Deutsche Post AG POSTIDENT E-Signing SUB CA Certification Practice Statement

PL
Policy

Domain: Security

SubDomain: PKI

Reference: "OID" 1.3.6.1.4.1.5064.2.1.1.1.2.4

Status: Final

Validated by: Olga Schönfeld

Role: Product Owner

Date: 13.05.2024

Signature:

Approved by: Achim Hügen

Role: Security Architect

Application Date: 13.05.2024

Signature:

Diffusion:

Access: Public. Available on the website POSTIDENT e-Signing Zertifizierungsrichtlinien

Localisation: English

Version	Date	Modifications	Author
1.0	05.04.2017	Initial Draft	André Glenzer
1.7	13.09.2017	Updated contact Data, Modified OCSP + Certificate URL	Achim Hügen
1.8	28.09.2017	More detailed information regarding the revocation process in chapter 3.4 and 4.9.	André Glenzer
1.9	16.11.2017	Switched from qualified to advanced certificates	Achim Hügen
2.0	13.06.2018	Added qualified certificates	Achim Hügen
2.2	14.10.2022	Rework of chapter 3, New Identification Method based on existing data	Achim Hügen
2.3	09.05.2023	Updated contact data	Olga Schönfeld
2.4	13.05.2024	Identification via online eID added in chapter 3.2.3, 6.4.1.2 and 6.4.2.2	Olga Schönfeld

Complete Table of Content

Copyright Notice **9**

1. INTRODUCTION **10**

1.1 General presentation *10*

1.2 Document Identification *10*

1.3 ENTITIES INVOLVED IN THE PKI *10*

1.4 CERTIFICAT USAGE *10*

1.4.1. Appropriate certificate uses 10

1.4.2. Prohibited certificate uses 11

1.5 Policy administration *11*

1.5.1. Organization managing the document 11

1.5.2. Contact 11

1.5.3. Entity determining CPS suitability for the Certificate Policy 11

1.5.4. CPS Approval Procedure 12

1.6 Definitions and acronyms *12*

1.6.1. Acronyms 12

1.6.2. Definitions 13

2. Publications and Repository Responsibilities **17**

2.1 Identification of entities operating repositories *17*

2.2 INFORMATION TO BE PUBLISHED *17*

2.3 Time of Frequency of Publication *18*

2.4 ACCESS CONTROL TO PUBLISHED INFORMATION *18*

3. IDENTIFICATION And AUTHENTIFICATION **19**

3.1 Naming *19*

3.1.1. Types of names 19

3.1.2. Need for names to be meaningful 19

3.1.3. Anonymity or pseudonym of Subscribers 19

3.1.4. Rules for interpreting various name forms 20

3.1.5. Uniqueness of names 20

3.1.6. Recognition, authentication, and role of trademarks 20

3.2 Initial Identity Validation *20*

3.2.1. Method to prove possession of private key 20

3.2.2. Authentication of organization identity 20

3.2.3. Authentication of natural person identity 20

3.2.4. Non-verified subscriber information 21

3.2.5. Authentication of individual identity 21

3.2.6. Criteria for interoperation 21

3.3 Identification and authentication for re-key & update requests *21*

3.3.1. Identification and authentication for routine re-key & update 21

3.3.2. Identification and authentication for re-key after revocation 21

3.4 Identification and authentication for revocation request *22*

3.4.1. Request originated by the holder, or the subscriber for the certificate 22

3.4.2. Request from the CA or GA 22

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS 23

4.1 Certificate Application *23*

4.1.1. Origin of an application for a certificate 23

4.1.2. Enrolment process and responsibilities 23

4.2 Certificate Application Processing *24*

4.2.1. Implementation of the identification process and application validation 24

4.2.2. Acceptance or rejection of application 24

4.2.3. Time to process certificate application 24

4.3 Certificate issuance *24*

4.3.1. CA Actions during certificate Issuance. 24

4.3.2. Notification to Subscriber by the CA of issuance of Certificate 25

4.4 Certificate Acceptance *25*

4.4.1. Conduct constituting Certificate acceptance 25

4.4.2. Publication of the Certificate by the CA 25

4.4.3. Notification of Certificate issuance by the CA to other entities 25

4.5 Key pair and certificate usage *25*

4.5.1. Subscriber private key and certificate usage 25
4.5.2. Relying Party public key and Certificate usage 25
4.5.3. Root CA public key and Certificate usage 25
4.5.4. CA public key and Certificate usage 25
4.6 Certificate renewal *25*
4.7 Certificate re-key *26*
4.7.1. Possible cause of a re-key 26
4.7.2. Origin of a re-key application 26
4.7.3. Processing of a re-key application 26
4.7.4. Notification of the issuance of the new certificate 26
4.7.5. Acceptance procedure for the new certificate 26
4.7.6. Publication of the new certificate 26
4.7.7. Notification by the CA to other entities 26
4.8 Certificate Modification *26*
4.9 Revocation AND suspension of certificates *26*
4.9.1. Circumstances for revocation 26
4.9.2. Origin of a revocation request 27
4.9.3. Procedure for processing a revocation request 27
4.9.4. Delay for requesting a revocation 28
4.9.5. Delay for processing a revocation request 28
4.9.6. Revocation checking requirement for Relying Parties 28
4.9.7. CRL Issuance Frequency 28
4.9.8. Maximum delay for CRL publication 28
4.9.9. On-line revocation status availability 28
4.9.10. On-line revocation status requirement 28
4.9.11. Other forms of revocation advertisements available 28
4.9.12. Special requirements regarding key compromise 28
4.9.13. Circumstances for suspension 29
4.9.14. Who can request suspension 29
4.9.15. Procedure for processing a suspension application 29

4.9.16. Limits of Certificate Suspension Period 29

4.10 Certificate Status services *29*

4.10.1. Operational characteristics 29

4.10.2. Service availability 29

4.10.3. Optional features 29

4.11 End of subscription *29*

4.12 Key escrow and recovery *30*

4.12.1. Recovery and practices in case of key escrow 30

4.12.2. Recovery and practices in case of session key encapsulation 30

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS 31

5.1 PHYSICAL CONTROLS *31*

5.1.1. Site location and construction 31

5.1.2. Physical access 32

5.1.3. Power and air conditioning 32

5.1.4. Water exposures 32

5.1.5. Prevention and fire protection 32

5.1.6. Media Storage 32

5.1.7. Waste disposal 33

5.1.8. Off-site backup 33

5.2 Procedural Controls *33*

5.2.1. Trusted Roles 33

5.2.2. Number of persons required per task 34

5.2.3. Roles requiring separation of duties 34

5.3 Personnel controls *34*

5.3.1. Qualifications, experience, and clearance requirements 34

5.3.2. Background check Procedures 35

5.3.3. Training requirements 35

5.3.4. Re-training frequency and requirements 35

5.3.5. Job rotation frequency and sequence 36

5.3.6. Sanction for unauthorized actions 36

5.3.7. External contractors requirements 36

5.3.8. Documentation supplied to personnel 36

5.4 Audit logging procedures *36*

5.5 Records Archival *36*

5.5.1. Type of records archived 37

5.5.2. Retention period for archive 37

5.5.3. Protection of archive 37

5.5.4. Archive backup procedures 37

5.5.5. Requirements for time-stamping of records 37

5.5.6. Archive collection system 37

5.5.7. Procedure to retrieve and verify archive information 37

5.6 Key Changeover *37*

5.7 Compromise and disaster recovery *38*

5.7.1. Incident and compromise handling procedures 38

5.7.2. Recovery Procedures in case of IT Disaster (Hardware, software and data) 38

5.7.3. Entity private key compromise procedures 39

5.7.4. Business continuity capabilities after a disaster 39

5.8 PKI Termination *39*

5.8.1. PKI TRANSFER 39

5.8.2. End of Activity 40

6. TECHNICAL SECURITY CONTROLS **41**

6.1 Key pair generation and installation *41*

6.1.1. Key pair generation 41

6.1.2. Private key delivery to Subscriber 41

6.1.3. Public key delivery to certificate issuer 41

6.1.4. CA public key delivery to Relying Parties 41

6.1.5. Key sizes 41

6.1.6. Validation of the key pair parameters 41

6.1.7. Key usage purposes 41

6.2 Private key protection and Cryptographic Module Engineering Controls *42*

6.2.1. Cryptographic module standards and controls 42
6.2.2. Private key multi-person control 42
6.2.3. Private key escrow 42
6.2.4. Private key backup 42
6.2.5. Private Key escrow 42
6.2.6. Private Key backup 43
6.2.7. Private key archival 43
6.2.8. Private key transfer into or from a cryptographic module 43
6.2.9. Private key storage on cryptographic module 43
6.2.10. Method for Private Key Activation 43
6.2.11. Method for Private Key Deactivation 44
6.2.12. Method for Private Key Destruction 44
6.2.13. Cryptographic module rating 44
6.3 Other aspects of key pair management *44*
6.3.1. Public key archival 44
6.3.2. Key pair and certificate usage period 44
6.4 activation Data *44*
6.4.1. Generation and installation of activation data 44
6.4.2. Activation Data Protection 45
6.5 Computer security controls *45*
6.5.1. Computer-specific technical security requirements 45
6.5.2. Level of qualification of computer systems 46
6.6 Life cycle technical controls *46*
6.6.1. Security measures related to system development 46
6.6.2. Security Management measures 46
6.7 Network Security *47*
6.7.1. Network Segmentation 47
6.7.2. Interconnections 47
6.7.3. Connections 47
6.7.4. Availability 48

6.8 Timestamping *48*

7. CERTIFICATES, OCSP And CRL Profiles **49**

7.1 Profiles of the certificate of the CA. *49*

7.2 End-user certificates *49*

7.3 CRL *49*

7.4 OCSP Certificate Profile *49*

7.5 OCSP Response Profile *49*

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS **50**

9. OTHER BUSINESS AND LEGAL MATTERS **51**

10. ANNEXE 1 : REFERENCE Documents **52**

10.1 Laws and Regulations *52*

10.2 Technical Documents *53*

COPYRIGHT NOTICE

1. INTRODUCTION

1.1 GENERAL PRESENTATION

This document constitutes the Certification Practice Statement (CPS) of the Certification Authority (AC) Deutsche Post AG POSTIDENT E-Signing SUB CA. This CA is intended to issue

- Qualified and advanced electronic signature Certificates in accordance with eIDAS European Regulation (ETSI EN 319411-2 Level QCP-n-QSCD).

The purpose of the CPS is to define the statement of the practices that the CA employs in issuing signature and authentication certificates for physical persons;

- OID = 1.3.6.1.4.1.5064.2.1.60.1.1: for ETSI EN 319411-2 advanced signature certificates,
- OID = 1.3.6.1.4.1.5064.2.1.61.1.1: for ETSI EN 319411-2 qualified signature certificates

This CPS complies with:

- ETSI EN 319 401
- ETSI EN 319411-1
- ETSI EB 319411-2

1.2 DOCUMENT IDENTIFICATION

This document is the CPS of the CA Deutsche Post AG POSTIDENT E-Signing SUB CA of DEUTSCHE POST AG Public Keys Infrastructure (PKI) aiming at issuing signature and authentication certificates for physical persons.

Its object identifier (OID) is as follows: 1.3.6.1.4.1.5064.2.1.1.1.2.0

1.3 ENTITIES INVOLVED IN THE PKI

The functional decomposition of the DEUTSCHE POST AG PKI which its used is described in the CP.

1.4 CERTIFICAT USAGE

1.4.1. Appropriate certificate uses

1.4.1.1. End-user Certificates and Key Pairs

The certificates issued by the CA are qualified and advanced electronic certificates. These certificates are used by the physical person subject of the certificate to generate a qualified or advanced electronic signature in remote mode. The generated signatures are compliant with:

- eIDAS Regulation
- ETSI EN 319411-2 level QCP-n-QSCD

The issued certificates may be used to sign documents, for example in PDF Format by its subscribers and could be verified by third parties for authentication reasons.

1.4.1.2. CA or Components Certificates and Key Pairs

Key pair and Certificates of CA Deutsche Post AG POSTIDENT E-Signing SUB CA are only used for:

- Issuing certificates for end-users
- Issuing CRL
- Optionally issuing certificates for OSCP servers.

1.4.2. Prohibited certificate uses

Any usage that is not explicitly described in the above section is prohibited.

1.5 POLICY ADMINISTRATION

1.5.1. Organization managing the document

The entity responsible for the administration and management of the CPS is the GA. The GA is responsible for the development, monitoring and modification of this CPS as soon as necessary.

1.5.2. Contact

The GA is the entity to contact for any questions concerning this CP.

Herr Steffen Ferrari

Deutsche Post AG
VATDE-169838187
Charles-de-Gaulle-Str. 20
53113 Bonn

Oder

postident@deutschepost.de

1.5.3. Entity determining CPS suitability for the Certificate Policy

In order to determine the compliance of the CPS with the current CP, the GA relies on internal or external DEUTSCHE POST AG specialists specialized in auditing and evaluating the safety of services and products.

DEUTSCHE POST AG has implemented several approval phases in every pre-publishing phase of this CPS, ensuring a high quality of CPS content and in minimum at least a four eyes principle before a new version of this CPS may be published.

The conformity of the delegated Registration Authority to this CPS is guaranteed, as it is an internal part of the Deutsche Post DHL group (Deutsche Post Customer Service Center GmbH).

1.5.4. CPS Approval Procedure

CP/CPS modification approval follows a formal audit procedure targeting the scope of the CP/CPS concerned by the modification.

The procedure of update and approval of the CPS is described within an internal document, living a well-managed internal document release process, called « Kompass » in Deutsche Post AG POSTIDENT E-Signing SUB CA.

1.6 DEFINITIONS AND ACRONYMS

1.6.1. Acronyms

Acronyms	Meaning of the acronym
ARL	Authority Revocation List
CA	Certification Authority
CC	Common Criteria
CEN	Comité Européen de Normalisation [European Standardization Committee]
CO	Certification Operator
CP	Certification Policy
CPS	Certification Practice Statement
CR	Certification Representatives
CRL	Certificate Revocation List
CSP	Cryptographic Service Provider
DN	Distinguished Name
EAL	Evaluation Assurance Level
ETSI	European Telecommunications Standards Institute
GA	Governance Authority
HRA	Head of Registration Authority
HSM	Hardware Security Module
KC	Key Ceremony
OCSP	Online Certificate Status Protocol

Acronyms	Meaning of the acronym
OID	Object Identifier
OR	Organization Representative
PP	Protection Profile (PP)
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure – X.509
RA	Registration Authority
RSA	Rivest Shamir Adelman
TA	Time-stamping Authority
TSP	Trust Service Provider
URL	Uniform Resource Locator

1.6.2. Definitions

Third Party Applications:

Application services using Certificates issued by the CA, for example, for electronic signature or signature verification purposes.

Authentication:

Action aiming at verifying the identity of a natural or legal person or/and the origin of a communication.

Certificate Authority (CA):

Entity issuing certificates and which is responsible for the electronic Certificates Issued and signed on its behalf in accordance with rules defined in its CP and in its associated CPS.

Note:

The CA may operate itself its own infrastructure or have it managed by an Certification Services Operator (CSOs or CO) with secure facilities, staff and technical infrastructure to enable it to perform all of the certificate management tasks on behalf of the CA.

Root Certification Authority (RCA):

An entity that has a PKI enabling it to register, generate, issue and revoke Certificates for CAs, in accordance with own CP and CPS defined by its GA.

Registration Authority (RA):

An entity with a set of resources (IT and human resources) to manage the relationship between CA and Certificate Holders. The role of the RA is to verify the identity of the future Certificate Holder.

Governance Authority (GA):

Entity responsible for all functions of the DEUTSCHE POST AG PKI with decision-making authority.

Key Pair:

Public key / private key couple.

Key Ceremony (KC):

Special meeting of authorized persons to generate the CA or Client Certificate (KC Client). The key pair of this Certificate must be generated with all necessary precautions (see CPS) to avoid any compromise.

Digital Certificate:

Electronic file attesting that a key pair belongs to the physical or legal person or to the material element identified, directly or indirectly (pseudonym), in the Certificate. This file is is issued by a CA. By signing the certificate, the CA validates the link between the identity of the physical or legal person or the material element and the key pair. The Certificate is valid for a specific period of time specified in it.

Encryption:

Cryptographic transformation of a (clear) data set to produce an encrypted set (called cryptogram).

Client:

A client is an entity that has decided to subscribe to the DEUTSCHE POST AG Service for its own purposes or in a way to make the service available to its own customers.

See also Certificate Holder.

Component of the PKI

A platform operated by an entity consisting of at least one computer station, an application and, where appropriate, a means of cryptology and playing a determined role in the operational implementation of at least one function of the PKI.

Confidentiality:

Property of information or resource to be accessible only to authorized users (creation, dissemination, backup, archiving, destruction).

Decryption:

Transformation of a cryptogram to retrieve the original data in plain text

Certification Pratice Statement (CPS):

A document that identifies the practices (organization, operational procedures, technical and human resources) that a CA applies in the provision of its electronic certification services to and in compliance with the PC(s) it has undertaken to comply with.

Time-stamping:

A service that reliably associates an event and a time in order to reliably establish the time at which that event has occurred

Public Key Infrastructure (PKI) :

A set of components, functions, and procedures dedicated to the management of cryptographic keys and their Certificates used by trusted services. A PKI can be composed of a CA, a CO, a centralized and / or local RA, a CR, an archiving entity, a publishing entity.

Integrity:

Property of accuracy, completeness and inalterability over time of the information and functions of the processed information.

List of revoked CA certificates (ARL)

A list of revoked CA certificates that have been revoked before the end of their period of validity.

Certificate Revocation List (CRL):

A list of revoked end-user certificates that have been revoked before the end of their period of validity.

Hardware Cryptographic Module (HSM):

An electronic hardware providing a security service consisting of generating, storing and protecting cryptographic keys.

Online Certificate Status Protocol (OSCP):

A protocol that allows a person or an application to verify the validity of a certificate in real time, especially if it has been revoked.

Non-repudiation:

Impossibility for a Holder, User or User Application to deny participation in an exchange of information; this participation concerns both the origin of information (accountability) and its content (integrity).

PKIX (Public Key Infrastructure – X509):

IETF (Internet Engineering Task Force) working group aiming to facilitate the development of PKIs based on the X.509 standard for internet applications. PKIX has produced standards such as X.509 extensions for the Internet, OCSP, etc.

Certification Policy (CP):

A set of rules, identified by a name (OID), defining the requirements that a CA follows in setting up and providing its services and indicating a Certificate's applicability to a particular community and/or a class of applications with common security requirements. A CP may also, if necessary, identify obligations and requirements for other stakeholders, including Holders and Third Party Applications.

Certificate Holder:

A physical person whose identity appears in a Certificate ("Subject" field) issued by the CA and who must comply with the conditions set out in this CP.

Security product:

Software and/or hardware device, which is required to implement security functions securing dematerialized information (during an exchange, processing and/or storage of this information). This generic term covers, in particular, electronic signature devices, authentication devices and confidentiality protection devices.

Application developer:

Supplier of a secure service offer (dematerialized exchanges).

Customer Representative:

An individual who has a contractual/hierarchical/regulatory relationship with the client entity and is the representative of the legal entity identified in the Certificate.

Head of Registration Authority (HRA):

Individual in charge of the RA.

DEUTSCHE POST AG **Service:**

One of the digital trust service provided by DEUTSCHE POST AG, that may be partially or completely deployed.

Electronic signature or Signature:

"Use of a reliable identification process guaranteeing its connection with the act to which it relates", in accordance with the French Civil Code.

Uniform Resource Locator (URL):

A website address.

User:

See « Third Party Application»

2. PUBLICATIONS AND REPOSITORY RESPONSIBILITIES

2.1 IDENTIFICATION OF ENTITIES OPERATING REPOSITORIES

The entity in charge of the publication of the repository is Deutsche Post AG POSTIDENT E-Signing SUB CA.

- Deutsche Post AG is in charge of providing the applicable documents: CP, CPS, Terms & Conditions, CA certificates
- Deutsche Post AG is in charge of controlling a supplier who provides the information function regarding the state of certificates, i.e. the operation of the OCSP server.
- Deutsche Post AG is also in charge of the publication of the information and the documents published on www.postident.de.

2.2 INFORMATION TO BE PUBLISHED

In conformity with the corresponding CP, the following CA information is published:

- Deutsche Post AG POSTIDENT E-Signing SUB CA Certification Policy
- This CPS
- Terms & Conditions and related documents of the service
- The PKI Disclosure Statement of the service
- The valid certificate chain of the Deutsche Post AG POSTIDENT E-Signing SUB CA, the corresponding CP and CPS of each certificate of the chain, and any other attached documents, until the Root CA certificate. For the present CA, this includes at least:
    - The certificate of the Root CA
    - The hash of the Root CA certificate
    - The ARL issued by the Root CA
    - The certificate of Deutsche Post AG POSTIDENT E-Signing SUB CA
    - The CP of Deutsche Post AG POSTIDENT E-Signing SUB CA

Notice that the present CPS is published. However, the published version of the CPS may differ from the CPS used internally for the operations. The internal version may only contain extra information that is confidential and that should not be published. However, in the specific case of an audit, a control or according to a legal request, the CA will provide the confidential version of the CPS and the complete list of procedures and documents described in this CPS.

The initial publication procedure of the documents named above is generally orientated on the main approval process of Deutsche Post AG, as described in 1.5.3. A Difference occurs in additional review and approval steps of external experts and auditors before its initial publications.

2.3 TIME OF FREQUENCY OF PUBLICATION

Time of frequency of publication depends on the type of information:

- CP and CPS are published as soon as the document is validated, and in a maximal delay of 72 opening hours after the formal validation of documents. The valid CP is published before the first transmission of an end-user certificate.

CA certificates are published 72 hours prior to any corresponding transmission of certificates.

Certificate status information, *i.e.*, via OCSP, is available 24/7.

Deutsche Post AG POSTIDENT E-Signing SUB CA has setup a Business Continuity and Disaster Recovery Plan (BCP/DRP). The scope of this plan includes the continuity of the publication of the repository information.

2.4 ACCESS CONTROL TO PUBLISHED INFORMATION

Published information is available to third parties on read-only mode.

All other operations such as adding, deleting, modifying or updating information is only allowed to authorized person or system of the Deutsche Post AG POSTIDENT E-Signing SUB CA.

The right management of the repository and in particular the list of people authorized to perform such operation is described within Deutsche Post AG POSTIDENT E-Signing SUB CA internal procedures.

3. IDENTIFICATION AND AUTHENTIFICATION

3.1 NAMING

3.1.1. Types of names

The names used in the Certificates issued by Deutsche Post AG POSTIDENT E-Signing SUB CA comply with the specifications of X.500.

Each entity is identified by a "Distinguished Name" (DN), within the subject field of the certificate. This DN allows distinguishing a subject easily to one another and this DN is unique for a given CA.

DN is encoded in printable string may use specific German characters and is not empty

3.1.2. Need for names to be meaningful

The names chosen to designate the certificate holder are explicit and contain all the necessary information allowing the identification of the subject. This information is present in the Subject DN field of the certificate.

The information within the Subject DN field is explicitly defined as follows:

For the end-user certificate, this information is explicit:

- The name of the CA representing the level of service of the issued certificate
- The certificate holder identity, appearing within the CommonName (CN) field of the Subject DN in conformity with the following structure: “NAME LASTNAME IDENTIFIER”. Rules for constructing this CN field are described in the CP.
- The country where the CA is registered.

The exact format of the "Subject DN" of the Holder’s Certificates is specified with field :

CN = <FirstName><LastName>

C = DE

SERIALNUMBER = PI:DE-< Vorgang-ID>

givenname = <FirstName>

surname = <LastName>

Vorgang-ID (=Process ID) is unique over all signatures applied by Deutsche Post.

3.1.3. Anonymity or pseudonym of Subscribers

Certificates of the Holders cannot be anonymous. The use of a pseudonym is prohibited.

3.1.4. Rules for interpreting various name forms

The rules for interpreting the various forms of names are explicit and therefore, no specific rules are needed to interpret the various name forms.

3.1.5. Uniqueness of names

The different cases of homonymy are taken into account by the CA. The CA ensures the uniqueness of names for the issued certificates.

For that, the unicity of the issued certificates is obtained by the CN field of the certificate containing:

- The name
- The last name
- A unique identifier.

Moreover, all certificates issued by the CA include a unique serial number within the CA domain, ensuring that each certificate is technically unique within the CA domain.

In case of certificates which are used for the described signing purposes of natural persons, this GUID is called: ´ProcessID´ or its translated expression in German ´VorgangID´ which is unique over all signatures applied by Deutsche Post. For more details also see the certification profiles in the CP in chapter 7.2.

3.1.6. Recognition, authentication, and role of trademarks

The RA ensures as much as possible the suitability of the names and trademarks appearing in a certificate application.

3.2 Initial Identity Validation

3.2.1. Method to prove possession of private key

The sole control of the user over his private key is enforced with a two-factor authentication. The first factor is established with the identification process and the second factor is achieved with the mTAN authentication of the certificate holder.

3.2.2. Authentication of organization identity

Not applicable. Only certificates for natural persons are issued.

3.2.3. Authentication of natural person identity

The authentication of the identity of a future certificate holder must be validated with either of the following methods:

- By a face-to-face video meeting (POSTIDENT durch Video) with a human operator. This video identification could be performed by using mobile devices as e.g. smartphones via a mobile app, or with the help of classical web browser and a PC. The validation of the identity of a Holder is based on the information and the picture contained on the identity document provided as evidence by the applicant.

Admissible documents are a National Identity Card, a Passport or a Residence Permit. The documents submitted must be valid at the time of application.

- By usage of personal data that was obtained at an earlier point in time according to VDG §11 (4). The personal data can be provided by a business client of Deutsche Post AG. Deutsche Post AG ensures that the business client has processed the identification in compliance with VDG §11 and has implemented all the necessary security measures.

- By the online ID function of the German ID card (POSTIDENT durch Online-Ausweisfunktion). For this purpose, the private customer uses his identity card with activated online ID function as well as his 5-digit transport PIN (received after activation of the online ID function) or his personal 6-digit PIN (assigned by the user himself). Furthermore, the private customer needs an NFC-enabled smartphone (Android device or iPhone).

The information also necessary to make an application for a certificate for a natural person is:

- First and last name of the Holder;
- The place of birth of the Holder;
- The Holder's date of birth;
- A postal address and/or an email address and a mobile phone number;

The Applicant must also view the Terms and Conditions of the service and shall accept them.

3.2.4. Non-verified subscriber information

Not applicable in the scope of this CPS.

3.2.5. Authentication of individual identity

See CP chapter 3.2.5.

3.2.6. Criteria for interoperation

See CP chapter 3.2.6.

3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY & UPDATE REQUESTS

3.3.1. Identification and authentication for routine re-key & update

Renewal procedures of certificates are not applicable, because the scope of this CPS is limited on one time certificates.

3.3.2. Identification and authentication for re-key after revocation

Renewal procedures of certificates are not applicable, because the scope of this CPS is limited on one time certificates.

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

3.4.1. Request originated by the holder, or the subscriber for the certificate

A certificate holder could ask for a revocation of its certificate by writing a letter under naming the reason of revoking to

Deutsche Post AG
c/o POSTIDENT E-Signing
Charles-de-Gaulle-Str. 20, 52113 Bonn

or via E-Mail to

postident@deutschepost.de

After proving conformity of these reasons certification service operator authorized personnel will connect to the PKI interface, performing a research of the certificate to be revoked. After this a revocation operation of the selected certificate will be performed. The identification and authentication aspects of such requests are described in section 4.9. However, as the lifetime of certificates described in this CPS is in any way no longer than 15 minutes, a revocation request by its holder would be a more or less theoretical issue.

A revocation of a certificate will be performed within 24 hours after Deutsche Post AG POSTIDENT E-Signing SUB CA has received all necessary information (see section 4.9. for former details).

3.4.2. Request from the CA or GA

In case of emergency, the Certification Authority or the Governance Authority may revoke a certificate.

The CA, or GA send revocation request to its known certification service operator by naming reasons of revoking. After proving conformity of these reasons certification service operator authorized personnel will connect to the PKI interface, performing a research of the certificate to be revoked. After this a revocation operation of the selected certificate will be performed. The identification and authentication aspects of such requests are described in section 4.9.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE APPLICATION

4.1.1. Origin of an application for a certificate

A certificate can only be requested if the future certificate holder is performing the identification process, as described in chapter 3.2 before. An indispensable presupposition for this request is a concrete requirement for an authenticated signing process of a document by a business partner of the Deutsche Post Ag.

4.1.2. Enrolment process and responsibilities

The applicant is responsible for the information and evidence provide to the Registration Authority. Based on this information, the RA:

- completes the application form in the presence of the holder
- validates the submitted evidence
- validate the request and triggers the technical procedures for requesting a certificate.

During the process the Provider specifies the unique name of the Subject and assigns a globally unique ID (OID) to the Subject. This happens as defined in section 3.1.

The Provider registers all the necessary information on the identity of the Subject and the Organization for the provision of service and for keeping contact.

The Provider registers the service agreement signed beforehand by the Subscriber that shall contain the Subscriber ’s statement that the Subscriber is aware of its obligations and undertakes the compliance.

The Provider registers the Certificate Application signed by the Subject – in case of an Organization, its representative – which shall contain the following:

- a confirmation, that the data provided in the Certificate Application are accurate;
- a consent, that the Provider records and processes the data provided in the application;
- the decision about the disclosure of the Certificate;
- a statement that there’s no brand name or trademark indicated in the requested Certificate,

or it is indicated and the applicant is entitled to use that.

The Provider keeps the aforementioned records for the time period required by law.

The Provider archives the contracts, the Certificate application form and every attestation that the Represented Organization, the Subject or the Subscriber handed in.

If the identity of the Subject – in case of an Organization, its representative – or in case of an Organizational Certificate the identity of the Organization or in case of an Organizational Certificate issued to a natural person , the Subject's inherency to the Represented Organization cannot be verified without a doubt or any of the indicated data on the Certificate application form is incorrect, then the Provider can, according to its inner regulations give the Client the opportunity to correct the missing or incorrect data, and to the hand over the missing attestations within 3 months from the submission of the Certificate Application.

4.2 CERTIFICATE APPLICATION PROCESSING

4.2.1. Implementation of the identification process and application validation

The Registration Authority must validate the identity of the applicant by ensuring the consistency of the evidence presented. In particular, it checks that the evidences are valid.

The registration procedure and the steps to validate the certificate are described in CA internal procedures.

4.2.2. Acceptance or rejection of application

As long as the application data is not validated by the Registration Authority, no certificate request is triggered.

If the identity of the natural person which is to be identified, cannot be verified without a doubt then the RA rejects the application.

4.2.3. Time to process certificate application

Once the application form is validated by the Registration Authority, the key pair generation and certificate issuance is triggered. This phase is carried out by the Registration Authority.

4.3 CERTIFICATE ISSUANCE

4.3.1. CA Actions during certificate Issuance.

The RA triggers:

- Key pair creation within the QSCD and the association of the key pair with an authentication mean.
- The technical certificate request to the PKI

The following steps are performed in an automatic way:

- Key pair creation within the QSCD and the association of the key pair with an authentication mean.
- certificate request generation and transmission to the PKI
- certificate signature by Deutsche Post AG POSTIDENT E-Signing SUB CA

- Installation of the certificate within the QSCD

4.3.2. Notification to Subscriber by the CA of issuance of Certificate

See CP chapter 4.3.2

4.4 CERTIFICATE ACCEPTANCE

4.4.1. Conduct constituting Certificate acceptance

Acceptance of the certificate is implicit. Deutsche Post AG POSTIDENT E-Signing SUB CA considers the following as implicit acceptance of the certificate:

- Download of a signed document containing the certificate.
- Absence of disputes within 24 hours after the certificate issuance.

4.4.2. Publication of the Certificate by the CA

Certificates issued by the Deutsche Post AG POSTIDENT E-Signing SUB CA are not published.

4.4.3. Notification of Certificate issuance by the CA to other entities

The CA informs the Registration Authority concerned with the deliverance of the certificate via the CA API.

4.5 KEY PAIR AND CERTIFICATE USAGE

4.5.1. Subscriber private key and certificate usage

See CP chapter 4.5.1

4.5.2. Relying Party public key and Certificate usage

See CP chapter 4.5.2

4.5.3. Root CA public key and Certificate usage

See CP chapter 4.5.3

4.5.4. CA public key and Certificate usage

See CP chapter 4.5.4

4.6 CERTIFICATE RENEWAL

See CP chapter 4.6.

4.7 CERTIFICATE RE-KEY

A change of key pair may be performed following the revocation of an existing Certificate (see 4.9 « Revocation AND suspension of certificates »).

4.7.1. Possible cause of a re-key

See CP chapter 4.7.1

4.7.2. Origin of a re-key application

See CP chapter 4.7.2.

4.7.3. Processing of a re-key application

See CP chapter 4.7.3.

4.7.4. Notification of the issuance of the new certificate

See CP chapter 4.7.4.

4.7.5. Acceptance procedure for the new certificate

See CP chapter 4.7.5.

4.7.6. Publication of the new certificate

See CP chapter 4.7.6.

4.7.7. Notification by the CA to other entities

See CP chapter 4.7.7.

4.8 CERTIFICATE MODIFICATION

Certificate modification - *i.e.* modification of certificate information without change of the public key, excluding the modification of validity dates, see [RFC3647] - is permitted and not in the scope of this CPS.

4.9 REVOCATION AND SUSPENSION OF CERTIFICATES

Deutsche Post AG POSTIDENT E-Signing SUB CA does not implement a process to suspend Certificates.

4.9.1. Circumstances for revocation

4.9.1.1. End-user certificates

See CP chapter 4.9.1.1

4.9.1.2. PKI Component Certificates

See CP chapter 4.9.1.2.

4.9.2. Origin of a revocation request

4.9.2.1. End-user Certificate

See CP chapter 4.9.2.1

4.9.2.2. PKI Component Certificate

See CP chapter 4.9.2.2.

4.9.3. Procedure for processing a revocation request

4.9.3.1. End-user Certificate

Requirements related to the identification and validation of a revocation request is defined in section 3.4 – "Identification and authentication for revocation request".

The revocation request shall at least contain the following information's:

- Identity of the Subject identified in the certificate to be revoked
    - Identity of the requester, which means at least
    - Name and surname
    - Full address
    - Telephone contact channel for queries
    - Handwritten signed revocation request
- Any additional information allowing to find the certificate to be revoked without ambiguity, which means at least
    - The serial number of the certificate and all information from the "Subject" field. This information can be obtained with the help of a PDF viewer application.
- Revocation reason.

The information described here is required so that any expiry of a revocation deadline does not start until all necessary information is available.

However, a signed contract which has been formerly signed by a certificate, will not be legally invalid within the revocation of a certificate.

Notice the revocation reason is not published within the CRL. However, it may be kept in the internal database of the RA or of the CA.

Events related to revocation life-cycle are logged.

Details of revocation procedures are documented in the CA internal procedures.

4.9.3.2. Revocation of a PKI component certificate

See CP 4.9.3.2.

4.9.4. Delay for requesting a revocation

See CP 4.9.4.

4.9.5. Delay for processing a revocation request

4.9.5.1. End-user revocation.

See CP 4.9.5.1.

4.9.5.2. Revocation of a PKI Component Certificate

See CP 4.9.5.2

4.9.6. Revocation checking requirement for Relying Parties

See CP 4.9.6.

4.9.7. CRL Issuance Frequency

Not applicable, because Deutsche Post AG POSTIDENT E-Signing SUB CA will only use OCSP Services.

4.9.8. Maximum delay for CRL publication

Not applicable, because Deutsche Post AG POSTIDENT E-Signing SUB CA will only use OCSP Services.

4.9.9. On-line revocation status availability

See CP chapter 4.9.9.

4.9.10. On-line revocation status requirement

See section 4.9.6 « Revocation checking requirement for Relying Parties » above.

4.9.11. Other forms of revocation advertisements available

Not applicable

4.9.12. Special requirements regarding key compromise

In case of compromise of the private key of a CA, the revocation of the corresponding certificate is revoked.

In this case, the Deutsche Post AG POSTIDENT E-Signing SUB CA will inform the RAs concerned as soon as possible and will revoke all the certificates issued by the CA whose certificate is to be revoked.

DEUTSCHE POST AG will also publish on its website clear information concerning the revocation of this certificate. This publication will be validated by the DEUTSCHE POST AG communication department.

The supervisor body is notified by the DEUTSCHE POST AG within 24 hours following the procedure published by the supervisory body.

4.9.13. Circumstances for suspension

Not applicable.

4.9.14. Who can request suspension

Not applicable.

4.9.15. Procedure for processing a suspension application

Not applicable

4.9.16. Limits of Certificate Suspension Period

Not applicable

4.10 Certificate Status services

4.10.1. Operational characteristics

See CP chapter 4.10.1

4.10.2. Service availability

The certificate status information feature is available 24/7.

The architecture in place has been setup to target

- a minimal 99,5% availability of the Publication server,
- a minimal 99% availability of the OCSP server.

The architecture in place to ensure such availability rate is described in the CA internal documentation.

4.10.3. Optional features

Not applicable

4.11 End of subscription

See CP chapter 4.11.

4.12 KEY ESCROW AND RECOVERY

4.12.1. Recovery and practices in case of key escrow

Not applicable.

4.12.2. Recovery and practices in case of session key encapsulation

Not applicable

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

Several controls are setup to ensure a high level of security and confidence for the CA operations.

5.1 PHYSICAL CONTROLS

Physical controls are setup on the operational site. This site hosts:

- The PKI "Bunker". The critical PKI services are operated within this bunker.
- The Card Management System service, that is a technical RA used by the CA processes and that handles the certificate life cycle. This service is hosted in the server room.
- The Secured Key management service of the CA. This critical service is also operated within the bunker.

The person responsible for this operation site shall respect the rules and principle that are defined in the security policy of the physical site.

The operational site is declared in conformity with APSAD R81 rule (Intrusion Detection System).

Operational procedure derived from the above rule and from the PKI list of requirements is documented in an internal document. This document describes:

- General principles of protection of the site
- General principles of protection of the facilities
- General principles of the protection of the restricted areas
- Access control mechanism and access modalities
- Fire protection mechanism
- Protections against flooding
- Power supply
- Air conditioning.

5.1.1. Site location and construction

Several security area are used according to the type of security component that is used by DP CA, All these area are protected through numbered zones:

- Faraday cage: These very highly secure areas are used to operate software/hardware used by component services like Certificate Generation Services, and Time-Stamping Services.
- Bunker: Highly secure areas used to operate RA services and OCSP responder,
- Front end premises: used for to operate front end web publication server.

All these area are equipped with physical and logical security protection that prevents illegitimate access, including internal and external intrusion detection systems, internal and external video surveillance system,

access control system with dual control. Further description of the site is documented in the CA internal documentation.

5.1.2. Physical access

Physical access is controlled by several physical security controls and procedures. In particular physical access is restricted by implementing mechanisms to control access from one area to another or access into high-security zones, such Faraday cages, and bunkers, all secure area are physically monitored and supported by security alarms and requiring movement from zone to zone to be accomplished using a token, and biometric readers.

Highly secure areas are protected against unauthorized access by at least three (3) perimeters protections, allowing access for only one person at a time and under dual control.

Access to the secure areas is limited to authorized personnel listed on an access list, which is subject to audit and control.

Additional detailed description of these measures is confidential and documented in the CA internal documentation.

5.1.3. Power and air conditioning

Power and air conditioning supplies are scaled and duplicated to ensure that the CA is operated in correct conditions and to ensure the availability of the services provided by the CA.

The detailed description of these measures is confidential and documented in the CA internal documentation.

5.1.4. Water exposures

Secure areas are protected from any water exposures.

More detailed description of these measures is confidential and documented in the CA internal documentation.

5.1.5. Prevention and fire protection

Fire protection mechanisms are in place to prevent potential damages caused by fire in the secure areas.

The detailed description of these measures is confidential and documented in the CA internal documentation.

5.1.6. Media Storage

All media containing sensitive data (e.g. disk, CD-ROM) along with sensitive paper documents (Key Ceremony script and reports, registration folder …) are stored within secure vault and safe that protect them from potential external attacks (including fire and humidity).

The CA also ensures that sensitive data are backed up in a way that ensures:

- Access to the data during the whole retention period;
- Availability and integrity of the data, allowing to replay them during the whole retention period;
- Protection against obsolescence of media
- Availability of the stored evidence, if necessary.

The detailed description of the applicable measures is confidential and documented in the CA internal documentation.

5.1.7. Waste disposal

At the end of life, the media will either be destroyed or reinitialized for reuse, depending on the level of confidentiality of the corresponding information.

The procedures related to destruction and to the reuse of media are confidential and documented in the CA internal documentation.

In particular, hard disks involved in the Key Ceremony are in the scope of these procedures.

Documents in paper forms, and particularly confidential documents are destroyed in a systematic way with a shredder before being sent to the waste-disposal system of the site.

5.1.8. Off-site backup

In addition to site backups, the PKI components implement offsite backups of their applications and information. These backups are organized to ensure the fastest recovery of incident services.

Backup is tested on a regular basis and allows the execution of the disaster recovery plan.

Details of backup management is provided in the disaster recovery plan.

5.2 PROCEDURAL CONTROLS

5.2.1. Trusted Roles

The trust roles defined below are those required for the PKI components:

- PKI Security Officer - The Security Officer is responsible for the implementation of the security policy of Deutsche Post AG POSTIDENT E-Signing SUB CA. It manages the physical access controls to the entity's equipment systems. It is empowered to look at the records kept, and is responsible for the analysis of the event logs in order to detect any incident, anomaly, attempted compromise, etc.

- Application manager - The application manager is responsible, within the component of the PKI concerned, for the implementation of the various CPs and CPSs of the CA Deutsche Post AG POSTIDENT E-Signing SUB CA. Its responsibility covers all the functions rendered by the applications and the corresponding performances.

- System engineer - It is responsible for the start-up, configuration and technical maintenance of the IT equipment of the entity. It provides technical administration of the entity's systems and networks.

- Operator - An operator within the component of the PKI concerned carries out, within the scope of his attributions, the operation of the applications for the services delivered by the component of the PKI.

- Controller - A designated person whose role is to analyze logs and incidents related to the PKI. The controller is independent of other trust roles.

All tasks, roles and responsibilities with respect to Deutsche Post AG POSTIDENT E-Signing SUB CA services are described in job descriptions and made available to the concerned personnel.

These job descriptions are defined from the view point of segregation of duties and least privileges, determining position sensitivity based on the duties and access levels, background screening and employee training and awareness.

5.2.2. Number of persons required per task

Where dual control is required at least two trusted staff members need their respective and split knowledge in order to be able to proceed with the on-going operation.

For tasks related to critical CA functions such as but not limited to key management and in particular CA key generation, at least two persons are required.

The restoration of a HSM is only possible if a minimal number of Key Custodian is present.

Access to the bunker area is only possible with dual control of authorized trusted role.

Each member of the personnel staff are issued a Smart Card and Pin code in order to ensure proper identification and authentication prior being allowed to perform any trusted action.

All actions can be attributed to the member of the staff that has performed the action.

More identification and authentication modalities of Trusted Roles are confidential and documented in the CA internal documentation.

This documentation covers at least all the roles described in the CP.

5.2.3. Roles requiring separation of duties

The same physical person may perform several roles, under the condition that the cumulative effect of the role does not impact the security of the PKI functions. However, it is recommended that the same physical person does not cumulate several Trusted Roles. The following rules concerning the segregation of duties shall at least prohibit the following cumulative:

- Security officer and systems engineer/operator,
- Controller and any other role,
- System engineers and operators.

The CA maintains a nominative inventory of the roles in the CA internal documentation. This inventory is confidential.

5.3 PERSONNEL CONTROLS

5.3.1. Qualifications, experience, and clearance requirements

All personnel required to work in a position identified as sensible is subject to a confidentiality clause.

The head of the CA ensure that the attributions of his/her personnel, who are required to work at the positions, correspond to their professional competencies.

Supervisory staff must have the expertise appropriate to their role and be familiar with the security procedures in place within the PKI and the measures related to personal data protection.

Any persons involved in the PKI's trust roles are informed of:

- His/her responsibilities relating to the services of the PKI,

The procedures related to security and control of the system to which he or she must comply.

Personnel in Trusted Role are formally appointed by Head of CA via a written agreement form which is signed by the person in Trusted Role for acceptation.

The qualifications, skills and clearances required for the key ceremony are defined in specific procedures. These procedures are part of the CA internal documentation and are confidential.

Access and authorization are provided based on least privilege policy. The rules and procedures related to access and authorization are documented within the CA internal documentation and are confidential.

5.3.2. Background check Procedures

Personnel required to work within a component of the PKI, and depending on the applicable context, are required to submit a certificate on the honor of a non-conviction, a criminal record, or a confidentiality undertaking.

Persons in Trusted Role must not have conflicts of interest that are prejudicial to the impartiality of their tasks.

In particular, the certification operator ensures that that person in Trusted Role provides:

- A valid copy of an ID document
- An extract of criminal record

The background checks are:

- Performed before the access and authorization are granted
- Reviewed at least every 3 years.

5.3.3. Training requirements

Personnel are trained in the software, hardware and internal operating and security procedures that they implement and which they must comply with within the component of the PKI in which they operate. In particular, CA provides a set of documents, including policies and procedures, to all personnel involved in the PKI.

Staff have knowledge and understanding of the implications of the operations for which they are responsible.

5.3.4. Re-training frequency and requirements

The CA ensures that the concerned staff shall receive adequate information and training in line with the staff tasks. Ca employees may also express their needs regarding training during a face-to-face meeting with management. This face to face meeting is performed every six month and allows planning the future training.

Moreover, a yearly training targeting the new threat and the security procedure is performed to all Trusted Role.

5.3.5. Job rotation frequency and sequence

Job rotation mainly occurs when a change of position or function of an employee in Trusted Role or in an operational role.

Job attribution is reviewed at each internal audit.

5.3.6. Sanction for unauthorized actions

Sanction for unauthorized actions are described in the CA internal documentation and are confidential

5.3.7. External contractors requirements

The staff of external service providers working on the premises of Deutsche Post AG POSTIDENT E-Signing SUB CA and/or on the components of the PKI shall also comply with the requirements of this Chapter 5.3.

This is translated into appropriate clauses in the contracts with the providers.

When applicable, the following clauses may be added to the contract between Deutsche Post AG POSTIDENT E-Signing SUB CA and its subcontractors.

- The subcontractor shall employ for the whole duration of the contract qualified personnel with the adequate professional competencies.

- The subcontractor ensures to maintain an up-to-date knowledge and know-how of its field of operations. The subcontractor shall implement the appropriate information awareness principle to be informed of the best practices to be implemented. The subcontract shall set up training session for its personnel each time the best state-of-the-art practices evolved in a significant way. At least, a yearly training related to new threat and security measures shall be setup.

The subcontractor shall take any necessary measures, in particular regarding its employees, to maintain the confidentiality of any confidential information provided by DEUTSCHE POST AG or any entity involved in the Deutsche Post AG POSTIDENT E-Signing SUB CA.

5.3.8. Documentation supplied to personnel

Security policies and procedures are communicated to Deutsche Post AG POSTIDENT E-Signing SUB CA staff, as soon as the authorization is granted and before they perform their tasks. The subset of communicated policies and procedures is selected with respect to the tasks to be performed. Any person performing an operational task within Deutsche Post AG POSTIDENT E-Signing SUB CA has access to the adequate documentation to perform its tasks.

5.4 AUDIT LOGGING PROCEDURES

See CP for general descriptions of Audit logging procedures. Further details are described in CA internal documentation. This documentation is confidential.

5.5 RECORDS ARCHIVAL

See CP for general descriptions of record archival rules and procedures. Further details are described in CA internal documentation. This documentation is confidential.

5.5.1. Type of records archived

See CP for general descriptions of records archived.

5.5.2. Retention period for archive

See CP for general descriptions of retention periods archived.

5.5.3. Protection of archive

Deutsche Post AG POSTIDENT E-Signing SUB CA ensures:

- implementation of proper copy mechanisms to prevent data loss or data access loss over time and,- that the confidentiality and integrity of the archive and its physical storage media is maintained during its retention period, and

- that records concerning certificates are completely and confidentially.

Archives are accessible to the authorized personnel of the CA and designated auditors.

5.5.4. Archive backup procedures

The level of protection of backups is at least equivalent to the level of protection of the archives. See chapter 5.5.3.

5.5.5. Requirements for time-stamping of records

The precise time of archiving all events, records and documents listed in section 5.4 and

5.5 is recorded. This is accomplished through accurate NTP synchronization of all systems.

5.5.6. Archive collection system

Archive collection systems are internal to the CA component service.

5.5.7. Procedure to retrieve and verify archive information

Archives are accessible to the authorized personnel of the CA, and designated auditors as described in internal documents. Records are retained in electronic or in paper-based format.

5.6 KEY CHANGEOVER

CA Keys shall be changed at most 7 year after their generation during the key ceremony.

Taking into account the expiry date of this certificate, its renewal must be requested within a period at least equal to the lifetime of the certificates signed by the corresponding private key.

As soon as a new key pair is generated and operated, only this new key pair is used to sign certificates. For that, after the successful execution the renewal procedures, the certificate requests are automatically redirected to be signed by the new private key of the CA.

The old CA certificate is afterwards still available to verify the certificates issued with its associated private key, at least until the expiration or revocation of the last certificate issued with this key. Therefore, during this transition period, two CA certificates will be available:

- The old certificate to validate the end-user certificate issued with the associated private key;
- The new certificate to sign and issue new end-user certificates and to be able to validate them.

5.7 COMPROMISE AND DISASTER RECOVERY

Deutsche Post AG POSTIDENT E-Signing SUB CA maintains a Disaster Recovery Plan that covers the requirements regarding the compromise and the disaster recovery. This additional, more granular documentation is confidential.

5.7.1. Incident and compromise handling procedures

If a disaster may occur, Deutsche Post AG takes all necessary measures in order to minimize the damage

resulting from this issue, and it restores the services as quickly as possible.

Based on the assessment of the incident that occurred, it takes the necessary amendments,

corrective measures to prevent future occurrence of the incident.

Once the problem has been resolved, the incident will be reported to all relevant stakeholders.

n the case of a major incident, such as loss, suspicion of compromise, compromise, theft of the private key of Deutsche Post AG POSTIDENT E-Signing SUB CA, the triggering event is the recognition of this incident. The Deutsche Post AG PKI GA is immediately informed. The case of the major incident is imperatively dealt with upon detection and publication of certificate revocation information, where applicable, must be made in the utmost urgency, or even immediately, by any useful and available means.

In the case of a major security incident or integrity loss that may have a major impact DP CA operation or on personal data of the users of the service, Deutsche Post AG will notify the impacted parties. In particular, Deutsche Post AG will notify the Supervisory Body (and, if applicable, the impacted users) within 24 hours after the identification of the incident, as required by eIDAS Regulation.

5.7.2. Recovery Procedures in case of IT Disaster (Hardware, software and data)

Deutsche Post AG POSTIDENT E-Signing SUB CA has a business continuity plan to meet the availability requirements of its sensitive functions.

Disaster recovery resources are established at Two location to avoid that a disaster would corrupt resources at both location. Sufficiently fast communications are established between locations to ensure data integrity. Secured communications infrastructures are established from both locations to the RAs, the Internet, the certificate revocation status.

Disaster recovery infrastructure and procedures are fully tested at least once per 3 year

5.7.3. Entity private key compromise procedures

The case of compromise of an infrastructure key or control of a component of the Deutsche Post AG PKI is treated in accordance with Chapter 5.7.2 « Procedures in case of IT Disaster (Hardware, software and data) ».

In particular, in case of CA Key compromise, Deutsche Post AG:

- will notify all the impacted Clients and Certificate Holders, and will also notifies the impacted third parties.
- will provide in the published information on the status of the certificates that these certificates are no longer valid.
- will immediately revoke the compromised CA certificate.

In case of algorithm compromise, Deutsche Post AG will apply all the above actions excepting the immediate revocation of the CA Certificate. Instead, Deutsche Post AG will setup a planned revocation date for this certificate that will be in line with the state of the art related to the weaknesses of the compromised Algorithm.

5.7.4. Business continuity capabilities after a disaster

The various components of the Deutsche Post AG PKI have the means reasonably necessary to ensure the continuity of their activities in accordance with the requirements of the CP (See. section 5.7.2 « Procedures in case of IT Disaster (Hardware, software and data) »).

Deutsche Post AG has an up-to-date Business Continuity Plan that allows the CA to treact in an effective manner in case of disaster by restoring the IT systems in the delay specified within the Business Continuity Plan. This plan includes the CA Key compromise scenario and the loss of activation data scenario.

5.8 PKI TERMINATION

5.8.1. PKI TRANSFER

If DEUTSCHE POST AG decides to transfer the Deutsche Post AG POSTIDENT E-Signing SUB CA activity, the following organizational steps will be performed:

In the specific case where the transfer implies to stop the operations, for example a change of the Certification Operator, the following steps will be performed:

- The CA will first ensure that CRL and ARL are up-to-date before starting the transfer procedure
- The CA will notify subscribers, client and third parties the temporary non-availability of the certificate issuance service.
- The CA will stop the CA certificate issuance infrastructure.
- The CA will start the new CA infrastructure.
- If necessary, transfer of the secret elements will be securely transferred to new Key Custodians.

The technical operation shall be performed in such a way that the CRL publication is maintained during the whole transfer procedure.

In the specific case where the transfer is simply a transfer of responsibility of the PKI between two entities without any impact on the Certification Operator, only the transfer of secret element to new key custodians shall be performed.

In any case, any activity transfer implies a review and an update of the CA documentation

5.8.2. End of Activity

In case of the end of activity, the CA has to perform the operation described in the Termination Plan.

The termination plan is in line with the requirements in CP chapter 5.8. This termination plan is confidential but audited and revisited meticulously by internal and external auditors.

6. TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1. Key pair generation

6.1.1.1. CA Key Pair

Generation of a new key pair by a CA is only performed during a Key Ceremony (KC). The actions to be performed during a Key Ceremony are described within a Key Ceremony Script. Key Ceremony Scripts are confidential.

6.1.1.2. End-users keys

The End-users private keys for signing certificates are generated inside the cryptographic module of an HSM (Hardware Security Module), as defined in the CEN TS 419-241:2014.

This module is hosted within the Certification Operator premises with strictly restricted access. The keys are of the type RSA and they are generated automatically on request for the user.

6.1.2. Private key delivery to Subscriber

See CP chapter 6.1.2.

6.1.3. Public key delivery to certificate issuer

See CP chapter 6.1.3.

6.1.4. CA public key delivery to Relying Parties

The public CA signature verification keys are made available to certificate users and publicly viewable as defined in Section 2.

6.1.5. Key sizes

See CP chapter 6.1.5.

6.1.6. Validation of the key pair parameters

See CP chapter 6.1.6.

6.1.7. Key usage purposes

See CP chapter 6.1.7.

6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1. Cryptographic module standards and controls

6.2.1.1. Cryptographic Module of the CA

See CP chapter 6.2.1.1

6.2.1.2. End-user Signature Creation Device

See CP chapter 6.2.1.2.

6.2.2. Private key multi-person control

Management of CA HSM and QSCD activation data is described within the CA internal documentation. In particular, the CA maintains a list of key custodians and of the secret under their responsibilities. All procedures regarding the usage of the secret elements are documented.

Private keys of the end-users are under their sole control.

Protection of CA's private keys are, amongst other appropriate measures, ensured by splitting-up of a strong encryption key over several (N) tamper resistant devices (smart card PED keys) that are protected with passphrases.

The CA secret shares are held by multiple authorized holders, to safeguard and improve the trustworthiness of private keys. A certain number of shares ('M' out of 'N'), and at least three ('M' ≥ 2), out of the total shares need to be available and used concurrently to activate or re-activate the CA private key.

Before secret share-holders accept a secret share they must personally have observed the creation, re-creation, and distribution of the share or its subsequent chain of custody. They must receive the secret share within a physical medium, tamper resistant device. The CA keeps written, auditable, records of secret share distribution. In case secret share custodians (or shareholders) are to be replaced in their role of shareholder, the CA shall keep track of the renewed share device distribution.

6.2.3. Private key escrow

Key escrow is never allowed.

6.2.4. Private key backup

CAs' private keys are backed-up, stored and recovered by multiple and appropriately authorized CA trusted roles requiring M of N share holder.

At the end of a key generation ceremony, new CA keys are encrypted on a back-up key storage media (e.g. dedicated and secure backup token) that ensures similar level of protection as provided by the HSM holding CA keys.

6.2.5. Private Key escrow

Neither the CA private keys nor the Holder's private keys are escrowed.

6.2.6. Private Key backup

6.2.6.1. CA Private Keys

Backup copy of the CA is performed. The media and mechanism used to handle the private key ensure a level of protection that is at least equal to the one of the private key. This mechanism is confidential and is described within the CA documentation. In particular, backup procedure is described in the Key Ceremony Script (see 6.1.1.1 - CA Key Pair).

6.2.6.1. End User Private Keys

End-user private key are generated for a one-time signature. Therefore, no backup of the end-user key is performed.

6.2.7. Private key archival

The private keys of the CA are not archived.

The private keys of the Holders are not archived, either by the CA, or by any of the components of the PKI.

6.2.8. Private key transfer into or from a cryptographic module

See CP chapter 6.2.6.

6.2.9. Private key storage on cryptographic module

See section 6.2.1 « Cryptographic module standards and controls ».

6.2.10. Method for Private Key Activation

6.2.10.1. CA keys

At the end of the life of a private CA key, either normal or anticipated (revocation), the key is destroyed, as well as any copy and any element allowing its reconstitution.

The Key destroy is performed using PKI product and HSM product security procedures (using PKCS#11crypto API of the HSM).

In case the HSM is not use any more, the Key destroy of all CA keys within the HSM is done by HSM initialization following the HSM product vendor security procedure, and the physical destruction of the HSM.

All backup of CA private key are destroyed using HSM key backup initialization security procedure provided by HSM product vendor. Furthermore see 6.2.2 « Private key multi-person control ».

6.2.10.2. End user keys

Activation of the Holder's private key is controlled via data or activation actions (see section 6.4 « activation ») that are specific to the holder. Activation is performed in a secure way.

6.2.11. Method for Private Key Deactivation

6.2.11.1. CA Keys

See CP chapter 6.2.9.1.

6.2.11.2. End-user keys

The holder private key is used only once with associated activation code. After the usage of the activation code, the key is automatically deactivated, waiting for its deletion at expiracy of the certificate.

6.2.12. Method for Private Key Destruction

6.2.12.1. CA Keys

At the end of the life of a private CA key, either normal or anticipated (revocation), the key is destroyed, as well as any copy and any element allowing its reconstitution.

6.2.12.2. End-user keys

The keys and certificates are generated for one-time-usage and so the private keys are deleted automatically by the system shortly, not more than 15 Minutes, after they were used. This deletion is performed in a secure way.

6.2.13. Cryptographic module rating

See section 6.2.1 « Cryptographic module standards and controls ».

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1. Public key archival

See section 5.5.

6.3.2. Key pair and certificate usage period

The Key Pair and Certificates covered by this CP have a lifetime of 15 minutes Key Pairs and Certificates have the same lifetime.

6.4 ACTIVATION DATA

6.4.1. Generation and installation of activation data

6.4.1.1. Generation and installation of activation data for the CA Keys

See section 6.2.8.1

6.4.1.2. Generation and installation of activation data for the end-user Keys

The signature activation data are generated on behalf of the end-user. They are provided to the end-user via SMS or push notification in case of identification via online ID. The signature activation data has a length of six characters.

6.4.2. Activation Data Protection

6.4.2.1. Activation Data Protection of the CA Keys

Activation data of the private key of the CA are secret elements generated during the Key Ceremony. At the end of the key ceremony, each secret element is provided to a key custodian, which is in charge of its protection.

Before secret share-holders accept a secret share they must personally have observed the creation, re-creation, and distribution of the share or its subsequent chain of custody. They must receive the secret share within a physical medium, tamper resistant device.

Rules and practiced regarding the protection of the secret elements is described within the CA Documentation. This documentation is confidential.

6.4.2.2. Activation Data Protection of the end-user Keys

Activation data of the end-user private key are protected created on request inside an HSM (Hardware Security Module). They are delivered to the mobile phone of the end-user by SMS or push notification in case of identification via online ID.

For each signature, a new activation data is created.

The mobile phone number of the end-user is protected with a key that is stored on the HSM. This key is generated during a Key Ceremony under dual control.

6.5 COMPUTER SECURITY CONTROLS

6.5.1. Computer-specific technical security requirements

6.5.1.1. Identification and authentication

All system administrators can only connect to PKI infrastructure after a strong authentication based on a certificate stored on a smart card. All system administrators are engaged to respect the rules and practices that are described within the CA Documentation.

6.5.1.2. Access Control

Physical and logical access control management is performed. Physical and logical Access monitoring is managed by security personals witch is not in charge of any administration task.

6.5.1.3. Administration and Operation

All administration tasks are only allowed from secure area, using dedicated administration computed on a closed dedicated network.

6.5.1.4. PKI Component integrity

Penetration testing campaign is performed on PKI components to ensure the application of the security practices and the absence of vulnerabilities.

6.5.1.5. Information flow control

The CA has setup security measures to ensure control of the information flow and flow network change monitoring.

6.5.1.6. Events Journaling and audit

Dashboards are generated and reviewed on a regular basis. These dashboards show, in particular, the following information:

- Operation performed on certificates (issuance, revocation, renewal…)
- Incidents occurring on the PKI components and systems.

6.5.1.7. Monitoring

Monitoring of the PKI components and system is performed by the teams of the Certification Operator in charge of the operation.

6.5.1.8. Security Awareness

The CA has written a set of documents in the aim of developing the security awareness of the employees. This set of documents covers various topics such as:

- Good practices and security measures
- Classification of information and assets
- Protection of the information (in particular confidential information and personal data)

This documentation is provided to all trusted roles.

6.5.2. Level of qualification of computer systems

Not applicable.

6.6 LIFE CYCLE TECHNICAL CONTROLS

6.6.1. Security measures related to system development

Implementation of any system supporting a PKI function of the PKI is documented.

Any implementation is performed in conformity with the CA Security Policy and the requirements defined in the CP associated with this CPS

6.6.2. Security Management measures

Any planned significant change in a PKI component or system shall be notified to the GA to be validated.

The change is documented.

6.7 NETWORK SECURITY

For security reason, the network architecture and the details of the flow matrix cannot be disclosed in a public document and are part of the CA internal documents that are confidential.

This documentation is in line with all the rules and requirements described in the CP chapter 6.7. In particular, the architecture respects:

- The principle of network segmentation
- The security requirements regarding the connection between PKI components and the interconnection with external systems
- The redundancy measures ensuring the availability of the critical components of the PKI

6.7.1. Network Segmentation

Based on the risk assessment result, Deutsche Post AG POSTIDENT E-Signing SUB CA has segmented its systems into separated networks (separation is functional, logical or physical). Deutsche Post AG POSTIDENT E-Signing SUB CA applies the same security controls to all systems co-located in the same zone.

Each PKI component is operated in a secured network area. The component is installed following procedures and configurations guidance ensuring the security of the operation. The most critical components, such as Root CAs, are operated in the most secured areas.

The Deutsche Post AG POSTIDENT E-Signing SUB CA production systems are separated from other systems (development and testing, qualification)

6.7.2. Interconnections

Interconnection to public networks and Interconnection between network area are protected by security gateways configured to accept only the protocols necessary for the functioning of the component within the PKI.

The CA ensures that components of the LAN (eg routers) are maintained in a physically and logically secure environment.

Moreover, exchanges between components within the Deutsche Post AG POSTIDENT E-Signing SUB CA PKI are subject to the implementation of distinct and logically secured channels that ensures identification of its end points and protection of the channel data from modification or disclosure.

6.7.3. Connections

Only employees in Trusted roles can establish an access to the secured network area.

Any connection with a user account able to directly create a certificate is only allowed after a multi-factor authentication. Operational and administrative network are separated. Administrative network is dedicated to administrative functions and is not used for another purpose.

Deutsche Post AG POSTIDENT E-Signing SUB CA has configured all CA systems by removing or disabling all accounts, applications, services, protocols, and ports that are not used in the CA's operations

6.7.4. Availability

To ensure availability of components, Deutsche Post AG POSTIDENT E-Signing SUB CA has implemented redundancy measures allowing a high availability of critical services.

6.8 TIMESTAMPING

Synchronization mechanism of the server operated by the CA used several NTP servers, etch NTP server use several time sources including GPS, and PFZ.

The mechanism in place ensure the requirements described in CP chapter 6.8.

7. CERTIFICATES, OCSP AND CRL PROFILES

7.1 PROFILES OF THE CERTIFICATE OF THE CA.

See CP chapter 7.1.

7.2 END-USER CERTIFICATES

See CP chapter 7.2.

7.3 CRL

See CP chapter 7.3.

7.4 OCSP CERTIFICATE PROFILE

See CP chapter 7.4.

7.5 OCSP RESPONSE PROFILE

See CP chapter 7.5.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

Deutsche Post AG is regularly performing internal audits and revisions by well-known and proven international standards. They are planned and performed by a neutral and independent team of internal auditors of Deutsche Post AG. In addition to this every aspect of the here described CA Operations are audited by external confirmation assessment body accredited by the german supervisory body (Bundesnetzagentur).

9. OTHER BUSINESS AND LEGAL MATTERS

See CP chapter 9.

10. ANNEXE 1 : REFERENCE DOCUMENTS

10.1 LAWS AND REGULATIONS

Reference	Document
[REG_eIDAS]	eIDAS European Regulation

10.2 TECHNICAL DOCUMENTS

Reference	Document
[ETSI_NQCP]	ETSI TS 102 042 V2.1.1 (2009-05) Policy Requirements for Certification Authorities issuing public key certificates
[ETSI_101456]	ETSI TS 101 456 Policy Requirements for Certification Authorities qualified certificates
[ETSI_319401]	ETSI EN 319 401 General Policy Requirements for Trust Service Providers
[ETSI_319411-1]	ETSI EN 319-411-1 Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
[ETSI_319411-2]	ETSI EN 319-411-2 Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
[RFC3647]	IETF - Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practice Framework - 11/2003
[CC]	ISO/IEC 15408 : Common Criteria version 2.1
[X.509]	Information Technology–Open Systems Interconnection – The Directory: Authentication Framework, Recommendation X.509, version 3
[RFC822]	Standard for the format of Arpa internet text messages, August 13, 1982, Revised by David H. Crocker
[RFC5280]	Internet X.509 Public Key Infrastructure, Certificate and CRL Profile, RFC 5280 May 2008
[CWA14167-1]	CWA 14167-1 (2003-06) Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures – Part 1
[CWA14167-2]	CWA 14167-2 (2004-02) Cryptographic Module for CSP Signing Operations with Backup - Protection Profile (CMCSOB-PP)

[CWA14167-4]	CWA 14167-4 (2004-02) Cryptographic Module for CSP Signing Operations with Backup - Protection Profile (CMCSO-PP)
[CWA14169]	CWA 14169 (2003-08) Secure Signature Creation Device, version « EAL 4 +»