system using his valid authentication certificate from the SubCA XXXI oder SubCA XXXII so that the party requesting revocation is thereby authenticated.

Other procedures for authenticating revocation requests can be agreed to with the subscriber.

Revocation procedures are defined in section 4.9.

4. Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Application authorization

Requests may only be triggered by certain end entities of Uniper who have been authorized by the company (KID (GroupID)) and who are able to authenticate themselves to the RA.

When the contract of an employee or service provider with Uniper comes into effect, the HR or contract department in charge creates a data record in a defined and trusted source system. On this basis, an identity is created once a day in the central access-protected enterprise directory of Uniper. This directory is an essential part of the so-called Uniper identity management system (EIDM). Any modifications of these programs/processes are subject to stringent change management and are agreed to with the TSP.

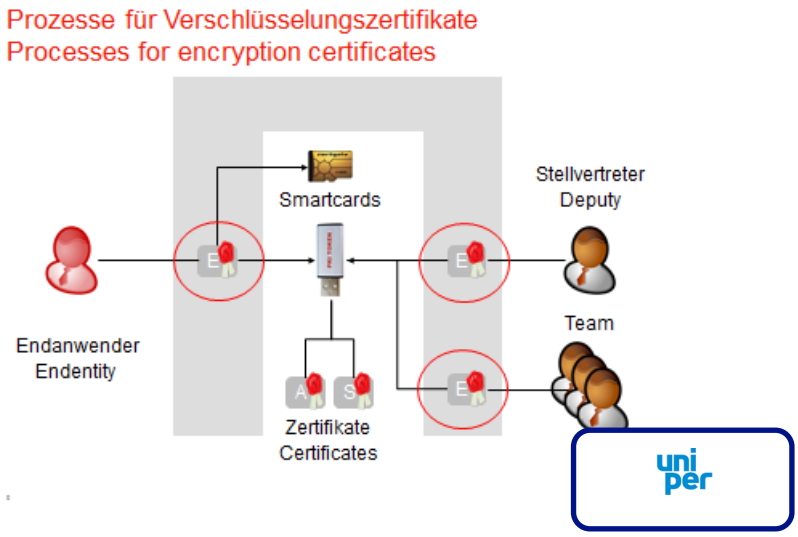
Non-authorized changes in EIDM data are not foreseen; they can only be carried out by a limited group of persons in leading data sources subject to a specific order to this effect (in writing and reproducible in order to ensure auditability) and they are logged individually there.

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

Private EE keys other than signature and authentication keys[2] can be stored in a secure manner by a body authorized by the TSP in accordance with the specifications of the CPS for subsequent re-use (key escrow, re-use in a new token).

At first, only the authenticated end-entity can access the end-entity's encryption keys stored from the SubCA XXXIII. The end-entity can transfer the encryption keys as history certificates to his PKI medium in order to use the pertinent private keys in order to access previously encrypted data.

[2] A signature key is a key for which a certificate is created that contains the public key of the key pair and includes "digital signature" or "contentCommitment" and/or "nonRepudiation" as key use.



An end-entity can use a workflow in order to define so-called deputies who can then access the end-entity's private encryption keys and additionally transfer them to their PKI media in order to be able to access encrypted e mails in the user's inbox as part of deputy or support tasks.

Team certificates are different in that the team leader can act via a function KID as the owner of the certificate and set up his primary KID and the KIDs of the team members as deputies.

This means that deputies can also obtain the private keys of these certificates if these certificates can be used exclusively for decryption.

In view of the need to protect this application, administration of the SCM is limited to a small group of persons and subject to the four-eyes principle, and changes must be explicitly released by PKI supervisors of Uniper.

CA certificates of the Uniper PKI are issued exclusively to Uniper.

To send the registration data, communication between the external registration authority and the internal registration authority at the TSP end is encrypted and authenticated via an SSL/TLS connection.

The TSP is entitled to reject applications (see section 0).

4.1.2 Registration process and responsibilities

At the beginning of registration process, this CPS and a subscriber agreement as well as further documents are already available to the subscriber and to the end-entity so that he can inform himself about the terms and conditions for use of the certificate to be requested.

Two registration processes (standard and standard plus) are foreseen in the Uniper PKI which are based on pre-registered data from the identity management system and its audited data updating processes.

The standard process focuses on the shift of user identification to the collegial environment, where the fact that the end-entity and the confirmer personally know each other is expected to increase the effectiveness and efficiency of the secure identification process.

The authentication of the confirmer and confirmations with advanced signatures have the effect of deterring misuse. These characteristics and the exact checking task are clearly explained to the

confirmers prior to confirmation. It should be noted in this context that the confirmer must state which means of identification (ID card, passport or personal collegial relationship) was used to identify the end-entity.

Strict application of the multi-eyes principle during the check makes it difficult for an individual to take possession of a third party's key pairs without being noticed.

4.1.3 Standard and standard plus process

The standard process is the usual process used to identify end entities.

The standard plus process is designed for certain sites of the Uniper Group where extended process requirements must be met. In this case, confirmation tasks may only be performed by confirmers who belong to an explicitly defined group of confirmers. Both processes issue identical certificates, i.e. authentication and signature certificates, with certificates under the standard plus process being issued by a separate SubCA.

Encryption certificates are also issued by a separate SubCA which can also issue authentication certificates on its own. These certificates can be used outside certified PKI media, i.e. on mobile devices or in encryption or authentication applications that cannot access smartcards and similar devices.

At the software end, the process is controlled by a workflow engine and modelled to reflect the specific requirements of Uniper which enables the secure execution of the process and the data flow between the end-entity, the confirmer and the TSP.

4.1.4 Standard process

This process can only be used by natural persons who have an active IT account of Uniper which is unambiguously identified by a primary KID (GroupID). The standard process is made up of the following steps:

1. An end-entity uses the standard browser in order to open the request URL on the intranet of Uniper. The end-entity logs in with the KID (GroupID) and the related password (if he does not yet have a token) or with the existing certificate.
2. When prompted, the end-entity inserts into his computer a PKI token that has been pre-initialized for Uniper. This step can be omitted if a VSC is used. He then starts the card initialization process specific for the end-entity.

   The applicant confirms that he has read the terms of use as well as the subscriber agreement and accepts these.

   During this process, authentication and signature keys are generated for the end-entity on the card and/or in the TPM. Only the public keys are transmitted to the SCM. The key pair for the encryption certificate is generated centrally by the SCM. By setting a personal PIN, the end-entity takes possession of the PKI medium. The Uniper smartcard management system (SCM) then generates the corresponding certificate requests which must be released by one or two confirmers.
3. The end-entity must propose two confirmers from the EIDM who must already have a valid EE certificate.
4. If the applicant has already been authenticated with a valid certificate, only one confirmer is required because the identity check was already performed once.

5. At the end of this process step, the end-entity receives an e mail which he can use at any time in order to access the status of this process and to abort and restart the process, when necessary.
6. The first confirmer receives an e mail with a link to the confirmation process step in the standard process. This can only be executed in an authenticated manner with a valid authentication and signature certificate. The consent is signed with the confirmer's token and stored in the database together with the request.
7. The first confirmer answers the questions displayed, i.e. whether he knows the end-entity in person, how he identified the applicant, whether the request data displayed is plausible, and signs the confirmation with his signature certificate, if applicable.
8. The second confirmer performs the same steps as the first confirmer.

   The second confirmer is not necessary if the end-entity has already logged in with a valid certificate of the Uniper PKI.
9. If the preconditions for creating EE certificates are fulfilled after successful confirmation, the certificate requests are then sent to the CA. After the certificates have been received, the end-entity receives an e mail with a URL to download the certificates and install them on the smartcard.
10. As a precondition for installing the certificates on the token, the end-entity must authenticate himself once again using an existing token or with his username/password. Besides his token, he also needs the PIN which he has chosen.

    The end-entity confirms again that he has read the terms of use as well as the subscriber agreement and accepts these.

    Following installation, the end-entity confirms receipt of the certificates in that the newly issued card signs the confirmation of receipt. Exception: If no signature certificate exists, the end-entity issues manual confirmation of receipt of the certificates requested.

4.1.5 Standard plus process

The standard plus registration process is needed in order to fulfil special registration requirements in certain organizational units. Suitably configured applications and processes can therefore recognize and verify certificates which were issued on the basis of this slightly stronger registration process.

In contrast to the standard registration process, first confirmation is carried out locally by a local confirmer determined by the system (an employee with a defined role).

4.1.6 Variant of the process for all Uniper entities for mobile devices

For the users of the above-described processes, authentication and encryption certificates from the SubCA XXXIII are also available as a software certificate. These certificates must be transmitted to an application in encrypted form. The application must give the end-entity exclusive control of the use of the private key.
End entities can order their up-to-date encryption certificate, an encryption certificate to be newly generated as well as a corresponding authentication certificate as a software certificate via the known self-service portal.
This order is checked and approved in the same way as in the standard process. The certificate is subsequently created and transmitted in a multi-stage process.

1. An end-entity uses the standard browser in order to open the request URL on the intranet of Uniper. He logs in with the KID (GroupID) and Windows password (if he does not yet have a token) or with his existing authentication certificate of the standard (SubCA XXXI) or standard+ SubCA (CA XXXII). Certificates of the SubCA XXXIII are excluded for this purpose.

2. The applicant confirms that he has read the terms of use as well as the subscriber agreement and accepts these.
3. When necessary, a key pair for an authentication certificate or for a new encryption certificate is subsequently centrally generated for the user in the Uniper smartcard management system (SCM). A key pair for the current encryption certificate was either previously generated and stored centrally by the SCM, and this key pair is either re-used or, if no valid encryption key is available, generated during the course of the process. The SCM generates the corresponding certificate requests for all new key pairs which, depending on the previous confirmation level, must be released by one or two confirmers who, for their part, must also have valid certificates (authentication for SCM access, encryption for access to the P12 file in the case of the system with two confirmers).
4. The end-entity decides whether he wants to receive an encrypted e-mail with the randomly generated PIN which is necessary for installation or whether he prefers the alternative approach of choosing two users where each of these two users receives an encrypted e-mail that contains half of the 12-digit PIN if the end-entity himself does not have a valid encryption certificate.
5. If the preconditions for creating EE certificates are fulfilled after successful confirmation, the certificate requests are then sent to the CA. After the certificates have been received, the end-entity receives an e-mail with a URL to download the certificates and install them in the application released by Uniper. Loading of the certificates can also be triggered by the released application.
6. If the user already has encryption keys on a PKI medium, he receives a message during the process of issuing the encryption key stored by the software indicating that the user himself is responsible for synchronizing these media.
7. When the certificates are retrieved via a desktop PC, the end-entity confirms again that he has read the terms of use as well as the subscriber agreement and accepts these.
8. In order to perform the certificate installation process, the end-entity must enter the complete PIN from step 4.

The real installation process then starts on the basis of a P12 file. Following successful installation, the end-entity confirms receipt of the certificates either personally or via the application used for installation which automatically confirms receipt via the self-service portal.

4.2 Certificate Application Processing

4.2.1 Identification and authentication (I&A) procedure

The identification and registration process described herein must be completed and all necessary proof must be provided.

The TSP defines the following verification methods:

HR-DB

The TSP enters into an agreement with an organization (subscriber) and stipulates that only valid data is to be transmitted which meets with the requirements of this CPS. The organization uses a secure communication channel in order to send requests to the TSP that were generated on the basis of the identity management system EIDM with auditable policy administration processes. The organization is obliged to respect the relevant data protection requirements. The TSP trusts in the correctness and unambiguity of the data transmitted. At the time the tokens are handed over at the latest, the subscriber informs the subject about the latter's obligations under the subscriber agreement.

In the Uniper PKI, the end entities are identified and the request data is checked in accordance with the processes defined in this CPS: standard and standard plus (see section 4.1) including a variant for certificates for mobile devices according to the methods of the standard process. The SCM checks

against a blacklist whether the applicant was excluded from use of software certificates and, if applicable, displays a corresponding error message.

Domain

The control over a domain is validated using the following methods:

According to [BRG] section 3.2.2.4.2 Email, Fax, SMS, or Postal Mail to Domain Contact[3], [BRG] 3.2.2.4.4 Constructed Email to Domain Contact, [BRG] 3.2.2.4.7 DNS Change, [BRG] 3.2.2.4.13 Email to DNS CAA Contact, [BRG] 3.2.2.4.14 Email to DNS TXT Contact and [BRG] 3.2.2.4.18 Agreed-Upon Change to Website v2.

IP addresses
IP addresses are not permitted and are not validated.

The results of the enquiry are filed.

The certificate request is not released and sent to D-Trust until all request preconditions are available in a signed form.

Identification and authentication (I&A) are carried out according to sections 3.2.2 and 3.2.3.

4.2.2 Acceptance or rejection of certificate applications

If the certificate request via the agreed online interface contains any technical or context-related errors, the request will be rejected. The corresponding online interface then generates a message showing the reason(s) why the request was rejected. The request must be amended accordingly and submitted again.

Other reasons for rejection include:

- Suspected violation of third-party name rights;
- Non-adherence to deadlines for proof of data;
- Circumstances justifying suspicion that the issuance of a certificate could discredit the operator of the CA.

The request is not deemed to be unconditionally accepted until the TSP has made a positive decision regarding the certificate request and the certificate requested has been handed over (see section 4.4).

4.2.3 Deadlines for processing certificate applications

No stipulation.

4.3 Certificate Issuance

4.3.1 Procedure of the TSP for the issuance of certificates

The corresponding certificates are produced in the high-security area of the trust service provider.

The TSP either files the complete request documentation in accordance with section 0 in an auditable manner, or the TSP concludes agreements with partners pursuant to which the request

[3] With this method, only the e-mail address is used for validation.

documents and/or requests have to be filed in a safe manner and completely until the period according to section 5.5.2 expires.

This ensures that the correct time is used during certificate production.

4.3.2 Notification of the subscriber that the certificate was issued

The TSP does not provide the subscriber with separate notification of completion of the certificate.

End entities are informed by the subscriber.

4.4 Certificate Acceptance

4.4.1 Procedure during certificate handover

If a certificate is issued for a key pair that is already available at the end-entity, the certificate is either made available for downloading (for instance, published in the repository service) or sent electronically.

Automatic certificate requests require certain information to be sent to the system as follows:

- applicant information,
- request data and data format,
- desired certificate product,
- revocation password.

In the event that the subscriber detects errors in his certificates or in conjunction with the function of the keys and tokens, he must communicate this to the TSP without delay. The certificates are then revoked.

Incorrect data in the certificate is only deemed to be a contractual defect within the meaning of the contract if the TSP was obliged to check the functions affected by such defect according to this CPS.

Acceptance by the customer does not take place.

4.4.2 Publication of the certificate by the TSP

EE certificates are generally not published by the TSP. Publication is carried out by the subscriber.

The status can be retrieved via CRLs and OCSP after production of the certificate.

4.4.3 Notification of other PKI entities concerning the issuance of the certificate

Certificates of the Uniper PKI and its revocation information are fully automatically stored in a smartcard management system. On the basis of this data, revocation can be initiated and requested in accordance with defined processes. See section also 4.9.3.

4.5 Key Pair and Certificate Usage

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

End entities are entitled to use their private keys exclusively for those applications that are in conformity with the types of use stated in the certificate.

Key material for signature and authentication certificates from the SubCAs XXXI and XXXII is generated exclusively on certified PKI tokens or TPMs that meet the ISO/IEC 11889 standard (TCG specification family 2) in the sphere of the subscriber.

Key material for authentication and encryption certificates from the SubCA XXXIII is generated in a protected server environment by the subscriber.

The provisions in section 1.4 apply to subscribers.

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

The certificates of the Uniper PKI can be used by all relying parties. **They can, however, only be relied upon** if:

- the certificates are used in line with the types of use shown there (key use, extended key use, restricting certificate extensions, if applicable),
- verification of the certificate chain can be carried out successfully right through to a trusted root certificate[4], if there are no other applicable methods available to determine trust (e.g. EU Trusted List according to eIDAS (Regulation (EU) No 910/2014 and its implementing decisions) or software vendor root stores),
- the check of the status of the certificates via CRL or the certificate status service (OCSP) had a positive outcome, and
- all other precautionary measures determined in agreements or otherwise were taken and if restrictions, if any, in the certificate as well as any application-specific measures were taken by the relying party and found to be compatible.

4.6 Certificate Renewal

Certificate renewal is not offered.

4.7 Certificate Re-key

Re-keying is not offered.

4.8 Certificate Modification

Certificate modification is not offered.

4.9 Certificate Revocation and Suspension

4.9.1 Conditions for revocation

The procedures of the TSP fulfil the requirements of EN 319 411-1 and [GL-BRO]. A certificate is revoked in the following cases:

- when requested by the subscriber and/or the third party concerned (for instance, the organization named in the certificate),
- if the certificate was issued on the basis of incorrect data,
- if the original certificate request was not authorized and authorization is not granted retroactively,
- if the TSP becomes aware that the private CA or EE key has been communicated to an unauthorized person or organization that is not affiliated with the subscriber,

[4] Verification of the certificate chain is to be carried out according to the PKIX model (also called shell model) according to [RFC 5280], [RFC 6818]. A formal description of the algorithm used to verify the certificate chain can be found in [ETSI EN 319 412].

- if the private key of the subscriber associated with the public key in the certificate has been compromised,
- if it can be proven to the TSP that the associated private key can be calculated based on the public key in the certificate,
- if the TSP determines that the certificate has not been issued in accordance with the applicable CP and CPS or that the sub-CA does not meet the requirements of the applicable CP and CPS,
- if the TSP determines that the requester has breached the Subscriber Agreement or the applicable CP or CPS,
- if certificate contents that were valid at the time the request was submitted become invalid during the validity period, e.g. due to a change in name or loss of organizational affiliation,
- if the TSP discontinues its activities and if such activities are not continued by another TSP.

Irrespective of the foregoing, the TSP is entitled to revoke certificates if:

- D-Trust as the trust service provider (TSP) is obliged by law to revoke the certificate,
- the private key of the issuing or of a higher-level CA was compromised,
- the certificate of the issuing or of a higher-level CA has been revoked,
- weaknesses are detected in the encryption algorithm used which pose serious risks for the permitted applications during the certification life cycle,
- the hardware and software used show security shortcomings which constitute serious risks for the permitted applications during the certification life cycle,
- unambiguous assignment of the key pair to the subscriber is no longer ensured,
- there are reasonable grounds to suspect that a certificate is being misused,
- no confirmation of receipt is sent to the TSP within the agreed period of time indicating that the certificate was transmitted in a correct manner with regard to form and contents via a contractually agreed online interface,
- the contract was terminated or expired in any other manner,
- the CA is transferred to another TSP without the relevant revocation information of the issued EE certificates being transferred too.

NCP, LCP

Certificates that are capable of signing or encrypting e-mails and contain an e-mail address are also subject to the revocation reasons listed in Mozilla Root Store Policy 2.7, Chapter 6.2. Depending on the reason for revocation, the certificate must be revoked within 24 hours or can be revoked within five days.

Revocations are marked with the time of revocation. Retroactive revocation is not possible. Furthermore, revocation cannot be reversed.

Personnel employed for revocation management are not subject to any commercial, financial or other influence by the organization.

Parties authorized to request revocation must identify themselves according to section 3.4.

4.9.2 Authorization for revocation

- The TSP is authorized to revoke certificates.
- Subscribers are always authorized to have their certificates revoked.

Otherwise any individual will be deemed to be authorized to request revocation from the TSP if such individual states the correct revocation password.

4.9.3 Revocation request procedure

The end-entity can revoke his certificates both via the global service desk of the subscriber within the infrastructure of Uniper and directly in his personal area of the smartcard management system via the online interface.

Revocations via the global service desk are passed on from the global service desk to the TSP.

E-mail address: pki@uniper.energy

Other revocation methods can be agreed to.

A certificate revocation request via an online interface should contain the following details:

- the issuer of the certificate,
- the agreed revocation password,
- the serial number of the certificate (in decimal format, if possible) in order to enable unambiguous identification of the certificate.

Via the personal area of the smartcard management system, it is also possible to revoke certificates for third parties within the Uniper PKI. In this case, the party requesting revocation must log in and authenticate himself to the smartcard management system with his personal token in the request.

Revocation takes place in the sphere of responsibility of the TSP and can only be carried out in an authorized manner by authorized personnel.

Revocation of a certificate is final. A certificate, once revoked, cannot be re-activated.

All revocation information is logged accordingly. The end-entity receives a message regarding revocation of his certificates, for instance, by e-mail.

4.9.4 Revocation request deadlines

The end-entity or subscriber is solely responsible for ensuring that they or a person authorized to request revocation on their behalf immediately request revocation as soon as reasons for revocation become known. The procedure which promises fastest processing of the revocation request must be used.

4.9.5 Time span for the processing of a revocation request by the TSP

Revocation requests can be submitted 24/7 by phone or via the online interface. Revocation takes place according to section 4.9 [BRG] within 24 hours after successful authorization of the revocation requester.

4.9.6 Methods available for checking revocation information

Up-to-date revocation information is maintained in certificate revocation lists which can be retrieved via the LDAP protocol or the link shown in section 2.1. An OCSP service is additionally available. The

availability of these services is indicated in the form of URLs in the certificates. Revocation information can also be obtained via the EIDM. Delta-CRLs are not offered.

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

Information on status and revocation (OCSP and CRL) is consistent.

Status changes in the OCSP are available for query immediately after revocation. Status changes in a CRL contain the same revocation information. However, distribution of a new CRL takes place with a time delay after revocation.

4.9.7 Publication frequency of certificate revocation lists

See section 2.3.

4.9.8 Maximum latency time for certificate revocation lists

Certificate revocation lists are published immediately following their generation.

4.9.9 Online availability of revocation information

An OCSP service is available for online verification.

The OCSP responder only returns a "good" result if the certificate is stored in the repository and if it is valid.

The availability of this service is indicated in the form of a URL in the certificates.

4.9.10 Need for online verification of revocation information

There is no obligation for an online verification of revocation information; however, section 4.5.2 applies.

4.9.11 Other forms for notification of revocation information

No stipulation.

4.9.12 Special requirements in the case of compromising of the private key

D-Trust revokes a certificate due to a compromised private key if key compromise can be proven using one of the following methods:

- Transmission of the compromised private key or
- Signing of a CSR with the common name entry "Proof of Key Compromise for D-TRUST" by the compromised private key

D-Trust provides a Certificate Problem Report for reporting a key compromise. This is described in the section 1.5.2 of the CP and must be used.

If a key compromise is successfully proven, D-Trust will revoke the certificate according to the specifications in section 4.9. of [BRG].

4.9.13 Conditions for suspension

Certificate suspension is not offered.

4.10 Certificate Status Services

4.10.1 Operation of the status request service

The certificate status service is available via the OCSP protocol. The availability of the service is indicated as a URL in the certificates.

The system time of the OCSP responder is synchronized daily using the DCF77 time signal and reliable time servers (NTP) on the Internet.

The formats and protocols of the services are described in sections 0 and 0.

4.10.2 Availability of the status request service

The status check service is available 24 hours a day, 7 days a week and has an availability of 99.95%. The TSP ensures that in the event of a malfunction, downtime is limited to a maximum of four hours.

4.10.3 Optional services

The relying party can obtain information regarding the status of a received certificate at the following e-mail address: pki@uniper.energy

4.11 End of Subscription

The validity of the certificate ends on the expiry date shown in the certificate. The request to revoke a certificate by a subscriber or party authorized to request revocation leads to revocation by the TSP. The TSP's main contractual duties are thereby completely fulfilled.

4.12 Key Escrow and Recovery

Private EE key escrow is implemented by the subscriber. Signature and authentication keys of EE certificates from the SubCAs XXXI and XXXII as well as authentication keys from the SubCA XXXIII are not placed in escrow.

In the case of the Uniper PKI, the EE keys of encryption certificates from the SubCA XXXIII are kept separately by the subscriber.

The decryption keys are stored by a system operated by a service provider on behalf of Uniper. The relevant requirements of EN 319 411-1 must be adhered to. Compliance with the requirements is subject to regular revision.

See also section 6.2.3.

4.12.1 Conditions and procedures for escrowing and restoring private keys

Private key escrow is not provided by the TSP.

The subscriber (Uniper) places in escrow keys for encryption certificates from the SubCA XXXIII in his own sphere of responsibility according to the following rules:

The SCM offers a defined and specially protected repository area for escrow of the master keys of the cards and personal keys in symmetrically encrypted form. All private decryption keys from the SubCA XXXIII are generated by an HSM module and are available in encrypted form in a repository.

Only the authenticated end-entity is authorized to access the encryption keys in escrow and transfer these to his mobile device (see section 4.1.3) or as history certificates to his token. This ensures access to currently and previously valid certificates and the pertinent private keys in order to decrypt older data.

KIDs (GroupIDs) of employees who leave the company are deactivated and archived by an internal process. However, this does not mean that the employee's private keys and certificates are removed from the SCM repository.

By registration via the central portal of the smartcard management system, an end-entity can use a workflow in order to configure so-called deputies who can then access the end-entity's private encryption keys and additionally transfer them to their tokens in order to be able to access all encrypted e-mails of the end-entity's inbox as part of deputy or support tasks.

This confirmation of the deputies takes place exclusively in an authenticated form via the portal of the smartcard management system where deputy requests are confirmed and the currently existing deputies can be displayed and deactivated when necessary.

Before using new deputy keys, the deputies must also register via the portal of the smartcard management system and are then offered the deputy keys available to them in order to add or delete their own PKI medium and/or mobile device.

When a deputy authority is added and deleted and when a deputy key is installed and deinstalled on the PKI medium, the deputy and the party represented automatically receive an e-mail for their information, so that parties represented can request that deputies who are no longer supposed to act in this function remove the keys. This also happens when the party represented changes his PKI medium or mobile device so that the decryption keys of the party represented must be newly installed.

Deputies can continue using the private keys after termination of their deputy status until the PKI token of the party represented is re-configured via the portal of the smartcard management system.

On the basis of applicable laws, the head of information security in charge can, in exceptional cases and in conformity with the requirements of the multi-eyes principle, authorize other end entities to use the encryption certificates in order to enable access to encrypted e-mails. He is responsible for involving the relevant supervisory bodies, for comprehensible documentation and, when necessary, for subsequent notification of the end entities concerned.

In the case of team certificates, the team leader can act via a function KID as the owner of the certificate and set up his primary KID and the KIDs of the team members as deputies. In this way, they can also obtain the private keys of these certificates.

4.12.2 Conditions and procedures for depositing and restoring session keys

Session keys are not offered.

5. Facility, Management, and Operational Controls

The descriptions of sections 5.4 to 5.6 specifically refer to the SubCAs of the Uniper PKI operated by D-Trust GmbH within the scope of [EN 319 411-1].

D-Trust operates an information security management system (ISMS) in accordance with ISO/IEC 27001. Operation of the TSP is subject to this ISMS. An Information Security Policy regulates the binding requirements for operation. This was approved by the management of D-Trust GmbH and communicated to all employees of the TSP. The Security Policy is reviewed and updated each year, and also on an event basis.

If changes due to processes or operations lead to an update of the Security Policy, the resulting changes for TSP operation must be approved by the management. The updated and approved Security Policy must be communicated promptly by the managers to all affected employees and, if necessary, the manager must initiate training measures.

5.1 Physical Security Controls

Detailed documentation is available for physical security controls and the relevant parts of this can be made available for inspection to any party proving a justified interest in such disclosure. The security concept has been audited by a recognised conformity assessment body. Conformity assessment is regularly repeated in accordance with [EN 319 411-1] and [EN 319 411-2].

Furthermore, TÜV-IT has certified that the trust service provider of D-Trust GmbH applies and implements in its security area the "Infrastructure measures for high protection requirements – level 3" ["Infrastrukturmaßnahmen für hohen Schutzbedarf – Level 3"] (according to the catalogue of audit criteria for "Trusted Site Infrastructure"). This TÜV-IT certificate for a "Trusted Site Infrastructure" audits and evaluates all infrastructure-relevant aspects. This audit is repeated every two years. The above-mentioned certificate confirms that D-Trust GmbH fulfils this demanding security standard for its facility, management, and operational Controls.

The SubCAs of the Uniper PKI are operated by the TSP under the same conditions as the CAs of D-Trust GmbH.

5.2 Procedural Controls

5.2.1 Role concept

Documentation includes a role concept where TSP management assigns employees to one or more roles and they receive the corresponding authorizations. The authorizations of the individual roles are limited to those authorizations which these roles need to fulfil their tasks. The assignment of authorizations is revised on a regular basis, and authorizations are cancelled immediately when no longer needed.

Roles with security responsibility for TSP operation, known as "Trusted Roles" (including the tasks of security officer, system administrator, system operator, system auditor, registration officer, revocation officer and validation specialist) are defined in D-Trust's authorization concepts. These roles may only be assumed by competent and reliable employees.

Job descriptions are created for the respective roles. These define the tasks, the minimum level of qualification and experience required for each role. An employee may fill one or more roles, provided the roles are not mutually exclusive and the employee can demonstrate that he or she has the qualifications and experience required for the role.

Employees are regularly trained to fulfill their roles and related responsibilities, and they are made aware of compliance with applicable security regulations. They can attend training course in order to qualify for further roles.

The requirements for the roles are documented in the job descriptions and can be viewed by employees at any time.

Before employees can perform their assigned roles, they must agree to these roles. In the case of mutually exclusive roles, a person can assume only one of these roles (four-eyes principle).

A risk assessment is carried out on a regular basis.

Employees working in the area of certification and revocation services act independent and are free from commercial and financial constraints that could influence their decisions and acts. The organization structure of the TSP considers and supports employees in the independence of their decisions.

5.2.2 Four-eyes principle

The four-eyes principle is the minimum requirement for particularly security-critical operations. This is ensured by technical and organizational measures, such as access authorization and verification of knowledge.

Security-critical systems used for certificate issuance are generally protected by multi-factor authentication.

5.2.3 Identification and authentication (I&A) for individual roles

The role concept is ensured by technical and organizational measures, such as access authorization and verification of knowledge. Before being allowed to access any security-critical applications and/or CA systems, the employee concerned must have been successfully authenticated. Event logs enable the identification of employees who performed past actions; the employees are accountable for their acts.

Relevant events of the CA environment relating to the certificate management as well as CA keys and CA certificates must be released and recorded in an auditable manner.

5.2.4 Role exclusions

The role concept includes various role exclusions in order to prevent any conflict of interests, ensure the four-eyes principle and avoid any harmful acts.

5.3 Personnel Controls

The TSP meets the requirements concerning personnel as laid down in EN 319 411-1. Employees who have security-relevant roles of the TSP are officially appointed. Documentation is carried out within the scope of the internal personnel life cycle.

5.3.1 Requirements in terms of qualification, experience and reliability

The TSP ensures that persons employed in the area of the trust service have the required knowledge, experience and skills.

The identity, reliability and professional qualifications of employees are verified before they commence work. Regular and demand-driven training ensures competency in the respective fields of activity as well as general information security. Training and proficiency check results are documented.

Line managers, in particular, are selected according to special criteria. They must demonstrate that they have knowledge of security procedures for staff with security responsibility and that they have sufficient experience of information security and risk assessment in relation to the trust service provided. Evidence can be provided in the form of certificates and CVs. If the required qualification cannot be proven sufficiently, it must be acquired through appropriate training before the employee can take over management functions in TSP operations.

5.3.2 Security screening

Individuals who work in security-relevant areas of the TSP are also regularly required to present clearance certificates.

The TSP also operates an ISMS certified according to ISO 27001 that provides employees with security-relevant requirements and/or rules of conduct.

5.3.3 Training

The TSP trains trust service personnel.

5.3.4 Frequency of training and information

The TSP trains trust service personnel at the beginning of their employment, annually and as required.

5.3.5 Frequency and sequence of job rotation

Role changes are documented. The corresponding employees are trained.

5.3.6 Controls in the case of unlawful acts

The TSP does not employ any unreliable persons in the certification service.

Violations by employees of the policies or processes of TSP operations are analyzed and evaluated. If the relationship of trust cannot be ensured, these employees are excluded from security-relevant activities.

5.3.7 Controls for external personnel

External staff who work with trust services fulfil the requirements of section 0 of this CPS and are subject to the sanctions pursuant to section 5.3.6 of this CPS.

5.3.8 Documentation handed over

Comprehensive process instructions and procedures for all production steps define the relevant employee roles and rights as well as the corresponding manual and automated checks.

The technical security infrastructure of D-Trust GmbH ensures that deviations from these defined processes are not possible in the production process.

5.4 Audit Logging Procedures

5.4.1 Monitoring access

The TSP implements comprehensive surveillance controls (for instance, video surveillance) in order to warrant the security of its trust services and the underlying IT systems and documents.

The audit logging procedures are supplemented by organizational rules. Visitor rules, for instance, require that visitors be announced and registered by name at least 24 hours before their visit. While in the area of the trust service provider's premises, visitors must be accompanied at all times by an employee of the TSP.

5.4.2 Monitoring organizational controls

Monitoring organizational controlss is another part of the security concept.

This includes a regular risk analysis that provides a comprehensive analysis of threats to the TSP's operations and defines requirements and counter-measures. It also includes an analysis of the residual risk where the appropriateness of the residual risk is identified and, if reasonable, accepted.

Within the scope of internal and external audits, regular tests are carried out in order to reduce risks due to external and internal attacks.

Furthermore, all relevant assets are correctly identified, and the corresponding changes to these assets are checked or, if applicable, released by the TSP staff commissioned by management.

5.5 Records Archival

5.5.1 Types of records archived

A distinction is made between electronic and printed documents.

The complete request data, the certificates, the revocation documentation, the electronic files and reports concerning the certificate life cycle are electronically archived by Uniper. Uniper can delegate the recording obligation to a partner company within the EU.

The records are archived for a minimum period of seven years after the expiry date of the certificates issued on this day.

The TSP ensures that unauthorized modification of the data archived by it is not possible during the archiving periods.

Furthermore, security-relevant events are suitably recorded. The system time is synchronized daily using the DCF77 time signal and reliable time servers (NTP) on the Internet.

5.5.2 Archiving times for data

Request and verification documents as well as data concerning the certificate life cycle and the certificates themselves are archived for a period of at least seven years and until the end of the year. The period begins after expiration of the term of validity of the certificate that was issued last on the basis of these documents.

Event logs of IT systems are stored for at least six months. Video recordings of persons and recordings of administrative activities are stored for a period of 90 days.

For the archiving system, the system time is synchronized daily using the DCF77 time signal and reliable time servers (NTP) on the Internet.

5.5.3 Archiving (internally/externally)

Archiving is carried out internally at the TSP as well as externally in rooms affording equivalent protection.

5.5.4 Archive protection

The external archives are located in protected rooms of Uniper or its partner companies and are subject to a corresponding role and access control concept.

5.5.5 Archive data backup

Confidentiality and integrity of data are maintained. Documentation is set up immediately so that subsequent changes are discovered. European and German data protection requirements are adhered to.

5.5.6 Procedure for obtaining and verifying archive information

The process of obtaining and verifying archive information is subject to the role concept of the TSP and/or outsourcing partner of Uniper.

5.6 Key Changeover

In due time before a (Sub)CA expires, new CA keys are generated, and new CA instances set up and published.

5.7 Compromise and Disaster Recovery

The TSP has implemented measures to prevent any interruption of operations as a result of loss, damage or compromising

5.7.1 Treatment of incidents and cases of compromising

The TSP has a contingency concept and a restart plan which are known to the roles involved and which can be implemented by these when necessary. Responsibilities are clearly distributed and are known.

Should a system recovery be necessary, the responsibilities and corresponding "Trusted Roles" are laid down in D-Trust's authorization concept and are known to the respective employees. See section 5.2.1.

Security-relevant incidents and cases of compromise are documented and investigated accordingly.

5.7.2 Restoring after compromising of resources

The security concept describes the implementation of recovery procedures for restoring the operability of the TSP. Backups are made on a daily basis and after changes. Backups are stored in a different fire zone. The recovery of critical CA systems is regularly tested in emergency drills.

5.7.3 Compromising of the private CA key

In the event of compromising or communication of uncertainty of algorithms or associated parameters by the issuers of the relevant catalogues according to section 6.1.6, the TSP initiates the following:

- The CA certificates as well as their certificates already issued and not yet expired are revoked.
- Subscribers affected are informed about the incident and its effects.
- The respective supervisory body is informed and the incident is published on the websites of the TSP including a statement that any certificates that were issued by this CA are no longer valid and that the revocation status can be verified.

The analysis of the reasons for compromising is used, if possible, to design suitable measures in order to prevent future cases of compromising. Taking the reasons for compromising into consideration, new CA signature keys are generated and new CA certificates issued.

5.7.4 Ways of continuing business following compromising and disaster

In an emergency, the TSP decides, depending on the type of incident, whether a recovery of the backup of the CA described in section 6.2.4 is to be carried out or whether the procedure described in section 5.7.3 is to be adopted in the case of compromising.

5.8 CA or RA Termination

D-Trust has a continuously updated termination plan.

When the services of CAs are terminated, the TSP informs all subscribers and terminates all access possibilities for the TSP's subcontractors with regard to the CAs concerned. All certificates issued by the CAs concerned which are still valid are revoked. Private CA keys which are concerned are destroyed.

In the event of a planned discontinuation of its operations, the TSP informs all end-entities, subscribers and third party in advance.

The repository service and application documents as well as the repository (CP, CPS and CA certificates) are handed over to Bundesdruckerei GmbH and continued there under equivalent conditions. Continuation of the repository service until the end of the term of validity of the EE certificates is warranted and handed over either to another TSP or to Bundesdruckerei GmbH.

Bundesdruckerei has warranted to the TSP compliance with these minimum requirements.

On completion of operations, the functionality of the CAs will be discontinued so that certification is no longer possible.

6. Technical Security Controls

The descriptions contained in this section refer to the CAs of the Uniper PKI which are operated by D-Trust GmbH.

6.1 Key Pair Generation and Installation

At this point, a distinction is made between key pairs for

- CA certificates (Uniper Group CA 2 2015 and Uniper Group CA 3 2020 and its SubCAs) and
- end-entity certificates (EE certificates)

6.1.1 Generation of key pairs

CA keys are generated in a "FIPS 140 2 Level 3"-compliant hardware security module (HSM). The HSM is located in the high-security area of the trust service provider. The key ceremony takes place according to defined procedures. Depending on the CA, the key ceremony is performed by Trusted Roles in the presence of the security officer and, if necessary, under the supervision of an independent third party. The activities during the key ceremony are checked and recorded using a checklist. The role concept and hence the 4-eyes principle are compulsory for key generation. Whenever CA keys are generated, an independent auditor is present, if necessary, or, following key generation, the auditor can use a video recording in order to verify the correctness of the key generation process. The generation of CA keys is also documented in accordance with [EN 319 411-1].

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

During generation of EE keys, the subscriber is required to generate these in a cryptographically secure manner in accordance with the requirements of [EN 319 411 1].

The private EE keys for signature and authentication certificates are generated on PKI tokens (smartcards certified according to EAL4+ or USB tokens with the same functionality) or TPMs corresponding to the ISO/IEC 11889 standard (TCG specification family 2).

6.1.2 Delivery of private keys to subscribers

Private keys in the Uniper PKI are not generated by the TSP.

6.1.3 Delivery of public keys to the TSP

Certificate requests can be submitted by subscribers for an existing key pair in the form of certificate requests which must be signed. The certificate request is signed with a previously agreed certificate. Transmission of the signed certificate request is additionally carried out via a TLS-protected channel.

The certificate request contains the public key. The corresponding response returns the complete certificate.

6.1.4 Delivery of public CA keys to relying parties

The public CA key is contained in the CA certificate. Furthermore, CA certificates can be obtained from the public repository (see section 2.1) where they are published after their generation.

6.1.5 Key lengths

RSA keys with a key length of at least 2048 bits are currently used for CA certificates.

RSA keys with a key length of at least 2048 bits are currently used for EE certificates.

6.1.6 Determining the key parameters and quality control

CA and EE certificates are issued on the basis of keys that comply with [ETSI-ALG] in its latest applicable version in as far as compatibility in the use environment is ensured.

The signature and encryption algorithms are mentioned in section 7.1.3 of the CPS.

Regular tests are carried out in order to ensure the quality of the cryptographic material.

6.1.7 Key uses

Private CA keys are exclusively used to sign certificates and revocation lists (see section 7.1.2).

The EE keys may only be used for the types of use stated in the certificate. The types of use are defined in the *KeyUsage* and *ExtKeyUsage* fields in the certificate and may be restricted by further extensions (see section 7.1.2).

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Standards and security controls for cryptographic modules

The cryptographic modules used by the TSP work perfectly. Throughout their entire life cycle (including delivery and storage), the modules are protected against manipulation by suitable technical and organizational measures.

The CA keys are protected by an HSM that was evaluated according to FIPS 140-2 Level 3. The subscriber is responsible for ensuring a sufficient quality during the key generation process for EE keys.

Furthermore, the CA systems are protected against viruses or other unlawful software.

6.2.2 Multi-person access protection for private keys (n of m)

The HSM on which the CA keys are stored is located in the secure environment of the trust service provider. A private key must be activated by two authorized persons. Following activation, the HSM can sign any number of certificates.

Access to private EE keys is only possible in the case of keys in escrow according to section 6.2.3.

6.2.3 Private key escrow

The TSP does not offer escrow of private CA.

Private EE key escrow can be applied for and will be implemented by the subscriber according to section 0.

The TSP does not offer signature key escrow of EE certificates.

In the case of the Uniper PKI, the EE keys for encryption certificates from the SubCA XXXIII are kept separately by the subscriber.

The encryption keys are stored by a system operated by Uniper or a service provider retained for this purpose. The relevant requirements of EN 319 411 1 must be adhered to. Compliance with the requirements is checked.

Private keys of the Uniper SubCA XXXIII can be used for decryption and/or authentication for use in mobile devices or SoftPSEs even outside a certified PKI medium or VSC.

6.2.4 Backup of private keys

A backup of the private CA keys exists. A CA key backup must be carried out at the HSM by two persons authorized for this activity and takes place in the secure environment of the trust service provider. The backup system is subject to the same requirements and protection measures as the production system. Recovery of private keys also requires two authorized persons. Further copies of the private CA keys do not exist.

The TSP does not offer a backup service for private EE keys.

6.2.5 Archiving of private keys

Private CA and EE keys are not archived by the TSP. The subscriber is responsible for archiving encryption keys of end entities from the SubCA XXXIII.

6.2.6 Transfer of private keys to or from cryptographic modules

Transfers of private CA keys to or from the HSM are limited to backup and recovery purposes. Adherence to the 4-eyes principle is compulsory. Private CA keys exported to/imported from another HSM are protected by encryption.

In the case of certificates to be used on mobile devices, the key material generated by the subscriber in the HSM is encrypted using the end-entity's existing encryption key and transmitted in a protected manner to the end-entity's device. Installation of the key material is only possible after the complete correct PIN of the encryption key has been entered. A backup of the P12 file at the end-entity is not foreseen.

The corresponding application transmits the encryption certificates to the mobile device together with the e mail profile. The end-entity does not have to implement any further measures in this context.

6.2.7 Storage of private keys in cryptographic modules

The private CA keys are contained in encrypted form in the HSM at the TSP.

The private EE keys for signature and authentication certificates are generated on PKI tokens (smartcards certified according to EAL4+ or USB tokens with the same functionality) or TPMs corresponding to the ISO/IEC 11889 standard (TCG specification family 2) or in encrypted form on a VSC.

The subscriber is responsible for storing encryption keys of end entities from the SubCA XXXIII. Private keys of the Uniper SubCA XXXIII can be used for decryption and/or authentication for use in mobile devices or SoftPSEs even outside a certified PKI medium or VSC.

6.2.8 Activation of private keys

The private CA keys can only be activated according to the 4-eyes principle, by the authorized roles and for the permitted types of use (keyCertSign, cRLSign).

Private signature keys are activated at the end-entity's end by entering a PIN with at least six digits.

6.2.9 Deactivation of private keys

The private CA keys are deactivated by disconnecting the connection between the HSM and the application.

The respective application deactivates the private EE key. Deactivation takes place at the latest when the PKI token is removed.

6.2.10 Destruction of private keys

The private CA keys are deleted when their term of validity expires. This is accomplished by deleting the private key on the HSM and simultaneous deleting of the backups on data media. When the HSM is shut down, the private keys in the device are deleted.

6.2.11 Assessment of cryptographic modules

6.2.11 Assessment of cryptographic modules
The TSP operates suitable hardware-based and software-based key generators in order to warrant the quality of the EE keys. The HSMs used are FIPS 140 2 Level 3-compliant.

6.3 Other Aspects of Key Pair Management

6.3.1 Archiving of public keys

Public CA and EE keys are archived in the form of the certificates generated.

6.3.2 Validity periods of certificates and key pairs

The term of validity of the CA keys and certificates is variable and shown in the certificate. The maximum possible validity period totals 30 years.

The term of validity of the EE keys and certificates is variable and shown in the certificate. The maximum possible term of validity of NCP or LCP certificates of the Uniper PKI totals 36 months.

6.4 Activation Data

6.4.1 Generation and installation of activation data

The activation data of the CA keys is requested by the HSM. The PIN is assigned during the bootstrap procedure. Adherence to the 4-eyes principle is compulsory.

Since the key pair is generated by the subscriber, the activation secret is available directly and exclusively to the subscriber.

6.4.2 Protection of activation data

The activation data of the CA keys is made up of two secrets with each one known to one authorized employee. Only certain, designated employees can access the activation data.

6.4.3 Other aspects of activation data

PKI tokens in the Uniper PKI are configured in such a manner that they are blocked after three incorrect PIN entries. End entities have no personal unblocking key number (PUK) to unblock the PKI token. The PIN is set by the end-entity himself, it can be changed by the end-entity and reset by him with the help of the smartcard management system.

6.5 Computer Security Controls

D-Trust operates an information security management system (ISMS) in accordance with ISO/IEC 27001. Operation of the TSP is subject to this ISMS. A Security Policy regulates the binding requirements for IT operations. This was approved by the management of D-Trust GmbH and communicated to all employees of the TSP. The Security Policy is reviewed and updated each year, and also on an event basis.

Evaluation and, if necessary, elimination of identified vulnerabilities takes place within 48 hours. If it is not possible to resolve the problem within 48 hours, the assessment will include a concrete treatment plan.

6.5.1 Specific technical security requirements for the computer systems

The computers, networks and other components used by the TSP ensure in their given configuration that only those actions can be carried out which are not in conflict with the CP and EN 319 411 1.

It is ensured that security-relevant software updates are installed at the appropriate point in time on the relevant systems. Any deviations are suitably documented by the TSP and, if necessary, addressed in the TSP's risk management.

The subscriber and end-entity must use trusted computers and software: This requirement is fulfilled according to the policy determined by Uniper.

The system time of the relevant CA systems is ensured by a radio clock with a redundant connection.

6.5.2 Assessment of computer security

The computers, networks and other components used for the CA keys are regularly checked, inspected and audited by recognised conformity assessment bodies and are suitably monitored in accordance with [EN 319 401].

6.5.3 Monitoring

The relevant systems are continuously monitored in order to ensure their availability. Each failure is recorded, documented, classified according to its severity and prioritized. The handling of critical notifications is part of the incident management process. Notifications on security-relevant events are sent to a central place and assessed according to their criticality.

In case of failures where one service is no longer available, the parties affected will be informed every 24 hours on the current status of trouble-shooting.

6.6 Life Cycle Security Controls

Productive server systems receive security relevant configurations via central management systems. The configurations are checked every 15 minutes. Any deviations from the central security guidelines are immediately corrected in the configurations.

During the planning of all systems operated by the TSP or on behalf of the TSP, the requirements of section 5 [BRG] are already adequately considered.

6.6.1 Security controls during development

During the course of all system development projects carried out by or on behalf of the TSP, security requirements are already analyzed during the draft design phase. The results are defined as requirements for development.

D-Trust’s test environment for development, testing and staging systems is separate from its production systems.

6.6.2 Security controls in conjunction with computer management

Administration of computers, networks and other components is strictly limited to personnel authorized according to the role concept. Relevant systems are protected by multi-factor authentication. Log files are regularly analyzed with a view to rule violations, attempted attacks and other incidents. Audit logging procedures begin when a device is set into operation and end when it is disposed of.

6.6.3 Security controls during the lifecycle

Any devices used are operated in accordance with their manufacturers' instructions. Prior to being set into operation, they are meticulously checked and inspected. They are only set into operation if it is clear beyond any doubt that they were not manipulated. Hardware and software checks, for instance, are sealed in order to be able to detect manipulation and attempted manipulation during any activity or inspection. Furthermore, methods and systems are used that monitor security-relevant and/or CA systems on a permanent basis in order to detect any irregularities (unauthorized access, failure, etc.). In the case of suspected manipulation of a component, any action planned will not be carried out and the incident is reported. In order to enable an immediate and co-ordinated response to any security-relevant incidents, the TSP defines clear-cut escalation rules for the individual roles. All relevant events of the CA environment and of the key and certificate management system are detected by the system and filed in a signed form.

Capacity requirements and utilization as well as the suitability of the systems involved are monitored and adapted as required. Devices that have been exchanged are taken out of service and disposed of in such a manner that any misuse of functionalities or data is ruled out. Modifications of systems or processes are subject to a documented change management process. Security-critical modifications are checked by the security officer. After expiration of the term of validity of CAs, the private keys are destroyed.

Electronic data or printed reports are used to document all relevant events which influence the life cycle of the CA, of the certificates issued and of the keys generated, and such electronic data or printed reports are stored on long-lived media in an auditable form.

Special care is taken in this context in order to ensure that the media used are treated safely and protected against damage. Furthermore, these media are stored safely, checked at regular intervals and protected against wear and/or obsolescence.

Penetration tests are carried out at least once a year by an independent and competent body. Furthermore, vulnerability scans are initiated at least once every three months. The results of the penetration test report are archived internally.

The features and characteristics of the processes used for identification are developed on a case-by-case basis within Uniper and/or between Uniper and its service providers and initially agreed to and co-ordinated with D-Trust.

Modifications of the processes described in the CP, CPS and process-related contracts are subject to D-Trust's prior confirmation regarding policy conformity on the basis of a change description within two weeks and, when necessary, prior updating of the relevant documents.

The representatives of D-Trust GmbH's executive management and the PKI supervisors of Uniper are responsible for compliance and must be involved in the change management process as parties

whose consent is mandatory in as far as implications for the PKI identification and registration processes are foreseeable

6.7 Network Security Controls

A network concept is implemented at the CAs that ensures that the relevant CA systems are operated in particularly well-protected network zones. The network architecture of the TSP features a multi-level concept of network security zones. The root CAs are operated in the network security zone with the highest security requirements. Detailed documentation is available for the network concept and the relevant parts of this can be made available for inspection to any party proving a relevant interest in such disclosure.

In order to protect the processes of the TSP, firewalls and intrusion detection/prevention mechanisms are used, for instance, that allow explicitly permitted connections only. The TSP operates network segments with different protection requirements and separates networks for employees and Internet uses on the one hand from server networks on the other. The systems are subject to regular inspection and revision, the employees in charge are accountable. Anomalies are reported by technical systems and organizational processes and addressed by a defined incident handling procedure as well as related processes.

Redundancy ensures the availability of the Internet connection. There are two permanent connections to the provider on two different routes. If the provider's access point fails, the system automatically switches to the second connection.

Cryptographic mechanisms are used to protect data traffic with a high protection demand outside the networks protected by the TSP for which integrity or confidentiality must be ensured.

The physical security of the networks operated and used by the TSP is ensured and adapted to the structural conditions and any changes therein.

A network security concept is implemented for the operation of the SCM in the data center for Uniper.

6.8 Timestamping

Timestamping is not offered within the scope of this CPS.

7. Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

7.1.1 Version numbers

Certificates are issued in X.509v3 format and in accordance with EN 319 412-2.

The certificate serial number is randomly generated and contains an entropy of 128 bits.

7.1.2 Certificate extensions

The selection of the extension is primarily product-dependent.

CA certificates contain the following *critical* extensions ("mandatory field"):

Extension	OID	Parameter
keyUsage	2.5.29.15	*keyCertSign,* *cRLSign*

Extension	OID	Parameter
basicConstraints	2.5.29.19	*Ca=TRUE,* *(pathLenConstraint)*

CA certificates can include the following *non-critical* extensions ("optional"):

Extension	OID	Parameter
authorityKeyIdentifier	2.5.29.35	160-bit SHA-1 hash of the issuer key
subjectKeyIdentifier	2.5.29.14	160-bit SHA-1 hash of the subject public key
cRLDistributionPoints	2.5.29.31	Address of the CRL issuing authority
authorityInfoAccess	1.3.6.1.5.5.7.1.1	*accessMethod=OCSP {1.3.6.1.5.5.7.48.1}, accessLocation {…}* *accessMethod=Certification Authority Issuers {1.3.6.1.5.5.7.48.2}, accessLocation {…}*
certificatePolicies	2.5.29.32	OID of the CPs supported

Further extensions can be added; they must comply with [X.509], [RFC 5280], [RFC 6818], [ETSI EN 319 412] and [ETSI-ALG] or they must be described in a referenced document.

EE certificates contain the following *critical* extensions:

Extension	OID	Parameter
keyUsage	2.5.29.15	Possible are: *digitalSignature, contentCommitment, keyEncipherment, dataEncipherment, keyAgreement, encipherOnly, decipherOnly* and combinations thereof

EE certificates can include the following non-critical extensions:

Extension	OID	Parameter
extKeyUsage	2.5.29.37	Corresponding to [RFC 5280], [RFC 6818]
authorityKeyIdentifier	2.5.29.35	160-bit SHA-1 hash of the issuer key
subjectKeyIdentifier	2.5.29.14	160-bit SHA-1 hash of the subject public key
cRLDistributionPoints	2.5.29.31	CRL issuing authority as ldap address

Extension	OID	Parameter
authorityInfoAccess	1.3.6.1.5.5.7.1.1	*accessMethod=OCSP {1.3.6.1.5.5.7.48.1}, accessLocation* *accessMethod= Certification Authority Issuer {1.3.6.1.5.5.7.48.2}, accessLocation*
certificatePolicies	2.5.29.32	OID of the CPs supported *cpsURI*
subjectAltName	2.5.29.17	Alternative holder's name

Further extensions can be added; they must comply with [X.509], [RFC 5280], [RFC 6818], [ETSI EN 319 412] and [ETSI-ALG] or they must be described in a referenced document.

7.1.3 Algorithm OIDs

The following encryption algorithm is currently used in the CA and EE certificates:

- RSA with OID 1.2.840.113549.1.1.1.

The following signature algorithms are currently used in CA and EE certificates:

- SHA256 RSA with OID 1.2.840.113549.1.1.11.

7.1.4 Name formats

In the *subject* (here: name of the subject/end-entity) and *issuer* (name of the issuer) fields, names are assigned according to [X.501] as DistinguishedName. The attributes described in section 3.1.4 can be assigned. Coding is carried out as UTF8 string or PrintableString for the C (Country) attribute.

The *SubjectAltName* (alternative subject name) and *Issuer-AltName* (alternative issuer name) fields can contain names according to [RFC 5280], [RFC 6818] (coded as IA5String).

7.1.5 Name constraints

"NameConstraints" is not used.

7.1.6 Certificate Policy Object Identifier

"CertificatePolicies" can contain the OID of CPs supported.

7.1.7 Use of the "PolicyConstraints" extension

"PolicyConstraints" is not used.

7.1.8 Syntax and semantics of "PolicyQualifiers"

"PolicyQualifiers" can be used.

7.1.9 Processing the semantics of the critical CertificatePolicies extension

In CA and EE certificates, the *CertificatePolicies* extension is not critical. Subscribers and relying parties are free to decide whether this extension is evaluated.

7.2 CRL Profiles

7.2.1 Version number(s)

Certificate revocation lists v2 according to [RFC 5280], [RFC 6818] are generated. Delta-CRLs are not foreseen.

7.2.2 Extensions of certificate revocation lists and certificate revocation list entries

Certificate revocation lists can contain the following non-critical extensions:

Extension	OID	Parameter
cRLNumber	2.5.29.20	Number of the certificate revocation list
authorityKeyIdentifier	2.5.29.35	160-bit SHA-1 hash of the issuer key
expiredCertsOnCRL	2.5.29.60	**Is currently not used.** Revocation entries remain in the associated revocation lists after the respective certificate validity has expired.

7.3 OCSP Profile

In addition to RFC 6960, the OCSP responder also supports positive information (Certificate is authentic and valid).

The OCSP-Responder provides the following answers:

- „Good"[5], if the responder recognizes the certificate as valid,
- „Unknown"[6], if the responder cannot determine the status of the certificate and
- „Revoked", if the responder recognizes that the certificate has been revoked.

7.3.1 Version number(s)

OCSP v1 according to [RFC 6960] is used.

7.3.2 OCSP extensions

The OCSP responder supports the extension shown below for queries:

Extension	Parameter
retrieveIfAllowed	If set, the certificate is delivered in the response (optional).

[5] OCSP responder will not respond with a "good" status for a certificate that has not been issued. Instead the status "unknown" will be used.

[6] The OCSP responder does not monitor requests identified as "unknown". These are currently discarded.

The OCSP responder uses the extensions shown below in the responses:

Extension	Parameter
archiveCutoff	Period of time for which the OCSP responder makes the status information available after issuance of the certificate.
certHash	In the case of the good or revoked status, the SHA-1 hash value of the certificate is entered.
certInDirSince	Time of publication of the certificate in the central repository service.
requestedCertificate	Contains the certificate if *RetrieveIfAllowed* was set.

All extensions are non-critical. Further non-critical extensions can be contained.

8. Compliance Audit and Other Assessment

Revisions, revision objects and processes are described in more detail in the documentation of D-Trust GmbH as the trust service provider. The role concept documents the qualification and position of the internal auditor.

An independent conformity assessment body recurrently checks TSP's documentation and operational procedures in annual audits over the entire period. Relevant parts of these documents can be inspected against proof of a legitimate interest.

The CP and CPS fulfil the requirements for certificates in accordance with [EN 319 411-1], respectively, including the requirements of [BRG] and [NetSec-CAB]. Regular assessment by a qualified and competent independent party pursuant to [EN 319 411-1], respectively, serves as proof of compatibility.

The TSP does not issue certificates with a policy OID reference to [EN 319 411-1] until after initial and successfully completed auditing by an independent external certification body. Regular follow-up audits are conducted. When procedures and processes are found to be no longer in conformity with the current guidelines of [EN 319 411-1], respectively, the TSP discontinues the issuance of the above-mentioned certificates until conformity with the guidelines is restored and has been audited accordingly.

This audit takes place annually.

Furthermore, internal audits are carried out and documented independently by the TSP and Uniper on a regular basis.

9. Other Business and Legal Matters

The rules in chapter 9 of the CP of D-Trust GmbH are applicable.

Certification Practice Statement der Uniper PKI

Version 2.6

Teil der Bundesdruckerei-Gruppe

COPYRIGHT UND NUTZUNGSLIZENZ

Certification Practice Statement der Uniper PKI

©2022 D-Trust GmbH

This work is licensed under the Creative Commons Attribution-NoDerivatives 4.0 International License.

Anfragen zu einer sonstigen, in der vorgenannten Lizenz nicht enthaltenen Nutzungsart dieses CPS der D-Trust GmbH sind zu richten an:

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

Dokumentenhistorie

Version	Datum	Beschreibung
1.0	01.02.2014	▪ Initialversion – basierend auf D-TRUST Root PKI v. 1.9
1.1	10.10.2016	▪ Umstellung auf EN 319 411-1
1.2	01.10.2017	▪ Anpassung Nutzungslizenz an „Creative Commons Attribution"
2.0	28.03.2018	▪ Anpassung Nutzungslizenz an „Creative Commons Attribution" ▪ Editorische Änderungen
2.1	05.07.2018	▪ Änderung der Domain-Validierungsmethoden in 4.2.1 ▪ Redaktionelle Anpassungen
2.2	30.11.2018	▪ Änderung der Archivierungszeiten in Abschnitt 5.5.1 und 5.5.2 ▪ Dieses CPS entspricht den Anforderungen der Mozilla Policy 2.6.1 ▪ Jährliches Review des gesamten CPS ▪ Redaktionelle Anpassungen
2.3	19.03.2020	▪ Dieses CPS entspricht den Anforderungen der Mozilla Policy 2.7 ▪ Jährliches Review des gesamten CPS ▪ Update nach observation report vom CAB ▪ Editorische Änderungen
2.4	27.04.2020	▪ Aufnahme von Rollover CAs, siehe Abschnitt 1.1.3 ▪ Ergänzungen zur Verifikation der Zertifikatskette in Abschnitt 4.5.2 ▪ Ergänzungen in den Abschnitten 5.3.7 und 5.5.2
2.5	18.08.2021	▪ Jährliches Review des gesamten CPS ▪ Editorische Änderungen in Abschnitt 3.1.4, 7.1.2, 7.2.2, 7.3.2 ▪ Ergänzungen in den Abschnitten 1.1.3, 4.2.1, 4.9.1, 4.9.12, 7.1.1, 8
2.6	18.11.2022	▪ Informative Einführung des Policy Levels NCP ▪ Ergänzungen in den Abschnitten 1.1.3, 1.4.2, 1.6.2, 2.4, 4.9.1, 4.10.1, 4.10.2, 5.5.1, 5.5.2, 6.3.2, 8 ▪ Jährliches Review des gesamten CPS

Teil der Bundesdruckerei-Gruppe

Inhaltsverzeichnis

1. Einleitung ... 6
1.1 Überblick ... 6
1.2 Name und Kennzeichnung des Dokuments ... 9
1.3 PKI-Teilnehmer ... 10
1.4 Verwendung von Zertifikaten ... 10
1.5 Pflege und Aktualisierung des CPS ... 11
1.6 Begriffe und Abkürzungen ... 12
2. Verantwortlichkeit für Verzeichnisse und Veröffentlichungen ... 13
2.1 Verzeichnisse ... 13
2.2 Veröffentlichung von Informationen zu Zertifikaten ... 13
2.3 Häufigkeit von Veröffentlichungen ... 14
2.4 Zugriffskontrollen auf Verzeichnisse ... 14
2.5 Zugang und Nutzung von Diensten ... 14
3. Identifizierung und Authentifizierung (I&A) ... 14
3.1 Namensregeln ... 14
3.2 Initiale Überprüfung der Identität ... 16
3.3 Identifizierung und Authentifizierung von Anträgen auf Schlüsselerneuerung (re-keying) ... 17
3.4 Identifizierung und Authentifizierung von Sperranträgen ... 17
4. Betriebsanforderungen ... 18
4.1 Zertifikatsantrag und Registrierung ... 18
4.2 Verarbeitung des Zertifikatsantrags ... 22
4.3 Ausstellung von Zertifikaten ... 23
4.4 Zertifikatsübergabe ... 24
4.5 Verwendung des Schlüsselpaars und des Zertifikats ... 25
4.6 Zertifikatserneuerung (certificate renewal) ... 25
4.7 Zertifikatserneuerung mit Schlüsselerneuerung ... 25
4.8 Zertifikatsänderung ... 25
4.9 Widerruf und Suspendierung von Zertifikaten ... 26
4.10 Statusabfragedienst für Zertifikate ... 29
4.11 Austritt aus dem Zertifizierungsdienst ... 29
4.12 Schlüsselhinterlegung und –wiederherstellung ... 29
5. Nicht-technische Sicherheitsmaßnahmen ... 31
5.1 Bauliche Sicherheitsmaßnahmen ... 31
5.2 Verfahrensvorschriften ... 31
5.3 Eingesetztes Personal ... 32
5.4 Überwachungsmaßnahmen ... 33
5.5 Archivierung von Aufzeichnungen ... 34
5.6 Schlüsselwechsel beim TSP ... 35
5.7 Kompromittierung und Geschäftsweiterführung beim TSP ... 35
5.8 Schließung des TSP ... 36
6. Technische Sicherheitsmaßnahmen ... 36
6.1 Erzeugung und Installation von Schlüsselpaaren ... 36
6.2 Sicherung des privaten Schlüssels und Anforderungen an kryptographische Module ... 38
6.3 Andere Aspekte des Managements von Schlüsselpaaren ... 40
6.4 Aktivierungsdaten ... 40
6.5 Sicherheitsmaßnahmen in den Rechneranlagen ... 40
6.6 Technische Maßnahmen während des Life Cycles ... 41
6.7 Sicherheitsmaßnahmen für Netze ... 42
6.8 Zeitstempel ... 43
7. Profile von Zertifikaten, Sperrlisten und OCSP ... 43
7.1 Zertifikatsprofile ... 43
7.2 Sperrlistenprofile ... 45
7.3 Profile des Statusabfragedienstes (OCSP) ... 46

8. Auditierungen und andere Prüfungen 47
9. Sonstige finanzielle und rechtliche Regelungen 47

1. Einleitung

1.1 Überblick

Dieses Dokument ist das Certification Practice Statement (CPS) der von der D-Trust GmbH betriebenen Uniper PKI.

Die Uniper PKI wird durch eine SubCA-Struktur unterhalb der „D-TRUST Root CA 3 2013" referenziert.

1.1.1 Vertrauensdiensteanbieter

Diese Regelungen sind in der CP der D-Trust GmbH festgehalten.

1.1.2 Über dieses Dokument

Dieses CPS definiert Abläufe und Vorgehensweisen im Rahmen der Vertrauensdienste während der gesamten Lebensdauer der CA- und Endanwenderzertifikate (EE-Zertifikate). Es werden Mindestmaßnahmen festgelegt, die von allen PKI-Teilnehmern zu erfüllen sind.

Dieses CPS nimmt Bezug auf die CP (Zertifikatsrichtlinie) der D-Trust GmbH mit der OID 1.3.6.1.4.1.4788.2.200.1 und die [EN 319 411-1]. Es beschreibt die Umsetzung der daraus resultierenden Anforderungen für die PKI der Uniper.

Dieses CPS ist Teil des extIDENT-Vertrages zwischen dem TSP und der Uniper und damit rechtsverbindlich, soweit dies im Rahmen der deutschen bzw. europäischen Gesetzgebung zulässig ist.

Die Rechtsverbindlichkeit sowie die Prozesse, die die Punkte a) Bereitstellung der CA, b) Produktion von Zertifikaten zu bereitgestelltem Schlüsselmaterial,

c) Bereitstellung von Sperrlisten sowie d) Bereitstellung des OCSP-Dienstes betreffen, sind abschließend durch die Dokumente CP und CPS definiert. Sie stellen einen nichtqualifizierten Vertrauensdienst im Sinn der eIDAS dar.

Dieses Dokument wird jährlich überprüft. Eine neue Version wird bei festgestelltem Änderungsbedarf erstellt und veröffentlicht.

Die Kenntnis der in dieser CPS beschriebenen Zertifizierungsverfahren und -regeln sowie der rechtlichen Rahmenbedingungen erlaubt es Zertifikatsnutzern Vertrauen in die Komponenten dieser PKI und PKI-Teilnehmern aufzubauen und Entscheidungen zu treffen, inwieweit das durch die PKI gewährte Vertrauens- und Sicherheitsniveau für Anwendungen geeignet ist.

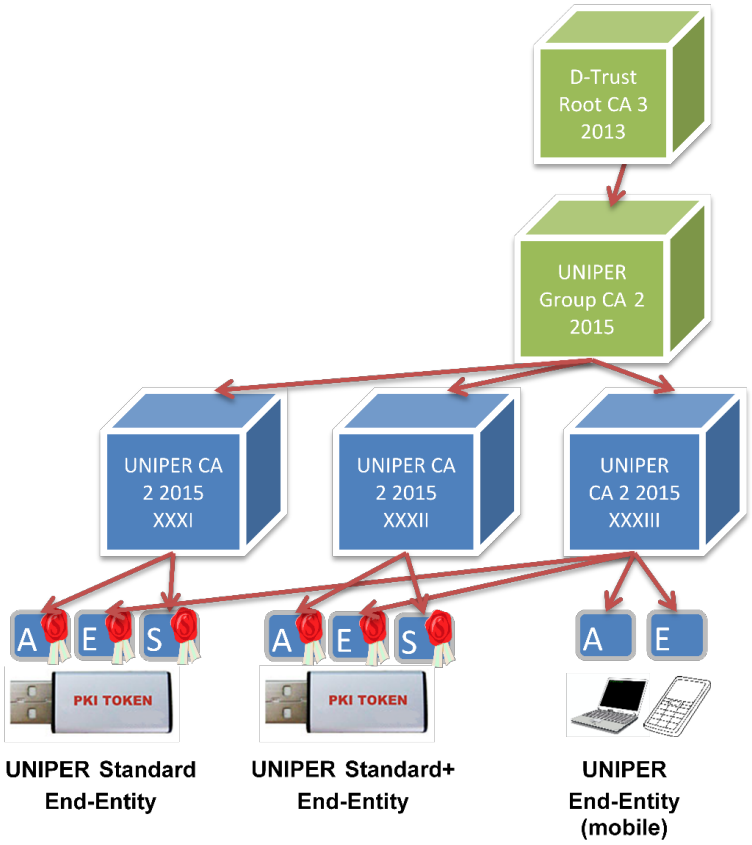
Die Struktur dieses Dokumentes folgt dem Internet-Standard RFC 3647 „Internet X.509 Public Key Infrastructure*: Certificate Policy and Certification Practices Framework"*.

Teil der Bundesdruckerei-Gruppe

1.1.3 Eigenschaften der PKI

Die Hierarchie der Uniper PKI ist mehrstufig. Abbildung 1 zeigt die Konstellation der Uniper PKI.

Die PKI-Hierarchie aus 2015 wird zukünftig durch die neue PKI-Hierarchie 2020 abgelöst. Bis auf Weiteres sind beide parallel in Betrieb und nutzbar.



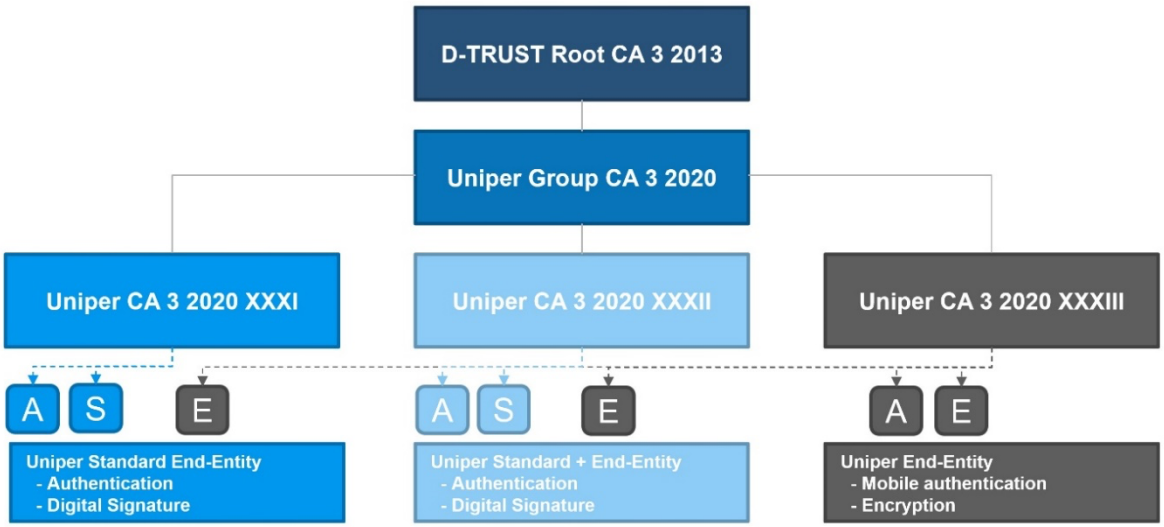


Abbildung 1: Struktur der ausstellenden CAs und Endanwender-Zertifikate

Anforderungen der PKI

Die EE- und CA-Zertifikate unterliegen dem Sicherheitsniveau NCP oder LCP. NCP- bzw. LCP-Zertifikate sind hochwertige, aber nicht qualifizierte Zertifikate, die die Anforderungen von EN 319 411-1 NCP bzw. LCP und [BRG] erfüllen. Der Nachweis der erfolgreichen Prüfungen ist dem „Audit Attestation Letter" zu entnehmen. Die Konformitätsbewertungsstelle (conformity assessment body) TÜV IT stellt diesen unter folgendem Link bereit: https://www.tuvit.de/de/leistungen/zertifizierung/anforderungen-des-cabrowser-forum

Uniper verwendet unter der D-Trust Root CA eine Uniper Group CA und darunter die Uniper Issuing CAs, die die Endanwenderzertifikate ausstellen.

Es werden Authentifizierungs-, Signatur- und Verschlüsselungszertifikate ausgegeben. Diese beinhalten für LCP die OID 1.3.6.1.4.1.4788.2.212.1 und für NCP die OID 1.3.6.1.4.1.4788.2.212.2.

CA-Zertifikate

Die Gesamtübersicht aller RootCAs und SubCAs mit den Zertifizierungsstufen QCP-w, EVCP, OVCP, DVCP, NCP und LCP aus der hervorgeht welches CPS auf die jeweilige CA Anwendung findet, ist im Repository zu finden:

https://www.d-trust.net/files/dokumente/pdf/pki_structure_and_applicable_documents.pdf

Die folgende Tabelle liefert eine Übersicht über alle RootCAs und der dazugehörigen SubCAs, für die dieses CPS Anwendung findet.

D-TRUST Root CA 3 2013 http://www.d-trust.net/cgi-bin/D-TRUST_Root_CA_3_2013.crt SHA256: A1A86D04121EB87F027C66F53303C28E5739F943FC84B38AD6AF009035DD9457
Uniper Group CA 2 2015 http://www.d-trust.net/cgi-bin/Uniper_Group_CA_2_2015.crt SHA256: B4B2810E787B8E6DBB8B0EA9242D8E195AD5BF4201FD98A09AEDAC8B5F23FAFE OID: 1.3.6.1.4.1.4788.2.212.1
Uniper CA 2 2015 XXXI http://www.d-trust.net/cgi-bin/Uniper_CA_2_2015_XXXI.crt SHA256: F471920D5679EE48219F51CBF44F0F22A7305332B869025E26050C5BED762F72 OID: 1.3.6.1.4.1.4788.2.212.1
Uniper CA 2 2015 XXXII http://www.d-trust.net/cgi-bin/Uniper_CA_2_2015_XXXII.crt SHA256: EFA0A2F29EABB43EAD97AD067297656088679C0B2E297C2D898C4F12C9759805 OID: 1.3.6.1.4.1.4788.2.212.1

Teil der Bundesdruckerei-Gruppe

Uniper CA 2 2015 XXXIII http://www.d-trust.net/cgi-bin/Uniper_CA_2_2015_XXXIII.crt SHA256: 79B9D31504B604293570ECCDC8A92553F937FD823380E560793987037C8B181D OID: 1.3.6.1.4.1.4788.2.212.1
Uniper Group CA 3 2020 http://www.d-trust.net/cgi-bin/Uniper_Group_CA_3_2020.crt SHA256: A502172DEAF811DD7FA9BC3329AEA72589F2FAEC9401CB7348819C75F2E705B9 SHA1: F6B7B49CC413C27D69BD7EFC12E4638D1B98BEEC OID: 1.3.6.1.4.1.4788.2.212.1
Uniper CA 3 2020 XXXI http://www.d-trust.net/cgi-bin/Uniper_CA_3_2020_XXXI.crt SHA256: 19D99B7FDD7EC707AC3023D72F50D4AB5199AF1FDD3013A96815CBC99B63BFD6 SHA1: 70997F9622B0341A9E3AE1EFF739714C10DBB643 OID: 1.3.6.1.4.1.4788.2.212.1
Uniper CA 3 2020 XXXII http://www.d-trust.net/cgi-bin/Uniper_CA_3_2020_XXXII.crt SHA256: B576C4A703CB973079F8374EF359E4FD8788584B4E9FB4BC90A7E9F8C3838791 SHA1: 15222F266E381B983A6B83CE705F4AADA8944B7A OID: 1.3.6.1.4.1.4788.2.212.1
Uniper CA 3 2020 XXXIII http://www.d-trust.net/cgi-bin/Uniper_CA_3_2020_XXXIII.crt SHA256: 364ED83755EA3EA8533856EFF72DE38271B54FF44905785EBF735BFFC29B6636 SHA1: 1e2c28405eeb2ef22567d8155e685d656ea0a12f OID: 1.3.6.1.4.1.4788.2.212.1

Sowohl in CA- als auch in EE-Zertifikaten können CPs oder OIDs referenziert werden, die detailliert Anforderungen und Beschränkungen definieren.

1.2 Name und Kennzeichnung des Dokuments

Dokumentname:	Certification Practice Statement der Uniper PKI
Version	2.6

1.3 PKI-Teilnehmer

1.3.1 Zertifizierungsstellen (CA)

Die Zertifizierungsstellen (Certification Authority – CA) stellen Zertifikate sowie Sperrlisten aus. Möglich sind folgende Arten von Zertifikaten:

- Personenzertifikate für natürliche Personen (EE-Zertifikat),
- Gruppenzertifikate für Personengruppen, Funktionen und IT-Prozesse (EE-Zertifikat),
- Zertifizierungsinstanzen (untergeordnete CA-Zertifikate des TSP).

Die Wurzelinstanzen stellen Zertifikate ausschließlich mit der Erweiterung basicConstraints: cA=TRUE (CA-Zertifikat) gemäß [X.509] aus. Untergeordnete CAs stellen EE-Zertifikate und/oder weitere CA-Zertifikate aus. Die Zertifizierungsstelle ist in den ausgestellten Zertifikaten und CRLs namentlich im Feld issuer benannt.

Das Personal für die Zertifikatserzeugung ist frei von kommerziellen, finanziellen und sonstigen Einflussnahmen der Organisation.

1.3.2 Registrierungsstellen (RA)

Die Uniper als RA identifiziert und authentifiziert mit Hilfe definierter Prozesse (siehe Abschnitt 4) Endanwender, erfasst und prüft Anträge für verschiedene Zertifizierungsdienstleistungen.

1.3.3 Zertifikatsnehmer (ZNE)

Zertifikatsnehmer (subscriber) ist die Uniper mit Sitz in Deutschland, welche die EE-Zertifikate beantragt und innehat. Der Zertifikatsnehmer ist nicht mit dem im Zertifikat genannten subject identisch. Die Pflichten des Zertifikatsnehmers unterliegen gesonderten vertraglichen Vereinbarungen.

Andere Zertifikatsnehmer sind in der Uniper PKI nicht vorgesehen.

Die Verantwortung für Schlüssel und Inhalt des Zertifikats trägt der Zertifikatsnehmer. Darüber hinaus ergeben sich nach EN 319 411-1 weitere Pflichten. Spätestens zum Zeitpunkt der Antragstellung wird der Zertifikatsnehmer diese Pflichten dem Endanwender kenntlich machen.

1.3.4 Endanwender (EE)

Endanwender (subject; End-Entity (EE)) verwenden die privaten Endanwenderschlüssel (EE-Schlüssel). Die Identität des Endanwenders ist mit dem Zertifikat und dem zugehörigen Schlüsselpaar verknüpft. Zulässige Endanwender sind natürliche Personen oder Personengruppen, die eine mittels des Identitymanagement der Uniper (EIDM) verwaltete KonzernID besitzen, (z. B. Uniper Mitarbeiter oder Vertragspartner und Dienstleister mit einem aktiven IT-Konto) sowie Funktionen und IT-Prozesse.

1.3.5 Zertifikatsnutzer (ZNU)

Zertifikatsnutzer (englisch relying parties) sind natürliche oder juristische Personen, die die Zertifikate dieser Uniper PKI nutzen (z.B. zur Verifikation signierter Dokumente) und Zugang zu den Diensten des TSP haben.

1.4 Verwendung von Zertifikaten

1.4.1 Erlaubte Verwendungen von Zertifikaten

Diese Regelungen sind in der CP der D-Trust GmbH festgehalten.

1.4.2 Verbotene Verwendungen von Zertifikaten

Andere Verwendungsarten (keyUsage) als die im Zertifikat festgelegten, sind nicht zulässig.

Weiterhin gelten die Regelungen der CP der D-Trust GmbH.

1.4.3 Verwendung von Dienstezertifikaten

Diese Regelungen sind in der CP der D-Trust GmbH festgehalten.

1.5 Pflege und Aktualisierung des CPS

1.5.1 Zuständigkeit für das Dokument

Dieses CPS wird durch die D-Trust GmbH in Kooperation mit der Uniper gepflegt. Der Beauftragte der Geschäftsführung der D-Trust GmbH übernimmt die Abnahme des Dokuments.

Dieses CPS wird regelmäßig jährlich durch den TSP überprüft und ggf. aktualisiert. Eine Änderung wird durch eine neue Versionsnummer dieses Dokumentes kenntlich gemacht.

1.5.2 Ansprechpartner/Kontaktperson/Sekretariat

Eine Kontaktaufnahme kann über folgende Adressen erfolgen:

D-Trust GmbH
Redaktion CP und CPS
Kommandantenstr. 15
10969 Berlin, Germany

Tel: +49 (0)30 259391 0

E-Mail: info@d-trust.net

Die Uniper als Zertifikatsnehmer wird vertreten durch die:

Uniper
Information Security
E.ON-Platz 1

40479 Düsseldorf, Germany

E-Mail: pki@uniper.energy

Fragen zur Gültigkeit konkreter Zertifikate aus der Uniper PKI zu einem bestimmten Zeitpunkt richten Sie bitte per Mail an pki@uniper.energy.

1.6 Begriffe und Abkürzungen

1.6.1 Begriffe und Namen

Diese Regelungen sind in der CP der D-Trust GmbH festgehalten.

Innerhalb der Uniper PKI werden zusätzlich die folgenden Begriffe verwendet:

Authentifizierungszertifikat	Zertifikat, mit dem sich ein Endanwender gegenüber einem IT-System authentifizieren kann
Bestätiger	Mitarbeiter oder Vorgesetzte, die die Identität der Kollegen für die Zertifikatsanträge bestätigen.
Uniper PKI	Von der D-Trust GmbH für Uniper betriebene PKI
Global Service Desk	Globaler Service Desk für die Endanwender der Uniper PKI (GSD).
History-Zertifikate	Abgelaufene Verschlüsselungszertifikate, deren Schlüssel zur späteren Entschlüsselung von Daten gespeichert und von berechtigten Endanwendern wiederhergestellt werden können.
KonzernID	Eindeutige, aber nicht eineindeutige und nicht wiederverwendbare IT Kennung jedes IT Endanwenders im globalen Verzeichnis der Uniper. Nur natürliche Personen erhalten primäre KonzernIDs und können damit Endanwender-Zertifikate erhalten, solange sie aktiv sind. Zweit-KonzernIDs (z.B. für E-Mail Gruppenpostfächer) sind auch immer einer natürlichen Person als Besitzer zuzuordnen, es ist also immer eine verantwortliche natürliche Person eindeutig identifizierbar. Attribute (Eigenschaften) die einer KonzernID zugeordnet werden können, werden über auditierte Prozesse aus dem HR und Vertragsmanagementsystemen angelegt und gepflegt.
PKI-Supervisoren	PKI-Supervisoren bilden die zentrale Schnittstelle zwischen der Uniper und D-Trust GmbH in allen Prozessfragen des extIDENT-Vertrags inkl. CP und CPS für die Uniper PKI. Diese Gruppe beantwortet Fragen zu allen PKI-Prozessen der Uniper PKI und entscheidet alle Uniper internen Anfragen für die Uniper PKI in Übereinstimmung mit dem extIDENT-Vertrag inkl. CP und CPS.
PKI-Token	Für die Uniper PKI werden unter der Bezeichnung PKI-Token verschiedene Formfaktoren von Smartcards eingesetzt, welche alle mit Hilfe eines Smartcardmanagementsystems verwaltet werden. Zu den PKI-Token zählen momentan sowohl ISO-konforme Smartcards, Smartcards in der Form eines USB-Token und einer microSD-Karte als auch TPM 2.0 gestützte Virtuelle Smartcards (VSC). PKI Token, USB-PKI Token, Smartcard, PKI-Medium und VSC werden in Anleitungen und Dokumentationen synonym verwendet.
Q-Umgebung	Qualitätssicherungs-Systeme, die der Erprobung von Konfigurationsänderungen und Upgrades dienen.
Trusted Platform Module	Das Trusted Platform Module (TPM) ist ein Chip nach der TCG-Spezifikation, Family 2, der einen Computer oder ähnliche Geräte um grundlegende Sicherheitsfunktionen erweitert
Virtuelle Smartcard	Virtuelle Smartcards (VSCs) bilden die allgemein zugänglichen Funktionalitäten einer klassischen Smartcard in Software ab. Sensitive Daten sind durch ein TPM 2.0 geschützt.

1.6.2 Abkürzungen

Diese Regelungen sind in der CP der D-Trust GmbH festgehalten.

Innerhalb der Uniper PKI werden zusätzlich die folgenden Begriffe verwendet:

CP	Certificate Policy (Zertifikatsrichtlinie)
EIDM	Uniper Identity Management-System
GSD	Global Service Desk
KID	Uniper KonzernID
LCP	Leightweight Certificate Policy
NCP	Normalized Certificate Policy
SCM	Smartcardmanagement-System
TPM	Trusted Platform Module
TSP	Vertrauensdiensteanbieter (vormals ZDA)
VSC	Virtual Smartcard

1.6.3 Referenzen

Diese Regelungen sind in der CP der D-Trust GmbH festgehalten.

2. Verantwortlichkeit für Verzeichnisse und Veröffentlichungen

2.1 Verzeichnisse

Der TSP veröffentlicht CRLs und CA Zertifikate im LDAP-Verzeichnis unter: ldap://directory.d-trust.net bzw. ldap://cdp-ldap.intranet.uniper.energy. Alternativ per http sind die CRLs unter http://crl.d-trust.net/crl/ zu finden. Die vollständigen zertifikatsspezifischen Links sind den Zertifikaten selbst zu entnehmen. Zusätzlich sind CA Zertifikate, wie im Abschnit 1.1.3 angegeben, veröffentlicht.

Der TSP stellt einen Online-Dienst (OCSP) zur Abfrage des Sperrstatus von Zertifikaten der Uniper PKI zur Verfügung. Der Status der Zertifikate kann dort bis mindestens ein Jahr nach Ablauf der Gültigkeit der Zertifikate abgerufen werden.

Dieses CPS und die Verpflichtungserklärung (Subscribers‘ Obligations) werden dem Antragsteller im PDF-Format auf den Antragsseiten der Uniper während der Antragstellung zur Verfügung gestellt. Weiterhin können diese Dokumente auch über das Internet unter der folgenden Adresse heruntergeladen werden:

https://www.d-trust.net/de/support/repository

Es wird die jeweils aktuelle Version der genannten Dokumente an dieser Stelle veröffentlicht.

2.2 Veröffentlichung von Informationen zu Zertifikaten

Der TSP veröffentlicht folgende Informationen zur Uniper PKI:

- CA-Zertifikate,
- die CP der D-Trust GmbH,
- dieses CPS,

- Sperrlisten (CRLs) und Statusinformationen.

Die Verzeichnisse und Adressen über die diese Informationen bezogen werden können, sind in Kapitel 2.1 beschrieben.

EE-Zertifikate werden in der Uniper PKI grundsätzlich nicht durch den TSP veröffentlicht.

2.3 Häufigkeit von Veröffentlichungen

CA-Zertifikate werden nach ihrer Erstellung veröffentlicht und mindestens 1 Jahr und bis zum Jahresende nach Ablauf der Gültigkeit der CA vorgehalten.

Sperrlisten werden regelmäßig und bis zum Ende der Gültigkeit des ausstellenden CA-Zertifikats ausgestellt. Sperrlisten werden unmittelbar dem Widerruf von Zertifikaten erstellt und veröffentlicht. Auch wenn kein Widerruf von Zertifikaten erfolgt, stellt der TSP sicher, dass mindestens alle 24 Stunden Sperrlisten ausgestellt werden. Die Sperrlisten werden mindestens ein Jahr nach Ablauf der Gültigkeit der CA vorgehalten.

CA-Sperrlisten, die von Root-CAs ausgestellt werden, werden mindestens alle 12 Monate erstellt und veröffentlicht, auch wenn kein Widerruf von Zertifikaten vorgenommen wurde.

Dieses CPS wird – wie unter Abschnitt 2.1 genannt – veröffentlicht und bleibt dort mindestens so lange abrufbar, wie Zertifikate, die auf Basis dieser CP ausgestellt wurden, gültig sind.

2.4 Zugriffskontrollen auf Verzeichnisse

Zertifikate, Sperrlisten und dieses CPS können öffentlich und unentgeltlich 24x7 abgerufen werden. Der Verzeichnisdienst hat eine Verfügbarkeit von mindestens 98,5%. Der TSP stellt sicher, dass im Falle einer Störung die Ausfalldauer (downtime) maximal vier Stunden beträgt.

Es gibt keine Zugriffsbeschränkungen für lesenden Zugriff. Änderungen der Verzeichnis- und Webinhalte werden ausschließlich vom TSP vorgenommen.

Weitere, nicht öffentliche Dokumente, können bei begründetem Interesse auf Nachfrage in den relevanten Teilen ausgegeben werden.

2.5 Zugang und Nutzung von Diensten

Diese Regelungen sind in der CP der D-Trust GmbH festgehalten.

3. Identifizierung und Authentifizierung (I&A)

3.1 Namensregeln

3.1.1 Arten von Namen

CA- und EE-Zertifikate enthalten grundsätzlich Angaben zu Aussteller (issuer) und Zertifikatsnehmer bzw. Endanwender (subject). Diese Namen werden entsprechend dem Standard [X.501] als DistinguishedName vergeben.

Alternative Namen können registriert und in die subjectAltName-Erweiterung der Zertifikate aufgenommen werden.

3.1.2 Notwendigkeit für aussagefähige Namen

Der verwendete DistinguishedName ist eindeutig innerhalb der Uniper PKI. Eine eindeutige Zuordnung des Zertifikats zum Endanwender ist durch die Verwendung der Uniper KonzernID gegeben.

Bei alternativen Namen (subjectAltName gemäß [X.509]) gibt es keine Notwendigkeit für aussagefähige Namen.

Diese Angaben dürfen keine Referenzen auf das Zertifikat selbst enthalten. IP-Adressen sind nicht zugelassen.

3.1.3 Anonymität oder Pseudonyme von Zertifikatsnehmern

Pseudonyme werden ausschließlich für natürliche Personen benutzt.

KonzernIDs, die bei Authentifizierungzertifikaten als Pseudonym im CN verwendet werden, bestehen ausschließlich aus einem lateinischen Buchstaben gefolgt von mindestens vier arabischen Ziffern. Diese KonzernIDs werden nicht gesondert als Pseudonym gekennzeichnet (persönliche und eindeutige KonzernID der Uniper).

3.1.4 Regeln für die Interpretation verschiedener Namensformen

Die Attribute des DistinguishedNames (DN-Bestandteile) von EE-Zertifikaten werden wie folgt interpretiert:

DN-Bestandteil	Interpretation
CN (commonName)	*Gebräuchlicher Name:* Folgende Varianten werden verwendet: - Natürlichen Personen ohne Pseudonym: „(optional)akademischer Titel<Leerzeichen>Vorname<Leerzeichen>Familienname". - Natürliche Personen mit Pseudonym: „Pseudonym", wenn dieses ausschließlich aus einem lateinischen Buchstaben, gefolgt von mindestens vier arabischen Ziffern besteht (Persönliche und eindeutige KonzernID innerhalb der Uniper. - Funktion oder Personengruppe: Teambezeichnung gebildet aus E-Mail-Präfix und „Team Certificate".
serialNumber	*Seriennummer*: Namenszusatz, welcher die Eindeutigkeit des DNs sicherstellt (Persönliche und eindeutige KonzernID innerhalb der Uniper.).
O (organizationName)	Offizielle Bezeichnung der Organisation, der zugehörigen PKI-Struktur (Uniper).
OU (organizationalUnitName)	OU-Felder werden ausschließlich zu technischen Zwecken befüllt.
C (countryName)	Das aufzuführende Land wird gemäß [ISO 3166] notiert und ergibt sich wie folgt: Ist eine Organisation O im Distinguished-Name aufgeführt, so bestimmt der Sitz der Organisation das Land C.

Die Schreibweise von Namen im Zertifikat wird durch die EIDM-Pflegeprozesse bestimmt. Im Zweifelsfall sind die Personen durch den Zertifikatsnehmer eindeutig über die KonzernID identifizierbar.

Es müssen nicht alle oben genannten DN-Bestandteile verwendet werden. Weitere können ergänzt werden.

Ergänzende DN-Bestandteile müssen [RFC 5280], [RFC 6818] und [EN 319 412] entsprechen.

3.1.5 Eindeutigkeit von Namen

Der TSP stellt sicher, dass ein in EE-Zertifikaten verwendeter Name (DistinguishedName) des Zertifikatsnehmers bzw. des Endanwenders (Feld subject) innerhalb der Uniper PKI und über den Lebenszyklus des Zertifikats hinaus stets eindeutig ist und stets dem gleichen Zertifikatsnehmer bzw. Endanwender zugeordnet ist. Die Eindeutigkeit wird mittels der KonzernID erzielt. Dadurch ist die eindeutige Identifizierung[1] des Zertifikatsnehmers anhand des im EE-Zertifikat verwendeten Namens (subject) gewährleistet. Einem Endanwender können unter Umständen mehrere KonzernIDs zugewiesen sein.

Im Rahmen der Uniper PKI wird die Eindeutigkeit von Benutzerzertifikaten durch Angabe der KonzernID im Zertifikatssubject dauerhaft (auch über Namensänderungen z.B. durch Heirat etc. hinweg) erreicht.

Der TSP stellt die Eindeutigkeit von DistinguishedNames in CA-Zertifikaten sicher.

3.1.6 Anerkennung, Authentifizierung und die Rolle von Markennamen

Der Zertifikatsnehmer haftet für die Einhaltung geistiger Eigentumsrechte in den Antrags- und Zertifikatsdaten (siehe Kapitel 9 der CP der D-Trust GmbH Abschnitt 9.5).

3.2 Initiale Überprüfung der Identität

3.2.1 Nachweis für den Besitz des privaten Schlüssels

Schlüsselpaare werden im Verantwortungsbereich des Zertifikatsnehmers produziert. Der Besitz des privaten Schlüssels muss entweder technisch nachgewiesen werden oder vom Zertifikatsnehmer nachvollziehbar bestätigt werden.

Siehe weiterhin Abschnitt 6.1.3.

3.2.2 Identifizierung und Authentifizierung von Organisationen

Zertifikate für juristische Personen werden nicht ausgestellt.

Organisationen, die im Zertifikat genannt werden, sind Tochter- und Partnerunternehmen der Uniper bzw. Unternehmen, an denen die Uniper eine Beteiligung hält. Uniper übernimmt als RA die Authentifizierung der Organisationen, welche im Zertifikat genannt werden.

Im DN-Feld „O" ist somit für die CAs der Uniper PKI ausschließlich der Organisationseintrag „Uniper" zulässig. Die Einträge und die entsprechende Organisation werden durch den TSP automatisiert überprüft.

Da für das DN-Feld „C" der Sitz der Organisation (Uniper) maßgeblich ist, ist für diesen Eintrag ausschließlich der Wert „DE" zulässig. Der Eintrag wird durch den TSP automatisiert überprüft.

---

[1] Unter Identifizierung sind hier die Benennung des Zertifikatsnehmers und dessen zum Zeitpunkt der Erstantragstellung (nicht Folgeantrag) aktuellen Daten zu verstehen. Nicht gemeint ist das Eruieren aktueller Daten oder das Auffinden des Zertifikatsnehmers zu einem späteren Zeitpunkt.

Teil der Bundesdruckerei-Gruppe

3.2.3 Identifizierung und Authentifizierung natürlicher Personen

Natürliche Personen müssen sich eindeutig authentisieren und ggf. ihre Berechtigung zur Antragstellung durch die Organisation nachweisen.

Die Identifizierung und Authentifizierung natürlicher Personen findet im Kontrollbereich des Zertifikatsnehmers als RA statt und wird durch einen technischen Dienstleister unterstützt. (siehe auch 4.2.1)

Bei der Identifizierung nach dem Standardprozess benennt der Endanwender zwei Bestätiger der RA über ihre E-Mailadresse, die bereits im Besitz eines gültigen und zulässigen EE-Zertifikats sein müssen. Zulässig sind hier allein EE-Zertifikate aus der Uniper PKI der D-Trust GmbH.

Ist der Antragsteller selbst bereits mit einem gültigen Authentifizierungs- und Signaturzertifikat aus der Uniper PKI der D-Trust GmbH authentifiziert, ersetzt dies einen der beiden Bestätiger der RA, da die Überprüfung der Identität bereits einmal vorgenommen wurde.

Liegen nach zwei erfolgreichen Bestätigungen der RA die Voraussetzungen für die Ausstellung eines Zertifikats vor, wird der Zertifikatsrequest vollautomatisch an den TSP übertragen. Nach dem Eintreffen der Zertifikate bekommt der Endanwender eine E-Mailbenachrichtigung mit einer URL, über die er die Zertifikate herunterladen und auf der Smartcard installieren kann.

3.2.4 Ungeprüfte Angaben zum Zertifikatsnehmer

Die Angaben des Zertifikatsnehmers werden entsprechend den Abschnitten 3.2.2, 3.2.3 und 4.2.1 geprüft bzw. nicht geprüft. Bei alternativen Namen werden generell nur die E-Mail-Adressen bzw. deren Domainbestandteile geprüft. Andere Zertifikatsinhalte wie z.B. LDAP-Verzeichnisse etc. sowie eventuelle Zertifikats-Extensions (AdditionalInformation, monetaryLimit, etc.) werden nicht auf Korrektheit geprüft.

3.2.5 Prüfung der Berechtigung zur Antragstellung

Es gelten die Regelungen aus Abschnitt 3.2.3.

Zertifikatsanträge werden durch die Uniper über eine abgestimmte Online-Schnittstelle übergeben.

Nach erfolgreicher Identifizierung gegenüber der Online-Schnittstelle erfolgt eine technische Signatur der Antragsdaten durch den Kommunikationsprozess. Die Anträge werden somit über einen verschlüsselten Kanal und zusätzlich elektronisch signiert übertragen.

Zusätzlich sind nur freigegebene Artikelnummern, korrespondierend mit den Produkten des TSP, durch die Schnittstelle verfügbar.

Somit wird sichergestellt, dass ausschließlich der beabsichtigte Zertifikatsnehmer die beantragten Zertifikate erhalten kann.

3.2.6 Kriterien für die Interoperabilität

Siehe Kapitel 1 der CP der D-Trust GmbH Abschnitt 1.5.3.

3.3 Identifizierung und Authentifizierung von Anträgen auf Schlüsselerneuerung (re-keying)

Schlüsselerneuerung wird nicht angeboten.

3.4 Identifizierung und Authentifizierung von Sperranträgen

Der TSP prüft vor der Sperrung eines EE-Zertifikates die Berechtigung des Sperrantragstellers zur Antragstellung.

Die Sperrberechtigung wird wie folgt geprüft:

Teil der Bundesdruckerei-Gruppe

Bei einem Sperrantrag, der in einer signierten E-Mail eingeht, muss der Sperrantragsteller entweder der Zertifikatsnehmer selbst sein oder als sperrberechtigter Dritter benannt worden sein, dessen in der Sperr-E-Mail verwendetes Signaturzertifikat dem TSP vorliegen muss.

Bei einer Sperrung über die Online-Schnittstelle wird die Übertragung einerseits durch ein SSL Zertifikat abgesichert und der Sperrauftrag an sich mit einer technischen Signatur versehen. Weiterhin wird mit dem Sperrantrag das Sperrpasswort an den TSP übertragen.

Sperranträge über die Online-Schnittstelle können auch für Dritte innerhalb der Uniper PKI gestellt werden. Hierzu ist es notwendig, dass der Sperrende im Auftrag mit seinem gültigen Authentifizierungszertifikat aus der SubCA XXXI oder SubCA XXXII am Smartcardmanagementsystem angemeldet und somit authentifiziert ist.

Andere Verfahren zur Authentifizierung von Sperranträgen können mit dem Zertifikatsnehmer vereinbart werden.

Sperrverfahren werden in Abschnitt 0 definiert.

4. Betriebsanforderungen

4.1 Zertifikatsantrag und Registrierung

4.1.1 Berechtigung zur Antragstellung

Anträge dürfen von bestimmten Endanwendern der Uniper ausgelöst werden, die durch das Unternehmen die Berechtigung erhalten haben (KonzernID) und sich gegenüber der RA authentisieren können.

Beim Vertragsbeginn eines Mitarbeiters oder Dienstleisters in der Uniper wird von der zuständigen Personal- bzw. Vertragsabteilung ein Datensatz in einem definierten und vertrauenswürdigen Quellsystem angelegt. Daraus wird einmal pro Tag eine Identität im zentralen zugriffsgeschützten Enterprise Directory der Uniper erzeugt. Dieses Directory ist wesentlicher Teil des Identity Management Systems (EIDM). Änderungen an diesen Programmen/Prozessen unterliegen einem strikten Changemanagement und sind mit dem TSP abgestimmt.

Unautorisierte Änderungen an EIDM-Daten sind nicht vorgesehen, sondern dürfen nur auftragsbasiert (schriftlich, nachvollziehbar für Revisionssicherheit) durch einen eingeschränkten Personenkreis in führenden Datenquellen durchgeführt werden und werden dort individuell geloggt.

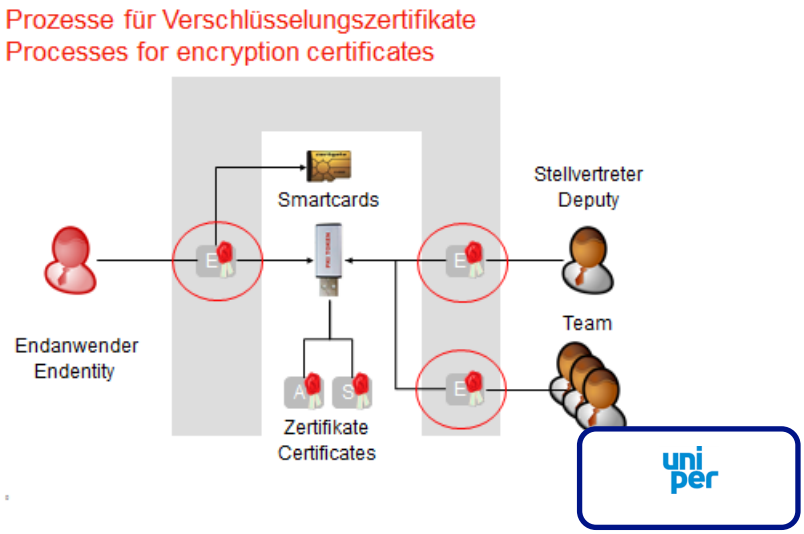
Sämtliche EE-Schlüssel (Signatur, Verschlüsselung und Authentifizierung) werden im Kontrollbereich des Zertifikatsnehmers generiert.

Private EE-Schlüssel, die keine Signatur- und Authentifikationsschlüssel[2] sind, können gemäß den Vorgaben des CPS für eine spätere Wiederverwendung (key escrow, Wiederverwendung in einem neuen Token) von einer vom TSP autorisierten Stelle sicher hinterlegt werden.

Auf die hinterlegten Verschlüsselungs-Schlüssel eines Endanwenders aus der SubCA XXXIII kann zunächst nur der authentisierte Endanwender selbst zugreifen. Die Verschlüsselungsschlüssel kann der Endanwender als Historyzertifikate auf sein PKI-Medium übertragen, um mit den zugehörigen privaten Schlüsseln auf früher verschlüsselte Daten zugreifen zu können.

[2] Ein Signaturschlüssel ist ein Schlüssel, zu dem ein Zertifikat erstellt wird, dass den öffentlichen Schlüssel des Schlüsselpaars enthält und die Schlüsselverwendung entweder "digital signature" oder "contentCommitment" bzw. "nonRepudiation" beinhaltet.

Teil der Bundesdruckerei-Gruppe



Über einen Workflow kann ein Endanwender sogenannte Stellvertreter festlegen, die damit Zugriff auf seine privaten Entschlüsselungsschlüssel erhalten und sich diese zusätzlich auf ihre PKI-Medien übertragen können, um im Rahmen von Stellvertretungs- oder Assistenzaufgaben auf verschlüsselte E-Mails im Postfach des Benutzers zugreifen zu können.

Teamzertifikate unterscheiden sich darin, dass der Teamleiter über eine Funktions-KID als Besitzer des Zertifikats agieren und seine primäre KID und die KIDs der Teammitglieder als Stellvertreter einrichten kann.

Damit bekommen auch Stellvertreter die Möglichkeit, sich die privaten Schlüssel dieser Zertifikate zu beschaffen, wenn diese Zertifikate ausschließlich zur Entschlüsselung genutzt werden können.

Auf Grund des Schutzbedarfs dieser Applikation wird das SCM nur von einer kleinen Personengruppe im Vieraugenprinzip administriert und Änderungen durch PKI-Supervisoren der Uniper explizit freigegeben.

CA-Zertifikate der Uniper PKI werden ausschließlich an Uniper vergeben.

Zur Übermittlung der Registrierungsdaten ist die Kommunikation zwischen der RA und dem TSP über eine SSL-/TLS-Verbindung verschlüsselt und authentisiert.

Der TSP ist berechtigt, Anträge abzulehnen (siehe Abschnitt 4.2.2).

4.1.2 Registrierungsprozess und Zuständigkeiten

Dem Zertifikatsnehmer und dem Endanwender stehen bereits zu Beginn des Registrierungsprozesses dieses CPS und die Verpflichtungserklärung (Subscriber Agreement) sowie weitere Dokumente zur Verfügung, um ihm zu ermöglichen, sich über die Bedingungen für die Verwendung des zu beantragenden Zertifikats zu informieren.
In der Uniper PKI sind zwei Registrierungsprozesse vorgesehen (Standard und Standard Plus), die sich auf vorregistrierte Daten aus dem Identitymanagementsystem und dessen auditierten Datenpflegeprozesse abstützen.
Der Schwerpunkt des Standardprozesses ist die Verlagerung der Benutzeridentifikation in das kollegiale Umfeld, wobei durch persönliche Kenntnis zwischen Endanwender und Bestätiger die Effektivität und Effizienz der sicheren Identifizierung gesteigert werden soll.
Authentifizierung der Bestätiger und Bestätigungen mit fortgeschrittenen Signaturen stellt eine Abschreckung vor Missbrauch dar. Diese Eigenschaften und die genaue Prüfaufgabe werden den

Bestätigern vor der Bestätigung deutlich gemacht. Es ist dabei zu beachten, dass der Bestätiger angeben muss, mit welchem Identifizierungsmerkmal (Personalausweis, Reisepass oder persönliche Kollegenbeziehung) der Endanwender identifiziert wurde.
Ein konsequent durchgesetztes Mehraugenprinzip bei der Überprüfung erschwert es dem Einzelnen, unbemerkt in Besitz fremder Schlüsselpaare zu gelangen.

4.1.3 Standard und Standard Plus Prozess

Der Standardprozess ist der übliche Prozess zur Identifizierung von Endanwendern.
Der Standard Plus Prozess ist für bestimmte Standorte im Uniper Konzern vorgesehen, die erweiterte Prozessanforderungen stellen. Hier dürfen nur Bestätiger aus einer explizit benannten Gruppe von Bestätigern die Bestätigungsaufgabe ausführen. Beide Prozesse geben gleichartige Zertifikate aus: Authentifizierungs- und Signaturzertifikate, wobei Zertifikate nach dem Standard Plus Prozess von einer gesonderten SubCA ausgegeben werden.
Verschlüsselungszertifikate werden ebenfalls von einer gesonderten SubCA ausgestellt, die weiterhin auch eigene Authentifikationszertifikate ausstellen kann, deren Einsatz außerhalb von zertifizierten PKI-Medien zulässig ist, um sie auf mobilen Geräten oder in Anwendungen zur Verschlüsselung oder Authentifikation nutzen zu können, die nicht auf Smartcards o.ä. zugreifen können.
Der Prozess wird softwareseitig von einer Workflow-Engine gesteuert und ist nach den speziellen Anforderungen von Uniper modelliert, die den sicheren Ablauf des Prozesses und den Datenfluss zwischen Endanwender, Bestätiger und dem TSP ermöglicht.

4.1.4 Standardprozess

Er ist nur für natürliche Personen nutzbar, die ein aktives, durch eine primäre KonzernID eindeutig bezeichnetes IT Konto der Uniper besitzen. Der Standardprozess besteht aus folgenden Schritten:

1. Ein Endanwender ruft per Standard-Browser die Antrags-URL im Intranet der Uniper auf. Er meldet sich mit KonzernID und dem zugehörigen Passwort (sofern er noch kein Token besitzt) oder bereits existierendem Zertifikat an.

2. Nach Aufforderung legt der Endanwender ein für Uniper vorinitialisiertes PKI-Token in seinen Rechner ein. Bei Verwendung einer VSC erübrigt sich dieser Schritt. Dann startet er die endanwenderspezifische Karteninitialisierung.

   Der Antragsteller bestätigt, dass er die Benutzungsbedingungen sowie die Verpflichtungserklärung gelesen hat und akzeptiert diese.

   Dabei werden für den Endanwender Schlüssel für Authentifizierung und Signatur auf der Karte bzw. im TPM generiert. Dem SCM werden nur die öffentlichen Schlüssel übertragen. Das Schlüsselpaar für das Verschlüsselungszertifikat wird zentral durch das SCM generiert. Mit dem Setzen einer individuellen PIN nimmt der Endanwender das PKI-Medium in Besitz. Nun werden vom Uniper Smartcardmanagementsystem (SCM) die entsprechenden Zertifikats-Requests erstellt, welche von einem oder zwei Bestätigern freigegeben werden müssen.

3. Der Endanwender muss zwei Bestätiger aus dem EIDM vorschlagen, die bereits im Besitz eines gültigen EE-Zertifikats sein müssen.

4. Ist der Antragsteller mit einem zulässigen Zertifikat bereits authentifiziert, ist nur noch ein Bestätiger notwendig, da die Überprüfung der Identität bereits einmal vorgenommen wurde.

5. Als Abschluss dieses Prozessschrittes bekommt der Endanwender eine E-Mail, mit der er jederzeit auf den Status dieses Prozesses zugreifen und ihn ggf. auch abbrechen und neu starten kann.

6. Der Erstbestätiger bekommt eine E-Mail mit einem Link auf den Bestätigungsprozessschritt im Standardprozess. Dieser kann nur authentifiziert mit einem zulässigen Authentifikations- und Signatur-Zertifikat durchgeführt werden. Dabei wird die Zustimmung mit dem Token des Bestätigers signiert und mit dem Request in der Datenbank abgelegt.
7. Der Erstbestätiger beantwortet die angezeigten Fragen, ob er den Endanwender persönlich kennt, wie er den Antragsteller identifiziert hat, ob die angezeigten Antragsdaten stimmig sind und signiert die Bestätigung ggf. mit seinem Signaturzertifikat.
8. Der Zweitbestätiger führt die gleichen Schritte wie der Erstbestätiger aus.

   Der Zweitbestätiger kann entfallen, wenn sich der Endanwender bereits mit einem gültigen Zertifikat der Uniper PKI angemeldet hat.
9. Liegen nach erfolgreicher Bestätigung die Voraussetzungen für die Erstellung von EE-Zertifikaten vor, werden die Zertifikatsanträge an die CA übermittelt. Nach dem Eintreffen der Zertifikate bekommt der Endanwender eine E-Mailbenachrichtigung mit einer URL, über die er die Zertifikate herunterladen und auf der Smartcard installieren kann.
10. Für den Installationsprozess der Zertifikate auf den Token muss sich der Endanwender erneut per vorhandenem Token oder Username/Passwort authentifizieren. Er benötigt neben seinem Token auch die von ihm vergebene PIN.

    Der Endanwender bestätigt erneut, dass er die Benutzungsbedingungen und Verpflichtungserklärung gelesen hat und akzeptiert diese.

    Nach der Installation quittiert der Endanwender den Erhalt der Zertifikate, indem die neu ausgestellte Karte die Empfangsbestätigung signiert. Ausnahme: ist kein Signaturzertifikat vorhanden, bestätigt der Endanwender manuell, die bestellten Zertifikate erhalten zu haben.

4.1.5 Standard Plus Prozess

Der Standard Plus Registrierungsprozess wird für die Erfüllung besonderer Registrierungsanforderungen in bestimmten organisatorischen Einheiten benötigt. Damit ist es für entsprechend konfigurierte Anwendungen und Portale möglich, nach diesem geringfügig stärkeren Registrierungsprozess ausgegebene Zertifikate zu erkennen und verifizieren.
Im Gegensatz zum Standard Registrierungsprozess wird die erste Bestätigung vor Ort bei einem lokalen und vom System vorgegebenen Bestätiger (Mitarbeiter mit festgelegter Rolle) durchgeführt.

4.1.6 Variante des Prozesses für alle Uniper Endanwender für mobile Endgeräte

Für die Anwender der vorher beschriebenen Prozesse gibt es Authentifikations- und Verschlüsselungszertifikate aus der SubCA XXXIII auch als Softwarezertifikat. Diese sind verschlüsselt in eine Applikation zu übertragen. Die Anwendung muss dem Endanwender die ausschließliche Kontrolle über die Nutzung des privaten Schlüssels ermöglichen.

Endanwender können ihr aktuelles Verschlüsselungszertifikat, ein neu zu generierendes Verschlüsselungszertifikat sowie ein ebensolches Authentifikationszertifikat im bekannten Selbstserviceportal als Softwarezertifikat bestellen.

Diese Bestellung wird analog zum Standard Prozess geprüft und genehmigt. Die Zertifikatserzeugung und -übergabe findet nachfolgend in einem mehrstufigen Prozess statt:

1. Ein Endanwender ruft per Standard Browser die Antrags-URL im Intranet der Uniper auf. Er meldet sich mit KonzernID und Windows-Passwort (sofern er noch kein Token besitzt) oder mit seinem bereits existierenden Authentifikations-Zertifikat der Standard (SubCA XXXI) oder Standard+ SubCA (CA XXXII) an. Zertifikate der SubCA XXXIII sind hierfür ausgeschlossen.

Teil der Bundesdruckerei-Gruppe

2. Der Antragsteller bestätigt, dass er die Nutzungsbedingungen und Verpflichtungserklärung gelesen hat und diese akzeptiert.
3. Danach wird für den Endanwender zentral im Uniper Smartcardmanagementsystem (SCM) ggf. ein Schlüsselpaar für ein Authentifizierungszertifikat oder für ein neues Verschlüsselungszertifikat generiert. Ein Schlüsselpaar für das aktuelle Verschlüsselungszertifikat wurde entweder zuvor bereits zentral durch das SCM generiert und gespeichert, welches wiederverwendet oder bei Fehlen eines gültigen Verschlüsselungsschlüssels während des Prozessablaufs erstellt wird. Vom SCM werden für alle neuen Schlüsselpaare die entsprechenden Zertifikats-Requests erstellt, welche je nach vorigem Bestätigungslevel von einem oder zwei Bestätigern freigegeben werden müssen, die selbst gültige Zertifikate haben (Authentifizierung für Zugang SCM, Verschlüsselung für Zugang zu P12-Datei bei Ansatz mit zwei Bestätigern).
4. Der Endanwender bestimmt, ob er sich die zur Installation notwendige zufällig generierte PIN per verschlüsselter E-Mail schicken lassen möchte oder alternativ zwei Benutzer auswählt, die per verschlüsselter E-Mail jeweils eine Hälfte der 12-stelligen PIN zugeschickt bekommen, falls er selbst kein gültiges Verschlüsselungszertifikat besitzt.
5. Liegen nach erfolgreicher Bestätigung die Voraussetzungen für die Erstellung von EE-Zertifikaten vor, werden die Zertifikatsanträge an die CA übermittelt. Nach dem Eintreffen der Zertifikate bekommt der Endanwender eine E-Mailbenachrichtigung mit einer URL, über die er die Zertifikate herunterladen und in der von Uniper freigegebenen Anwendung installieren kann. Das Laden der Zertifikate kann auch durch die freigegebene Anwendung initiiert werden.
6. Sollte der Anwender bereits Verschlüsselungsschlüssel auf einem PKI-Medium vorliegen haben, so wird er während des Ausstellungsprozesses des von der Software gespeicherten Verschlüsselungsschlüssels darauf hingewiesen, dass er diese Medien selbständig und eigenverantwortlich synchronisieren muss.
7. Bei Abruf der Zertifikate über einen Arbeitsplatzrechner bestätigt der Endanwender erneut, dass er die Nutzungsbedingungen und Verpflichtungserklärung gelesen hat und akzeptiert diese.
8. Für den Installationsprozess der Zertifikate muss der Endanwender die vollständige PIN aus Schritt 4 eingeben.

Danach startet der eigentliche Installationsprozess auf Basis einer P12-Datei. Nach der erfolgreichen Installation quittiert der Endanwender den Erhalt der Zertifikate, indem er oder die zur Installation verwendete Anwendung automatisch den Empfang im Selbstserviceportal bestätigt.

4.2 Verarbeitung des Zertifikatsantrags

4.2.1 Durchführung der Identifizierung und Authentifizierung

Der beschriebene Identifizierungs- und Registrierungsprozess muss vollständig durchlaufen und alle nötigen Nachweise dabei erbracht werden.

Der TSP definiert die folgenden Prüfverfahren:

HR-DB
Der TSP schließt vertragliche Vereinbarungen mit einer Organisation (Zertifikatsnehmer) und vereinbart, dass nur valide Daten übermittelt werden, die die Vorgaben dieser CPS erfüllen. Die Organisation übermittelt dem TSP über einen sicheren Kommunikationskanal Requests, die auf Basis des Identity Managementsystems EIDM mit revisionssicheren Pflegeprozessen entstanden sind. Die anwendbaren Datenschutzanforderungen sind seitens der Organisation zu beachten. Der TSP vertraut auf die Richtigkeit und Eindeutigkeit der übermittelten Daten. Spätestens bei Übergabe der

Token setzt der Zertifikatsnehmer den Endanwender über dessen Pflichten aus der Verpflichtungserklärung in Kenntnis.

Bei der Uniper PKI findet die Identifizierung der Endanwender und Prüfung der Antragsdaten gemäß in dieser CPS definierten Prozessen statt: Standard und Standard Plus (siehe Abschnitt 4.1) inklusive einer Variante für Zertifikate für mobile Endgeräte gemäß den Verfahren des Standard-Prozesses. Der SCM prüft gegen eine schwarze Liste, ob der Antragsteller von der Nutzung von Softwarezertifikaten ausgeschlossen wurde und zeigt ggf. die entsprechende Fehlermeldung.

Domain
Die Kontrolle über eine Domain wird wie folgt nachgewiesen:

gemäß [BRG] 3.2.2.4.2 Email, Fax, SMS, or Postal Mail to Domain Contact[3], [BRG] 3.2.2.4.4 Constructed Email to Domain Contact, [BRG] 3.2.2.4.7 DNS Change, [BRG] 3.2.2.4.13 Email to DNS CAA Contact, [BRG] 3.2.2.4.14 Email to DNS TXT Contact und [BRG] 3.2.2.4.18 Agreed-Upon Change to Website v2.

IP-Adressen
IP-Adressen werden nicht validiert und sind nicht zugelassen.

Die Ergebnisse der Abfrage werden hinterlegt.

Erst wenn alle Antragsvoraussetzungen signiert vorliegen, wird der Zertifikatsantrag freigegeben und an D-Trust übermittelt.

Identifizierung und Authentifizierung finden gemäß den Abschnitten 3.2.2 und 3.2.3 statt.

4.2.2 Annahme oder Ablehnung von Zertifikatsanträgen

Enthält der Zertifikatsrequest über die vereinbarte Online-Schnittstelle technische oder inhaltliche Fehler wird der Antrag abgelehnt. Die entsprechende Online-Schnittstelle übermittelt hierbei eine Begründung, warum der Antrag abgelehnt wurde. Der Antrag ist entsprechend zu korrigieren und erneut zu stellen.

Weitere Gründe für die Antragsablehnung können sein:

- Verdacht auf die Verletzung der Namensrechte Dritter,
- Nichteinhalten von Fristen für den Nachweis der Daten,
- Umstände, die den Verdacht begründen, dass eine Zertifikatsausstellung den Betreiber der CA in Misskredit bringt.

Erst nachdem der TSP den Zertifikatsantrag positiv überprüft hat und das beantragte Zertifikat übergeben wurde (vgl. Abschnitt 0), gilt der Antrag als vorbehaltlos angenommen.

4.2.3 Fristen für die Bearbeitung von Zertifikatsanträgen

Keine Vorgaben.

4.3 Ausstellung von Zertifikaten

4.3.1 Vorgehen des TSP bei der Ausstellung von Zertifikaten

Im Hochsicherheitsbereich des Trustcenters werden die entsprechenden Zertifikate ausgefertigt.

[3] Bei dieser Methode wird ausschließlich eine Validierung über die E-Mail Adresse durchgeführt.

Teil der Bundesdruckerei-Gruppe

Die vollständige Antragsdokumentation wird entweder vom TSP gemäß Abschnitt 5.5 abgelegt oder der TSP schließt vertragliche Vereinbarungen mit Partnern, dass die Antragsunterlagen und/oder Requests sicher und vollständig bis zum Ablauf der Frist nach Abschnitt 5.5.2 zu verwahren sind.

Dabei wird sichergestellt, dass bei der Zertifikatserstellung die korrekte Zeit verwendet wird.

4.3.2 Benachrichtigung des Zertifikatsnehmers über die Ausstellung des Zertifikats.

Es erfolgt keine gesonderte Benachrichtigung des Zertifikatsnehmers nach der Fertigstellung des Zertifikats durch den TSP.

Endanwender werden durch den Zertifikatsnehmer informiert.

4.4 Zertifikatsübergabe

4.4.1 Verhalten bei der Zertifikatsübergabe

Wird ein Zertifikat zu einem beim Endanwender vorhandenen Schlüsselpaar ausgestellt, wird das Zertifikat entweder zum Download bereitgestellt (z. B. im Verzeichnisdienst veröffentlicht) oder elektronisch versendet.

Für die automatische Zertifikatsbeantragung sind Informationen erforderlich, die an das System übertragen werden müssen:

- Angaben zum Antragsteller,
- Antragsdaten und deren Format,
- gewünschtes Zertifikatsprodukt,
- Sperrpasswort.

Entdeckt der Zertifikatsnehmer Fehler in seinen Zertifikaten oder bei der Funktion der Schlüssel und Token, so hat er dies dem TSP unverzüglich mitzuteilen. Die Zertifikate werden widerrufen.

Fehlerhafte Angaben in den Zertifikaten gelten nur insoweit als vertraglicher Mangel im Sinne des Vertrages, wenn der TSP nach dieser CPS eine Überprüfung der von dem Fehler betroffenen Angaben vorzunehmen hatte.

Eine Abnahme durch den Kunden erfolgt nicht.

4.4.2 Veröffentlichung des Zertifikats durch den TSP

EE-Zertifikate werden grundsätzlich nicht vom TSP veröffentlicht. Die Veröffentlichung übernimmt der Zertifikatsnehmer.

Der Status ist nach der Produktion des Zertifikats über CRLs und OCSP

abrufbar.

4.4.3 Benachrichtigung anderer PKI-Teilnehmer über die Ausgabe des Zertifikats

Zertifikate der Uniper PKI und deren Sperrinformationen werden in einem Smartcardmanagementsystem vollautomatisch gespeichert. Auf der Basis dieser Daten können Sperrungen nach definierten Prozessen veranlasst und beauftragt werden. Siehe hierzu auch Abschnitt 4.9.3.

4.5 Verwendung des Schlüsselpaars und des Zertifikats

4.5.1 Verwendung des privaten Schlüssels und des Zertifikats durch den Zertifikatsnehmer

Endanwender dürfen ihre privaten Schlüssel ausschließlich für die Anwendungen nutzen, die in Übereinstimmung mit den im Zertifikat angegebenen Nutzungsarten stehen.

Schlüsselmaterial für Signatur- und Authentifizierungszertifikate aus den SubCAs XXXI und XXXII wird ausschließlich auf zertifizierten PKI-Token oder TPMs, die den ISO/IEC 11889 Standard (TCG Spezifikation Family 2) erfüllen, im Bereich des Zertifikatsnehmers erzeugt.

Schlüsselmaterial für Authentifizierungs- und Verschlüsselungszertifikate aus der SubCA XXXIII wird in einer gesicherten Serverumgebung durch den Zertifikatsnehmer erzeugt.

Für Zertifikatsnehmer gelten die Bestimmungen aus Abschnitt 1.4.

4.5.2 Verwendung des öffentlichen Schlüssels und des Zertifikats durch Zertifikatsnutzer

Die Zertifikate der Uniper PKI können von allen Zertifikatsnutzern verwendet werden. **Es kann jedoch nur dann darauf vertraut werden**, wenn

- die Zertifikate entsprechend den dort vermerkten Nutzungsarten (Schlüsselverwendung, erweiterte Schlüsselverwendung, ggf. einschränkende Zertifikatserweiterungen) benutzt werden,
- die Verifikation der Zertifikatskette bis zu einem vertrauenswürdigen Root-Zertifikat erfolgreich durchgeführt werden kann[4], wenn keine andere Methode anwendbar ist, um den Vertauensstatus der PKI zu überprüfen (z.B. EU Trusted List gemäß eIDAS (Regulation (EU) No 910/2014 und dazugehörige Durchführungsrechtsakte) oder Rootstores von Softwareherstellern),
- der Status der Zertifikate über CRL oder den Statusabfragedienst (OCSP) positiv geprüft wurde und
- alle weiteren in Vereinbarungen oder an anderer Stelle angegebenen Vorsichtsmaßnahmen getroffen wurden, eventuelle Einschränkungen im Zertifikat und jegliche anwendungsspezifischen Vorkehrungen seitens des Zertifikatsnutzers berücksichtigt und als kompatibel erkannt wurden.

4.6 Zertifikatserneuerung (certificate renewal)

Zertifikatserneuerung wird nicht angeboten.

4.7 Zertifikatserneuerung mit Schlüsselerneuerung

Schlüsselerneuerung wird nicht angeboten.

4.8 Zertifikatsänderung

Zertifikatsänderungen werden nicht angeboten.

[4] Die Verifikation der Zertifikatskette soll entsprechend dem PKIX-Modell (auch Schalenmodell genannt) gemäß [RFC 5280], [RFC 6818] erfolgen. Eine formale Beschreibung des Algorithmus zur Verifikation der Zertifikatskette ist zu finden in [ETSI EN 319 412].

4.9 Widerruf und Suspendierung von Zertifikaten

4.9.1 Bedingungen für einen Widerruf von Zertifikaten

Die Verfahren des TSP erfüllen die Bedingungen aus EN 319 411-1 und [GL-BRO].

Der Widerruf eines Zertifikats wird bei folgenden Ereignissen durchgeführt:

- auf Verlangen des Zertifikatsnehmers bzw. betroffenen Dritten (bspw. im Zertifikat genannte Organisation),
- wenn das Zertifikat auf Grund falscher Angaben ausgestellt wurde,
- wenn die ursprüngliche Zertifikatsanforderung nicht autorisiert wurde und die Autorisierung nicht rückwirkend erteilt wird,
- wenn der TSP Kenntnis davon erlangt, dass der private CA- bzw. EE-Schlüssel einer nicht autorisierten Person oder Organisation kommuniziert wurde, die dem Zertifikatsnehmer nicht zugehörig ist,
- wenn der private Schlüssel des Zertifikatsnehmers zugehörig zum öffentlichen Schlüssel im Zertifikat kompromittiert wurde,
- wenn dem TSP nachgewiesen werden kann, dass auf der Grundlage des öffentlichen Schlüssels im Zertifikat der zugehörige private Schlüssel errechnet werden kann,
- wenn die TSP feststellt, dass das Zertifikat nicht gemäß der anwendbaren CP und CPS ausgestellt wurde oder dass die SubCA die Anforderungen der anwendbaren CP und CPS nicht erfüllt,
- wenn die TSP feststellt, dass der Antragsteller gegen die Verpflichtungserklärung bzw. gegen die anwendbaren CP oder CPS verstößt,
- wenn zur Antragsstellung gültige Zertifikatsinhalte während des Gültigkeitszeitraums ungültig werden, z.B. durch eine Namensänderung oder mit dem Verlust der Organisationszugehörigkeit,
- wenn der TSP seine Tätigkeit beendet und diese nicht von einem anderen TSP fortgeführt wird.

Unabhängig davon ist der TSP berechtigt Zertifikate zu widerrufen, wenn:

- die D-Trust als Trust Service Provider (TSP) gesetzlich zum Widerruf verpflichtet ist,
- der private Schlüssel der ausstellenden oder einer übergeordneten CA kompromittiert wurde,
- das Zertifikat der ausstellenden oder einer übergeordneten CA widerrufen wurde,
- Schwächen im verwendeten Kryptoalgorithmus bekannt werden, die ernste Risiken für die erlaubten Anwendungen während der Zertifikatslaufzeit darstellen,
- die eingesetzte Hard- und Software Sicherheitsmängel aufweist, die ernste Risiken für die erlaubten Anwendungen während der Zertifikatslaufzeit darstellen,
- die eindeutige Zuordnung des Schlüsselpaars zum Zertifikatsnehmer nicht mehr gegeben ist,
- ein begründeter Verdacht des Missbrauchs eines Zertifikats besteht,

Teil der Bundesdruckerei-Gruppe

- eine Empfangsbestätigung, dass das Zertifikat formal und inhaltlich korrekt über eine vertraglich vereinbarte Onlineschnittstelle übertragen wurde, nicht innerhalb der vereinbarten Zeitspanne an den TSP übersendet wurde,
- das Vertragsverhältnis gekündigt oder in sonstiger Weise beendet wurde,
- die CA an einen anderen TSP übergeben wird, ohne dass die dazugehörigen Sperrinformationen der ausgestellten EE-Zertifikate mit übergeben werden.

NCP, LCP

Für Zertifikate, die in der Lage sind, E-Mails zu signieren oder zu verschlüsseln und eine E-Mail-Adresse enthalten gelten ebenfalls die Sperrgründe gemäß Mozilla Root Store Policy 2.7, Kapitel 6.2. Je nach Sperrgrund muss das Zertifikat innerhalb von 24 Stunden gesperrt werden bzw. kann die Sperrung innerhalb von fünf Tagen erfolgen.

Der Widerruf enthält eine Angabe des Zeitpunkts des Widerrufs und wird nicht rückwirkend erstellt. Weiterhin kann ein Widerruf nicht rückgängig gemacht werden.

Das Personal des Sperrmanagements ist frei von kommerziellen, finanziellen oder sonstigen Einflussnahmen der Organisation.

Sperrberechtigte müssen sich gemäß Abschnitt 3.4 authentifizieren.

4.9.2 Berechtigung zur Sperrung bzw. zum Widerruf

- Der TSP ist sperrberechtigt.
- Der Zertifikatsnehmer hat stets die Berechtigung seine Zertifikate zu widerrufen.

Im Übrigen gilt jede Person als sperrberechtigt gegenüber dem TSP, soweit sie das zutreffende Sperrpasswort mitteilt.

4.9.3 Verfahren für einen Sperrantrag

Der Endanwender kann seine Zertifikate sowohl über den Global Service Desk des Zertifikatsnehmers innerhalb der Infrastruktur der Uniper sperren, als auch direkt in seinem persönlichen Bereich des Smartcardmanagementsystems über die Online-Schnittstelle.

Der Widerruf über den Global Service Desk wird von diesem an den TSP übersendet.

E-Mail-Adresse: pki@uniper.energy

Andere Sperrverfahren können vereinbart werden.

Ein Antrag zum Widerruf eines Zertifikats über eine Online-Schnittstelle soll folgende Angaben enthalten:

- den Aussteller des Zertifikates,
- das vereinbarte Sperrpasswort,
- Zertifikatsseriennummer (wenn möglich als Dezimalzahl), damit das Zertifikat eindeutig identifiziert werden kann.

Über den persönlichen Bereich des Smartcardmanagementsystems können auch Zertifikate für Dritte innerhalb der Uniper PKI gesperrt werden. Hierzu ist es notwendig, dass sich der Sperrende im Auftrag mit seinem persönlichen Token am Smartcardmanagementsystem anmeldet und authentifiziert.

Sperrungen finden im Verantwortungsbereich des TSP statt und können ausschließlich durch hierfür berechtigte Mitarbeiter autorisiert durchgeführt werden.

Die Sperrung eines Zertifikats ist endgültig. Ein Zertifikat kann nach einer Sperrung nicht wieder aktiviert werden.

Alle Sperrinformationen werden entsprechend protokolliert. Der Endanwender wird über die Sperrung seiner Zertifikate informiert, z.B. per E-Mail.

4.9.4 Fristen für einen Sperrantrag

Der Endanwender oder Zertifikatsnehmer muss in eigener Verantwortung dafür sorgen, dass er oder eine für ihn sperrberechtigte Person unverzüglich die Sperrung beantragt, sobald Gründe zur Sperrung bekannt werden. Dabei ist dasjenige Verfahren zu nutzen, welches die schnellste Bearbeitung des Sperrantrags erwarten lässt.

4.9.5 Zeitspanne für die Bearbeitung des Sperrantrags durch den TSP

Sperranträge können 24x7 über die Online-Schnittstelle eingereicht werden. Der Widerruf erfolgt gemäß Abschnitt 4.9 [BRG] innerhalb von 24 Stunden nach erfolgreicher Autorisierung des Sperrantragstellers.

4.9.6 Verfügbare Methoden zum Prüfen von Sperrinformationen

Aktuelle Sperrinformationen sind in Sperrlisten vorgehalten, die über das Protokoll LDAP oder über den in Abschnitt 2.1 angegebenen Link abgerufen werden können. Zusätzlich steht ein OCSP-Dienst zur Verfügung. Die Erreichbarkeit dieser Dienste wird in Form von URLs in den Zertifikaten angegeben. Ferner können Sperrinformationen über das EIDM bezogen werden. Delta-CRLs werden nicht angeboten.

Integrität und Authentizität der Sperrinformationen wird durch eine Signatur gewährleistet.

Status- und Sperrinformationen (OCSP und CRL) sind konsistent.

Statusänderungen im OCSP sind unverzüglich nach einem Widerruf zur Abfrage verfügbar. Statusänderungen in einer CRL beinhalten dieselben Sperrinformationen. Die Distribution einer neuen CRL erfolgt jedoch zeitversetzt zum Widerruf.

4.9.7 Häufigkeit der Veröffentlichung von Sperrlisten

Siehe Abschnitt 2.3.

4.9.8 Maximale Latenzzeit für Sperrlisten

Sperrlisten werden unmittelbar nach ihrer Erzeugung veröffentlicht.

4.9.9 Online-Verfügbarkeit von Sperrinformationen

Zur Onlineprüfung steht ein OCSP-Dienst zur Verfügung.

Der OCSP Responder liefert nur dann ein "good", wenn das Zertifikat in der Datenbank gespeichert und gültig ist.

Die Erreichbarkeit dieses Dienstes wird in Form eines URL in den Zertifikaten angegeben.

4.9.10 Notwendigkeit zur Online-Prüfung von Sperrinformationen

Es gibt keine Pflicht zur Online-Prüfung von Sperrinformationen, es gilt jedoch Abschnitt 4.5.2.

4.9.11 Andere Formen zur Anzeige von Sperrinformationen

Keine Vorgaben.

4.9.12 Spezielle Anforderungen bei Kompromittierung des privaten Schlüssels

D-Trust sperrt ein Zertifikat aufgrund der Kompromittierung des privaten Schlüssels, wenn über eine der folgenden Methoden die Schlüsselkompromittierung demonstriert werden kann:

- Übermittlung des kompromittierten privaten Schlüssels oder
- Signierung eines CSRs mit dem Common Name Eintrag „Proof of Key Compromise for D-TRUST" durch den kompromittierten privaten Schlüssel

Zur Meldung der Schlüsselkompromittierung bietet D-Trust einen Certificate Problem Report an. Dieser wird in der CP Kapitel 1.5.2 beschrieben und ist zu nutzen.

Sollte eine Schlüsselkompromittierung erfolgreich nachgewiesen werden, sperrt D-Trust das Zertifikat gemäß den Vorgaben aus Abschnitt 4.9. des [BRG].

4.9.13 Bedingungen für eine Suspendierung

Suspendierungen von Zertifikaten werden nicht angeboten.

4.10 Statusabfragedienst für Zertifikate

4.10.1 Funktionsweise des Statusabfragedienstes

Der Statusabfragedienst ist über das Protokoll OCSP verfügbar. Die Erreichbarkeit des Dienstes wird als URL in den Zertifikaten angegeben.

Die Systemzeit des OCSP-Responder wird über täglich mit dem deutschen DCF77-Zeitsignal und verlässlichen Zeitservern (NTP) im Internet synchronisiert.

Die Formate und Protokolle der Dienste sind in den Abschnitten 7.2 und 7.3 beschrieben.

4.10.2 Verfügbarkeit des Statusabfragedienstes

Der Statusabfragedienst steht 24 Stunden an 7 Tagen der Woche bereit und hat eine Verfügbarkeit von 99,95%. Der TSP stellt sicher, dass im Falle einer Störung die Ausfalldauer (downtime) maximal vier Stunden beträgt.

4.10.3 Optionale Leistungen

Der Zertifikatsnutzer kann sich über die folgende E-Mail-Adresse über den Status eines erhaltenen Zertifikats informieren: pki@uniper.energy

4.11 Austritt aus dem Zertifizierungsdienst

Die Gültigkeit eines Zertifikats endet mit dem im Zertifikat vermerkten Ablaufdatum. Der Sperrauftrag zu einem Zertifikat durch Zertifikatsnehmer oder Sperrberechtigte Dritte löst die Sperrung durch den TSP aus. Die vertraglichen Hauptleistungspflichten des TSP sind damit vollständig erfüllt.

4.12 Schlüsselhinterlegung und –wiederherstellung

Das Hinterlegen privater EE-Schlüssel wird vom Zertifikatsnehmer umgesetzt. Signatur- und Authentifizierungsschlüssel von EE-Zertifikaten aus den SubCAs XXXI und XXXII und Authentifizierungsschlüssel aus der SubCA XXXIII werden nicht hinterlegt.

Bei der Uniper PKI werden die EE-Schlüssel von Verschlüsselungszertifikaten aus der SubCA XXXIII vom Zertifikatsnehmer gesondert gehalten.

Die Speicherung der Entschlüsselungsschlüssel erfolgt durch ein System, das im Auftrag von Uniper durch einen Dienstleister betrieben wird. Diesbezügliche Vorgaben der EN 319 411-1 müssen eingehalten werden. Die Einhaltung der Vorgaben wird regelmäßig revisioniert.

Vergleiche hierzu auch Abschnitt 0.

4.12.1 Bedingungen und Verfahren für die Hinterlegung und Wiederherstellung privater Schlüssel

Der TSP bietet die Hinterlegung privater Schlüssel nicht an.

Der Zertifikatsnehmer (Uniper) hinterlegt Schlüssel für Verschlüsselungszertifikate aus der SubCA XXXIII im eigenen Verantwortungsbereich nach folgenden Regelungen:

Das SCM bietet einen abgegrenzten und speziell gesicherten Datenbankbereich, in dem die MasterKeys der Karten und persönliche Schlüssel symmetrisch verschlüsselt hinterlegt werden. Alle privaten Entschlüsselungsschlüssel aus der SubCA XXXIII sind mit Hilfe eines HSM Moduls erzeugt und liegen verschlüsselt in einer Datenbank vor.

Auf die hinterlegten Entschlüsselungsschlüssel darf nur der authentisierte Endanwender zugreifen und sich diese auf sein mobiles Endgerät (vgl. Kapitel 4.1.3) oder als Historyzertifikate auf seinen Token übertragen. Damit ist der Zugriff auf aktuell und ehemals gültige Zertifikate und zugehörige private Schlüssel zum Entschlüsseln älterer Daten gewährleistet.

KonzernIDs von Mitarbeitern, die das Unternehmen verlassen, werden über einen internen Prozess deaktiviert und archiviert. Das führt aber nicht dazu, dass die privaten Schlüssel und Zertifikate des Mitarbeiters aus dem SCM Repository entfernt werden.

Durch Anmeldung am zentralen Portal des Smartcardmanagementsystems kann ein Endanwender sogenannte Stellvertreter konfigurieren, die damit Zugriff auf seine Entschlüsselungsschlüssel erhalten und sich diese zusätzlich auf ihre Token übertragen können, um im Rahmen von Stellvertretungs- oder Assistenzaufgaben auf alle verschlüsselten E-Mails des Endanwenders zugreifen zu können.

Diese Bestätigung der Stellvertreter erfolgt nur authentifiziert über das Portal des Smartcardmanagementsystems, bei dem Vertretungsrequests bestätigt sowie die aktuell eingerichteten Vertreter angezeigt und bei Bedarf wieder deaktiviert werden können.

Vor Nutzung neuer Vertreterschlüssel müssen sich die Vertreter ebenfalls am Portal des Smartcardmanagementsystems anmelden und erhalten für sie verfügbare Vertreterschlüssel zum Hinzufügen oder Löschen vom eigenen PKI-Medium bzw. mobilen Endgerät angeboten.

Beim Hinzufügen und Löschen einer Vertreterberechtigung sowie Installation und Deinstallation eines Vertreterschlüssels auf dem PKI-Medium werden Vertreter und Vertretene automatisch per E-Mail informiert, so dass Vertretene die Möglichkeit haben nicht mehr gewünschte Vertreter zum Entfernen der Schlüssel aufzufordern. Dies passiert gleichermaßen, wenn der Vertretende sein PKI-Medium oder mobiles Endgerät wechselt und somit die Entschlüsselungsschlüssel des Vertretenen neu installiert werden müssen.

Für Vertreter ist die Verwendung der privaten Schlüssel nach dem Entzug der Vertretung noch solange möglich, bis das PKI-Token des Vertreters erneut am Portal des Smartcardmanagementsystems konfiguriert wurde.

Auf Basis geltenden Rechts kann der zuständige Leiter Information Security unter Wahrung des Mehraugenprinzips Vertreter ausnahmsweise für die Nutzung von Verschlüsselungszertifikaten anderer Endanwender berechtigen, um Zugriff auf verschlüsselte E-Mails zu ermöglichen. Er ist für die Einbeziehung der relevanten Kontrollorgane, die nachvollziehbare Dokumentation und ggf. anschließende Benachrichtigung der betroffenen Endanwender verantwortlich.

Bei Teamzertifikaten kann der Teamleiter über eine Funktions-KID als Besitzer des Zertifikats agieren und seine primäre KID und die KIDs der Teammitglieder als Stellvertreter einrichten. Damit erhalten auch diese die Möglichkeit, sich die privaten Schlüssel dieser Zertifikate zu beschaffen.

Teil der Bundesdruckerei-Gruppe

4.12.2 Bedingungen und Verfahren für die Hinterlegung und Wiederherstellung von Sitzungsschlüsseln

Sitzungsschlüssel werden nicht angeboten.

5. Nicht-technische Sicherheitsmaßnahmen

Die Beschreibungen der Kapitel 5.4 bis 5.6 beziehen sich speziell auf die Sub-CAs der Uniper PKI, die bei der D-Trust GmbH im Rahmen von [EN 319 411-1] betrieben werden.

Die D-Trust betreibt ein Informationssicherheitsmanagementsystem (ISMS) gemäß ISO/IEC 27001. Der Betrieb des TSP unterliegt diesem ISMS. Eine Information Security Policy regelt die verbindlichen Vorgaben für den Betrieb. Diese wurde von der Geschäftsführung der D-Trust freigegeben und an alle Mitarbeiter des TSP kommuniziert. Es erfolgt ein jährliches als auch anlassbezogenes Review und Update der Security Policy.

Führen prozess- bzw. betriebsbedingte Änderungen zu einem Update der Security Policy, sind die daraus resultierenden Änderungen für den TSP Betrieb von der Geschäftsführung zu genehmigen. Die aktualisierte und genehmigte Security Policy ist zeitnah durch die Führungskräfte an alle davon betroffenen Mitarbeiter zu kommunizieren bzw. bei Bedarf muss die Führungskraft Schulungsmaßnahmen einleiten.

5.1 Bauliche Sicherheitsmaßnahmen

Für die baulichen Sicherheitsmaßnahmen liegt eine detaillierte Dokumentation vor, die bei begründetem Interesse in den relevanten Teilen eingesehen werden kann. Das Sicherheitskonzept wurde durch eine anerkannte Konformitätsbewertungsstelle geprüft. Die Konformitätsbewertung wird gemäß [EN 319 411-1] und [EN 319 411-2] regelmäßig wiederholt.

Ferner wurde dem Sicherheitsbereich des Trustcenters der D-Trust GmbH durch den TÜV-IT die Anwendung und Umsetzung der „Infrastrukturmaßnahmen für hohen Schutzbedarf – Level 3" beurkundet (gemäß Prüfkriterienkatalog für „Trusted Site Infrastructure"). Mit diesem TÜV-IT-Zertifikat „Trusted Site Infrastructure" werden alle Infrastruktur-relevanten Aspekte untersucht und bewertet. Diese Prüfung wird alle zwei Jahre wiederholt. Das genannte Zertifikat bestätigt der D-Trust GmbH diesen hohen Sicherheitsstandard der nicht-technischen Sicherheitsmaßnahmen.

Die SubCAs der Uniper PKI werden vom TSP unter den gleichen Bedingungen betrieben wie die CAs der D-Trust GmbH.

5.2 Verfahrensvorschriften

5.2.1 Rollenkonzept

Teil der Dokumentation ist ein Rollenkonzept, in dem Mitarbeiter einer oder mehreren Rollen durch das Management des TSP zugeordnet werden und entsprechende Berechtigungen erhalten. Die Berechtigungen der einzelnen Rollen beschränken sich auf diejenigen, die sie zur Erfüllung ihrer Aufgaben benötigen. Die Zuordnung der Berechtigungen wird regelmäßig revisioniert und umgehend nach Entfall des Bedarfs entzogen.

Rollen mit Sicherheitsverantwortung für den Betrieb des TSP, genannt „Trusted Roles", (mit unter anderem den Aufgaben des Sicherheitsbeauftragten, System Administrator, System Operator, System Auditor, Registration Officer, Revocation Officer und Validation Specialist) werden in den Berechtigungskonzepten der D-Trust festgelegt. Diese Rollen dürfen nur von fachkundigen und zuverlässigen Mitarbeitern übernommen werden.

Für die jeweiligen Rollen werden Tätigkeitsbeschreibungen erstellt. Diese legen die Aufgaben, das geforderte Mindestmaß an Qualifikation und Erfahrungen für die jeweilige Rolle fest. Ein Mitarbeiter, kann eine bzw. mehrere Rollen ausfüllen, vorausgesetzt die Rollen schließen sich nicht gegenseitig aus und der Mitarbeiter kann nachweisen, dass er die nötige Qualifikation und Erfahrung für diese Rolle erworben hat.

Mitarbeiter werden regelmäßig geschult, um ihre Rollen und damit verbundenen Verantwortlichkeiten zu erfüllen und sie werden bezüglich der Einhaltung geltender Sicherheitsvorgaben sensibilisiert. Sie können sich im Rahmen von Schulungen die Qualifikation für weitere Rollen erwerben.

Die Anforderungen an die Rollen werden in Tätigkeitsbeschreibungen dokumentiert und können von den Mitarbeitern jederzeit eingesehen werden.

Bevor Mitarbeiter ihre zugewiesenen Rollen ausüben, müssen sie diesen zustimmen. Im Falle von sich ausschließenden Rollen, kann eine Person nur eine dieser Rollen übernehmen (Vier-Augen-Prinzip).

Eine Risikobewertung findet regelmäßig statt.

Mitarbeiter, die im Bereich der Zertifizierungs- und Sperrdienste tätig sind, agieren unabhängig und sind frei von kommerziellen und finanziellen Zwängen, die ihre Entscheidungen und Handlungen beeinflussen könnten. Die organisatorische Struktur des TSP berücksichtigt und unterstützt die Mitarbeiter in der Unabhängigkeit ihrer Entscheidungen.

5.2.2 Mehraugenprinzip

Besonders sicherheitskritische Vorgänge müssen mindestens im Vier-Augen-Prinzip durchgeführt werden. Dies wird durch technische und organisatorische Maßnahmen wie beispielsweise Zutrittsberechtigungen und Abfrage von Wissen durchgesetzt.

Sicherheitskritische Systeme zur Zertifikatsausstellung sind zusätzlich durch eine Multi-Faktorauthentisierung geschützt.

5.2.3 Identifikation und Authentifizierung für einzelne Rollen

Das Rollenkonzept wird durch technische und organisatorische Maßnahmen, wie beispielsweise Zutrittsberechtigungen und Abfrage von Wissen, durchgesetzt. Die durchführende Person muss sich, bevor sie Zugriff auf sicherheitskritische Anwendungen bzw. CA-Systeme erhält, erfolgreich authentifizieren. Über Event-Logs kann die durchführende Person nachträglich einer Aktion zugeordnet werden; sie ist rechenschaftspflichtig.

Relevante Ereignisse der CA-Umgebung, die sich auf das Zertifikatsmanagement sowie CA-Schlüssel und CA-Zertifikate beziehen müssen freigegeben und nachvollziehbar protokolliert werden.

5.2.4 Rollenausschlüsse

Das Rollenkonzept sieht diverse Rollenausschlüsse vor, um Interessenskonflikte zu verhindern, das Mehraugenprinzip zu erzwingen und schädliches Handeln vorzubeugen.

5.3 Eingesetztes Personal

Der TSP erfüllt die Anforderungen an das Personal aus EN 319 411-1. Personal in sicherheitsrelevanten Rollen des TSPs wird offiziell ernannt. Die Dokumentation erfolgt im Rahmen des internen Personallebenszyklus.

5.3.1 Anforderungen an Qualifikation, Erfahrung und Zuverlässigkeit

Der TSP gewährleistet, dass die im Bereich des Vertrauensdienstes tätigen Personen über die für diese Tätigkeit notwendigen Kenntnisse, Erfahrungen und Fertigkeiten verfügen.

Die Identität, Zuverlässigkeit und Fachkunde des Personals wird vor Aufnahme der Tätigkeit überprüft. Regelmäßige und anlassbezogene Schulungen gewährleisten die Kompetenz in den Tätigkeitsbereichen sowie die allgemeine Informationssicherheit. Schulungen und Leistungsnachweise werden dokumentiert.

Insbesondere Führungskräfte werden nach speziellen Kriterien ausgewählt. Sie müssen nachweisen, dass sie in Bezug auf den bereitgestellten Vertrauensdienst über Kenntnisse der Sicherheitsverfahren

für Mitarbeiter mit Sicherheitsverantwortung und über ausreichende Erfahrung in Bezug auf Informationssicherheit und Risikobewertung verfügen. Nachweise können in Form von Zertifikaten und Lebensläufen erbracht werden. Kann die erforderliche Qualifikation nicht ausreichend nachgewiesen werden, muss diese durch eine entsprechende Schulungsmaßnahme erworben werden bevor der Mitarbeiter im TSP Betrieb Managementfunktionen übernehmen darf.

5.3.2 Sicherheitsprüfungen

Personen, die in sicherheitsrelevanten Bereichen des TSP tätig sind, müssen unter anderem regelmäßig polizeiliche Führungszeugnisse vorlegen.

Übergreifend betreibt der TSP ein nach ISO 27001 zertifiziertes ISMS. Hierdurch werden den Mitarbeitern entsprechend sicherheitsrelevante Vorgaben bzw. Verhaltensregeln zugänglich gemacht.

5.3.3 Schulungen

Der TSP schult Personen, die im Zertifizierungsdienst tätig sind.

5.3.4 Häufigkeit von Schulungen und Belehrungen

Der TSP schult Personen, die im Zertifizierungsdienst tätig sind zu Beginn ihres Einsatzes, jährlich und bei Bedarf.

5.3.5 Häufigkeit und Folge von Job-Rotation

Rollenwechsel werden dokumentiert. Die entsprechenden Mitarbeiter werden geschult.

5.3.6 Maßnahmen bei unerlaubten Handlungen

Der TSP schließt unzuverlässige Mitarbeiter von den Tätigkeiten im Zertifizierungsdienst aus.

Verstöße von Mitarbeitern gegen die Richtlinien oder die Prozesse des TSP-Betriebs werden analysiert und bewertet. Kann das Vertrauensverhältnis nicht sichergestellt werden, werden diese Mitarbeiter von sicherheitsrelevanten Tätigkeiten ausgeschlossen.

5.3.7 Maßnahmen für externe Mitarbeiter

Externe Mitarbeiter, welche im Bereich der Vertrauensdienste aktiv sind, erfüllen die Anforderungen aus 5.3und unterliegen den Sanktionen nach 0.

5.3.8 Ausgehändigte Dokumentation

Umfangreiche Verfahrensanweisungen definieren für alle Produktionsschritte die zuständigen Mitarbeiterrollen und -rechte sowie entsprechende manuelle und maschinelle Prüfungen. Durch die sicherheitstechnische Infrastruktur der D-Trust GmbH ist gewährleistet, dass von diesen definierten Verfahren im Produktionsbetrieb nicht abgewichen werden kann.

5.4 Überwachungsmaßnahmen

5.4.1 Überwachung des Zutritts

Der TSP betreibt umfangreiche Überwachungsmaßnahmen (beispielsweise durch Videoüberwachung) zur Absicherung der Vertrauensdienste und deren zugrunde liegenden IT-Systemen und Dokumenten.

Die Überwachungsmaßnahmen werden durch organisatorische Regelungen ergänzt. Beispielsweise sieht die Besucherregelung unter anderem vor, dass Besucher mindestens 24 Stunden vor dem Besuch namentlich angemeldet sein müssen. Im Bereich des Trustcenters müssen Besucher stets in Begleitung eines Mitarbeiters des TSP sein.

5.4.2 Überwachung von organisatorischen Maßnahmen

Ein weiterer Bestandteil ist die Überwachung von organisatorischen Maßnahmen.

Hierzu gehört eine regelmäßige Risikoanalyse, die die Bedrohung für den Betrieb des TSP umfassend analysiert sowie Anforderungen und Gegenmaßnahmen definiert. Ferner ist eine Restrisikoanalyse enthalten, in der die Vertretbarkeit des Restrisikos aufgezeigt und ggf. akzeptiert wird.

Im Rahmen interner und externer Audits werden regelmäßig Tests durchgeführt, um die Risiken durch externe und interne Angriffe zu reduzieren.

Weiterhin werden relevante Assets angemessen erfasst, sowie entsprechende Änderungen dieser Assets überprüft bzw. wenn anwendbar durch das vom Management beauftragte Personal des TSP freigegeben.

5.5 Archivierung von Aufzeichnungen

5.5.1 Arten von archivierten Aufzeichnungen

Es wird zwischen Aufzeichnungen in elektronischer Form und papierbasierten unterschieden.

Die vollständigen Antragsdaten, die Zertifikate, die Sperrdokumentation, die elektronischen Dateien und Protokolle zum Zertifikatslebenszyklus werden durch die Uniper elektronisch archiviert. Die Uniper kann die Aufzeichnungspflicht an ein Partnerunternehmen innerhalb der EU übertragen.

Die Aufzeichnungen werden für mindestens sieben Jahre über das Ablaufdatum der an dem Tag ausgestellten Zertifikate hinaus aufbewahrt.

Der TSP stellt sicher, dass von ihm archivierte Daten während ihrer Speicherfristen nicht unberechtigt manipuliert werden können.

Weiterhin werden sicherheitsrelevante Ereignisse entsprechend aufgezeichnet. Die Systemzeit wird täglich mit dem deutschen DCF77-Zeitsignal und verlässlichen Zeitservern (NTP) im Internet synchronisiert.

5.5.2 Aufbewahrungsfristen für archivierte Daten

Dokumente zur Antragstellung und Prüfung sowie die Daten zum Zertifikatslebenszyklus sowie die Zertifikate selbst werden mindestens sieben Jahre und bis zum Jahresende aufbewahrt. Die Frist beginnt nach Ablauf der Gültigkeit des Zertifikates, das zuletzt auf der Basis dieser Dokumente ausgestellt wurde.

Event-Logs der IT-Systeme werden mindestens 6 Monate gespeichert. Die Speicherdauer von personenbezogenen Videoaufzeichnungen und Aufzeichnungen der administrativen Tätigkeiten beträgt 90 Tage.

Für das Archivierungssystem wird die Systemzeit täglich mit dem deutschen DCF77-Zeitsignal und verlässlichen Zeitservern (NTP) im Internet synchronisiert.

5.5.3 Archivierung (intern / extern)

Die Archivierung erfolgt intern beim TSP, sowie extern in gleichwertig gesicherten Räumen.

5.5.4 Sicherung des Archivs

Die externen Archive befinden sich in gesicherten Räumen der Uniper oder deren Partnerunternehmen und unterliegen einem entsprechenden Rollen- und Zutrittskontrollkonzept.

5.5.5 Datensicherung des Archivs

Vertraulichkeit und Integrität der Daten werden gewahrt. Die Dokumentation erfolgt unverzüglich, so dass sie nachträglich nicht unbemerkt verändert werden kann. Die europäischen und deutschen Datenschutzanforderungen werden eingehalten.

5.5.6 Verfahren zur Beschaffung und Verifikation von Archivinformationen

Das Verfahren zur Beschaffung und Verifikation von Archivinformationen unterliegt dem Rollenkonzept des TSP bzw. des Outsourcingpartners der Uniper.

5.6 Schlüsselwechsel beim TSP

Eine angemessene Zeit vor Ablauf einer (Sub)CA werden neue CA-Schlüssel generiert, neue CA-Instanzen aufgesetzt und veröffentlicht.

5.7 Kompromittierung und Geschäftsweiterführung beim TSP

Der TSP hat Maßnahmen ergriffen, dass eine Unterbrechung des Betriebs durch Verlust, Beschädigung oder Kompromittierung verhindert wird.

5.7.1 Behandlung von Vorfällen und Kompromittierungen

Der TSP verfügt über ein Notfallkonzept sowie einen Wiederanlaufplan, die den beteiligten Rollen bekannt sind und von ihnen im Bedarfsfall umgesetzt werden. Die Verantwortlichkeiten sind klar verteilt und bekannt.

Sollte eine System Recovery erforderlich sein, sind die Verantwortlichkeiten und entsprechenden „Trusted Roles" im Berechtigungskonzept der D-Trust deklariert und den jeweiligen Mitarbeitern bekannt. Siehe Abschnitt 5.2.1.

Sicherheitsrelevante Vorfälle und Kompromittierungen werden entsprechend dokumentiert und nachverfolgt.

5.7.2 Wiederherstellung nach Kompromittierung von Ressourcen

Das Sicherheitskonzept beschreibt die Durchführung von Recovery-Prozeduren für die Wiederherstellung der Betriebsfähigkeit des TSP. Es erfolgt ein tägliches Backup und ein Backup nach Veränderungen. Backups werden in einem anderen Brandabschnitt aufbewahrt. Die Wiederherstellungen von kritischen CA-Systemen werden im Rahmen von Notfallübungen regelmäßig getestet.

5.7.3 Kompromittierung des privaten CA-Schlüssels

Im Fall einer Kompromittierung oder der Bekanntgabe von Insuffizienz von Algorithmen oder assoziierten Parametern durch die Herausgeber der maßgeblichen Kataloge nach Abschnitt 6.1.6, veranlasst der TSP folgendes:

- betroffene CA-Zertifikate sowie deren ausgestellte und bisher nicht ausgelaufene Zertifikate werden widerrufen,
- involvierte Zertifikatsnehmer werden über den Vorfall und dessen Auswirkungen informiert,
- die zuständige Aufsichtsstelle wird informiert und der Vorfall auf den Webseiten des TSP veröffentlicht mit dem Hinweis, dass Zertifikate, die von dieser CA ausgestellt wurden, ihre Gültigkeit verlieren und der Sperrstatus verifiziert werden kann.

Aus der Analyse der Gründe für die Kompromittierung werden, wenn möglich, Maßnahmen ergriffen, um zukünftige Kompromittierungen zu vermeiden. Unter Berücksichtigung der Gründe für die Kompromittierung werden neue CA-Signaturschlüssel generiert und neue CA-Zertifikate ausgestellt.

Teil der Bundesdruckerei-Gruppe

5.7.4 Möglichkeiten zur Geschäftsweiterführung nach Kompromittierung und Desaster

In einem Notfall entscheidet der TSP je nach Art des Vorfalls, ob ein Recovery des in Abschnitt 6.2.4 beschriebenen Backups der CA durchgeführt oder bei Kompromittierung gemäß Abschnitt 5.7.3 verfahren wird.

5.8 Schließung des TSP

D-Trust verfügt über einen fortlaufend aktualisierten Beendigungsplan.

Bei Beendigung der Dienste von CAs informiert der TSP alle Zertifikatsnehmer und beendet alle Zugriffsmöglichkeiten von Unterauftragnehmern des TSP in Bezug auf die betroffenen CAs. Alle noch gültigen und von den betroffenen CAs ausgestellten Zertifikate werden gesperrt. Betroffene private CA-Schlüssel werden zerstört.

Im Fall einer geplanten Betriebseinstellung informiert der TSP alle Endanwender, Zertifikatsnehmer und Dritte vorab.

Der Verzeichnisdienst und Dokumente zur Antragstellung sowie das Repository (CP, CPS und CA-Zertifikate) werden an die Bundesdruckerei GmbH übergeben und unter äquivalenten Bedingungen weitergeführt. Die Aufrechterhaltung des Verzeichnisdienstes wird bis Ablauf der EE-Zertifikatsgültigkeit, zugesichert und entweder einem anderen TSP oder der Bundesdruckerei GmbH übergeben.

Der TSP verfügt über eine entsprechende Zusicherung der Bundesdruckerei für die Erfüllung dieser Mindestanforderungen.

Mit Beendigung des Betriebes wird alle Funktionalität der CAs eingestellt, so dass eine Zertifizierung nicht mehr möglich ist.

6. Technische Sicherheitsmaßnahmen

Die Beschreibungen dieses Kapitels beziehen sich auf die CAs der Uniper PKI, die bei der D-Trust GmbH betrieben werden.

6.1 Erzeugung und Installation von Schlüsselpaaren

An dieser Stelle wird zwischen Schlüsselpaaren für die

- CA-Zertifikate (Uniper Group CA 2 2015 sowie der Uniper Group CA 3 2020 und deren SubCAs) und
- Endanwenderzertifikate (EE-Zertifikate)

unterschieden.

6.1.1 Erzeugung von Schlüsselpaaren

CA-Schlüssel werden in einem „FIPS 140 2 Level 3" konformen Hardware Security Module (HSM) erzeugt. Das HSM befindet sich im Hochsicherheitsbereich des Trustcenters. Die Key-Ceremony erfolgt nach festgelegten Verfahren. In Abhängigkeit der CA erfolgt die Key-Ceremony durch dafür vorgesehen Trusted Roles im Beisein des Security Officers und falls erforderlich unter Aufsicht eines unabhängigen Dritten. Die Tätigkeiten während der Key Ceremony werden mittels Checkliste geprüft und protokolliert. Bei der Schlüsselerzeugung wird die Durchsetzung des Rollenkonzepts und somit das 4-Augen-Prinzip erzwungen. Bei der Erzeugung von CA-Schlüsseln ist gegebenenfalls ein unabhängiger Auditor anwesend oder der Auditor kann sich nach der Schlüsselerzeugung durch eine Videoaufzeichnung vom ordnungsgemäßen Ablauf der Schlüsselerzeugung überzeugen. Weiterhin wird die Erstellung von CA-Schlüsseln gemäß [EN 319 411-1] dokumentiert.

Sämtliche EE-Schlüssel (Signatur, Verschlüsselung und Authentifizierung) werden im Kontrollbereich des Zertifikatsnehmers generiert.

Der Zertifikatsnehmer ist bei der Erzeugung von EE-Schlüsseln verpflichtet, diese entsprechend der Vorgaben aus [EN 319 411-1] kryptographisch sicher zu erzeugen.

Die privaten EE-Schlüssel zu Signatur- und Authentifizierungszertifikaten werden auf PKI Token (Smartcards gem. EAL4+ zertifiziert oder USB Token gleicher Funktionalität) oder TPMs, die den ISO/IEC 11889 Standard (TCG Spezifikation Family 2) erfüllen, erzeugt.

6.1.2 Lieferung privater Schlüssel an Zertifikatsnehmer

Private Schlüssel in der Uniper PKI werden nicht vom TSP erstellt.

6.1.3 Lieferung öffentlicher Schlüssel an den TSP

Zertifikatsanforderungen können von Zertifikatsnehmern zu einem vorhandenen Schlüsselpaar per Zertifikats-Request gestellt werden, der signiert werden muss. Der Zertifikats-Request wird mit eine vorher vereinbarten Zertifikat signiert, Die Übertragung des signierten Zertifikats-Request wird zusätzlich durch eine TLS-gesicherte Verbindung durchgeführt.

Der Zertifikats-Request enthält den öffentlichen Schlüssel. Die entsprechende Response gibt das vollständige Zertifikat zurück.

6.1.4 Lieferung öffentlicher CA-Schlüssel an Zertifikatsnutzer

Der öffentliche Schlüssel der CA ist im CA-Zertifikat enthalten. CA-Zertifikate können aus dem öffentlichen Verzeichnis (siehe Abschnitt 2.1) bezogen werden, in dem sie nach ihrer Erstellung veröffentlicht werden.

6.1.5 Schlüssellängen

Für CA-Zertifikate werden derzeit RSA-Schlüssel mit einer Schlüssellänge von mindestens 2048 Bit verwendet.

Für EE-Zertifikate werden derzeit RSA-Schlüssel mit einer Schlüssellänge von mindestens 2048 Bit verwendet.

6.1.6 Festlegung der Schlüsselparameter und Qualitätskontrolle

CA- und EE-Zertifikate werden auf Grundlage von Schlüsseln ausgestellt, die [ETSI-ALG] in der aktuell gültigen Fassung entsprechen, soweit Kompatibilität im Verwendungsumfeld gewährleistet ist.

Signatur- und Verschlüsselungsalgorithmus sind im Abschnitt 0 dieses CPS genannt.

Es werden regelmäßig Tests durchgeführt, um die Güte des kryptographischen Materials sicherzustellen.

6.1.7 Schlüsselverwendungen

Private CA-Schlüssel werden ausschließlich zum Signieren von Zertifikaten und Sperrlisten benutzt (siehe Abschnitt 7.1.2).

Die EE-Schlüssel dürfen nur für die im Zertifikat benannten Nutzungsarten verwendet werden. Die Nutzungsarten werden in den Feldern KeyUsage und Ext-KeyUsage im Zertifikat definiert und ggf. durch weitere Extension eingeschränkt (siehe Abschnitt 7.1.2).

6.2 Sicherung des privaten Schlüssels und Anforderungen an kryptographische Module

6.2.1 Standards und Sicherheitsmaßnahmen für kryptographische Module

Die vom TSP eingesetzten kryptographischen Module funktionieren einwandfrei. Während des gesamten Lebenszyklus (einschließlich Lieferung und Lagerung) werden die Module durch technische und organisatorische Maßnahmen vor unbefugter Manipulation geschützt.

Zur Sicherung der CA-Schlüssel wird ein HSM eingesetzt, das entsprechend FIPS 140-2 Level 3 evaluiert wurde. Der Zertifikatsnehmer ist dafür verantwortlich, dass eine ausreichende Qualität bei der Schlüsselerzeugung für EE-Schlüssel gewährleistet ist.

Des Weiteren werden die CA-Systeme vor Viren oder sonstiger unerlaubter Software geschützt.

6.2.2 Mehrpersonen-Zugriffssicherung zu privaten Schlüsseln (n von m)

Das HSM, auf dem die CA-Schlüssel aufbewahrt werden, befindet sich in der sicheren Umgebung des Trustcenters. Die Aktivierung des privaten Schlüssels erfordert zwei autorisierte Personen. Nach der Aktivierung kann der HSM beliebig viele Zertifikate signieren.

Ein Zugriff auf private EE-Schlüssel besteht nur im Fall von Schlüsselhinterlegung gemäß Abschnitt 0.

6.2.3 Hinterlegung privater Schlüssel (key escrow)

Private CA-Schlüssel werden vom TSP nicht hinterlegt.

Das Hinterlegen privater EE-Schlüssel kann beantragt werden und wird vom Zertifikatsnehmer gemäß Abschnitt 4.12 umgesetzt.

Signaturschlüssel von EE-Zertifikaten werden vom TSP nicht hinterlegt.

Bei der Uniper PKI werden die EE-Schlüssel für Verschlüsselungszertifikate aus der SubCA XXXIII vom Zertifikatsnehmer gesondert gehalten.

Die Speicherung der Verschlüsselungsschlüssel erfolgt durch ein System, das durch Uniper oder durch einen beauftragten Dienstleister betrieben wird. Diesbezügliche Vorgaben der EN 319 411-1 müssen eingehalten werden. Die Einhaltung der Vorgaben wird überprüft.
Private Schlüssel der Uniper SE SubCA XXXIII dürfen für die Verwendung in Mobilgeräten oder SoftPSEs auch außerhalb eines zertifizierten PKI-Mediums oder VSC zur Entschlüsselung bzw. Authentifikation verwendet werden.

6.2.4 Backup privater Schlüssel

Es ist ein Backup der privaten CA-Schlüssel vorhanden. Ein CA-Schlüssel-Backup erfordert zwei für diese Tätigkeit am HSM autorisierte Personen und findet in der sicheren Umgebung des Trustcenters statt. Für das Backupsystem gelten die gleichen Voraussetzungen und Sicherungsmaßnahmen wie für das Produktivsystem. Eine Wiederherstellung privater Schlüssel erfordert ebenfalls zwei autorisierte Personen. Weitere Kopien der privaten CA-Schlüssel existieren nicht.

Für private EE-Schlüssel wird kein Backup durch den TSP angeboten.

6.2.5 Archivierung privater Schlüssel

Private CA- und EE-Schlüssel werden vom TSP nicht archiviert. Der Zertifikatsnehmer archiviert Verschlüsselungsschlüssel von Endanwendern aus der SubCA XXXIII in eigener Verantwortung.

6.2.6 Transfer privater Schlüssel in oder aus kryptographischen Modulen

Ein Transfer privater CA-Schlüssel in oder aus dem HSM erfolgt nur zu Backup- und Wiederherstellungszwecken. Ein 4-Augen-Prinzip wird erzwungen. Bei Export/Import in ein anderes HSM schützt eine Verschlüsselung den privaten CA-Schlüssel.

Für Zertifikate, die auf mobilen Endgeräten zum Einsatz kommen sollen, wird das vom Zertifikatsnehmer im HSM erzeugte Schlüsselmaterial mit dem bestehenden Verschlüsselungsschlüssel des Endanwenders verschlüsselt und geschützt auf das Endgerät des Endanwenders übertragen. Das Schlüsselmaterial kann dort nur nach Eingabe der vollständigen, korrekten PIN des Verschlüsselungsschlüssels installiert werden. Ein Backup der P12-Datei beim Endanwender ist nicht vorgesehen.

Verschlüsselungszertifikate werden durch die entsprechende Anwendung gemeinsam mit dem E-Mail-Profil auf das mobile Endgerät übertragen. Der Endanwender hat hierbei keine weiteren Maßnahmen zu ergreifen.

6.2.7 Speicherung privater Schlüssel in kryptographischen Modulen

Die privaten CA-Schlüssel liegen verschlüsselt im HSM beim TSP vor.

Die privaten EE-Schlüssel zu Signatur- und Authentifizierungszertifikaten werden auf PKI Token (Smartcards gem. EAL4+ zertifiziert oder USB Token gleicher Funktionalität) oder TPMs, die den ISO/IEC 11889 Standard (TCG Spezifikation Family 2) oder auf einer VSC verschlüsselt gespeichert.

Der Zertifikatsnehmer speichert Verschlüsselungsschlüssel von Endanwendern aus der SubCA XXXIII in eigener Verantwortung. Private Schlüssel der Uniper SubCA XXXIII dürfen für die Verwendung in Mobilgeräten oder SoftPSEs auch außerhalb eines zertifizierten PKI-Mediums oder VSC zur Entschlüsselung bzw. Authentifikation verwendet werden.

6.2.8 Aktivierung privater Schlüssel

Die privaten CA-Schlüssel können nur im 4-Augen-Prinzip und von den zuständigen Rollen und für die zulässigen Nutzungsarten (keyCertSign, cRLSign) aktiviert werden.

Private Signaturschlüssel werden auf Endanwenderseite durch Eingabe einer mindestens sechsstelligen PIN aktiviert.

6.2.9 Deaktivieren privater Schlüssel

Die privaten CA-Schlüssel werden durch Beendigung der Verbindung zwischen HSM und Anwendung deaktiviert.

Die jeweilige Anwendung deaktiviert den privaten EE-Schlüssel. Die Deaktivierung geschieht spätestens durch das Ziehen des PKI-Tokens.

6.2.10 Zerstörung privater Schlüssel

Nach Ablauf der Gültigkeit der privaten CA-Schlüssel werden diese gelöscht. Dies erfolgt durch Löschen auf dem HSM und gleichzeitigem Löschen der auf Datenträgern angelegten Backups. Bei Stilllegung des HSMs werden die privaten Schlüssel auf dem Gerät gelöscht.

6.2.11 Beurteilung kryptographischer Module

Der TSP betreibt geeignete hard- und softwarebasierte Schlüsselgeneratoren um die Qualität der EE-Schlüssel zu sichern. Die eingesetzten HSM sind FIPS 140 2 Level 3 konform.

6.3 Andere Aspekte des Managements von Schlüsselpaaren

6.3.1 Archivierung öffentlicher Schlüssel

Öffentliche CA- und EE-Schlüssel werden in Form der erstellten Zertifikate archiviert.

6.3.2 Gültigkeitsperioden von Zertifikaten und Schlüsselpaaren

Die Gültigkeitsdauer der CA-Schlüssel und Zertifikate ist variabel und dem Zertifikat zu entnehmen. Die maximal mögliche Gültigkeitsdauer beträgt 30 Jahre.

Die Gültigkeitsdauer der EE-Schlüssel und Zertifikate ist variabel und dem Zertifikat zu entnehmen. Die maximal mögliche Gültigkeitsdauer beträgt für NCP- bzw. LCP-Zertifikate bei der Uniper PKI 36 Monate.

6.4 Aktivierungsdaten

6.4.1 Erzeugung und Installation von Aktivierungsdaten

Die Aktivierungsdaten der CA-Schlüssel werden durch das HSM abgefragt. PIN-Vergabe erfolgt während der Bootstrap-Prozedur. Ein 4-Augen-Prinzip wird erzwungen.

Da das Schlüsselpaar vom Zertifikatsnehmer erzeugt wird, steht das Aktivierungsgeheimis dem Zertifikatsnehmer unmittelbar und ausschließlich zur Verfügung.

6.4.2 Schutz von Aktivierungsdaten

Die Aktivierungsdaten der CA-Schlüssel setzen sich aus zwei Geheimnissen zusammen, von denen jeweils ein berechtigter Mitarbeiter eines kennt. Der Zugriff auf die Aktivierungsdaten ist nur bestimmten vorgesehenen Mitarbeitern möglich.

6.4.3 Andere Aspekte von Aktivierungsdaten

PKI-Token in der Uniper PKI sind so konfiguriert, dass sie nach dreimaliger Fehleingabe der PIN gesperrt sind. Endanwender besitzen keine Personal Unblocking Key-Nummer (PUK) zum Entsperren des PKI-Tokens. Die PIN wird durch den Endanwender selbst gesetzt, kann durch ihn geändert werden und kann mit Unterstützung des Smartcardmanagementsystems durch den Endanwender zurückgesetzt werden.

6.5 Sicherheitsmaßnahmen in den Rechneranlagen

Die D-Trust betreibt ein Informationssicherheitsmanagementsystem (ISMS) gemäß ISO/IEC 27001. Der Betrieb des TSP unterliegt diesem ISMS. Eine Security Policy regelt die verbindlichen Vorgaben für den IT Betrieb. Diese wurde von der Geschäftsführung der D-Trust GmbH freigegeben und an alle Mitarbeiter des TSP kommuniziert. Es erfolgt ein jährliches als auch anlassbezogenes Review und Update der Security Policy.

Die Bewertung und ggf. die Behebung von identifizierten Schwachstellen erfolgt innerhalb von 48 Stunden. Ist die Behebung innerhalb von 48 Stunden nicht möglich, so enthält die Bewertung einen konkreten Behandlungsplan.

6.5.1 Spezifische technische Sicherheitsanforderungen in den Rechneranlagen

Die vom TSP eingesetzten Computer, Netze und andere Komponenten stellen in der eingesetzten Konfiguration sicher, dass nur Aktionen durchgeführt werden können, die mit der CP und EN 319 411-1 vereinbar sind.

Es wird sichergestellt, dass sicherheitsrelevante Softwareupdates in angemessener Zeit auf den relevanten Systemen installiert werden. Abweichungen hiervon werden vom TSP angemessen dokumentiert und ggf. im Risikomanagement des TSP adressiert.

Zertifikatsnehmer und Endanwender müssen vertrauenswürdige Computer und Software verwenden: diese Bedingung ist nach den von Uniper vorgegebenen Richtlinien erfüllt.

Die Systemzeit der relevanten CA-Systeme wird durch eine redundant angeschlosse Funkuhr sichergestellt.

6.5.2 Beurteilung von Computersicherheit

Die für die CA-Schlüssel eingesetzten Computer, Netze und andere Komponenten wurden durch anerkannte Konformitätsbewertungsstellen regelmäßig geprüft und unterliegen gemäß [EN 319 401] einem entsprechenden Monitoring.

6.5.3 Monitoring

Zur Sicherstellung der Verfügbarkeit erfolgt ein kontinuierliches Monitoring der relevanten Systeme. Jede Störung wird erfasst, dokumentiert und gemäß ihrer Auswirkung mit einem Schweregrad gekennzeichnet und daraufhin priorisiert. Die Behandlung von kritischen Meldungen erfolgt im Rahmen des Prozesses Incident Management. Meldungen zu sicherheitsrelevanten Ereignissen werden an eine zentrale Stelle übermittelt und gemäß Kritikalität ausgewertet.

Bei Störungen mit Verfügbarkeitsverlust eines Services werden die betroffenen Parteien mindestens alle 24 Stunden über einen aktuellen Status zur Störungsbeseitigung informiert.

6.6 Technische Maßnahmen während des Life Cycles

Produktive Serversysteme erhalten sicherheitsrelevante Konfigurationen über zentrale Managementsysteme. Es erfolgt alle 15 Minuten eine Überprüfung der Konfigurationen. Festgestellte Abweichungen gegen die zentralen Sicherheitsrichtlinien werden unmittelbar in den Konfigurationen korrigiert.

Bereits bei der Planung aller vom TSP oder im Auftrag des TSP betriebener Systeme werden die Anforderungen aus Abschnitt 5 [BRG] angemessen berücksichtigt.

6.6.1 Sicherheitsmaßnahmen bei der Entwicklung

Bei der Entwicklung aller vom TSP oder im Auftrag des TSP durchgeführter Systementwicklungsprojekte werden Sicherheitsanforderungen im Entwurfsstadium analysiert. Die gewonnenen Erkenntnisse werden als Anforderungen bei der Entwicklung festgelegt.

Die Testumgebung der D-Trust für Entwicklungs-, Test- und Staging-Systeme ist getrennt von ihren Produktionssystemen.

6.6.2 Sicherheitsmaßnahmen beim Computermanagement

Ausschließlich entsprechend dem Rollenkonzept autorisiertes Personal darf Computer, Netze und andere Komponenten administrieren. Relevante Systeme werden mit einer Mehrfaktorauthentisierung gesichert. Es findet eine regelmäßige Auswertung von Logfiles auf Regelverletzungen, Angriffsversuche und andere Vorfälle statt. Überwachungsmaßnahmen beginnen mit Inbetriebnahme eines Gerätes und enden mit dessen Entsorgung.

6.6.3 Sicherheitsmaßnahmen während des Life Cycles

Eingesetzte Geräte werden gemäß Herstellerangaben betrieben. Vor Inbetriebnahme werden sie eingehend geprüft und kommen nur zum Einsatz, wenn zweifelsfrei feststeht, dass sie nicht manipuliert wurden. Durch Versiegelung der Hardware und Softwarechecks beispielsweise werden Manipulationen und Manipulationsversuche bei jeder Aktion oder Revision erkennbar. Weiterhin werden Verfahren und Systeme eingesetzt, die sicherheitsrelevante bzw. CA-Systeme permanent überwachen, um Unregelmäßigkeiten (unautorisierte Zugriffe, Ausfall, etc.) zu erkennen. Bei

Verdacht auf Manipulation einer Komponente, wird eine ggf. geplante Aktion an der Komponente nicht durchgeführt und der Vorfall gemeldet. Um kurzfristig und koordiniert auf eventuelle sicherheitsrelevante Vorfälle reagieren zu können, definiert der TSP klare Eskalationsrichtlinien für die einzelnen Rollen. Alle relevanten Ereignisse der CA-Umgebung, sowie des Schlüssel- und Zertifikat-Management werden von den Systemen erfasst und signiert abgelegt.

Kapazitätsanforderungen und -auslastungen sowie Eignung der beteiligten Systeme werden überwacht und bei Bedarf angeglichen. Ausgetauschte Geräte werden derart außer Betrieb genommen und entsorgt, dass Funktionalitäts- oder Datenmissbrauch ausgeschlossen wird. Änderungen an Systemen oder Prozessen durchlaufen einen dokumentierten Change-Management-Prozess. Sicherheitskritische Änderungen werden durch den Sicherheitsbeauftragten geprüft. Nach Ablauf der Gültigkeit von CAs werden die privaten Schlüssel vernichtet.

Elektronische Daten oder papiergebundene Protokolle dokumentieren alle relevanten Ereignisse, die den Life-Cycle der CA sowie der ausgestellten Zertifikate und generierten Schlüssel beeinflussen und werden auf langlebigen Medien revisionssicher gespeichert.

Hierbei wird speziell darauf geachtet, dass eingesetzte Medien sicher behandelt und vor Beschädigung geschützt werden. Des Weiteren werden diese Medien sicher gelagert, regelmäßig überprüft und vor Verschleiß bzw. Überalterung geschützt.

Penetrationstests werden durch eine unabhängige und fachkundige Stelle mindestens einmal pro Jahr durchgeführt. Weiterhin werden mindestens einmal pro Quartal Schwachstellenscans veranlasst. Die Ergebnisse des Penetrationstestberichts werden intern archiviert.

Die Eigenschaften der Prozesse zur Identifizierung werden innerhalb der Uniper bzw. zwischen Uniper und seinen Dienstleistern individuell erarbeitet und initial mit D-Trust abgestimmt.

Änderungen an den in CP, CPS und verfahrensbezogenen Verträgen beschriebenen Prozessen bedürfen einer vorherigen Bestätigung der D-Trust zur Policykonformität auf der Basis einer Changebeschreibung innerhalb von zwei Wochen und ggf. einer vorherigen Aktualisierung der betroffenen Dokumente.

Für die Einhaltung sind die Beauftragten der Geschäftsführung der D-Trust GmbH und die PKI Supervisoren der Uniper verantwortlich, die in den Changemanagementprozess als zustimmungspflichtig eingebunden werden müssen, sofern Auswirkungen auf die PKI Identifizierungs- und Registrierungsprozesse absehbar sind.

6.7 Sicherheitsmaßnahmen für Netze

Im Betrieb der CAs wird ein Netzkonzept realisiert, welches sicherstellt, dass die relevanten CA-Systeme in besonders gesicherten Netzwerkzonen betrieben werden. Die Netzwerkarchitektur des TSP beinhaltet ein mehrstufiges Konzept der Netzwerksicherheitszonen. Die Root CAs werden in der Netzwerksicherheitszone mit dem höchsten Schutzbedarf betrieben. Für das Netzkonzept liegt eine detaillierte Dokumentation vor, die bei begründetem Interesse in den relevanten Teilen eingesehen werden kann.

Zum Schutz der Prozesse des TSP werden beispielsweise Firewall und Intrusion Detection / Prevention Mechanismen eingesetzt, die nur explizit erlaubte Verbindungen zulassen. Der TSP betreibt Netzsegmente unterschiedlichen Schutzbedarfs und trennt dabei Mitarbeiter- und Internet-nahe Netze sorgfältig von Servernetzwerken. Die Systeme unterliegen regelmäßigen Revisionen, die Verantwortlichen sind berichtspflichtig. Auffälligkeiten werden durch technische Systeme und organisatorische Prozesse gemeldet und in einem definierten Incidentverfahren und daran ansetzenden Prozessen behandelt.

Die Verfügbarkeit der Internetanbindung ist durch Redundanz abgesichert. Es bestehen zwei ständige Verbindungen zum Provider auf zwei unterschiedlichen Streckenführungen. Beim Ausfall des Zugangspunktes des Providers erfolgt die automatische Umschaltung auf die zweite Anbindung.

Datenverkehr mit hohem Schutzbedarf außerhalb der durch den TSP geschützten Netzwerke, für den Integrität oder Vertraulichkeit sichergestellt werden muss, wird durch kryptographische Mechanismen geschützt.

Die physische Sicherheit der durch den TSP betriebenen und genutzten Netze ist sichergestellt und wird den baulichen Gegebenheiten und ihren Veränderungen angepasst.

Im Betrieb des SCM im Datacenter für Uniper wird ein Netzwerksicherheitskonzept umgesetzt.

6.8 Zeitstempel

Zeitstempel werden im Rahmen dieses CPS nicht angeboten.

7. Profile von Zertifikaten, Sperrlisten und OCSP

7.1 Zertifikatsprofile

7.1.1 Versionsnummern

Es werden Zertifikate im Format X.509v3 und gemäß EN 319 412-2 ausgegeben.

Die Zertifikatsseriennummer wird zufällig erzeugt und enthält eine Entropie von 128 Bit.

7.1.2 Zertifikatserweiterungen

Die Wahl der Erweiterung ist weitestgehend produktabhängig.

CA-Zertifikate enthalten folgende *kritische* Erweiterungen („Pflichtfeld"):

Erweiterung	OID	Parameter
keyUsage	2.5.29.15	*keyCertSign,* *cRLSign*
basicConstraints	2.5.29.19	*Ca=TRUE,* *(pathLenConstraint)*

CA-Zertifikate können folgende *unkritische* Erweiterungen enthalten („optional"):

Erweiterung	OID	Parameter
authorityKeyIdentifier	2.5.29.35	160-bit SHA-1 Hash des Ausstellerschlüssels
subjectKeyIdentifier	2.5.29.14	160-bit SHA-1 Hash des Subject Public Key
cRLDistributionPoints	2.5.29.31	Adresse der CRL-Ausgabestelle
authorityInfoAccess	1.3.6.1.5.5.7.1.1	*accessMethod=OCSP {1.3.6.1.5.5.7.48.1}, accessLocation {…}* *accessMethod=Certification Authority Issuer {1.3.6.1.5.5.7.48.2}, accessLocation {…}*

Teil der Bundesdruckerei-Gruppe

Erweiterung	OID	Parameter
certificatePolicies	2.5.29.32	OIDs der unterstützten CPs

Ergänzende Erweiterungen können aufgenommen werden, müssen [X.509], [RFC 5280], [RFC 6818], [ETSI EN 319 412] und [ETSI-ALG] entsprechen oder in einem referenzierten Dokument beschrieben sein.

EE-Zertifikate enthalten folgende *kritische* Erweiterungen:

Erweiterung	OID	Parameter
keyUsage	2.5.29.15	Möglich sind: *digitalSignature, contentCommitment, keyEncipherment, dataEncipherment, keyAgreement, encipherOnly, decipherOnly* und Kombinationen

EE-Zertifikate können folgende unkritische Erweiterungen enthalten:

Erweiterung	OID	Parameter
extKeyUsage	2.5.29.37	Entsprechend [RFC 5280], [RFC 6818]
authorityKeyIdentifier	2.5.29.35	160-bit SHA-1 Hash des Ausstellerschlüssels
subjectKeyIdentifier	2.5.29.14	160-bit SHA-1 Hash des Subject Public Key
cRLDistributionPoints	2.5.29.31	CRL-Ausgabestelle als ldap-Adresse
authorityInfoAccess	1.3.6.1.5.5.7.1.1	*accessMethod=OCSP {1.3.6.1.5.5.7.48.1}, accessLocation {…}* *accessMethod= Certification Authority Issuer {1.3.6.1.5.5.7.48.2}, accessLocation {…}*
certificatePolicies	2.5.29.32	OIDs der unterstützten CPs *cpsURI*
subjectAltName	2.5.29.17	Alternativer Inhabername

Ergänzende Erweiterungen können aufgenommen werden, müssen [X.509], [RFC 5280], [RFC 6818], [ETSI EN 319 412] und [ETSI-ALG] entsprechen oder in einem referenzierten Dokument beschrieben sein.

7.1.3 Algorithmen-OIDs

In den CA- und EE-Zertifikaten wird derzeit folgender Verschlüsselungsalgorithmus verwendet:

- RSA mit OID 1.2.840.113549.1.1.1

Folgende Signaturalgorithmen werden in CA- und EE-Zertifikaten derzeit verwendet:

- SHA256 RSA mit OID 1.2.840.113549.1.1.11

7.1.4 Namensformate

In den Feldern *subject* (hier: Name des Endanwenders) und *issuer* (Name des Ausstellers) werden Namen nach [X.501] als DistinguishedName vergeben. Es können die Attribute aus Abschnitt 3.1.4 vergeben werden. Die Kodierung erfolgt als UTF8-String bzw. PrintableString für das Attribut C (Country).

In den Feldern *SubjectAltName* (Alternativer Zertifikatsnehmername) und *Issuer-AltName* (Alternativer Ausstellername) können Namen gemäß [RFC 5280], [RFC 6818] (kodiert als IA5String) stehen.

7.1.5 Name Constraints

„NameConstraints" wird nicht benutzt.

7.1.6 Certificate Policy Object Identifier

„CertificatePolicies" kann den OID unterstützter CPs enthalten.

7.1.7 Nutzung der Erweiterung „PolicyConstraints"

„PolicyConstraints" wird nicht benutzt.

7.1.8 Syntax und Semantik von „PolicyQualifiers"

„PolicyQualifiers" können benutzt werden.

7.1.9 Verarbeitung der Semantik der kritischen Erweiterung von CertificatePolicies

In CA- und EE-Zertifikaten ist die Erweiterung *CertificatePolicies* (Zertifikatsrichtlinie) nicht kritisch. Es liegt im Ermessen der Zertifikatsnehmer und Zertifikatsnutzer, diese Erweiterung auszuwerten.

7.2 Sperrlistenprofile

7.2.1 Versionsnummer(n)

Es werden Sperrlisten v2 gemäß [RFC 5280], [RFC 6818] erstellt. Delta-CRLs sind nicht vorgesehen.

7.2.2 Erweiterungen von Sperrlisten und Sperrlisteneinträgen

Sperrlisten können folgende unkritische Erweiterungen enthalten:

Erweiterung	OID	Parameter
cRLNumber	2.5.29.20	Nummer der Sperrliste
authorityKeyIdentifier	2.5.29.35	160-bit SHA-1 Hash des Ausstellerschlüssels

Teil der Bundesdruckerei-Gruppe

Erweiterung	OID	Parameter
expiredCertsOnCRL	2.5.29.60	**Wird aktuell nicht verwendet.** Sperreinträge verbleiben nach Ablauf der jeweiligen Zertifikatsgültigkeit in den zugehörigen Sperrlisten.

7.3 Profile des Statusabfragedienstes (OCSP)

Der OCSP-Responder unterstützt zusätzlich zu RFC 6960 auch Positivauskünfte („Zertifikat ist authentisch und gültig").

Der OCSP-Responder liefert folgende Antworten:

- „good"[5], wenn der Responder das Zertifikat als gültig erkennt,
- „unknown" [6], wenn der Responder den Status des Zertifikats nicht ermitteln kann und
- „revoked", wenn der Responder das Zertifikat als widerrufen erkennt.

7.3.1 Versionsnummer(n)

Es wird OCSP v1 gemäß [RFC 6960] eingesetzt.

7.3.2 OCSP-Erweiterungen

Der OCSP-Responder unterstützt bei Anfragen, die im folgenden angegebene Erweiterung (Extension):

Erweiterung	Parameter
retrieveIfAllowed	Falls gesetzt, wird Zertifikat in der Antwort mitgeliefert (optional).

Der OCSP-Responder verwendet in den Antworten, die im folgenden angegebenen Erweiterungen (Extensions):

Erweiterung	Parameter
archiveCutoff	Zeitraum, für den der OCSP-Responder nach Ausstellung des Zertifikats die Statusinformationen bereitstellt.
certHash	Bei Status good oder revoked wird der SHA-1 Hash-Wert des Zertifikats eingetragen.
certInDirSince	Zeitpunkt der Veröffentlichung des Zertifikats im zentralen Verzeichnisdienst.

[5] Ist ein Zertifikat nicht ausgestellt, gibt der OCSP Responder nicht "good", sondern "unknown" als Statusinformation zurück.

[6] Der OCSP-Responder überwacht die als „unknown" geprüften Anfragen nicht. Diese werden aktuell verworfen.

Teil der Bundesdruckerei-Gruppe

Erweiterung	Parameter
requestedCertificate	Enthält das Zertifikat, falls *RetrieveIfAllowed* gesetzt war.

Alle Erweiterungen sind nicht kritisch. Weitere unkritische Erweiterungen können enthalten sein.

8. Auditierungen und andere Prüfungen

Revisionen, Revisionsgegenstände und Prozesse sind detailliert in der Dokumentation des Vertrauensdiensteanbieters D-Trust GmbH beschrieben. Das Rollenkonzept dokumentiert die Qualifikation und die Stellung des Revisors.

Die Dokumentation sowie die operativen Verfahren des TSP werden regelmäßig wiederkehrend durch jährliche Audits über den gesamten Zeitraum durch eine unabhängige Konformitätsbewertungsstelle geprüft. Bei begründetem Interesse können diese Dokumente in den relevanten Teilen eingesehen werden.

CP und CPS erfüllen für Zertifikate die Anforderungen gemäß [EN 319 411-1] einschließlich der Anforderungen aus [BRG] und [NetSec-CAB]. Ein regelmäßiges Assessment durch einen qualifizierten und unabhängigen Dritten („competent independent party" gemäß [EN 319 411-1] belegt die Kompatibilität.

Der TSP gibt Zertifikate mit einer Policy-OID-Referenz auf [EN 319 411-1] erst nach der initialen und erfolgreich abgeschlossenen Prüfung durch einen unabhängigen externen Zertifizierer aus. Es finden regelmäßige Wiederholungsprüfungen statt. Sollten sich die Verfahren als nicht mehr konform zu den aktuellen Richtlinien von [EN 319 411-1] erweisen, unterlässt der TSP das Ausstellen o. g. Zertifikate bis die Richtlinienkonformität wiederhergestellt und entsprechend überprüft wurde.

Diese Auditierung findet jährlich statt.

Darüber hinaus finden regelmäßig interne Audits statt, die der TSP und die Uniper selbständig durchführen und dokumentieren.

9. Sonstige finanzielle und rechtliche Regelungen

Es gelten die Regelungen aus Kapitel 9 der CP der D-Trust GmbH.