Deutsche Post AG POSTIDENT E-Signing SUB CA Certificate Policy

PL
Policy

Domain :	Subdomain:	Reference :	Status :
Security	PKI	"OID" 1.3.6.1.4.1.5064.2.1.1.2.2.2	Final
Validated by :	**Role :**	**Date :**	**Signature :**
Olga Schönfeld	Product Owner	09.05.2023	
Approved by :	**Role :**	**Date :**	**Signature :**
Achim Hügen	Security Architect	09.05.2023	
Diffusion :	.....		
Access :	Public. Available on the website https://www.deutschepost.de/de/p/postident/zertifizierungsrichtlinien.html		
Localisation :	ENG		

Table of Content

Version	Date	Modifications	Author
1.0	05.04.2017	Draft	André Glenzer
1.1	30.06.2017	Final	Achim Hügen
1.2	13.09.2017	Updated conctact Data, Modified OCSP + Certificate URL	Achim Hügen
1.3	28.09.2017	Added GivenName and Surname to Enduser Profiles	Achim Hügen
1.4	16.11.2017	Switched from qualified to advanced certificates	Achim Hügen
2.0	13.06.2018	Added qualified certificates	Achim Hügen
2.1	16.04.2021	Corrected end user profiles: SerialNumber is sequential	Achim Hügen
2.2	14.10.2022	Rework of Chapter 3	Achim Hügen
2.3	09.05.2023	Contact data updated	Olga Schönfeld

Complete Table of Content

COPYRIGHT NOTICE

1. INTRODUCTION

1.1 GENERAL PRESENTATION

As a part of its current expansion of its digital solution portfolio and trust service offerings, Deutsche Post AG operates a Certification Authority available to its client entities (companies, administrations, etc.), Deutsche Post AG POSTIDENT E-Signing SUB CA.

In this context, this document constitutes the Certification Policy (CP) of the Certification Authority (CA) 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).

These certificates may be issued to Deutsche Post AG private endusers of E-Signing offerings, provided by Buisness Clients of Deutsche Post AG. In view to the Buisness Clients Deutsche Post AG is its own Registration Authority, in view to its private endusers see chapter 3.4 in the CPS for details.

The purpose of the CP is to define the requirements for signature certificate 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

in all phases of their life cycle. The Client entity, the owner of such a certificate, will be able to authenticate to the registration authority of Deutsche Post AG to, digitally sign electronic messages, documents or forms, thus ensuring their origin, integrity, and non-repudiation. Implementation of this certificate is provided by an automated service (set of computer servers) duly authorized to use the private signature key representing the legal person of the Client.

This Certification Policy complies with:

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

The issued certificates respect the X.509v3 standard and their use is dedicated to the electronic signature mechanism qualified for physical individuals.

The structure of this PCP is based on the following references: IETF RFC 5280, “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework”, and RFC 3647, “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework”

The following next section illustrates the value of these Certificates in the case of the electronic signature Service offered by Deutsche Post AG.

1.1.1. Signature Service description

Deutsche Post AG offers an electronic signature solution to its business partners who can then offer a qualified electronic signature certificate for signing purposes of electronic documents by their private customers.

1.2 DOCUMENT IDENTIFICATION

This document is the CP of the 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: 1.3.6.1.4.1.5064.2.1.1.2.2.0

This reference appears in all Signature Certificates for physical person issued by the CA Deutsche Post AG POSTIDENT E-Signing SUB CA (cf. section 9.12.2).

1.3 ENTITIES INVOLVED IN THE PKI

The functional decomposition of the Deutsche Post AG PKI which is used in this PC is as follows:

- **Registration Function** - This function verifies the identity of the future Certificate holder, and possibly other specific attributes, before transmitting the corresponding request to the PKI function. It is also responsible, where necessary, for customer re-verification upon renewal of its Certificate. Within the framework of this CP, registration is ensured either by Deutsche Post AG teams on-line, or by the teams of the Client of Deutsche Post AG, contractually bound for this function.
- **Certificate Generation Issuance Function** – This function generates (format creation, electronic signature with private key of the CA) the Certificates from the information transmitted by the Registration Authority and the Client's public key from the Client's secret elements generation function responsible for the creation of the Client's key pair. Within the scope of this CP, the keys are generated on a cryptographic token during the customization phase of the token before their delivery only for signing purposes of the electronic document by the holder.
- **Function for generating and storing the client's secret elements** – This function generates the Client's secret elements and prepares them for secure storage in the cryptographic token. This step is performed by the Registration Authority before the delivery of the token.
- **Delivery Function to the Client** – This function delivers the certificate to the Client as well as the means of control of his private key and his certificate. This function is ensured by the Registration Authority.
- **Publication Function** – This function publishes the CA's policies, certificates and any other relevant information available to the different parties, Clients/carriers and/or Applications using certificates, excluding status information of the certificates. The complete list of Valid Client Certificates is not publicly available.
- **Revocation management function** – This function handles revocation requests (including identification and authentication of the applicant) and determines the actions to be carried out. The processing results are published via the certificate status information function.
- **Certificate status information function** – This function provides information on the status of the certificates (revoked, suspended, etc.) to applications using the issued certificates. This function is implemented thanks to a information publication mode updated permantly on OCSP basis. This certificate status information function is provided by Deutsche Post AG.

The operational implementation of these functions, in particular the Registration Authority, may be delegated. Within the scope of the present CP, a contract is established between Deutsche Post AG and the delegated entity to establish the actions and responsibilities of each party.

1.3.1. Certification Authority (CA)

The Certification Authority (CA) Deutsche Post AG POSTIDENT E-Signing SUB CA is in charge of the provision of services for signature Certificates throughout their lifecycle (generation, diffusion, renewal, revocation). Therefore the CA is identified as the issuer within the Certificates.

1.3.2. Gouvernance Authority (GA)

The **Governance Authority (GA)** is the responsible authority for all the services of the Deutsche Post AG PKI. This authority has Decision-making power within the PKI. It defines and validates the CP and CPS. Concretely, it is one or more representatives of Deutsche Post AG with a specific mandate to ensure this function..

1.3.3. Registration Authority (RA)

The Registration Authority (RA) is a collection of resources (computer and human) aiming at managing the relationship between the CA and the certificate Holders.

the RA ensures:

- the information verification, in particular personal information, presented by the future certificate holder, and the filing of his registration record;
- the preparation and transmission of the Certificate Application to the appropriate function of the CA Deutsche Post AG POSTIDENT E-Signing SUB CA;
- the archiving of the documents in the registration record (or sending to the component responsible for archiving);
- the preservation and protection in privacy and integrity of the Holder entrusted personal data (in particular, it complies with the legislation on the protection of personal data). This is ensured in particular when exchanging such data with the other functions of the PKI.

At a minimum, Deutsche Post AG requires from its Registration Authorities that:

- Verification of applicant identity for a certificate shall be processed according to article 24 (1) of regulation 910/2014 and VDG §11
- The subscriber is aware of and signs the certificate's General Terms and Conditions

The RA therefore establishes the procedures necessary to ensure this level of assurance and ensures its operational implementation.

1.3.4. Delegated Registration Authority (DRA)

The DRA is an entity in contractual relationship with Deutsche Post AG and which performs the function of RA (paragraph 1.3.3) by delegation of Deutsche Post AG CA. In this document the term RA also applies to an DRA.

1.3.5. Client

The Client is the client entity of Deutsche Post AG which has decided to issue qualified and advanced signatures and/or certificates issued by the CA Deutsche Post AG POSTIDENT E-Signing SUB CA, and which it issues to its clients. The Client is contractually bound to Deutsche Post AG.

1.3.6. The Certificate Holder

The certificate holder is the end-user to whom the RA has delivered an electronic certificate and a Cryptographic support.

The certificate holder is either:

- A direct customer of Deutsche Post AG;
- A customer of one of the Clients of Deutsche Post AG

Depending on the case, the Holders may apply for certificates:

- In personal context, this is an application for a special certificate. The certificate, then, displays only identity information to appear in the “Subject” field.

1.3.7. Applications using certificates

Since this PC is dealing with signature and authentication Certificates of a natural person, a Certificate-using application is an application that aims either at:

- establishing an electronic signature;
- Verifying an electronic signature;
- Authenticating the holder of the certificate electronically;

Such applications may include (but are not limited to):

- the Deutsche Post AG signature verification service or an Deutsche Post AG partner that allows information or a document signed with a certificate issued by the CA Deutsche Post AG POSTIDENT E-Signing SUB CA, to verify and display the status of the used certificate or signature;
- the Adobe™ Acrobat Reader ™ application that allows to view a document in PDF format signed by a certificate issued by the CA Deutsche Post AG POSTIDENT E-Signing SUB CA, as well as the cartridge of information about the signatures associated with the document. This application must be configured to accept CA certificates Deutsche Post AG POSTIDENT E-Signing SUB CA;

1.3.8. Other participants

1.3.8.1. Trusted Service Provider Operator (TSPO)

The Deutsche Post AG delegates to his Trusted Service Provider Operator the set of task of:

- Defining the technical infrastructure of the PKI;
- Ensuring the configuration and administration of the PKI components
- Ensuring operation, maintenance in operational condition and supervision of components.

1.4 CERTIFICATE USAGE

1.4.1. Appropriate certificate uses

1.4.1.1. End-user Certificates and Key Pairs

Certificates issued by Deutsche Post AG POSTIDENT E-Signing SUB CA are

- Qualified or advanced electronic signature certificates in accordance with eIDAS regulation

These certificates can be used only for signing purposes of private Holders to sign documents provided by Deutsche Post AG business partners.

1.4.1.2. CA or Components Certificates and Key Pairs

The Deutsche Post AG POSTIDENT E-Signing SUB CA Certificates and Key Pair cannot be used for a purpose other than for the signature of end-user Certificates and CRL.

1.4.2. Prohibited certificate uses

All other uses of certificates issued by CA Deutsche Post AG POSTIDENT E-Signing SUB CA are not covered by this CP and thus remain the responsibility of the Holder.

1.5 POLICY ADMINISTRATION

1.5.1. Organization managing the document

The entity responsible for the administration and management of the certification policy is the GA. The GA is responsible for the development, monitoring and modification of this CP as soon as necessary. To this end, it implements and coordinates a dedicated organization, which decides at regular intervals on the need to make changes to this CP.

1.5.2. Contact

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

Frau Yuldon Klein

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 audit specialists specialized in auditing and evaluating the safety of services and products. An internal document, within the Deutsche Post AG and TSPO organization, specifies the entity ensuring this role.

1.5.4. CPS Approval Procedure

The approval of the compliance of a CPS with this CP is an internal procedure. The GA, is responsible for the management (updating, revision) of the CPS. Any request to update the CPS must follow the approval process in place.

1.6 DEFINITIONS AND ACRONYMS

1.6.1. Acronyms

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
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 in accordance with paragraph 1.3.3 of this CP. 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.

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

For providing availability the published information to Clients and Applications that use certificates and to Certificate Holders, the CA Deutsche Post AG POSTIDENT E-Signing SUB CA implements a publication function and a certificate status information function.

The provision of certificate status information is based on an OCSP mechanism.. Publication addresses are provided in Section 7 « CERTIFICATES, OCSP And CRL Profiles ».

2.2 INFORMATION TO BE PUBLISHED

The CA Deutsche Post AG POSTIDENT E-Signing SUB CA publishes the following information on its site https://www.deutschepost.de/

- This CP, which contains, in particular, the certificate and CRL profiles, the delays and frequencies of publication, the glossary containing acronyms and applicable definitions, main publication addresses);
- the valid certificates of the CAs belonging to the Deutsche Post AG POSTIDENT E-Signing SUB CA, the corresponding CPs and any additional documents;
- the corresponding ARL;
- the general conditions for the use of the Certificates.

The repository is available 24/24 7/7.

2.3 TIME OF FREQUENCY OF PUBLICATION

For the CP, publication is effective as soon as necessary to ensure consistency CA at all times between the published information and the actual commitments, means and procedures of the. 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 and/or CRLs.

Certificate status information, *i.e.*, the Revoked Certificate Lists, is updated within a maximum of 24 hours. Once the update is complete, the CRL is published within a maximum of 60 minutes

2.4 ACCESS CONTROL TO PUBLISHED INFORMATION

The level of confidentiality of all information published is the «public distribution».

The publication function and the certificate status information function ensure the integrity of the published information.

Modification access to publishing systems (addition, deletion, modification of published information) is strictly limited to the authorized internal functions of the CA Deutsche Post AG POSTIDENT E-Signing SUB CA, and to persons duly authorized after authentication by strong authentication means.

3. IDENTIFICATION AND AUTHENTIFICATION

3.1 NAMING

3.1.1. Types of names

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

In each X.509v3 Certificate, the issuing CA and the Subject (Client and/or the Holder) are identified by a "Distinguished Name" (DN). The format of the DN is specified in Section section 7 « CERTIFICATES, OCSP And CRL Profiles ».

3.1.2. Need for names to be meaningful

In the case of “business” certificates, the names chosen to designate the organization are explicit and correspond to the organization name defined on the evidence provided by the subscriber at the time of the Certificate request.

This information is written in the "Object" field of the DN. In addition to this information, the field "Organizational Unit" contains also an identifier of the Holder’s Organization.

In the case of "natural person" certificates, the Holder's identity information is explicit and corresponds to the elements presented on the Holder's proof of identity provided at the time of the certificate request. This information is written in the "Common Name" field of the DN. This field also contains a unique identifier which corresponds to a Deutsche Post AG reference of the Holder.

The exact format of the "Subject DN" of the Holder’s Certificates is specified in Section 7 « CERTIFICATES, OCSP And CRL Profiles ».

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 explained in Section 7 describing the profile of Certificates and CRLs.

3.1.5. Uniqueness of names

Deutsche Post AG maintains a repository identifying on a unitary basis each of the Certificate Holders issued by the CA Deutsche Post AG POSTIDENT E-Signing SUB CA.

This identifier is an integral part of the DN of a certificate and is written in the "Common Name" or in accordance to Laut ETSI 319 411-2 in the field “SERIALNUMBER”.

Deutsche Post AG ensures that this identifier cannot be assigned to any other Holder.

It should be noted that the uniqueness of a Certificate is based on the uniqueness of its serial number within the CA domain but that this number is specific to the Certificate and not to the Client and therefore does not ensure a continuity of the identification in the successive Certificates of a given Client.

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, in particular information relating to the company in the case of a « business » certificate.

3.2 INITIAL IDENTITY VALIDATION

3.2.1. Method to prove possession of private key

The key generation and the certificate issuance operations occur only after identifying the user at the Registration Authority. A proof of possession of the private key is not required, because the key pair is generated on behalf of the certificate holder by the CA Services.

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 processed according to article 24 (1) of regulation 910/2014 and VDG §11 .

3.2.4. Non-verified subscriber information

Not applicable in the scope of this CP.

3.2.5. Authentication of individual identify

In any case, the Registration Authority first validates that the applicant is indeed one of its customers. Moreover, the Registration Authority ensures that the applicant is the future holder or someone mandated by the future holder.

3.2.6. Criteria for interoperation

Not applicable.

3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY & UPDATE REQUESTS

The renewal of the signature or authentication key pair of the Client automatically results in the generation and provision of a new signature Certificate and a new associated key pair. The old card of the Holder is destroyed.

Verification of identity in the context of a key renewal is the same as the initial registration. A new Certificate cannot be issued to the Client without renew it the corresponding key (see chapter 4.6).

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

In the case of renewals, the RA must identify the Client according to the same procedure as for the initial registration, a new certificate application record is then implemented and a new activation code will be given to the Holder.

3.3.2. Identification and authentication for re-key after revocation

In the case of renewals, the RA must identify the Client according to the same procedure as for the initial registration, a new certificate application file is then implemented and a new activation code will be given to the Holder.

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

3.4.1. Request originated by relevant stakeholders

All relevant stakeholders like e.g. he certificate Holder or Subscriber, Registration Authority, the Certification Authority or the Governance Authority cannot access the revocation services directly. They need clarified ways of contacting Deutsche Post AG to access revocation services. These ways should be exactly defined in the CPS.

4. -CYCLE OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE APPLICATION

4.1.1. Origin of an application for a certificate

See CPS for more details.

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
- ensures applicant signs the application form and the Terms and Conditions
- validates the request and triggers the technical procedures for requesting a certificate.

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 exhibits are valid.

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 following phases are then automatic and consist of:

- Generating a key pair on the QSCD;
- Generating certificate request for the PKI

- Signature of the Holder's public key by the CA Deutsche Post AG POSTIDENT E-Signing SUB CA;
- Installing the certificate on the QCSD.

In parallel, an activation code is generated to allow access to the private key of the cryptographic support. This code is transmitted as appropriate:

- Via SMS

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

No additional notification of the subscriber is done.

4.4 CERTIFICATE ACCEPTANCE

4.4.1. Conduct constituting Certificate acceptance

Upon delivery of the support to the Holder, the Holder must sign a receipt of the certificate and key pair. This receipt is kept by the RA and then sent to the Certification Authority.

4.4.2. Publication of the Certificate by the CA

Certificates issued by the CA 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 Deutsche Post AG POSTIDENT E-Signing SUB CA informs the Registration Authority concerned with the deliverance of the certificate.

4.5 KEY PAIR AND CERTIFICATE USAGE

The private key can be used for signing a document. After the document has been signed the private key is destroyed by the CA.

Relying parties can use the certificate contained in the signed document to verity the validity of the signature.

4.5.1. Subscriber private key and certificate usage

The use of the Holder’s Private Key and the associated Certificate is strictly limited to the usage that described in paragraph 1.4.

The authorized use of the Holder’s key pair and the associated Certificate is specified in the Certificate itself, via extensions concerning the uses of the keys (see Section 7.2 for details of the Certificate profile).

The use of a qualified Certificate necessarily requires the use of the QSCD provided by the Deutsche Post AG for the signature to be declared in conformity with the eIDAS Regulation.

The Holders must strictly respect the authorized uses of the key pair and the Certificates. Otherwise, their liability would be incurred.

In general, any unauthorized use is prohibited.

4.5.2. Relying Party public key and Certificate usage

See previous chapter and sections 1.4 «CERTIFICATE USAGE » and 1.3.7.

Applications using certificates must strictly respect the authorized usage of the Certificates.

Otherwise, their liability may be incurred.

4.5.3. Root CA public key and Certificate usage

Root CA private key is used to sign:

- Sub CA certificates
- CARL.

Root CA certificate is used to

- Verify SubCA certificates
- To verify the origin and integrity of the CARL.

4.5.4. CA public key and Certificate usage

CA private key is used to

- Sign end-user certificates
- To sign certificates for OCSP servers
- To sign CRL

CA Certificate is used to

- Verify the issued certificates and the electronic signature generated with the associated holders private keys.
- Verifiy the integrity and origin of the issued CRL
- Verifiy the integrity and origin of an OCSP server

4.6 CERTIFICATE RENEWAL

The renewal of a Certificate - i.e. issuance of a new Certificate for which only the validity dates are modified, all other information remaining identical to the previous Certificate (including the public key of the bearer), cf. [RFC3647] - is not permitted in the scope of this CP.

4.7 CERTIFICATE RE-KEY

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

4.7.1. Possible cause of a re-key

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

4.7.2. Origin of a re-key application

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

4.7.3. Processing of a re-key application

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

4.7.4. Notification of the issuance of the new certificate

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

4.7.5. Acceptance procedure for the new certificate

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

4.7.6. Publication of the new certificate

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

4.7.7. Notification by the CA to other entities

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

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 not permitted in the scope this CP.

4.9 REVOCATION AND SUSPENSION OF CERTIFICATES

The CA 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

The following circumstances may be the cause of revocation of the Holder's Certificates:

- the Certificate has become obsolete due to a change in the Holder's information contained in the Certificate,
- the Holder's information (including its title or attribute) within the certificate no longer complies with the identity or usage of the Certificate,
- the Certificate's applicable terms of use have not been respected by the Holder,
- the Holder, the Registration Authority or the Certification Authority have not respected their obligations defined by this CP,
- an error (intentional or not) has been detected in the Certificate application record,
- the Holder's private key is suspected of compromise, is compromised, is lost or is stolen,
- the activation code of the Holder is lost
- acceptance of the certificate does not occur by the holder
- the holder do not use his certificate/private key after 15 Minutes.

When any of the above circumstances occurs and CA Deutsche Post AG POSTIDENT E-Signing SUB CA or the Registration Authority becomes aware of it (*i.e.*, it is informed or obtains the information during verification when issuing a new Certificate), the relevant Certificate must be revoked.

4.9.1.2. PKI Component Certificates

The following circumstances may result in the revocation of a certificate from a PKI component (this may include a certificate from the CA Deutsche Post AG POSTIDENT E-Signing SUB CA used for the generation of Certificates and CRL):

- suspicion of compromise, compromise, loss or theft of the private key of the component;
- decision to change the PKI component following the detection of a non-conformity of the procedures applied within the component with those announced in the CPS (e .g. following a qualification audit or a non-conformity report);
- end of activity of the entity operating the component.

4.9.2. Origin of a revocation request

4.9.2.1. End-user Certificate

See 3.4

4.9.2.2. PKI Component Certificate

The revocation of a CA certificate can only be decided by the CA's GA or by the judicial authorities via a court decision.

The revocation of other certificate components shall be decided by the entity operating the relevant component, which must notify the CA without delay.

4.9.3. Procedure for processing a revocation request

4.9.3.1. End-user Certificate

The requirements for identifying and validating a revocation request are described in chapter 3.4 « Identification and authentication for revocation request ».

The following minimum information must be included in the Certificate revocation request,:

- the identity of the Holder as described in the Certificate (Company name, etc.);
- identification of the applicant for revocation;
- any information enabling the Certificate to be revoked quickly and without error (serial number, ...)
- the cause of revocation. This cause of revocation is not recorded in the CRL but can be recorded in the Service database.

The operational steps of the revocation are described in the DPC.

The revocation applicant shall be informed of proper operation conduct and of the effective revocation of the Certificate. In all cases, and regardless of the applicant for revocation, the Holder is notified.

The occurrence of the operation associated to the revocation is kept in the event logs with, where appropriate, enough information about the initial causes that have implied the revocation of the Certificate.

The causes of revocation of the Certificates are not published.

4.9.3.2. Revocation of a PKI component certificate

Deutsche Post AG POSTIDENT E-Signing SUB CA CPS specifies the procedures to be followed in the case of revocation of a PKI Component Certificate.

In the case of revocation of a Certificate within certification chain, the CA must inform by all means (and if possible in anticipation) all the concerned Holders that their Certificate is no longer valid.

4.9.4. Delay for requesting a revocation

As soon as an authorized entity (see 4.9.2 « Origin of a revocation request ») is aware of any possible cause of revocation, within its scope of operation, it must perform its request for revocation without delay.

4.9.5. Delay for processing a revocation request

DEUTSCHE POST AG ensure that a revocation request is effectively processed within a 60 minutes delay after the validation of the request. The computation of the delay is based on a schedule that is synchronized with UTC at least one time per day.

4.9.5.1. End-user revocation.

By nature a revocation request must be performed urgently. Therefore, the revocation function must have a unavailability period after service interruption (breakdown or maintenance) that is in line with the contractual commitments established between Deutsche Post AG and the Client.

In all cases the support services of this function are insured 24/7 and the processing of the request of revocation is ensured during the working days and hours.

4.9.5.2. Rovocation of a PKI Compoent Certificate

A PKI Component Certificate must be revoked upon detection of an event described in the possible revocation causes for this type of Certificate.

Revocation of a Certificate is effective when the serial number of the Certificate is entered in the revocation list of the CA that issued the Certificate, and the list is available for download. The revocation of a CA Signature Certificate (certificate signature and ARL) must be done immediately, especially in the case of key compromise.

4.9.6. Revocation checking requirement for Relying Parties

A third party application using a end-user certificate is required to verify, prior to its use, the state of the of the entire certification chain corresponding to the certificate, including the end-user Certificate itself.

4.9.7. CRL Issuance Frequency

Not applicable. In case of this CP only OCSP Services are available.

4.9.8. Maximum delay for CRL publication

Not applicable. In case of this CP only OCSP Services are available.

4.9.9. On-line revocation status availability

A OCSP service is in place. The address of the service is specified within the profile of the issued certificates. OCSP access is not available on the internet. The access is only granted through VPN access to TSPO IT systems.

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

For end-user Certificates, personnel authorized to make a revocation request are required to perform the revocation as soon as possible after notification of the compromise of the private key.

For CA Certificates, in addition to the requirements of Chapter 4.9.3.2, evocation following a compromise of the private key is clearly disseminated at least on the CA website..

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

The CA provides to Third Party Applications the means to verify and validate prior to its use the status of an issued certificate together with its certification chain (*i.e.* checking the signatures of the chain's certificates, signatures that guarantee the origin and integrity of OCSP and the status of the CA Certificates).

4.10.2. Service availability

The certificate status information feature is available 24/7. This function must have a maximum duration of unavailability per service interruption (breakdown or maintenance) in conformity with the contractual commitments established between Deutsche Post AG and the Client.

4.10.3. Optional features

Not applicable

4.11 End of subscription

In case of end of the contractual relationship between the CA and the corresponding certificate holder before the end of the certificate's validity, the certificate is revoked.

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

5.1 PHYSICAL CONTROLS

The head of Deutsche Post AG POSTIDENT E-Signing SUB CA ensures that the operating premises of the components of the PKI are implemented and maintened at the required level of physical safety.

5.1.1. Site location and construction

Depending on the sensitivity of the components of Deutsche Post AG internal PKI, the sites are defined in level 1 of the TSPO security policy: vital impact (major for the company).

In this respect, the safety of the building site meets the level 1 physical security measures for peripheral, perimeter and interior protection and in particular measures relating to:

- power supply and air conditioning;
- vulnerability to water damage;
- fire prevention and protection.

The measures also make it possible to respect the commitments made in this CP or in the contractual commitments with the TSPO, regarding the availability of services.

5.1.2. Physical access

In order to avoid loss, damage and compromise of the resources of the Deutsche Post AG POSTIDENT E-Signing SUB CA, access to the premises is controlled according to the level 1 zoning level: "very restricted access", or comparable.

For the functions of Certificate generation, generation of secret elements of the Client, and management of the revocations, access is strictly limited to the only persons authorized to enter the premises and the traceability of the accesses is ensured. Security is reinforced by the implementation of physical and logical intrusion detection means. In addition, the control in input and output is permanent in hours not worked (HNO). These requirements are also deferred contractually with the Client, when the Client is responsible for these functions.

In order to ensure the availability of systems, access to machines is limited only to those authorized to perform operations requiring physical access to the machines. For this purpose, the relevant components of the PKI define a physical security perimeter where these machines are installed. Any room used in common between the component concerned and another component (from or outside the PKI) is outside that perimeter.
The opening of the door is controlled by an access control system.

Root CAs are operated in perimeter that is physically isolated from the other operations. This environment is restricted to the person allowed to access to root CA keys.

5.1.3. Power and air conditioning

The characteristics of the power supply and air conditioning equipment make it possible to respect the conditions of use of the Deutsche Post AG POSTIDENT E-Signing SUB CA equipment as determined by their vendors.

5.1.4. Water exposures

The protection measures of Deutsche Post AG POSTIDENT E-Signing SUB CA ensures a protection of the infrastructure against water damage.

5.1.5. Prevention and protection against fire

Deutsche Post AG POSTIDENT E-Signing SUB CA set up protection measures against fire.

5.1.6. Media Storage

The media (paper, hard disk, floppy disk, CD, etc.) used in the Deutsche Post AG POSTIDENT E-Signing SUB CA are processed and stored in accordance with security requirements for sensitive assets (confidentiality, integrity and availability).
Particularly, security measures are in place to protect media against theft, damage, lost, unauthorized access and obsolescence. These measures are applicable for the whole retention period ofthese media.

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.
Destruction and resetting procedures and means are compliant to TSPO Security Policy.

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 are tested on a regular basis.

5.2 PROCEDURAL CONTROLS

The following procedural safeguards are in addition to those set out in the Key Ceremony during which the Deutsche Post AG POSTIDENT E-Signing SUB CA Key Pair is created.
Procedure and policies are communicated to authorized employees.
Procedures are documented and applied for all operation involving Trusted Roles and impacting the provision of service.

5.2.1. Trusted Roles

The trust roles defined below are those required for the PKI components, irrespective of the trust roles defined in the key ceremony.

- PKI Security Officer - The Security Officer is responsible for the implementation of the security policy of the 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.

5.2.2. Number of persons required per task

Deutsche Post AG POSTIDENT E-Signing SUB CA CPS specifies the operations requiring the intervention of several persons and the constraints that these persons must respect (positions in the organization, hierarchical links, etc.). In particular, it specifies the persons required for the key ceremony.

5.2.3. Identification and authentication for each role

Each entity operating a component of the PKI shall have the identity and authorizations of each member of its personnel verified before assigning to it a role and the corresponding rights, including:

- That his name is added to the access control lists for the premises of the entity hosting the systems concerned by the role
- that his name be added to the list of persons authorized to physically access those systems,
- that an account be opened in his name in those systems
- if applicable, cryptographic keys and/or a certificate are issued to him to fulfill the role assigned to him in the PKI.
- These checks are described in the CA's Deutsche Post AG POSTIDENT E-Signing SUB CA CPS and comply with TSPO Security Policy.

Operator, administrator and auditor role are under direct TSPO management. Administrators are in charge of user account management. Modification or deletion of a user accound is performed without delay.
All operation performed by Trusted Role are kept in event logs.

5.2.4. Roles requiring separation of duties

Several roles can be assigned to the same person, to the extent that cumulation does not compromise the security of the services offered..

The attributions associated with each role are described in Deutsche Post AG POSTIDENT E-Signing SUB CA CPS and are consistent with TSPO Security Policy.

For the various Trust roles, it is recommended that the same person does not hold several roles and the following cumulative are prohibited:

- security officer and system engineer/operator,
- controller and any other role,
- system engineer and operator.

5.3 PERSONNEL CONTROLS

The following procedural safeguards are in addition to those set out in the Key Ceremony ceremony during which the Deutsche Post AG POSTIDENT E-Signing SUB CA key pair is created.

5.3.1. Qualifications, experience, and clearance requirements

All personnel required to work within the PKI components are subject to a confidentiality clause.

The head of the CA must ensure that the attributions of his/her personnel, who are required to work within the PKI, 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.

Deutsche Post AG POSTIDENT E-Signing SUB CA informs any persons involved in the PKI's trust roles 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 Trusted Role for acceptation.

The qualifications, skills and clearances required for the key ceremony are defined in specific procedures. Responsibilities of Trusted Roles are attributed in a way that separation of duties is applied to avoid conflict of interest and to limit the opportunities of misuse (malicious or accidental) of PKI components.

Access and habilitation are provided based on least privilege policy.

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 non-conviction, a criminal record, or a confidentiality undertaking.

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

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.

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

5.3.4. Re-training frequency and requirements

Depending on the nature of these developments, the concerned staff shall receive adequate information and training prior to any changes in systems, procedures, organization, etc.

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

There are no specific requirements in this CP. Details can be provided in the Deutsche Post AG POSTIDENT E-Signing SUB CA CPS.

5.3.6. Sanction for unauthorized actions

There are no specific requirements in this CP. Details can be provided in the Deutsche Post AG POSTIDENT E-Signing SUB CA CPS.

5.3.7. External contractors requirements

The staff of external service providers working on the premises of Deutsche Post AG 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.

5.3.8. Documentation supplied to personnel

Each staff member has at least adequate documentation concerning the operational procedures and the specific tools that it implements, as well as the general policies and practices of the component in which it works, more specifically the Security Policy affecting it.

5.4 AUDIT LOGGING PROCEDURES

Event logging involves recording events in manual or electronic form by input or by automatic generation. The resulting files, in paper or electronic form, must make possible the traceability and the accountability of the performed operations.

5.4.1. Type of events to be recorded

Each entity operating a component of the PKI logs at least the following events, automatically from the start of a system and in electronic form:

- Creation / modification / deletion of the authentication data (passwords, certificates, etc.).),
- starting and stopping of computer systems and applications,
- events related to logging: starting and stopping the logging function, modifying the logging parameters, actions taken following a logging failure,
- Connection / disconnection of users with trusted roles, and unsuccessful attempts.
- Change in the security policy configuration
- Unexpected stops, crash and system failure
- Network component and firewall activity

Other events are also gathered by electronic or manual means. These are those relating to security and are not produced automatically by the computer systems, in particular:

- physical access,
- maintenance and changes to the configuration of systems,
- changes to personnel,
- Destruction and resetting of media containing confidential information (keys, activation data, personal information about holders, etc.).

In addition to these logging requirements common to all components and functions of the PKI, events specific to the various functions of the PKI are also logged, including:

- receipt of a Certificate request (initial and renewal) ,
- validation of a certificate request
- events related to signature keys and CA certificates (generation (key ceremony), backup/recovery, revocation, renewal, destruction, etc.),
- publication and updating of information related to the CA (CP, CA certificates, general conditions of use, etc.),
- generation of Holders' Certificates,
- of a request for revocation,
- validation/rejection of a request for revocation,
- generation and publication of the CRL

Each entry in the event journal contains, where applicable, the following fields:

- event type,
- name of the executant or system reference triggering the event,
- date and time of the event,
- result of the event (failure or success).

The accountability of an action rests with the person, organization or system that performed it. The name or identifier of the executant is explicitly entered in one of the fields of the event log.

In addition, depending on the type of the event, each record also contains the following fields:

- as far as possible: requestor and recipient of the operation or reference of the system creating the request,
- names of persons present (If it involves more than one person),
- cause of the event,
- any information characterizing the event (for example, for the generation of a Certificate, the serial number of this Certificate).

Logging operations are performed during the process.
In case of manual entry, the writing is made, except in exceptional cases, on the same business day as the event.

5.4.2. Frequency of processing event logs

The PKI event logs are analyzed 2 to 3 times each week on average. Moreover, automatic analysis of event logs are performed to identify abnormal behaviours and to alert PKI personnel of potential critical security events.

5.4.3. Retention period for audit log

Event logs are kept on-site for at least one month.
Event logs are archived for a retention period compliant with applicable Regulation, even in case of end of activity of the CA.

5.4.4. Protection of audit log

The CA implements event log protection appropriate to the level of sensitivity of the information contained in these logs. This level of sensitivity is the result of a risk analysis.

5.4.5. Audit log backup procedures

All events are written to a database that is in the scope of Deutsche Post AG or its suppliers infrastructure backup procedures.

5.4.6. Audit Collection System

All events are written centrally in a database

5.4.7. Notification to event-causing subject

The CP does not have specific requirements for this.

5.4.8. Vulnerability Assessment

The CA implements system vulnerability management Deutsche Post AG POSTIDENT E-Signing SUB CA. This is done in accordance with TSPO Security Policy.

Event logs are monitored regularly in accordance with the procedures set out in paragraph 5.4.2.

The logs are analyzed as soon as an anomaly is detected. This analysis gives rise to a summary in which important elements are identified, analyzed and explained. The summary shows the anomalies and falsifications found.

Any critical vulnerability is handled by Deutsche Post AG with 48 hours after its discovery. Depending on the results of the analysis Deutsche Post AG may either:

- Setup a correction plan, or
- Document the reasons why no correction will be performed.

5.5 RECORDS ARCHIVAL

5.5.1. Type of records archived

This archiving ensures the conservation of the event logs generated by the various components of the PKI. It also allows the storage of the paper-form documents related to the certification operations, as well as their availability in case of necessity.

The data to be archived are at least the following:

- the software (executables) and the configuration files of the computer equipment;
- CPs;
- the CPS;
- contractual agreements with other CAs;
- CRLs as issued or published;
- receipts or notifications (for informational purpose);
- the registration documents of the Subscribers.

5.5.2. Retention period for archive

All information of the following types:

- Personnel
- Traffic,
- Connection
- billing

and resulting from an automatic process of data processing , is not archived for more than a year.

The duration of the archive is as follows:

- CP: until the end of life of the CA,
- organizational documents for key ceremonies: until the end of life of the CA,
- CPS: until the end of life of the CA,
- Application for a certificate: at least 7 years,
- certificates issued by the CA after expiration: at least 7 years,
- last CRL issued by the CA after expiry: at least 7 years,
- event logs after generation: at least 7 years.

Deutsche Post AG has set up measures to ensure the conservation of the documents for the above period, event in case of end of activity.

5.5.3. Protection of archive

During all the retention period, archive and back-up of archive shall

- be protected in integrity;
- be accessible to only authorized persons;
- be readable and able to be processed.

The CPS specifies the means used to securely archive these elements.

5.5.4. Archive backup procedures

The procedure is specified in the CPS. The level of protection of backups is at least equivalent to the level of protection of the archives.

5.5.5. Requirements for time-stamping of records

Certificates issuance date is the time of their generation and this information is archived with the corresponding certificate.

Chapter 6.8 specifies the dating/timestamping requirements.

5.5.6. Archive collection system

The CPS specifies the means used to safety collect archives.

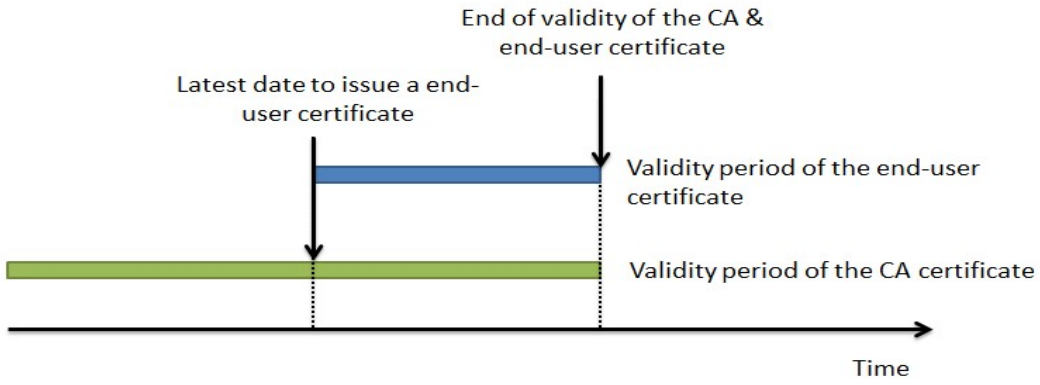
5.5.7. Procedure to retrieve and verify archive information

The archives (paper and electronic forms) are retrievable within 2 working days, it being noted that only the CA can access all the archives (as opposed to an entity operating a component of the PKI which cannot retrieve and consult the archives of the component concerned).

Archive Retrieval conditions are specified in the CPS.

5.6 KEY CHANGEOVER

The CA can not generate a certificate with an end date that is later than the expiration date of the corresponding CA certificate. For this purpose, the period of validity of the CA certificate must be longer than that of the certificates it signs.



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 CA key pair is generated, only the new private key must be used to sign certificates.

The previous certificate remains usable to validate the certificates issued with this key at least until the moment where all the certificates signed with the corresponding private key have expired.

5.7 COMPROMISE AND DISASTER RECOVERY

5.7.1. Incident and compromise handling procedures

Each PKI component implements reporting and incidence response procedures and measures in accordance with the requirements of TSPO Security Policy.

In 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 on TSPO 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)

In accordance with the TSPO Security Policy, Deutsche Post AG POSTIDENT E-Signing SUB CA has a business continuity plan to meet the availability requirements of its sensitive functions and specified in

- This CP
- Commitments in terms of quality of service of the various PKI components, in particular as regards the functions related to the publication and/or relaloted to the revocation of the Certificates. This plan is tested at least once every 3 years.

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 this 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 treat 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 lost of activation data scenario.

5.8 PKI TERMINATION

One or more components of the Deutsche Post AG PKI may be required to cease all or part of its business, or transfer it to another entity.
Deutsche Post AG has forecasted means in case of CA termination. These means are described in the up-to-date Deutsche Post AG termination plan.

The compromise of the Deutsche Post AG POSTIDENT E-Signing SUB CA key pair immediately implies the cessation of its activity and the revocation of all valid Certificates issued. To regain the level of service, the creation of a new CA and new Certificates are mandatory.

Transfer of activity or cessation of activity affecting a component of the Deutsche Post AG ***PKI***

In order to ensure a constant level of confidence during and after such events, the CA Deutsche Post AG POSTIDENT E-Signing SUB CA undertakes, among other obligations:

1) to set up procedures aiming at ensuring the continuity of the service, particularly in terms of archiving (in particular, archiving of Holder Certificates and information relating to Certificates);
2) to ensure the continuity of the revocation service (taking into account a request for revocation and publication of the CRL), in accordance with the availability requirements for its functions defined in this CP.

Deutsche Post AG POSTIDENT E-Signing SUB CA ensures the following points:

1) in the case where the planned changes may have an impact on the commitments with the Customers or the Third Parties using certificates, Deutsche Post AG POSTIDENT E-Signing SUB CA must notify them as soon as necessary and, at least, within 3 months.
2) Deutsche Post AG POSTIDENT E-Signing SUB CA must communicate to the Clients and Certificates Holders the principles of the action plan that will implement the technical and organizational measures intended manage activity termination or to organize the activity transfer. It will present in particular the arrangements in place for archiving (keys and information relating to certificates) in order to ensure this function this be ensured for the duration originally planned in the CP. Deutsche Post AG POSTIDENT E-Signing SUB CA shall communicate to the Clients and Certificates Holders the terms and conditions of the changes. Deutsche Post AG POSTIDENT E-Signing SUB CA will estimate the impact and will analyse the consequences (legal, economic, functional, technical, communication, etc.) of this event. It will present an action plan to remove or reduce the risk to the Third Parties and the discomfort to Customers and Holders.
3) Deutsche Post AG POSTIDENT E-Signing SUB CA shall keep Clients and other entities informed of any additional barriers or delays encountered in the change process.
4) Deutsche Post AG POSTIDENT E-Signing SUB CA will notify the Supervisory Body, and all appropriate authorities, in case of PKI Termination and will publish the information to notify the Trust Party Applications.

Termination affecting Deutsche Post AG POSTIDENT E-Signing SUB CA

The termination of activity may be total or partial (for example: cessation of activity for a given family of Certificates only). Partial discontinuance of activity must be phased in such a way that only the obligations

referred to in 1), 2) and 3) below are to be performed by the CA Deutsche Post AG POSTIDENT E-Signing SUB CA, or a third party entity which resumes the activities, at the expiration of the last Certificate issued by it.

In the case of a complete termination of activity Deutsche Post AG POSTIDENT E-Signing SUB CA or, in the case of impossibility for Deutsche Post AG POSTIDENT E-Signing SUB CA to perform the action, any entity that is substituted for it by the law, a regulation, a court decision or an agreement previously entered into with that entity, revokes the Certificates and publishes the CRLs in accordance with the commitments made in its CP.

Upon termination of the Service, Deutsche Post AG POSTIDENT E-Signing SUB CA:

1) deletes the private key used to issue Certificates, and all copies of this key
2) take all necessary measures to destroy the key or to made it inoperative;
3) revokes his Certificate;
4) revokes all the issued Certificates and which are still valid;
5) notifies (e.g. by receipt) all Holders of revoked certificates (or to be revoked).
6) transfers to a third party the requirement regarding the publication of information, in particular the publication of the public key.

6. TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1. Key pair generation

6.1.1.1. CA Key Pair

The CA signature keys are generated in a secure environment.

The CA signature keys are generated and implemented in a cryptographic module certified FIPS 140-2 Level 3 (also see section 6.2.1 « Cryptographic module standards and controls »).

The generation of CA signature keys is done under perfectly controlled circumstances by personnel in trusted roles as part of a Key Ceremony (KC). This ceremony takes place according to previously defined organizational and technical scripts.

The script of the Key Ceremony identifies:

- roles participating in the ceremony (internal and external from the organization);
- functions to be performed by every role and in which phases;
- responsibilities during and after the ceremony; and
- requirements of evidence to be collected of the ceremony.

The Key Ceremony is performed in the presence of:

- The Security Officer for a CA Key
- A Security Officer and a Bailiff for a Root CA.

A key ceremony report is signed by all participants who testify that the ceremony has been processed in conformity with the pre-defined script. Thus, the report provides evidence that the integrity and confidentiality of the key pair generation has been ensured.

Together with the generation of CA keys, various secrets and sensitive elements are generated. These secrets are data that are managed in a secured way (nobody can possess the entirety of the secret). These secrets are needed, after the Key Ceremony, to perform the operations on the HSM, in particular, to be able to restart, save, and restore the backup of the HSM partition.

Following their generation, the secrets are handed over to Key Custodian in advance and entitled to this Trusted role.

The renewal of the CA Certificate and Keys follows the same principles as the first generation of CA keys.

The issuance of a Certificate by the root CA is performed in dual control by two authorized persons in Trusted Role.

6.1.1.2. End-users keys

The end-user keys are generated on personalization sites whose contractual security conditions are established between the CA and the RA. Generation of the keys is done on a hardware cryptographic device that is

- a qualified QSCD (Qualified Signature Creation Device)

Generation of the end-user signature keys is carried out under perfectly controlled circumstances by authorized personnel of the Registration Authority.

6.1.2. Private key delivery to Subscriber

The end-user private key is generated and used within onboard within the QSCD. The QCSD qualification of this medium ensures that the private key cannot be exported in plain text outside the QSCD.

6.1.3. Public key delivery to certificate issuer

The public key is transmitted to Deutsche Post AG POSTIDENT E-Signing SUB CA within the certificate generation request. The key is protected in integrity and the origin is authenticated thanks to a PKCS # 10 envelopes that is signed by the private key associated with the public key.

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

The key sizes are as follows:

- Deutsche Post AG POSTIDENT E-Signing SUB CA Certificate : 4096 bits (RSA algorithm)
- End-user Certificates: 2048 bits (RSA algorithm)

6.1.6. Validation of the key pair parameters

The Key Pair generation equipment uses parameters respecting the security standards specific to the algorithm corresponding to the Key pair. These parameters are recalled in Chapter 7 « CERTIFICATES, OCSP And CRL Profiles ».

6.1.7. Key usage purposes

The use of the CA private key and the associated Certificate is strictly limited to the Certificate signatures and CRL.

The use of the Holder's private key and the associated certificate is strictly limited to:

- the qualified or advanced electronic signature

(See sections 1.4 « CERTIFICATE USAGE» et 7.2).

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

The cryptographic modules used by the CA to generate and implement its signature keys are certified in conformity with FIPS 140-2 Level 3.

6.2.1.2. End-user Signature Creation Device

The devices used for the Holders key pair are QSCD under one or more references published by the German supervisory body (Bundesnetzagentur) to the qualification of products.

6.2.2. Private key multi-person control

Control of the private key of the CA is ensured for the following actions:

- for export/import out/in a cryptographic module: the systems are configured to prohibit the unencrypted export of the private key, thus ensuring its non-compromise;
- for the generation of the key pair (see . 6.1.1.1): use of a secure cryptographic hardware module for the generation and storage of the private key, and the sharing of secrets ensures that no alone actor can access or interpret one of the secrets;
- to activate the private key (see section 6.2.8): the requests for certificates and revocation (updating the CRL) flows are controlled to ensure that only the authorized services can be registered;
- The authorization and configuration of these flows requires the presence of at least 2 PKI officers;
- for destruction (see section 6.2.10): destruction procedures ensure that nobody can use the private key.

6.2.3. Private Key escrow

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

6.2.4. Private Key backup

The private keys of the end-users are not the subject of a back-up copy, the private key is used only one time.

The partition containing the CA private key is backed up from cryptographic modules in encrypted form and with an integrity check mechanism. Installation and Restoration of CA keys within a cryptographic module can only be performed under the dual control of two authorized employees in Trusted Role.

6.2.5. 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.

6.2.6. Private key transfer into or from a cryptographic module

For CA private keys, all transfers are made in encrypted form, as described in section 6.2.4 «Private Key backup ». The procedure for transferring the private key requires the presence of at least 2 trust roles.

The private keys of the Holders cannot be transferred for any use outside QSCD.

6.2.7. Private key storage on cryptographic module

See section 6.2.1 « Cryptographic module standards and controls ».

6.2.8. Method for Private Key Activation

6.2.8.1. CA keys

See. 6.2.2 « Private key multi-person control »

6.2.8.2. 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.

6.2.9. Method for Private Key Deactivation

6.2.9.1. CA Keys

Deactivation of the CA private key in the cryptographic modules is automatic as soon as the environment of the module evolves in a sensitive way: shock, disconnection, etc. The deactivation modalities are specific to the module's technology; they are detailed in the Vendor documentation. In this case, it is necessary to disable the partition containing the corresponding private key.

6.2.9.2. End-user keys

The holder private key is used only one time with associated activation code.

6.2.10. Method for Private Key Destruction

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.

6.2.10.2. End-user keys

The destruction of the private key is carried out by the QSCD after its use.

6.2.11. 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

The public keys of the CA and the Holders are archived as part of the archiving of the corresponding Certificates.

6.3.2. Key pair and certificate usage period

The Key Pair and Certificates covered by this CP have a lifetime of 15mn. 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

The generation and installation of activation data for a cryptographic module of the PKI takes place during the initialization and personalization phase of this module.

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

A random one time activation code (mTAN) is generated and send by SMS to the holder;

6.4.2. Activation Data Protection

6.4.2.1. Activation Data Protection of the CA Keys

Activation data that is generated by the CA for the cryptographic modules of the PKI are protected in integrity and confidentiality until their delivery to their Key Custodian. The Key Custodian is responsible for ensuring confidentiality, integrity and availability.

6.4.2.2. Activation Data Protection of the end-user Keys

Upon delivery of the certificate, the Holder signs an acceptance record of its certificate using his activation code.

6.5 COMPUTER SECURITY CONTROLS

6.5.1. Computer-specific technical security requirements

A minimum level of assurance of security on the computer systems of the PKI is defined in the CPS of Deutsche Post AG POSTIDENT E-Signing SUB CA. In particular, it meets the following security objectives:

- strong identification and authentication of users for access to the system (two-factor authentication, physical and/or logical);
- management of user rights (to implement the access control policy defined by the CA, in particular to implement the principles of lower privileges, multiple controls and separation of roles),
- management of user sessions (disconnection after a period of inactivity, access to files controlled by role and user name);
- protection against computer viruses and all forms of compromising or unauthorized software and software updates;
- management of user accounts, including the modification and rapid deletion of access rights;
- protection of the network against intrusion by an unauthorized person;
- protection of the network to ensure the confidentiality and integrity of the data transiting it;
- audit functions (non-repudiation and nature of the actions carried out);

- Possibly, error recovery management.

Confidentiality and integrity protection of private or secret keys for infrastructure and control must be consistent with the Security Policy.

To meet these objectives, TSPO use trustworthy systems and products that are protected against modification and ensure the technical security and reliability of the processes supported by the PKI.
Security requirement are taken into account in the choice and/or the development of systems and products.

Monitoring systems (with automatic alarm features) and audit procedure of system configuration are in place. That allows:

- To detect and record any non-authorized access or attempt of access to the PKI systems and to react in a timely manner;
- To monitor the volume of service and requests ;
- To trigger alarms in case of detection of potential security violation ;
- To monitor start-up and shutdown of the logging functions ;
- To monitor the availability and utilization of needed services with the TSP network

Monitoring activities take account of the sensitivity of any information collected or analysed. Alert and critical security events follow-up is performed by employees in Trusted Roles. These ensures that relevant incidents are analysed and reported in line with the TSP's procedure

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 a system participating to a function of the Deutsche Post AG POSTIDENT E-Signing SUB CA PKI is documented.

The configuration of the Deutsche Post AG POSTIDENT E-Signing SUB CA PKI components system as well as any modifications and upgrades are documented. Change management procedures are in place and are applied for each system update (either planned or urgent) or configuration update.

Any development must be consistent with the TSPO Security Policy and the requirements contained in this CP.

6.6.2. Security Management measures

6.6.2.1. Update of PKI components

Any significant evolution of a component system of the Deutsche Post AG POSTIDENT E-Signing SUB CA PKI must be reported to the GA for validation. It must be documented.

In particular, Security Patch management procedure have been defined and implemented by TSPO, such that security patches are applied as soon as possible. If security patches may introduce additional vulnerabilities or instabilities that outweigh the benefits of applying them, then TSPO may not apply them and will document the reasons for not applying a patch.

6.6.2.2. Risk Assessment

Deutsche Post AG POSTIDENT E-Signing SUB CA a carried out a risk assessment to analyze and evaluate trust service risks taking into account business and technical issues. Base on the result of this risk assessment, TSPO has selected the appropriate risk treatment measures and the associated operational measures, such that the level of security is commensurate to the degree of risk.

The Risk assessment is approved by the Head of the CA, who accepts, through this approbation procedure, the residual risk that has been identified.

The risk assessment is regularly reviewed and revised, at least annually and each time significant evolution of system or component of the PKI is performed.

6.6.2.3. Vulnerability Scan

TSPO performs regular vulnerability scan on public and private IP addresses. Scans are performed by a qualified and independent person or organization.

6.6.2.4. Penetration Test

Deutsche Post AG or its suppliers undergoes a penetration test when new infrastructures are set up or when a component is modified in a significant manner. Evidence of qualification and independence of the person performing the test is kept by Deutsche Post AG.

6.7 NETWORK SECURITY

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 has implemented redundancy measures allowing a high availability of critical services.

6.8 TIMESTAMPING

The systems are synchronized with respect to a reliable source of universal time (UTC) with a time synchronization protocol (NTP) with an accuracy of at least one minute.

7. CERTIFICATES, OCSP AND CRL PROFILES

7.1 PROFILES OF THE CERTIFICATE OF THE CA DEUTSCHE POST AG POSTIDENT E-SIGNING SUB CA

The following table provide the values of the attributes of the certificate of Deutsche Post AG POSTIDENT E-Signing SUB CA issued by « ALMERYS ROOT CA ».

The format of this certificate and its attributes are compliant with the X.509v3 specification described in RFC 5280 « Internet X.509 Public Key Infrastructure – Certificate and Certificate Revocation List (CRL) Profile », ref. [RFC5280].

tbsCertList		Value
version		2 (meaning version 3)
serialNumber		Random Number
signature		
▶ algorithm		Sha256withRSAEncryption
▶ parameters		RSAParams : NULL
issuer CN=commonName OU=organizationalUnitName O=organizationName C=countryName		CN=ALMERYS ROOT CA OU=0002 432701639 O=ALMERYS C=FR
validity		
▶ notBefore		Creation Date
▶ notAfter		notBefore + 10 years
subject CN=commonName OU=organizationalUnitName O=organizationName C=countryName		CN= Deutsche Post AG POSTIDENT E-Signing SUB CA O= Deutsche Post AG C=DE
subjectPublicKeyInfo		
▶ algorithm ➥ algorithm ➥ parameters		rsaEncryption) RSAParams : NULL
▶ subjectPublicKey		DER encoded RSAPublicKey (4096 bits)
issuerUniqueID		This field is not used
subjectUniqueID		This field is not used
Standard extensions	Critique :	
▶ authorityKeyIdentifier	No	Hash of the public key of the issuer
▶ subjectKeyIdentifier	No	Hash of the public key of the subject
▶ keyUsage	Yes	keyCertSign (5), cRLSign (6)
▶privateKeyUsagePeriod		This Extension is not used
▶certificatePolicies	No	certificate policy : identifier of the policy = 1.3.6.1.4.1.5064.2.1.60.1.1 or any policy
▶ basicContraints ➥ cA ➥ pathLenConstraint	Yes	 True None
▶ cRLDistributionPoints	No	Distribution point of the CRL

		Name of the distribution point : Complete Name : URL=http://pki.almerys.com/almerysrootca.crl
Private extensions		
▶ authorityInfoAccess	No	[1] : accessMethod : id-ad-calssuers accessLocation : URL=http://pki.almerys.com/almerysrootca.cer
▶subjectInfoAccess		This Extension nis not used
signatureAlgorithm		
algorithm		Sha256withRSAEncryption, 4096 bits key length
parameters		NULL

7.2 END-USER CERTIFICATES

The following tables provide the default values of end-user certificates issued by Deutsche Post AG POSTIDENT E-Signing SUB CA.
Format of this Certificate and its attributes are compliant with X.509v3 profile described in RFC 5280 « Internet X.509 Public Key Infrastructure – Certificate and Certificate Revocation List (CRL) Profile », ref. [RFC5280].

7.2.1. Profile eIDAS qualified

tbsCertList		Value
version		2 (meaning v3)
serialNumber		Sequential
signature		
▶ algorithm		Sha256withRSAEncryption
▶ parameters		RSAParams : NULL
issuer CN=commonName OU=organizationalUnitName OI=organisationIdentifier O=organizationName C=countryName		CN= Deutsche Post AG POSTIDENT E-Signing SUB CA O= Deutsche Post AG C=DE
validity		
▶notBefore		Creation Date
▶notAfter		notBefore + 15MN
subject CN=commonName OU=organizationalUnitName OI= organisationIdentifier O=organizationName C=countryName		CN = <Name><LastName> GIVENNAME = <Name> SN = <LastName> C = DE SERIALNUMBER = PI:DE-<Unique identifier>
subjectPublicKeyInfo		
▶algorithm ➥algorithm ➥parameters		 rsaEncryption RSAParams : NULL
▶subjectPublicKey		DER encoded RSAPublicKey (2048 bits)

issuerUniqueID		This field is not used
subjectUniqueID		This field is not used
Standard extensions	Critical:	
▶authorityKeyIdentifier	No	hash of the issuer public key
▶ subjectKeyIdentifier	No	hash of the subject public key
▶keyUsage	yes	Qualified Signature Certificate nonRepudiation (contentCommitment)
▶privateKeyUsagePeriod		
▶certificatePolicies	No	*Qualified Signature Certificate* Certificate policy : Identifier of the policy =1.3.6.1.4.1.5064.2.1.61.1.1
▶ Qualified Certificate Statements	No	- id-etsi-qcs-QcCompliance true -id-etsi-qcs-QcSSCD true -id-etsi-qcs-QcPDS URL=https://www.deutschepost.de/de/p/postident/zertifizierungsrichtlinien.html -id-etsi-qcs-QcType id-etsi-qct-esign
▶SubjectDirectoryAttribute[1]	No	T= <Title >[2] C = FR
▶basicContraints ➥cA ➥pathLenConstraint	No	false None
▶extKeyUsage	No	This Extension is not used
▶cRLDistributionPoints	No	Distribution point of the CRL Name of the distribution point : Complete name:
Private extensions		
▶authorityInfoAccess	Nn	[1] : accessMethod : id-ad-caIssuers accessLocation : URL= http://postident.deutschepost.de/certs/DPAG.cer [2] accessMethod : id-ad-ocsp accessLocation : URL= http://postident.deutschepost.de/ocsp
▶subjectInfoAccess		This Extension is not used

[1] This extension is used to provide a attribute of the subject. It can be used only in a qualified certificate if evidence of the attribute has been provided during the registration process. Notice that this extension is used mainly for profession under the scope of a specific regulation

[2] Title or subject attribute as indicated in the evidence provided in the registration record

signatureAlgorithm		
algorithm		Sha256withRSAEncryption
parameters		NULL

7.2.2. Profile eIDAS advanced

tbsCertList		Value
version		2 (meaning v3)
serialNumber		Sequential
signature		
▶ algorithm		Sha256withRSAEncryption
▶ parameters		RSAParams : NULL
issuer CN=commonName OU=organizationalUnitName OI=organisationIdentifier O=organizationName C=countryName		CN= Deutsche Post AG POSTIDENT E-Signing SUB CA O= Deutsche Post AG C=DE
validity		
▶notBefore		Creation Date
▶notAfter		notBefore + 15MN
subject CN=commonName OU=organizationalUnitName OI= organisationIdentifier O=organizationName C=countryName		CN = <Name><LastName> GIVENNAME = <Name> SN = <LastName> C = DE SERIALNUMBER = PI:DE-<Unique identifier>
subjectPublicKeyInfo		
▶algorithm ➥algorithm ➥parameters		 rsaEncryption RSAParams : NULL
▶subjectPublicKey		DER encoded RSAPublicKey (2048 bits)
issuerUniqueID		This field is not used
subjectUniqueID		This field is not used
Standard extensions	Critical:	
▶authorityKeyIdentifier	No	hash of the issuer public key
▶ subjectKeyIdentifier	No	hash of the subject public key
▶keyUsage	yes	Advanced Signature Certificate nonRepudiation (contentCommitment)
▶privateKeyUsagePeriod		
▶certificatePolicies	No	*Qualified Signature Certificate* Certificate policy : Identifier of the policy =1.3.6.1.4.1.5064.2.1.60.1.1

▶ Qualified Certificate Statements	No	
▶SubjectDirectoryAttribute[3]	No	T= <Title >[4] C = FR
▶basicContraints ➥cA ➥pathLenConstraint	No	false None
▶extKeyUsage	No	This Extension is not used
▶cRLDistributionPoints	No	Distribution point of the CRL Name of the distribution point : Complete name:
Private extensions		
▶authorityInfoAccess	Nn	[1] : accessMethod : id-ad-caIssuers accessLocation : URL= http://postident.deutschepost.de/certs/DPAG.cer [2] accessMethod : id-ad-ocsp accessLocation : URL= http://postident.deutschepost.de/ocsp
▶subjectInfoAccess		This Extension is not used
signatureAlgorithm		
algorithm		Sha256withRSAEncryption
parameters		NULL

7.3 CRL

Not applicable.

7.4 OCSP CERTIFICATE PROFILE

tbsCertList		Value
version		2 (meaning v3)
serialNumber		Sequential

[3] This extension is used to provide a attribute of the subject. It can be used only in a qualified certificate if evidence of the attribute has been provided during the registration process. Notice that this extension is used mainly for profession under the scope of a specific regulation

[4] Title or subject attribute as indicated in the evidence provided in the registration record

signature		
▶ algorithm		Sha256withRSAEncryption
▶ parameters		RSAParams : NULL
issuer CN=commonName OU=organizationalUnitName OI=organisationIdentifier O=organizationName C=countryName		CN= Deutsche Post AG POSTIDENT E-Signing SUB CA O= Deutsche Post AG C=DE
validity		
▶notBefore		Creation date
▶notAfter		notBefore + 3 years Maximum
subject CN=commonName OU=organizationalUnitName OI= organisationIdentifier O=organizationName C=countryName		CN= Deutsche Post AG OCSP O= Deutsche Post AG C=DE
subjectPublicKeyInfo		
▶algorithm ➥algorithm ➥parameters		 rsaEncryption RSAParams : NULL
▶subjectPublicKey		DER encoded RSAPublicKey (2048 bits)
issuerUniqueID		This field is not used
subjectUniqueID		This field is not used
Standard extensions	Critical:	
▶authorityKeyIdentifier	No	**hash of issuer public key**
▶ subjectKeyIdentifier	No	**hash of subject public key**
▶keyUsage	yes	digitalSignature
▶certificatePolicies	No	Certificate profile Policy identifier = 1.3.6.1.4.1.5064.2.1.70.1.1
▶extKeyUsage	No	OCSPSigning
signatureAlgorithm		
algorithm		Sha256withRSAEncryption
parameters		NULL

7.5 OCSP Response Profile

Comment		Value	Note
Response Status		As specified in RFC 6960	

Response Type		id-pkix-ocsp-basic	
Version		V1 (0)	
Responder ID		Octet String (equaL to subject key identifier within the OCSP Certificate) or DN of the OCSP server.	
Produced At		Generalized Time	Signature Date of the response
List of Responses		Each response contains the following: certificate id; certificate status, thisUpdate, nextUpdate.	
Signature		sha256 WithRSAEncryption	
Certificates		The certificates	
Extensions			
Field	**CRITICAL**	**VALUE**	**Note**
Nonce	No	Value of the nonce attribute in the request (mandatory if nonce attribute is present within the request)	Optional

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

This chapter deals with audits and evaluations of the CA or RA management to ensure the adequate operation of its PKI.

8.1 FREQUENCIES AND/OR CIRCUMSTANCES OF EVALUATIONS

Following any significant modification of a component of the PKI, the GA carries out a security analysis and, if necessary, changes the technical and organizational measures to maintain or improve the expected level of security. The GA also regularly checks the compliance of the PKI, through a complete or partial audit of the PKI part. The frequency of this audit is provided in the CPS associated with this CP.

8.2 IDENTITY/QUALIFICATION OF EVALUATORS

The GA selects and assigns a team of auditors competent in the security of information systems and in the field of activity.

8.3 RELATIONSHIP BETWEEN EVALUATORS AND EVALUATED ENTITIES

The audit team shall not belong to the entity operating the PKI component, and shall be duly authorized to carry out the audits concerned.

8.4 SCOPE OF EVALUATION

Security audits cover all or part of the PKI and are intended to verify compliance with the commitments and practices set out in this CP and the associated CPS.

8.5 ACTIONS TAKEN ON THE CONCLUSIONS OF EVALUATIONS

At the end of a security audit, the audit team provide to the GA a report. Status on the report can either be "success", "failure", or "to be confirmed". According to the status, the consequences of the audit are as follows:

- In the case of failure and depending on the type and critical level of non-conformities, the audit team issues recommendations to the GA which may be cessation (temporary or permanent) of activity, revocation of the component Certificate, revocation of all Certificates issued since the last positive control, etc. The choice of the measure to be applied is under the responsibility of the GA and must respect its internal security policies;
- in the event of a "to be confirmed" result, the GA submits a notice to the component specifying how long the non-conformities must be corrected. Then, a "confirmation" check will verify that all the critical points have been solved;
- if successful, the GA confirms compliance with the requirements of the CP and the CPS to the controlled component.

8.6 COMMUNICATION OF RESULTS

The procedures for communicating the results of conformity audits are specified in the CPS.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 FEES

The following information is provided in the various contractual documents drawn up between the parties: (i.e. Deutsche Post AG, Clients of the service, and possibly suppliers performing some or all of the functions of Deutsche Post AG POSTIDENT E-Signing SUB CA or of the RA:

- the billing conditions of the Service proposed by Deutsche Post AG
- the responsibilities
- the financial responsibilities
- the amount of the indemnities.

Access to the function on the state of the certificates is not subject to pricing.

9.2 FINANCIAL RESPONSIBILITY

See 9.1 «Fees ».

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

9.3.1. Scope of Confidential Information

The classification of information is broken down into:

- secret (level 4 in the Security Policy);
- confidential (level 3 in the Security Policy);
- internal (level 2 in the Security Policy).

The information considered to be "secret" is at least the following:

- the private keys of the CAs of the Deutsche Post AG PKI, of the PKI components and of the certificate Holders
- all the secrets of the PKI, in particular the information related to the management of the cryptographic modules (HSM);
- the activation data associated with the private keys of CA and of the Holders

The information considered to be "confidential" is at least the following:

- the CPS of the CA;
- the event logs of the PKI components;
- causes of revocation, unless explicitly agreed to publication by the Holder
- the registration records of the subscribers.

9.3.2. Information not considered as confidential

By default, in addition to the information already explicitly listed in paragraphs 9.3.1 and 9.4, information is considered confidential except for the published information listed in section 2.2« INFORMATION TO BE PUBLISHED ». Dissemination of information is only permitted with the explicit consent of the GA of Deutsche Post AG PKI and only to people or organization who need to be aware about it.

9.3.3. Protection of confidential information and responsibilities

In particular, the CA respects the laws and regulations in force in Germany. In particular, it may have to make the Holders' registration record available to third parties in the case of legal proceedings.

9.4 PROTECTION OF PERSONAL DATA

9.4.1. Personal data Protection Policy

Any collection and processing of personal data by the RA and the CA Deutsche Post AG POSTIDENT E-Signing SUB CA are performed in conformity with the applicable regulation, in particular, with the German Federal Data Protection Act (Bundesdatenschutzgesetz).

9.4.2. Personal data

Information considered to be personal data is at least the following:

- causes of revocation of the Holder's Certificates (which are considered confidential unless expressly agreed by the Holder);
- The registration record.

They must be handled in strict compliance with the applicable law and regulations (see 9.4.1).

9.4.3. Responsibilities related to the protection of personal data.

The Holder and the Client are responsible for compliance with the applicable law (see 9.4.1).
The processing of personal data is the responsibility of Deutsche Post AG, and TSPO board. For compliance with the Law, Deutsche Post AG has set up an organization centered on the Personal Data Processing Manager.

In particular, Personal Data protection is ensure by Deutsche Post AG for the following processes or area:

- Registration process
- Confidentiality of archived information
- Personal data access protection
- User consent

9.4.4. Notification and consent to use personal data use

In accordance with the applicable laws and regulations in Germany, the personal data provided by the subscriber to the RA is not disclosed or transferred to a third party except in the following cases: prior consent of the person concerned, Judicial decision or authorization by legal authority.

9.4.5. Conditions for the disclosure of personal information to the judicial or administrative authorities

Any dissemination and communication of personal data to authorized third parties must comply with the applicable laws.

9.4.6. Other circumstances of disclosure of personal information

Not applicable

9.5 INTELLECTUAL PROPERTY RIGHTS

All intellectual property rights held by the Deutsche Post AG PKI are protected by applicable law, regulations and other international conventions. They may lead to civil and criminal liability in case of non-compliance. For example, according with the applicable law the databases operated by the components of the PKI are protected by intellectual property right.

The infringement of trademarks, commerce and services, designs, distinctive signs, copyrights (e.g. software, web pages, databases, original texts, etc.) is punishable by Articles of the Code of the intellectual property.

9.6 WARRANTIES

The common obligations of the PKI components are:

- to protect and guarantee the integrity and confidentiality of their secret and/or private keys,
- to use their cryptographic keys (public, private and/or secret) for the purposes for which they were issued and with the tools specified under the conditions laid down in this CP and the documents resulting therefrom
- to respect and apply the part of the CPS applicable to them (this part must be communicated to the corresponding component)
- to comply with the security audits and conformity checks requested by the duly identified and authorized stakeholders,
- to comply with the agreements or contracts binding them to each other or with the Clients,
- to document their internal operating procedures,
- to implement the technical and human means required to carry out the services under applicable conditions guaranteeing quality and safety.

9.6.1. Certification Authority

Deutsche Post AG POSTIDENT E-Signing SUB CA has the obligation to:

- be able to demonstrate to the Third Party Applications using its Certificates, that Certificate issuance and acceptation by the Holder Certificate has been performed in conformity with the requirements of the Chapter 4.4 « Certificate Acceptance »;
- ensure and maintain the consistency between this CP and the CPS.

9.6.2. Governance Authority

The GA acknowledges its responsibility in the event of fault or negligence of the CA Deutsche Post AG POSTIDENT E-Signing SUB CA or any of the components of the PKI, whatever their nature and gravity, which

would result in the divulgation, alteration or fraudulent use of the Holder's personal data, whether this data is contained or in transit in the applications of CA Deutsche Post AG POSTIDENT E-Signing SUB CA systems.

In addition, the GA acknowledges that it has a general duty to oversee the security and integrity of the Certificates issued by Deutsche Post AG POSTIDENT E-Signing SUB CA or one of the components of the PKI. The GA is responsible for maintaining the level of security of the technical infrastructure on which the provision of services relies.

9.6.3. Registration Authority

In addition to the responsibilities described in the introduction to section 9.6 and in sections 1.3.3 and 4, the RA shall :

- maintain and protect the manipulated information in integrity and confidentiality
- ensure that Certificate registration operational processes are in line the rules set out by the CA. This rule applies in particular in the case where the RA is one of Deutsche Post AG Client
- take all reasonable measures to ensure that the Applicants who perform certificate request are aware of their rights and obligations with respect to the use and management of keys, certificates, equipment and software.

9.6.4. Certificate Holders

A Certificate Holder shall :

- comply with of Terms and Conditions of the services of Deutsche Post AG he has agreed to
- manage the security of sensitive elements which are handed to it at the end of the procedure for generating his certificate. In particular, the certificate holder shall keep the private key under its sole control.
- accept the conditions of use of his private key and the corresponding certificate,

The relationship between the Holder and the CA or its components is formalized by a service contract between the Client and Deutsche Post AG.

9.6.5. Third Party Applications

The Third Party application shall :

- verify and respect the key usage for which a Certificate has been issued;
- check that the Certificate issued by the Deutsche Post AG POSTIDENT E-Signing SUB CA has a security level that is adequate for the service provided by the application ;
- verify the electronic signature of Deutsche Post AG POSTIDENT E-Signing SUB CA that has issued the Certicate by verifying the complete certification chain until the « Almerys Root CA » certificate ;
- verify and respect the obligations of the Third Party applications described in this CP;
- check the validity of the Certificates (validity dates, revocation status).

9.6.6. Other participants

Not applicable.

9.7 DISCLAIMERS OF WARRANTIES

See 9.1« Fees ».

9.8 LIMITATIONS OF LIABILITY

See9.1« Fees ».

9.9 INDEMNITIES

See 9.1« Fees ».

9.10 TERM AND TERMINATION OF THIS CP

9.10.1. Validity Period

The CP Deutsche Post AG POSTIDENT E-Signing SUB CA is applicable at least until the end of the life of the last Certificate issued under this CP.

9.10.2. Anticipated end of validity

Following the internal publication a new version of this CP within the PKI, the CA Deutsche Post AG POSTIDENT E-Signing SUB CA has a 1 year period for implementing the changes needed for ensuring the compliance.

In addition, such changes do not require the early renewal of Certificates already issued, except in exceptional cases related to security issues.

9.10.3. Effects of the end of validity and clauses remaining applicable

In case of Deutsche Post AG POSTIDENT E-Signing SUB CA end of activity and therefore, end of validity of this CP, the requirements of the following sections shall remain applicable until the end of the life of the last certificate issued:

- 2 « Publications and Repository Responsibilities »
- 3.4 « Identification and authentication for revocation request »
- 4.5« Key pair and certificate usage »

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

- Certificate Modification »
- 4.9 « Revocation »
- 4.10 « Certificate Status services »

9.11 INDIVIDUAL NOTIFICATIONS AND COMMUNICATIONS BETWEEN PARTICIPANTS

In the case of any change in the PKI partipants, the GA must, one month before the start of the operation at the latest, validate the change in order to assess the impacts on the quality level and on the functions of Deutsche Post AG POSTIDENT E-Signing SUB CA and its various components.

9.12 AMENDEMENTS ON THIS CP

9.12.1. Procedures for amendments

Any proposed amendments to this CP shall remain in compliance with the security policy requirements of the Deutsche Post AG PKI, and shall also respect the existing commitments with Clients and Certificate Holders. In the case of a significant change, the GA of Deutsche Post AG PKI may have the support of technical expertise to monitor the impact of the changes.

The amendment procedure should take into account notification and the associated delay for communicating the amendments. Details are provided in the CPS associated with this CP.

This CP should be reviewed at least annually, with or without an amendment.

9.12.2. Circumstances under which the OID is to be changed

The OID of the family of Certificate issued by Deutsche Post AG POSTIDENT E-Signing SUB CA is part of the issued certificates, therefore, any evolution of the CA that have a major impact on the already issued certificates (for example, stronger requirements for the registration of Holders, which therefore cannot apply to Certificates already issued) must result in an evolution of the OID, so that Third Party Applications can clearly distinguish the certificates families and the associated requirements.

9.13 DISPUTE

In the event of a dispute over the interpretation of the content or the execution of this CP, an amicable resolution of conflicts is preferred.

9.14 GOVERNING LAW AND JURISDICTION

The law applicable to any dispute relating to the interpretation and execution of this CP is German law.

9.15 COMPLIANCE WITH APPLICABLE LAW

The laws and regulations applicable to this CP are, in particular, those set out in Appendix 1. Deutsche Post AG respects the applicable law and regulations and keeps evidence of this conformity. In particular, each time it feasible, Deutsche Post AG:

- Provide access for persons with disabilities
- Ensures the protection of personal date in line with the applicable laws and Regulation.

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

Reference	Document
[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 +»