Deutsche Post CA
Certification Practice Statement

Date: March 28th, 2014

Version: 1.0

Table of Contents

Document History

Version	Release Date	Author	Status + Description
1.0	March 28th, 2014	Lukáš Geyer	Initial version

Detailed History of Changes

Changes in 1.0 (publication date : March 28th)

- Initial version of the CPS created.

Acknowledgments

This Deutsche Post CA CPS endorses in whole or in part the following industry standards:

- RFC2119, Request for Comments: 2119, Key words for use in RFCs to Indicate Requirement Levels, Bradner, March 1997.
- RFC2527, Request for Comments: 2527, Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework, Chokhani, et al, March 1999.
- RFC2560, Request for Comments: 2560, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP M. Myers, et al, June 1999.
- RFC3647, Request for Comments: 3647, Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework, Chokhani, et al, November 2003.
- RFC4366, Request for Comments: 4366, Transport Layer Security (TLS) Extensions, Blake-Wilson, et al, April 2006.
- RFC5019, Request for Comments: 5019, The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments, A. Deacon, et al, September 2007.
- RFC5280, Request for Comments: 5280, Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile, Cooper et al, May 2008.ETSI TS 101 042: Policy requirements for certification authorities issuing public key certificates (Normalised level only).
- The ISO 1-7799 standard on security and infrastructure
- FIPS 140-2, Federal Information Processing Standards Publication - Security Requirements For Cryptographic Modules, Information Technology Laboratory, National Institute of Standards and Technology, May 25, 2001.
- X509v3, ITU-T Recommendation X.509 (2005) | ISO/IEC 9594-8:2005, Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks.

This CPS is created according to the requirements of the following schemes and endorses these in whole or in part:

- AICPA/CICA, WebTrust 2.0 Program for Certification Authorities.
- AICPA/CICA, WebTrust For Certification Authorities – Extended Validation Audit Criteria.
- CABForum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates

1.0 Introduction

This Certification Practice Statement (CPS) applies to the products and services of Deutsche Post AG. Primarily this pertains to the issuance and lifecycle management of Digital Certificates including validity checking services. This CPS may be updated from time to time as outlined in section 1.5 *Policy Administration*. The latest version may be found on the following URL http://keyserver.dhl.com/repository .

A CPS highlights the *"procedures under which a Digital Certificate is issued to a particular community and/or class of application with common security requirements"*. This CPS meets the formal requirements of Internet Engineering Task Force (IETF) RFC 3647, dated November 2003 with regard to content, layout and format *(RFC 3647 obsoletes RFC 2527)*. An RFC issued by IETF is an authoritative source of guidance with regard to standard practices in the area of Electronic Signatures and Certificate Management. While certain section titles are included in this policy according to the structure of RFC 3647, the topic may not necessarily apply to Services of Deutsche Post CA. These sections have *'No stipulation'* appended. Where necessary additional information is presented in subsections to the standard structure. Meeting the format requirements of RFC 3647 enhances and facilitates the mapping and interoperability with other third party CAs and provides relying parties with advance notice on the practices and procedures. Additional assertions on standards used in this CPS can be found under section *"Acknowledgements"* on the previous page.

This CPS is final and binding between Deutsche Post AG, a company under public law, with registered office at Charles-de-Gaulle-Straße 20, 53113 Bonn, Germany (Hereinafter referred to as "Deutsche Post CA"),

and

the Subscriber and/or Relying Party, who uses, relies upon or attempts to rely upon certification services made available by the Certification Authority referring to this CPS.

This CPS addresses the technical, procedural and personnel policies and practices of the Deutsche Post CA during the complete life cycle of certificates issued by the Deutsche Post CA.

The Deutsche Post CA operates within the scope of activities of Deutsche Post AG. This CPS addresses the requirements of the CA that issues certificates of various types under the Certificate Policy of GlobalSign nv-sa and its TrustedRoot Program. The chaining to any particular issuing CA may well vary depending on the choice of intermediate certificate and/or cross certificate used or provided by a platform or client.

For Subscribers this CPS becomes effective and binding by accepting a Subscriber Agreement or Terms of use Agreement. For Relying Parties this CPS becomes binding by relying upon a certificate issued under this CPS. In addition, Subscribers are bound by the Subscriber Agreement to inform their Relying Parties that the CPS is itself binding toward those relying parties.

1.1 Overview

This CPS applies to the complete hierarchy of certificates issued by Deutsche Post CA. The purpose of this CPS is to present the practices and procedures in managing certificates and to demonstrate compliance with requirements pertaining to the issuance of digital certificates according to Deutsche Post CA's own and industry requirements pursuant to the standards set out above. This CPS aims at facilitating the Deutsche Post CA in delivering certification services and managing the certificate lifecycle of and issued client, server and other-purpose end entity certificates. The certificate types addressed in this CPS are the following:

SSL/TLS	A certificate to authenticate web servers
SMIME/Client Authentication	A personal certificate of medium assurance with reference to professional context

These certificates shall be issued and managed in accordance with CA/Browser Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates. An indication of compliance is the inclusion of CA/Browser Forum Policy OIDs as detailed in section 1.2.

Deutsche Post CA certificates:

- Can be used for electronic signatures in order to replace handwritten signatures where transacting parties choose for them

- Can be used for encryption of data.
- Can be used to authenticate web resources, such as servers and other devices.

This CPS identifies the roles, responsibilities and practices of all entities involved in the life cycle, use, reliance upon and management of Deutsche Post CA certificates. The provisions of this CPS with regard to practices, level of services, responsibilities and liability bind all parties involved, including Deutsche Post CA, their nominated RA, subscribers and relying parties. Certain provisions might also apply to other entities such as the certification service provider, application provider etc.

A GlobalSign Certificate Policy (CP) complements this CPS. The purpose of the GlobalSign CP is to state the *"what is to be adhered to"* and, therefore, set out an operational rule framework for the broad range of GlobalSign products and services. The latest version of the CP aligning to this CPS can be found on https://www.globalsign.com/repository

This CPS states *"how the Certification Authority adheres to the Certificate Policy".* In doing so this CPS features a greater amount of detail and provides the end user with an overview of the processes, procedures and conditions that the Deutsche Post CA uses in creating and maintaining the certificates that it manages. In addition to this CPS Deutsche Post CA maintains a range of adjacent documented polices which include but are not limited to addressing such issues as:

- Business Continuity and Disaster Recovery
- Security Policy
- Personnel Policies
- Key management Policies
- Registration Procedures

A subscriber or relying party of a certificate must refer to this CPS in order to establish trust in a certificate issued by Deutsche Post CA as well as for notices with regard to the prevailing practices thereof. It is also essential to establish the trustworthiness of the entire certificate chain of the hierarchy. This includes the Root CA as well as any operational certificates. This can be established on the basis of the assertions within this CPS.

1.1.1 Certificate Naming

The exact names of the Deutsche Post CA certificates that make use of this CPS are:

- DPDHL TLS CA I3 with serial number 20 78 f7 7a 21 0a dc ad 57 ae 9b b5 ba fb 41 ba f1
- DPDHL User CA I3 with serial numbers 1f 2c 8f 8b 43 a7 66 3a d0 71 51 d0 e8 87 e6 0d e0

Digital certificates allow entities that participate in an electronic transaction to prove their identity towards other participants or sign data digitally. By means of a digital certificate, Deutsche Post CA provides confirmation of the relationship between a named entity (subscriber) and its public key. The process to obtain a digital certificate includes the identification, naming, authentication and registration of the client as well as aspects of certificate management such as the issuance, revocation and expiration of the digital certificate. By means of this procedure to issue digital certificates, Deutsche Post CA provides adequate and positive confirmation about the identity of the user of a certificate and a positive link to the public key that such an entity uses. Deutsche Post CA makes available digital certificates that can be used for non-repudiation, encryption and authentication.

1.2 Document Name and Identification

This document is the Deutsche Post CA Certification Practice Statement.

The OID for Deutsche Post AG (Deutsche Post CA) is a is 1.3.6.1.4.1.5064. Deutsche Post CA organizes its OID arcs for the various certificates and documents described in this CPS (Which may be updated from time to time) as follows:

2.23.140.1.2.2	SSL/TLS Policy
1.3.6.1.4.1.5064.1.1	SMIME Client Authentication Policy

The OID for GlobalSign nv-sa (GlobalSign CA) is a iso(1) identified-organization (3) dod (6) internet (1) private (4) enterprise (1) GlobalSign nv-sa (4146). GlobalSign CA organizes its OID arcs for the various certificates and documents described in its CP (Which may be updated from time to time) as follows:

1.3.6.1.4.1.4146.1.60	CA Chaining Policy – TrustedRoot™

In addition to these identifiers, all certificates that comply with the CABForum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates will include the additional identifiers as follows:-

2.23.140.1.2.2 Organization Validation Certificates Policy

1.3 PKI participants

1.3.1 Certification Authorities

Deutsche Post CA is a Certification Authority (CA) that issues high quality and highly trusted certificates in accordance with this CPS. As a Certificate Authority, Deutsche Post CA performs functions related to PKI certificate LiveCycle Management such as subscriber registration, certificate issuance, certificate renewal, certificate distribution and certificate revocation. Deutsche Post CA also provides Certificate status information using an online repository in the form of a CRL (Certificate Revocation List) distribution point and/or OCSP (Online Certificate Status Protocol) responder.

Deutsche Post CA ensures the availability of all services pertaining to the management of certificates, including without limitation the issuing, revocation and status verification of a certificate, as they may become available or required in specific applications. Deutsche Post CA also manages a core online registration system and assorted API's for all certificate types, issued under Deutsche Post CA Subordinate/Issuing CAs.

1.3.2 Registration Authorities

A Registration Authority (RA) is an entity that identifies and authenticates applicants for certificates. A RA may also initiate or pass along revocation requests for certificates and requests for re-issuance and renewal (sometimes referred to as rekey) of certificates. Deutsche Post CAs may act as a Registration Authority for certificates it issues in which case they are responsible for:

- Accepting, evaluating, approving or rejecting the registration of certificate applications.
- Registering subscribers for certification services.
- Providing systems to facilitate the identification of subscribers (according to the type of certificate requested).
- Using officially notarised or otherwise authorised documents or sources of information to evaluate and authenticate a subscriber's application.
- Following approval of an application requesting issuance of a certificate via a multifactor authentication process.
- Initiating the process to revoke a certificate from the applicable GlobalSign subordinate issuing CA.

1.3.3 Subscribers

Subscribers to Deutsche Post CA are either legal persons or natural persons that successfully apply for and receive a certificate to support their use in transactions, communications and the application of digital signatures.
The *Subject* of a certificate is the party named in the certificate. A *Subscriber*, as used herein, refers to both the subject of the certificate and the entity that contracted with the Deutsche Post CA for the certificate's issuance. Prior to verification of identity and issuance of a certificate, a Subscriber is an *Applicant*.

Legal persons are identified on the basis of the published by-laws and appointment of Director as well as the subsequent government gazette or other QIIS or QGIS third party databases. Self-employed subjects are identified on the basis of proof of professional registration supplied by the competent authority in the country in which they reside.

For all categories of subscribers, additional credentials are required as explained on the online process for the application for a certificate.

Subscribers of end entity certificates issued under the Deutsche Post CA include employees and agents involved in day-to-day activities within GlobalSign that require access to GlobalSign network resources. Subscribers are also sometimes operational or legal owners of signature creation devices that are issued for the purpose of generating a key pair and storing a certificate.

1.3.4 Relying Parties

Relying parties are natural persons or legal persons that rely on a certificate and/or a digital signature verifiable with reference to a public key listed in a subscriber's certificate.

To verify the validity of a digital certificate, relying parties must always refer to Deutsche Post CA's revocation information either in the form of a Certificate Revocation List (CRL) distribution point or an OCSP responder.

1.3.5 Other Participants

Deutsche Post CA is cross signed by GlobalSign nv-sa via its TrustedRoot Program as detailed within the GlobalSign CP on https://www.globalsign.com/respository

1.4 Certificate Usage

A digital certificate is a specifically formatted data object that cryptographically binds an identified subscriber with a Public Key (supporting either RSA or ECC). A digital certificate allows an entity taking part in an electronic transaction to prove its identity to other participants in such transaction. Digital certificates are used in commercial environments as a digital equivalent of an identification card.

1.4.1 Appropriate certificate usage

End entity certificate use is restricted by using certificate extensions on key usage and extended key usage. Certificates issued by Deutsche Post CA can be used for public domain transactions that require:

- **Non-repudiation:** A party cannot deny having engaged in the transaction or having sent the electronic message.
- **Authentication:** The assurance to one entity that another entity is who he/she/it claims to be.
- **Confidentiality:** The assurance to an entity that no one can read a particular piece of data except the receiver(s) explicitly intended.
- **Integrity:** The assurance to an entity that data has not been altered intentionally or unintentionally) from sender to recipient and from time of transmission to time of receipt.

Digital signature: Digital (Electronic) signature can only be used for specific transactions that support digital signing of electronic forms, electronic documents, electronic mail etc. The signature certificate is only warranted to produce digital signatures in the context of applications that support digital certificates. Certificates that are appropriate for digital signatures are the following:

- SMIME/Client Authentication**:** authentication of a natural person (medium level assurance)
- SMIME/Client Authentication (Department) **:** authentication of a natural person within an organizational context or a role within an organizational context (medium level assurance)

Authentication (Users): User authentication certificates can be used for specific electronic authentication transactions that support accessing web sites and other online content, electronic mail etc. The Authentication function of a digital certificate can be ascertained in any transaction context with the purpose of authenticating the end user subscriber to a digital certificate. To describe the function of authentication, the term digital signature is often used.

- SMIME/Client Authentication**:** authentication of a natural person (medium level assurance)
- SMIME/Client Authentication (Department) **:** authentication of a natural person within an organizational context or a role within an organizational context (medium level assurance)

Authentication (Devices and objects): Device authentication certificates can be used for specific electronic authentication transactions that support the identifying of web sites and other on line resources, such as software objects etc. The authentication function of a digital certificate can be ascertained in any transaction context with the purpose of authenticating a device that the subscriber seeks to secure through a digital certificate. To describe the function of authentication, the term digital signature is often used.

- SSL/TLS: authentication of a remote domain name and associated organizational context and webservice and encryption of the communication channel
- SMIME/Client Authentication**:** authentication of a natural person (medium level assurance)

- SMIME/Client Authentication (Department) **:** authentication of a natural person within an organizational context or a role within an organizational context (medium level assurance)

Assurance levels: Subscribers should choose an appropriate level of assurance to which relying parties will confidently transact. For example Subscribers with an unknown brand name should positively assure relying parties of their identity with a High Assurance (EV) certificate where as a closed community with a well known URL may chose a Low Assurance solution.

- **Low assurance:** (Class 1) certificates are not suitable for identity verification as no authenticated identity information is included within the certificate. This in turn does not support non repudiation services.
- **Medium assurance:** (Class 2) certificates are individual and organizational certificates that are suitable for securing some inter- and intra-organizational, commercial, and personal e-mail requiring a medium level of assurances of the subject identity contained within the certificate.
- **High assurance:** (Class 3) certificates are individual and organizational certificates that provide a high level of assurance of the identity of the subject in comparison with Class 1 and 2.

Confidentiality: All certificate types can be used to ensure the confidentiality of communications effected by means of digital certificates. Confidentiality may apply to business and personal communications as well as personal data protection and privacy.

Any other use of a digital certificate is not supported by this CPS. When using a digital certificate the functions of electronic signature (non repudiation) and authentication (digital signature) are permitted together within the same certificate. The different terms relate to different terminologies used by IETF and the vocabulary adopted within the legal framework of the European Union Directive 1999/93/EC (A Community framework on electronic signatures).

1.4.2 Prohibited certificate usage

Certificate use is restricted by using certificate extensions on key usage and extended key usage. Any usage of the certificate inconsistent with these extensions is not authorised.

Certificates issued under this CPS do not guarantee that the Subject is trustworthy, operating a reputable business or that the equipment into which the certificate has been installed is not free from defect, malware or virus.

Certificates issued under this CPS may not be used:-

- for any application requiring fail safe performance such as
  - the operation of nuclear power facilities,
  - air traffic control systems,
  - aircraft navigation systems,
  - weapons control systems,
  - any other system whose failure could lead to injury, death or environmental damage;
- where prohibited by law.

1.4.2.1 Certificate extensions

Certificate extensions comply to X.509 v.3 standards. EKU = Enhanced or Extended Key usage

- SSL/TLS: Client and Server Authentication EKU
- SMIME/Client Authentication: Client Authentication and Secure email EKU

1.4.2.2 Critical Extensions

Deutsche Post CA also uses certain critical extensions in the certificates it issues such as:

- A basic constraint in the key usage to show whether a certificate is meant as a CA or not.
- To show the intended usage of the key.
- To show the number of levels in the hierarchy under a CA certificate.

1.5 Policy Administration

1.5.1 Organization Administering the Document

Request for information on the compliance of Issuing CAs with accreditation schemes as well as any other inquiry associated with this CPS can be addressed to:

dcns-sa-pki@dhl.com

1.5.2 Contact Person

isaac.bediako.odei@dhl.com
lukas.geyer@dhl.com

1.5.3 Person Determining CPS Suitability for the Policy

lukas.geyer@dhl.com

1.5.4 CPS Approval Procedures

The CPS is a subject to approval by the members of the Data Center Network Services SA PKI.

1.5.4.1 Changes with notification

Updated versions of this CPS are notified to parties that have a legal duty to receive such updates, for example auditors with a specific mandate to do so.

1.5.4.2 Version management and denoting changes

Changes are denoted through new version numbers for the CPS. New versions are indicated with an integer number followed by one decimal that is zero. Minor changes are indicated through one decimal number that is larger than zero. Minor changes include:

- Minor editorial corrections
- Changes to contact details

1.6 Definitions and acronyms

Affiliate: A corporation, partnership, joint venture or other entity controlling, controlled by, or under common control with another entity, or an agency, department, political subdivision, or any entity operating under the direct control of a Government Entity.

Applicant: The natural person or Legal Entity that applies for (or seeks renewal of) a Certificate. Once the Certificate issues, the Legal Entity is referred to as the Subscriber. For Certificates issued to devices, the Applicant is the entity that controls or operates the device named in the Certificate, even if the device is sending the actual Certificate Request.

Applicant Representative: A natural person or human sponsor who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant: (i) who signs and submits, or approves a Certificate Request on behalf of the Applicant, and/or (ii) who signs and submits a Subscriber Agreement on behalf of the Applicant, and/or (iii) who acknowledges and agrees to the Certificate Terms of Use on behalf of the Applicant when the Applicant is an Affiliate of the CA.

Application Software Supplier: A supplier of Internet browser software or other relying-party application software that displays or uses Certificates and incorporates Root Certificates.

Attestation Letter: A letter attesting that Subject Information is correct.

Audit Criteria: The requirements described in this document and any requirements that an entity must follow in order to satisfy the audit scheme selected under section 16.1

Audit Report: A statement, report, or letter issued by a Qualified Auditor stating a CA's or RA's compliance with these Requirements.

Binding: A statement by an RA of the relationship between a named entity and its public key.

CDS (Certified Document Services): A document signing architecture created by the Adobe Root CA policy authority implemented from Adobe PDF Reader version 6.0.

Certificate: An electronic document that uses a digital signature to bind a public key and an identity.

Certificate Data: Certificate Requests and data related thereto (whether obtained from the Applicant or otherwise) in the CA's possession or control or to which the CA has access.

Certificate Management Process: Processes, practices, and procedures associated with the use of keys, software, and hardware, by which the CA verifies Certificate Data, issues Certificates, maintains a Repository, and revokes Certificates.

Certificate Policy: A set of rules that indicates the applicability of a named Certificate to a particular community and/or PKI implementation with common security requirements.

Certificate Problem Report: Complaint of suspected Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to Certificates.

Certificate Request: Communications described in Section 10 requesting the issuance of a Certificate.

Certificate Revocation List: A regularly updated time-stamped list of revoked Certificates that is created and digitally signed by the CA that issued the Certificates.

Certification Authority: An organization that is responsible for the creation, issuance, revocation, and management of Certificates. The term applies equally to both Roots CAs and Subordinate CAs.

Certification Practice Statement: One of several documents forming the governance framework in which Certificates are created, issued, managed, and used.

Compromise: A violation of a security policy that results in loss of control over sensitive information.

Cross Certificate: A certificate that is used to establish a trust relationship between two Root CAs.

Digital Signature: To encode a message by using an asymmetric cryptosystem and a hash function such that a person having the initial message and the signer's public key can accurately determine whether the transformation was created using the private key that corresponds to the signer's public key and whether the initial message has been altered since the transformation was made.

Domain Authorization: Correspondence or other documentation provided by a Domain Name Registrant attesting to the authority of an Applicant to request a certificate for a specific Domain Namespace.

Domain Name: The label assigned to a node in the Domain Name System.

Domain Namespace: The set of all possible Domain Names that are subordinate to a single node in the Domain Name System.

Domain Name Registrant: Sometimes referred to as the "owner" of a Domain Name, but more properly the person(s) or entity(ies) registered with a Domain Name Registrar as having the right to control how a Domain Name is used, such as the natural person or Legal Entity that is listed as the "Registrant" by WHOIS or the Domain Name Registrar.

Domain Name Registrar: A person or entity that registers Domain Names under the auspices of or by agreement with: (i) the Internet Corporation for Assigned Names and Numbers (ICANN), (ii) a national Domain Name authority/registry, or (iii) a Network Information Center (including their affiliates, contractors, delegates, successors, or assigns).

Effective Date: The date, as determined by the eligible audit schemes, on which Requirements come into force.

Enterprise Certificate: A Certificate whose issuance is authorized by an Enterprise RA.

Enterprise RA: An employee or agent of an organization unaffiliated with the CA who authorizes issuance of Certificates to that organization.

Fully-Qualified Domain Name: A Domain Name that includes the labels of all superior nodes in the Internet Domain Name System.

Government Entity: A government-operated legal entity, agency, department, ministry, branch, or similar element of the government of a country, or political subdivision within such country (such as a state, province, city, county, etc.).

Hash: (e.g. SHA1 or SHA256) - An algorithm that maps or translates one set of bits into another (generally smaller) set in such a way that:

- A message yields the same result every time the algorithm is executed using the same message as input.
- It is computationally infeasible for a message to be derived or reconstituted from the result produced by the algorithm.
- It is computationally infeasible to find two different messages that produce the same hash result using the same algorithm.

HSM: Hardware Security Module: A HSM is type of secure crypto processor targeted at managing digital keys, accelerating crypto processes in terms of digital signings/second and for providing strong authentication to access critical keys for server applications.

Internal Server Name: A Server Name (which may or may not include an Unregistered Domain Name) that is not resolvable using the public DNS.

Issuing CA: In relation to a particular Certificate, the CA that issued the Certificate. This could be either a Root CA or a Subordinate CA.

Incorporate by Reference: To make one document a part of another by identifying the document to be incorporated, with information that allows the recipient to access and obtain the incorporated message in its entirety, and by expressing the intention that it be part of the incorporating message. Such an incorporated message shall have the same effect as if it had been fully stated in the message.

Independent Audit: An audit that is performed by a Qualified Auditor and that determines an entity's compliance with these Requirements and one or more of the audit schemes listed in Section 16.1.

Key Compromise: A Private Key is said to be compromised if its value has been disclosed to an unauthorized person, an unauthorized person has had access to it, or there exists a practical technique by which an unauthorized person may discover its value.

Key Pair: The Private Key and its associated Public Key.

Legal Entity: An association, corporation, partnership, proprietorship, trust, government entity or other entity with legal standing in a country's legal system.

Object Identifier: A unique alphanumeric or numeric identifier registered under the International Organization for Standardization's applicable standard for a specific object or object class.

OCSP Responder: An online server operated under the authority of the CA and connected to its Repository for processing Certificate status requests. See also, Online Certificate Status Protocol.

Online Certificate Status Protocol: An online Certificate-checking protocol that enables relying-party application software to determine the status of an identified Certificate. See also OCSP Responder.

Private Key: The key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create Digital Signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.

Public Key: The key of a Key Pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify Digital Signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.

Public Key Infrastructure: A set of hardware, software, people, procedures, rules, policies, and obligations used to facilitate the trustworthy creation, issuance, management, and use of Certificates and keys based on Public Key Cryptography.

Publicly-Trusted Certificate: A Certificate that is trusted by virtue of the fact that its corresponding Root Certificate is distributed as a trust anchor in widely-available application software.

Registered Domain Name: A Domain Name that has been registered with a Domain Name Registrar.

Registration Authority (RA): Any Legal Entity that is responsible for identification and authentication of subjects of certificates, but is not a CA, and hence does not sign or issue certificates. An RA may assist in the certificate application process or revocation process or both. When "RA" is used as an adjective to describe a role or function, it does not necessarily imply a separate body, but can be part of the CA.

Relying Party: Any natural person or Legal Entity that relies on a Valid Certificate. An Application Software Supplier is not considered a Relying Party when software distributed by such Supplier merely displays information relating to a Certificate.

Repository: An online database containing publicly-disclosed PKI governance documents (such as Certificate Policies and Certification Practice Statements) and Certificate status information, either in the form of a CRL or an OCSP response.

Reserved IP Address: An IPv4 or IPv6 address that the IANA has marked as reserved:

http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml

http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xml

Root CA: The top level Certification Authority whose Root Certificate is distributed by Application Software Suppliers and that issues Subordinate CA Certificates.

Root Certificate: The self-signed Certificate issued by the Root CA to identify itself and to facilitate verification of Certificates issued to its Subordinate CAs.

Root Key Generation Script: A documented plan of procedures for the generation of the Root CA Key Pair**.**

Subject: The natural person, device, system, unit, or Legal Entity identified in a Certificate as the Subject. The Subject is either the Subscriber or a device under the control and operation of the Subscriber.

Subject Identity Information: Information that identifies the Certificate Subject. Subject Identity Information does not include a domain name listed in the subjectAltName extension or the commonName field.

Subordinate CA: A Certification Authority whose Certificate is signed by the Root CA, or another Subordinate CA.

Subscriber: A natural person or Legal Entity to whom a Certificate is issued and who is legally bound by a Subscriber or Terms of Use Agreement.

Subscriber Agreement: An agreement between the CA and the Applicant/Subscriber that specifies the rights and responsibilities of the parties.

Terms of Use: Provisions regarding the safekeeping and acceptable uses of a Certificate issued in accordance with these Requirements when the Applicant/Subscriber is an Affiliate of the CA.

TPM: Trusted Platform Module – A hardware cryptographic device which is defined by the Trusted Computing Group. https://www.trustedcomputinggroup.org/specs/TPM.

Trustworthy System: Computer hardware, software, and procedures that are: reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy.

Unregistered Domain Name: A Domain Name that is not a Registered Domain Name.

Valid Certificate: A Certificate that passes the validation procedure specified in RFC 5280.

Validation Specialists: Someone who performs the information verification duties specified by these Requirements.

WebTrust Program for CAs: The then-current version of the AICPA/CICA WebTrust Program for Certification Authorities.

WebTrust Seal of Assurance: An affirmation of compliance resulting from the WebTrust Program for CAs.

Wildcard Certificate: A Certificate containing an asterisk (*) in the left-most position of any of the Subject Fully-Qualified Domain Names contained in the Certificate.

X.509: The standard of the ITU-T (International Telecommunications Union-T) for digital certificates.

LRA	Local Registration Authority
ETSI	European Telecommunications Standards Institute
GSCA	GlobalSign Certification Authority
IETF	Internet Engineering Task Force
ISO	International Standards organization
ITU	International Telecommunications Union
RFC	Request for Comments
SSCD	Secure Signature Creation Device
VAT	Value Added Tax
AICPA	American Institute of Certified Public Accountants
CA	Certification Authority
ccTLD	Country Code Top-Level Domain
CICA	Canadian Institute of Chartered Accountants
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DBA	Doing Business As
DNS	Domain Name System
FIPS	(US Government) Federal Information Processing Standard
FQDN	Fully Qualified Domain Name
IM	Instant Messaging
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ISO	International Organization for Standardization

NAESB	North American Energy Standards Board
NIST	(US Government) National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PKI	Public Key Infrastructure
RA	Registration Authority
S/MIME	Secure MIME (Multipurpose Internet Mail Extensions)
SSL	Secure Sockets Layer
TLD	Top-Level Domain
TLS	Transport Layer Security
VOIP	Voice Over Internet Protocol

2.0 Publication and Repository Responsibilities

2.1 Repositories

Deutsche Post CA publishes all CA certificates revocation data for issued certificates, CPS, and any Relying Party Agreements or Subscriber Agreements in online repositories. Deutsche Post CA ensures that revocation data for issued certificates is available through a repository 24 hours a day, 7 days a week with a minimum of 99% availability overall per year with a scheduled down-time that does not exceed 0.5% annually

Deutsche Post CA may publish submitted information on publicly accessible directories for the provision of certificate status information.

Deutsche Post CA refrains from making publicly available certain elements of documentation including security controls, procedures, internal security polices etc. However elements may be disclosed in audits associated with formal accreditation schemes such as WebTrust 2.0.

2.2 Publication of Certificate Information

Deutsche Post CA publishes its CPS, Subscriber Agreements, Relying Party Agreements on the following URL http://keyserver.dhl.com/repository/. CRLs are published in online repositories. The CRLs contain entries for all revoked un-expired certificates and are valid, depending on certificate type.

2.3 Time or Frequency of Publication

CRLs for end-user certificates are issued at least every 20 minutes. CRLs for CA certificates are issued at least every 6 months and within 24 hours if a CA certificate is revoked. Each CRL includes a monotonically increasing sequence number for each CRL issued.

New or modified versions of this CPS, Subscriber Agreements, or Relying Party Warranties are published within seven days.

2.4 Access control on repositories

Access to repositories is limited to Certificate Authority Administrators (CAA) appointed by DCNS SA PKI.

3.0 Identification and Authentication

Deutsche Post CA operates an RA that verifies and authenticates the identity and/or other attributes of an applicant applying for a certificate and that the Applicant is either a subsidiary or parent to Deutsche Post CA.

Certificate Applicants are prohibited from using names in their certificate that infringe upon the Intellectual Property Rights of others.

GlobalSign RAs authenticate the requests of parties wishing to revoke certificates.

3.1 Naming

3.1.1 Types of Names

Deutsche Post CA certificates are issued with subject DNs (Distinguished Names) which meet the requirements of X.500 naming, RFC-822 naming and X.400 naming. CNs (Common Names) respect name space uniqueness and are not misleading.

Non wildcard SSL Certificates are issued with a Fully Qualified Domain Name (FQDN) name or IP address.

Wildcard SSL Certificates include a wildcard asterisk character. Before issuing a certificate with a wildcard character (*) Deutsche Post CA follows best practices to determine if the wildcard character occurs in the

first label position to the left of a “registry-controlled” label or “public suffix”. (e.g. “*.com”, “*.co.uk”, see RFC 6454 Section 8.2 for further explanation.) and if it does, it will reject the request as the domain space must be owned or controlled by the subscriber. e.g. *.dhl.com

In the case of SSL certificates, whilst the FQDN or authenticated domain name is placed in the Common Name (CN) attribute of the Subject field, it may also be duplicated into the Subject Alternative Name extension along with a www version of the DNS-ID. Subject Alternative Names are marked non critical in line with RFC5280.

3.1.2 Need for Names to be Meaningful

Where possible, Deutsche Post CA uses distinguished names to identify both the subject and the Issuer of a certificate. In cases where a Deutsche Post CA product allows the use of role or departmental name then additional unique elements may be added to the DN within the OU field to allow differentiation by relying parties.

3.1.3 Anonymity or Pseudonymity of Subscribers

Deutsche Post CAs may issue end-entity anonymous or pseudonymous certificates provided that such certificates are not prohibited by applicable policy and where possible name space uniqueness is preserved. Deutsche Post CA reserves the right to disclose the identity of the subscriber if required by law or following a reasoned and legitimate request

3.1.4 Rules for Interpreting Various Name Forms

Distinguished Names in Certificates are interpreted using X.500 standards and ASN.1 syntax. See RFC 2253 and RFC 2616 for further information on how X.500 distinguished names in certificates are interpreted as Uniform Resource Identifiers and HTTP references.

3.1.5 Uniqueness of Names

Deutsche Post CA enforces the uniqueness of each subject name in a certificate as follows.

• SSL/TLS:	A domain name within the Common Name attribute as approved as unique by ICANN, the Internet Corporation for Assigned names and Numbers.
• SMIME/Client Authentication:	A unique e-mail address coupled with an organizations name and address plus the name of and individual.

3.1.6 Recognition, Authentication, and Role of Trademarks

Subscribers may not request certificates with any content that infringes the intellectual property rights of another entity. Unless otherwise specifically stated Deutsche Post CA does not require that an Applicant’s right to use a trademark be verified. Deutsche Post CA has the right to revoke any certificate that is part of a dispute.

3.2 Initial Identity Validation

Deutsche Post CA may perform identification of the applicant for a certificate using any legal means of communication or investigation necessary to identify the legal person or individual.

3.2.1 Method to Prove Possession of Private Key

Subscribers must prove possession of the private key corresponding to the public key being registered either as a CSR (Certificate Signing Request) in PKCS#10 format or as a Signed Public Key and Challenge (SPKAC).

3.2.2 Authentication of Organization Identity

For all certificates that include an Organization Identity, Applicants are required to indicate the Organization’s name and registered or trading address. For all certificates the Legal existence, Legal name, Legal form and requested address of the Organization is verified using one of the following:-

- A Government agency in the jurisdiction of the applicant
- A third party data base that is periodically updated and has been evaluated by GlobalSign to determine that it is reasonably accurate and reliable
- An Attestation letter confirming that Subject Information is correct written by an accountant, lawyer, government official, or other reliable third party customarily relied upon for such information

The authority of the Applicant to request a certificate on behalf of the Organization is verified in accordance with section 3.2.5.

For SSL/TLS Certificates, the applicant's ownership or control of all requested Domain(s) is authenticated by one of the following methods;

- Using GlobalSign's OneClickSSL protocol whereby the applicant is required to demonstrate control of a domain by installing a non publically trusted test certificate of GlobalSign's design, or;
- By uploading specific meta-data to a defined page on the domain, or;
- By direct confirmation with the contact listed by the Domain Name Registrar in the WHOIS record, or;
- By successfully replying to a challenge response e-mail sent to one or more of the following email addresses:
    - webmaster@domain.com, postmaster@domain, admin@domain.com, administrator@domain.com, hostmaster@domain, or
    - any e-mail address listed as a contact field of the WHOIS record, or
    - any address previously used for the successful validation of the control of the domain subject to the aging requirements of 3.3.1
- By receiving a reliable communication from the Domain Name Registrar stating that the Registrant gives the Applicant permission to use the Domain

Further information may be requested from the applicant and other information and or methods may be utilized in order to demonstrate an equivalent level of confidence.

3.2.2.1 Role Based Certificate Authentication

No stipulation.

3.2.3 Authentication of Individual identity

Deutsche Post CA Authenticates Individuals depending upon the class of certificate as indicated below.

3.2.3.1 Class 1

Class 1 certificates are not supported.

3.2.3.2 Class 2 (SMIME/Client Authentication)

The Applicant is required to demonstrate control of any email address to be included within a certificate.

Deutsche Post AG also authenticates the Applicant's identity through one of the following methods;

- Performing a telephone challenge/response to the Applicant using a number from a reliable source, or;
- Performing a postal challenge to the Applicant using an address obtained from a reliable source, or;
- Receiving an attestation from an appropriate Notary, Trusted Third Party that they have met the individual, and have inspected their National Photo ID document, and that the application details for the order are correct, or;
- The applicant's Seal Impression, (In jurisdictions that permit their use to legally sign a document) is included with any application received in writing.

Deutsche Post AG may request further information from the Applicant. Other information and/or methods may be utilized in order to demonstrate an equivalent level of confidence.

3.2.4 Non Verified Subscriber Information

Deutsche Post CA validates all information to be included within the Subject DN of a certificate except where highlighted within this section of the CPS. Deutsche Post CA uses the Subject:organizationalUnitName as a suitable location to highlight Non Verified Subscriber Information to relying parties or to highlight any specific disclaimers/notices.

- For all certificate types where Deutsche Post CA can explicitly identify a name, DBA, tradename, trademark, address, location, or other text that refers to a specific natural person or Legal Entity the Deutsche Post CA verifies the information and omits any disclaimer notice.

- For all certificate types where Deutsche Post CA cannot explicitly verify the identity e.g. a generic term such as “Marketing” then Deutsche Post CA also omits any disclaimer but notes within this CPS that this item is therefore classified as Non Verified Subscriber Information.

Specifically for SSL/TLS certificates, Deutsche Post CA maintains an enrolment process which ensures that Applicants cannot add self reported information to the subject:organizationalUnitName.

3.2.5 Validation of Authority

- **SSL/TLS -** Verification through a reliable means of communication with the organization or individual applicant together with verification that the applicant has ownership or control of the domain name by either a challenge response mechanism or direct confirmation with the contact listed with the Domain Name Registrar or WHOIS.
- **SMIME/Client Authentication -** Verification through a reliable means of communication with the organization or individual applicant together with verification that the applicant has control over the e-mail address to be listed within the certificate.

3.2.6 Criteria for Interoperation

Not applicable

3.3 Identification and Authentication for Re-key Requests

No stipulation

3.3.1 Identification and Authentication for Re-key After Revocation

No stipulation

3.4 Identification and Authentication for Revocation Request

All revocation requests are authenticated by Deutsche Post CA. Revocation requests may be granted following a suitable challenge response such as, logging into an account with a suitable username and password, proving possession of unique elements incorporated into the certificate e.g. domain name or e-mail address or authentication of specific information which is authenticated out of band.

Deutsche Post CA may also perform revocation on behalf of subscribers in line with requirements highlighted within its Subscriber Agreements. Examples include a breach of the subscriber agreement or non payment of applicable fees.

4.0 Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

Deutsche Post CA maintains its own blacklists of individuals from whom and entities from which it will not accept certificate applications. In addition, other external sources such as government denied lists or internationally recognised denied persons lists which are applicable to the jurisdictions in which Deutsche Post CA operates are used to screen out unwanted applicants.
Deutsche Post CA does not issue certificates to entities that reside in countries where the laws of a Deutsche Post CA office location prohibit doing business.

Applications are accepted as follows:-

- **On-line:** Via a web interface over a https session. A certificate applicant must submit an application via a secure ordering process according to a procedure maintained by Deutsche Post CA.

4.1.2 Enrolment Process and Responsibilities

Deutsche Post CA maintains systems and processes that sufficiently authenticate the applicants identity for all certificate types that present the identity to relying parties. Applicants must submit sufficient information to allow Deutsche Post CA and any RA to successfully perform the required verification. Deutsche Post CAs and RAs shall protect all communications and securely store all information presented by the applicant during the application process.

Generally the application process includes the following steps but not necessarily in this order as some workflow processes generate keys after the validation has been completed:-

- Generating a suitable key pair using a suitably secure platform.
- Generating a Certificate Signing Request (CSR) using an appropriately secure tool.
- Submitting a request for a certificate type and appropriate information
- Agreeing to a Subscriber Agreement or applicable Terms and Conditions
- Paying any Applicable Fees

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

Deutsche Post CA maintains systems and processes that sufficiently authenticate the applicants identity in line with the applicable statements made in this CPS. Initial identity vetting may be performed by Deutsche Post CA's Validation team in line with section 3.2 or by Registration Authorities under contract.

4.2.2 Approval or Rejection of Certificate Applications

Deutsche Post CA shall reject requests for certificates where validation of all items cannot successfully be completed. Deutsche Post CA may also reject requests based on potential brand damage to Deutsche Post CA in accepting the request. Deutsche Post CA may also reject requests for certificates from applicants who have previously been rejected or have previously violated a stipulation within their Subscriber Agreement or Terms of use Agreement.

Assuming all validation steps can be completed successfully following the procedures within this CPS then Deutsche Post CA shall approve the certificate request.

Deutsche Post CA is under no obligation to provide a reason to an applicant on why a request has been rejected.

4.2.3 Time to Process Certificate Applications

Deutsche Post CA shall ensure that all reasonable methods are used in order to evaluate and process certificate applications. Where issues occur which are outside of the control of Deutsche Post CA, then Deutsche Post CA shall strive to keep the applicant duly informed.

The following approximations are given for processing and issuance.

- **SSL/TLS -** Approximately 1 business day.
- **SMIME/Client Authentication -** Approximately 10 minutes.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

Deutsche Post CA shall ensure it communicates with any RA accounts capable of causing certificate issuance using multifactor authentication. This includes RAs directly operated by Deutsche Post CA or RAs contracted by Deutsche Post CA. RAs shall perform validation of all information sent to the CA and ensure that any database used to store any information is suitably protected from unauthorised modification or tampering.

4.3.2 Notifications to Subscriber by the CA of Issuance of Certificate

Deutsche Post CA shall inform the subscriber of the issuance of a certificate to an e-mail address which was supplied by the subscriber during the enrolment process or by any other equivalent method. The e-mail may contain the certificate itself or a link to download depending upon the workflow of the certificate requested.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

The Digital Certificate is deemed acceptable upon issuance.

4.4.2 Publication of the Certificate by the CA

Deutsche Post CA publishes the certificate by delivering it to the Subscriber.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

RAs, Local RA or partners/resellers or Deutsche Post CA may be informed of the issuance if they were involved in the initial enrolment.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

Subscribers must protect their Private Key taking care to avoid disclosure to third parties. Deutsche Post CA provides a suitable Subscriber Agreement or Terms of Use Agreement, which highlights the obligations of the subscriber with respect to Private Key protection. Private Keys must only be used as specified in the appropriate key usage and extended key usage fields as indicated in the corresponding digital certificate. Where it is possible to make a back up of a private key, Subscribers must use the same level of care and protection attributed to the live private key. At the end of the useful life of a Key, Subscribers must securely delete the key and any fragments that it has been split into for the purposes of backup.

4.5.2 Relying Party Public Key and Certificate Usage

Within this CPS Deutsche Post CA provides the conditions under which digital certificates may be relied upon by relying parties, including the appropriate certificate services to verify certificate validity, such as CRL and/or OCSP. Deutsche Post CA provides a Relying Party agreement to Subscribers the content of which should be presented to the Relying Party prior to reliance upon a digital certificate from the Deutsche Post CA. Relying Parties should use the information to make a risk assessment and as such are solely responsible for performing the risk assessment prior to relying on the certificate or any assurances made.
Software used by relying parties should be fully compliant with X.509 standards including best practice for chaining decisions around policies and key usage.

4.6 Certificate Renewal

4.6.1 Circumstances for Certificate Renewal

Subscribers may renew certificates issued by the Deutsche Post CA by submitting a CSR using the existing private/public key pair of the certificate to be renewed.

4.6.2 Who May Request Renewal

As per 4.1

4.6.3 Processing Certificate Renewal Requests

As per 4.2

4.6.4 Notification of New Certificate Issuance to Subscriber

As per 4.3.2

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

As per 4.4

4.6.6 Publication of the Renewal Certificate by the CA

As per 4.4.2

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

As per 4.4.3

4.7 Certificate Re-Key

4.7.1 Circumstances for Certificate Re-Key

The Deutsche Post CA certificates can be re-keyed. Re-keying refers to a process of creating a new certificate that has the same characteristics and level of assurance as the previous one but uses a different private/public key and has a different serial number.

4.7.2 Who May Request Certification of a New Public Key

As per 4.1

4.7.3 Processing Certificate Re-Keying Requests

As per 4.2

4.7.4 Notification of New Certificate Issuance to Subscriber

As per 4.3.2

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

As per 4.4.1

4.7.6 Publication of the Re-Keyed Certificate by the CA

As per 4.4.2

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

As per 4.4.3

4.8 Certificate Modification

4.8.1 Circumstances for Certificate Modification

Certificate modification is defined as the production of a new certificate that has the details which differ from a previously issued certificate. The new modified certificate may or may not have a new public key and may or may not have a new 'Not After' date.

- Deutsche Post CA treats Modification the same as 'New' issuance.

4.8.2 Who May Request Certificate Modification

As per 4.1

4.8.3 Processing Certificate Modification Requests

As per 4.2

4.8.4 Notification of New Certificate Issuance to Subscriber

As per 4.3.2

4.8.5 Conduct Constituting Acceptance of Modified Certificate

As per 4.4.1

4.8.6 Publication of the Modified Certificate by the CA

As per 4.4.2

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

As per 4.4.3

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

Certificate revocation is a process whereby the serial number of a certificate is effectively blacklisted by adding the serial number and the date of the revocation to a CRL (Certificate Revocation List). The CRL itself will then be digitally signed with the same key material, which originally signed the certificate to be revoked. Adding a serial number allows relying parties to establish that the lifecycle of a digital certificate has ended. Deutsche Post CA may remove serial numbers when revoked certificates pass their expiration date to promote more efficient CRL file size management. Prior to performing a revocation Deutsche Post CA will verify the authenticity of the revocation request. Revocation may be performed under the following circumstances:-

- The Subscriber requests revocation through an authenticated request to Deutsche Post CA's Support team or Deutsche Post CA's Registration Authority,
- Deutsche Post CA obtains reasonable evidence that the Subscriber's Private Key (corresponding to the Public Key in the Certificate) has been compromised, created using a weak algorithm, or that the Digital Certificate has otherwise been misused,
- Deutsche Post CA receives notice or otherwise becomes aware that a Subscriber violates any of its material obligations under the Subscriber Agreement or Terms of Use Agreement,
- Deutsche Post CA receives notice or otherwise becomes aware that a Subscriber uses the certificate for criminal activities such as phishing attacks, fraud, certifying or signing malware etc.,
- Deutsche Post CA receives notice or otherwise becomes aware that a court or arbitrator has revoked a Subscriber's right to use any of the elements within the 'Subject' or 'Subject Alternative

Name' of the Digital Certificate, or that the Subscriber has failed to renew or maintain control of any of those elements,

- Deutsche Post CA receives notice or otherwise becomes aware of a material change in the information contained in the Digital Certificate,
- A determination, in Deutsche Post CA's sole discretion, that the Digital Certificate was not issued according to best practice or any of Deutsche Post CA's own published policies,
- If Deutsche Post CA determines that any of the information appearing in the Digital Certificate is not accurate,
- Deutsche Post CA ceases operations for any reason and has not arranged for another CA to provide revocation support for the Digital Certificate,
- Deutsche Post CA's right to issue Digital Certificates expires or is revoked or terminated,
- Deutsche Post CA's Private Key for the relevant issuing CA Certificate is compromised,
- Deutsche Post CA receives notice or otherwise become aware that a Subscriber has been added as a denied party or prohibited person to a blacklist, or is operating from a prohibited destination under the laws of Deutsche Post CA's jurisdiction of operation,
- The continued use of the certificate is harmful to the business of Deutsche Post CA and relying parties.
- The subscriber suspects the loss of a pass phrase to any hardware token which therefore leads to the loss of control of the private key on the token.

When considering whether certificate usage is harmful to Deutsche Post CA then Deutsche Post CA considers, among other things, the following:

- The nature and number of complaints received,
- The identity of the complainant(s),
- Relevant legislation in force, and
- Responses to the alleged harmful use from the Subscriber.

4.9.2 Who Can Request Revocation

Deutsche Post CAs and RAs shall accept authenticated requests for revocation. Authorization for revocation shall be accepted if the revocation request is received from either the Subscriber or an affiliated organization named in the certificate. Deutsche Post CAs may also at its own discretion revoke certificates.

4.9.3 Procedure for Revocation Request

Once revoked, the serial number of the certificate and the date and time shall be added to the appropriate CRL. CRL reason codes may be included. CRLs are published according to this CPS.

4.9.4 Revocation Request Grace Period

The 'revocation request grace period' is the time available for a Subscriber to take any necessary actions themselves in order to request revocation of a suspected key compromise, use of a weak key or discovery of inaccurate information within an issued certificate. Subscribers are given 24-48 hours to take appropriate actions otherwise Deutsche Post CA may revoke the certificate. A risk analysis shall be completed and recorded for any revocations that cannot be processed by either party for any reason.

4.9.5 Time Within Which CA Must Process the Revocation Request

Deutsche Post CA will begin investigation procedures for a suspected key compromise or misuse of a certificate within 24 (twenty-four) hours of receipt of the report.

All revocation requests for End Entity Certificates, both those generated automatically via user accounts and those initiated by Deutsche Post CA itself must be processed within a maximum of 30 minutes of receipt.

4.9.6 Revocation Checking Requirements for Relying Parties

Prior to relying upon a certificate, relying parties must validate the suitability of the certificate to the purpose intended as well as ensuring the certificate is valid. Relying parties will need to consult CRL or OCSP information for each certificate in the chain as well as validating that the certificate chain itself is complete and follows IETF PKIX standards. This may include the validation of Authority Key Identifier (AKI) and Subject Key Identifier (SKI). Deutsche Post CA will include all applicable URIs within the certificate to aid relying parties perform the revocation checking process such as:-

- http://crl.globalsign.com/gs/
- http://ocsp2.globalsign.com
- http://keyserver.dhl.com/pki/i3/dpdhl_tls_i3.crl
- http://keyserver.dhl.com/pki/i3/dpdhl_user_i3.crl
- http://ocsp-g3.dhl.com/

4.9.7 CRL Issuance Frequency

The Deutsche Post CA revocation lists are generated every 20 minutes.

4.9.8 Maximum Latency for CRLs

Deutsche Post CA ensures that online CA CRLs are published every 20 minutes. A request for revocation received from Deutsche Post CA's RA system during the 3 hour period prior to the next scheduled CRL is included within the CRL if received up to 30 minutes prior.

4.9.9 On-Line Revocation/Status Checking Availability

Deutsche Post CA supports OCSP responses in addition to CRLs. Response times are no longer than 10 seconds under normal network operating conditions.

4.9.10 On-Line Revocation Checking Requirements

Relying parties must confirm revocation information.

4.9.11 Other Forms of Revocation Advertisements Available

No stipulation

4.9.12 Special Requirements Related to Key Compromise

Deutsche Post CA and any of its Registration Authorities shall use commercially reasonable methods to inform subscribers that their private key may have been compromised. This includes cases where new vulnerabilities have been discovered or where Deutsche Post CA at its own discretion decides that evidence suggests a possible key compromise has taken place. Where key compromise is not disputed, Deutsche Post CA shall revoke Issuing CA Certificates or Subscriber End Entity certificates within 24 hours and publish online CRLs within 30 minutes of creation.

4.9.13 Circumstances for Suspension

Deutsche Post CA does not support suspension

4.9.14 Who Can Request Suspension

Not applicable

4.9.15 Procedure for Suspension Request

Not applicable

4.9.16 Limits on Suspension Period

Not applicable

4.10 Certificate Status Services

4.10.1 Operational Characteristics

Deutsche Post CA provides a certificate status service either in the form of a CRL distribution point or an OCSP responder or both. These services are presented to relying parties within the Digital Certificate and may refer to any of the following URLs

- http://keyserver.dhl.com/pki/i3/dpdhl_tls_i3.crl
- http://keyserver.dhl.com/pki/i3/dpdhl_user_i3.crl
- https://ocsp-g3.dhl.com

4.10.2 Service Availability

Deutsche Post CA maintains 24x7 availability of certificate status services and may use additional Content Distribution Network cloud based mechanisms to aid service availability of cacheable results.

4.10.3 Operational Features

No stipulation

4.10.4 End of Subscription

Subscribers may end their subscription to certificate services by having their certificate revoked or naturally letting it expire.

4.11 Key Escrow and Recovery

4.11.1 Key Escrow and Recovery Policy and Practices

CA private keys are never escrowed. Deutsche Post CA does not offer Key Escrow Services to Subscribers.

4.11.2 Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

5.0 Facility, Management, and Operational Controls

5.1 Physical Controls

Deutsche Post CA maintains physical and environmental security policies for systems used for certificate issuance and management which cover physical access control, natural disaster protection, fire safety factors, failure of supporting utilities (e.g. power, telecommunications), structure collapse, plumbing leaks, protection against theft, breaking & entering, and disaster recovery, etc.

5.1.1 Site Location and Construction

Deutsche Post CA ensures that critical and sensitive information processing facilities are housed in secure areas with appropriate security barriers and entry controls. These are physically protected from unauthorized access, damage and interference and the protections provided are commensurate with the identified risks in risk analysis plans.

5.1.2 Physical Access

Deutsche Post CA ensures that the facilities used for certificate life cycle management are operated in an environment that physically protects the services from compromise through unauthorized access to systems or data. An authorized employee will always accompany any unauthorized person entering a physically secured area. Physical protections are achieved through the creation of clearly defined security perimeters (i.e. physical barriers) around the systems hosting the CA operations. No parts of the CA premises are shared with other organizations within this perimeter.

5.1.3 Power and Air Conditioning

Deutsche Post CA ensures that the power and air conditioning facilities are sufficient to support the operation of the CA system.

5.1.4 Water Exposures

Deutsche Post CA ensures that the CA systems are protected from water exposure.

5.1.5 Fire Prevention and Protection

Deutsche Post CA ensures that the CA system is protected with a fire suppression system

5.1.6 Media Storage

Deutsche Post CA ensures that any Media used is securely handled to protect it from damage, theft and unauthorized access.

5.1.7 Waste Disposal

Deutsche Post CA ensures that all media used for the storage of information is declassified or destroyed in a generally accepted manner before being released for disposal.

5.1.8 Off-Site Backup

Deutsche Post CA ensures that a full system backup of the certificate issuance system is sufficient to recover from system failures and is made on a regular basis. Back-up copies of essential business information and software are also taken on a regular basis. The backup procedure of Deutsche Post CA consists of creating a full system backup once a week accompanied by regular differential backups performed on a daily basis into an off-site location.

5.2 Procedural Controls

5.2.1 Trusted Roles

Deutsche Post CA ensures that all operators and administrators including vetting agents are acting in the capacity of a Trusted Role. Trusted roles are such that no conflict of interest is possible and the roles are distributed such that no single person can circumvent the security of the CA system.

Trusted Roles include but are not limited to the following:

Certificate Authority Administrator (CAA)

- Installation and configuration of the CA/OCSP
- Shutdown/restart of the CA
- Modification of certificate templates
- Modification of CRL schedule

Certificate Manager (CM)

- Acceptance of subscription and certificate revocation requests
- Approval of certificate renewal
- Verification of applicant's identity

5.2.2 Number of Persons Required per Task

Deutsche Post CA requires at least 2 people per task. The goal is to guarantee the trust for all CA services (key generation, certificate generation, revocation) so that any malicious activity would require collusion. Where multiparty control is required, at least one of the participants shall be an Administrator. All participants shall serve in a trusted role as defined in section 5.2.1 above.

5.2.3 Identification and Authentication for Each Role

Before appointing a person to a Trusted Role, Deutsche Post CA performs a background check. Each role described above is identified and authenticated in a manner to guarantee that the right person has the right role to support the CA.

5.2.4 Roles Requiring Separation of Duties

Deutsche Post CA enforces role separation either by the CA equipment or procedurally or by both means. Individual CA personnel are specifically designated to the roles defined in section 5.2.1 above. It is forbidden to own at the same time the following roles:

- CAA and CM

No individual shall be assigned more than one identity.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

Deutsche Post CA employs a sufficient number of personnel that possess the expert knowledge, experience and qualifications necessary for the offered services, as appropriate to the job function. Deutsche Post CA personnel fulfil the requirement through *expert knowledge, experience and qualifications* with formal training and education, actual experience, or a combination of the two. Trusted roles and responsibilities, as specified in 5.2.1 are documented in job descriptions. Deutsche Post CA personnel (both temporary and permanent) have job descriptions defined from the view point of separation of duties and least privilege, determining position sensitivity based on the duties and access levels, background screening and employee training and awareness. Deutsche Post CA personnel are formally appointed to trusted roles by senior management responsible for security.
The job descriptions include skills and experience requirements. Managerial personnel are employed who possess experience or training in electronic signature technology and familiarity with security procedures for personnel with security responsibilities and experience with information security and risk assessment sufficient to carry out management functions.

5.3.2 Background Check Procedures

All Deutsche Post CA personnel in trusted roles are free from conflicting interests that might prejudice the impartiality of the CA operations. Deutsche Post CA does not appoint to a trusted roles or management any person who is known to have a conviction for a serious crime or another offence, which affects his/her suitability for the position. Personnel do not have access to the trusted functions until any necessary checks are completed. Deutsche Post CA requires candidates to provide past convictions and turns down an application in case of refusal. All persons filling trusted roles shall be selected on the basis of loyalty, trustworthiness, and integrity, and shall be subject to background investigation.

5.3.3 Training Requirements

Deutsche Post CA ensures that all personnel performing duties with respect to the operation of the CA receive comprehensive training in:

- CA/RA security principles and mechanisms;
- Software versions in use on the CA system;
- Duties they are expected to perform;
- Disaster recovery and business continuity procedures.

Deutsche Post CA and RA personnel are retrained when changes occur in Deutsche Post CA or RA systems. Refresher training is conducted as required and Deutsche Post CA shall review refresher-training requirements at least once a year.

5.3.4 Retraining Frequency and Requirements

Individuals responsible for trusted roles are aware of changes in the Deutsche Post CA or RA operations, as applicable. Any significant change to the operations has a training (awareness) plan, and the execution of such plan is documented.

5.3.5 Job Rotation Frequency and Sequence

Deutsche Post CA ensures that any change in the staff will not affect the operational effectiveness of the service or the security of the system.

5.3.6 Sanctions for Unauthorized Actions

Appropriate disciplinary sanctions are applied to personnel violating provisions and policies within this CPS or CA related operational procedures.

5.3.7 Independent Contractor Requirements

Contractor personnel employed for Deutsche Post CA operations are subjected to the same process, procedures, assessment, security control and training as permanent CA personnel.

5.3.8 Documentation Supplied to Personnel

Deutsche Post CA makes available to its personnel this CPS, any corresponding CP and any relevant statutes, policies or contracts. Other technical, operational and administrative documents (e.g., Administrator Manuals, User Manuals, etc.) are provided in order for the trusted personnel to perform their duties.
Documentation is maintained identifying all personnel who received training and the level of training completed.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

Audit log files shall be generated for all events relating to the security and services of the CA. Where possible, the security audit logs shall be automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism shall be used. All security audit logs, both electronic and non- electronic, shall be retained and made available during compliance audits.
Deutsche Post CA ensures all events relating to the life cycle of certificates are logged in a manner to ensure the traceability to a person in a trusted role for any action required for CA services. At a minimum, each audit record includes the following (either recorded automatically or manually) elements:

- The type of event,
- The date and time the event occurred,
- Success or failure where appropriate,
- The identity of the entity and/or operator that caused the event,
- The identity to which the event was targeted,
- The cause of the event.

5.4.2 Frequency of Processing Log

Audit logs are reviewed periodically and reasonably for any evidence of malicious activity and following each important operation.

5.4.3 Retention Period for Audit Log

Audit log records are held for a period of time as appropriate to providing necessary legal evidence in accordance with any applicable legislation. Records may be required at least as long as any transaction relying on a valid certificate can be questioned.

5.4.4 Protection of Audit Log

The events are logged in a way that they cannot be deleted or destroyed (except for transfer to long term media) for any period of time that they are retained.

The events are logged in a manner to ensure that only authorized trusted access is able to perform any operations regarding their profile without modifying integrity, authenticity and confidentiality of the data.
The events are protected in a manner to keep them readable in the time of their storage.
The events are date stamped in a secure manner that guarantees, from the date of creation of the record to the end of the archive period that there is a trusted link between the event and the time of its realisation.

5.4.5 Audit Log Backup Procedures

Audit logs and audit summaries are backed-up in a secure location (For example a fire proof safe), under the control of an authorized trusted role, separated from their component source generation. Audit log backup is protected to the same degree as originals.

5.4.6 Audit Collection System (Internal vs. External)

Audit processes are invoked at system start up and finish only at system shutdown. The audit collection system ensures the integrity and availability of the data collected. If necessary, the audit collection system protects the data confidentiality. In the case of a problem occurring during the process of the audit collection then Deutsche Post CA determines whether to suspend Deutsche Post CA operations until the problem is solved duly informing the impacted asset owners.

5.4.7 Notification to Event-Causing Subject

No stipulation.

5.4.8 Vulnerability Assessments

Deutsche Post CA performs regular vulnerability assessments covering all Deutsche Post CA assets related to certificate issuance, products and services. Assessments focus on internal and external threats that could result in unauthorized access, tampering, modification, alteration or destruction of the certificate issuance process.

5.5 Records Archival

5.5.1 Types of Records Archived

Deutsche Post CAs and RAs archive records with enough detail to establish the validity of a signature and of the proper operation of the CA system. At a minimum, the following data is archived:

Deutsche Post CA key lifecycle management events, including:-

- Key generation, backup, storage, recovery, archival, and destruction;
- Cryptographic device lifecycle management events; and
- CA System equipment configuration.

Deutsche Post CA issuance system management events including:-

- System start-up and shutdown actions;
- Attempts to create, remove, or set passwords or change the system; and
- Changes to Issuer CA keys.

Deutsche Post CA and Subscriber Certificate lifecycle management events, including:-

- Certificate requests, renewal, and re-key requests, and revocation for both successful and unsuccessful attempts;
- All verification activities stipulated in this CPS;
- Date, time, phone number used, persons spoken to, and end results of verification telephone calls;
- Acceptance and rejection of Certificate requests;
- Issuance of Certificates; and
- Generation of Certificate Revocation Lists and OCSP entries including failed read-and-write operations on the certificate and CRL directory.

Security events, including:-

- Successful and unsuccessful PKI system access attempts;
- PKI and security system actions performed;
- Security profile changes;
- System crashes, hardware failures, and other anomalies;
- Firewall and router activities; and
- Entries to and exits from the CA facility.

Documentation and Auditing:-

- Audit documentation including all work related communications to or from Deutsche Post CA and compliance auditors;
- Certificate Policy and previous versions;
- Certification Practice Statement and previous versions; and
- Contractual agreements between subscribers and the Deutsche Post CA

Time stamping:-

- Clock synchronisation.

Miscellaneous

- Other data or applications sufficient to verify archive contents;
- Equipment failure
- UPS failure or Electrical power outages; and
- Violations of the CP or this CPS

5.5.2 Retention Period for Archive

The minimum retention period for archive data is 5 years.

5.5.3 Protection of Archive

The archives are created in such a way that they cannot be deleted or destroyed (except for transfer to long term media) within the period of time for which they are required to be held. Archive protections ensure that only authorized trusted access is able to make operations without modifying integrity, authenticity and confidentiality of the data. If the original media cannot retain the data for the required period, a mechanism to periodically transfer the archived data to new media will be defined by the archive site.

5.5.4 Archive Backup Procedures

Archive Backups are made which are either of the online Deutsche Post CA system or the offline system.
Online backups are duplicated weekly and each backup is stored in a location which is different to original online system. One backup is stored in a fire rated media safe.
An Offline backup is taken at the end of any key ceremony (with the exception of any encrypted material which is store separately in line with key ceremony procedures) and stored in an off site location within 30 days of the ceremony.

5.5.5 Requirements for Time-Stamping of Records

If a time stamping service is used to date the records, then it has to respect the requirements defined in section 6.8. Irrespective of time stamping methods, all logs must have must have data indicating the time at which the event occurred.

5.5.6 Archive Collection System (Internal or External)

The archive collection system respects the security requirements defined in section 5.3.

5.5.7 Procedures to Obtain and Verify Archive Information

Media storing of Deutsche Post CA archive information is checked upon creation. Periodically, statistical samples of archived information are tested to check the continued integrity and readability of the information. Only authorised Deutsche Post CA equipment, trusted role and other authorized persons are allowed to access the archive. Requests to obtain and verify archive information are co-ordinated by operators in Trusted Roles (Internal Auditor, the Manager in charge of the process and the Security Officer)

5.6 Key Changeover

Deutsche Post CA may periodically change over Key Material for issuing CAs in line with section 6.3.2. Certificate subject information may also be modified and certificate profiles may be altered to highlight new best practices. Keys used to sign previous Subscriber certificates are maintained until such time as all Subscriber Certificates have expired.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

Deutsche Post CA establishes business continuity procedures that outline the steps to be taken in the event of the corruption or loss of computing resources, software and/or data that could disturb or compromise the Deutsche Post CA services. Deutsche Post CA carries out risk assessments to evaluate business risk and

determine the necessary security requirements and operational procedures to be taken as a consequence of its disaster recovery plan. This risk analysis is regularly reviewed and revised if necessary *(threat evolution, vulnerability evolution etc).* This business continuity is in the scope of the audit process as described in section 8 to validate what are the operations that are first maintained after a disaster and the recovery plan.
Deutsche Post CA personnel that own a trusted role and operational role are specially trained to operate according to procedures defined in the Disaster Recovery plan for the most sensitive activities.
If a Deutsche Post CA detects a potential hacking attempt or another form of compromise, it should perform an investigation in order to determine the nature and the degree of damage. Otherwise, the Deutsche Post CA assesses the scope of potential damage in order to determine whether the CA or RA system needs to be rebuilt, whether only some certificates need to be revoked, and/or whether a CA hierarchy needs to be declared as compromised. The CA disaster recovery plan highlights which services should be maintained *(for example revocation and certificate status information).*

5.7.2 Computing Resources, Software, and/or Data Are Corrupted

If any equipment is damaged or rendered inoperative, however the signature keys are not destroyed, the operation should be re-established as quickly as possible, giving priority to the ability to generate certificates status information according to Deutsche Post CAs disaster recovery plan.

5.7.3 Entity Private Key Compromise Procedures

In case a Deutsche Post CA signature key is compromised, lost, destroyed or suspected to be compromised:

- Deutsche Post CA, after investigation of the problem decides whether the Deutsche Post CA certificate should be revoked. If so then:-
    - All the subscribers who have been issued a certificate will be notified at the earliest feasible opportunity;
    - A new Deutsche Post CA key pair shall be generated or an alternative existing CA hierarchy shall be used to create new subscriber certificates;

5.7.4 Business Continuity Capabilities After a Disaster

The disaster recovery plan deals with the business continuity as described in section 5.7.1. Certificate Status information systems should be deployed so as to provide 24 hours per day, 365 days per year availability (with a rate of 99.95% availability excluding planned maintenance operations).

5.8 CA or RA Termination

In the event of termination of an Deutsche Post CA or RA, Deutsche Post CA provides notice to all customers prior to the termination and:

- Stops delivering certificates according to and referring to this CPS
- Archive all audit logs and other records prior to termination;
- Destroys all private keys upon termination;
- Ensures archive records are transferred to an appropriate authority such as another Deutsche Post CA that delivers identical services;
- Use secure means to notify customers and software platform providers to delete all trust anchors.

6.0 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

Deutsche Post CA generates all issuing key pairs in a physically secure environment by personnel in trusted roles under, at least, dual control. Deutsche Post CA key generation is carried out within a device, which is at least certified to FIPS 140-2 level 3 or above.

6.1.2 Private Key Delivery to Subscriber

No stipulation.

6.1.3 Public Key Delivery to Certificate Deutsche Post CA

Deutsche Post CA only accepts Public Keys from RAs that have been protected during transit and have had the authenticity and integrity of their origin from the RA suitably verified. RA's shall only accept Public keys from Subscribers in line with section 3.2.1 of this CPS.

6.1.4 CA Public Key Delivery to Relying Parties

Deutsche Post CA relies on the processes of GlobalSign nv-sa (The Root Authority) to deliver Root certificates to relying parties, and upon chain verification mechanisms within the relying parties software platform to establish the chain of trust for the relying party.

6.1.5 Key Sizes

Deutsche Post CA follows NIST recommended timelines and best practice in the choice of size of its Keys for Root CAs, Issuing CAs and only signs end entity certificates following best practice.

The following Key sizes and hashing algorithms are used for Root Certificates, Issuing Certificates and End Entity Certificates and CRL/OCSP certificate status responders in line with CABForum Base Requirements:-

- 2048 bit RSA key with Secure Hash Algorithm 1 (SHA-1)

Where possible, the entire certificate chain and any certificate status responses use the same level of security and cryptography. Exceptions due to cross-certified certificates are acceptable.

Existing certificates with an unsuitable cryptographic strength are replaced in sufficient time as to protect relying parties, Subscribers and Issuing CAs.

6.1.6 Public Key Parameters Generation and Quality Checking

Deutsche Post CA generates keys in accordance with FIPS 186 and uses reasonable techniques to validate the suitability of keys presented by Subscribers. Known weak keys shall be tested for and rejected at the point of submission.

6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field)

Deutsche Post CA sets Key Usage of certificates depending on their proposed field of application via the v3 Key Usage Field for X.509 v3 (See section 7.1).

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

Deutsche Post CA ensures that all systems signing Certificates and CRLs or generating OCSP responses use FIPS 140-2 level 3 as the minimum level of cryptographic protection.

6.2.2 Private Key (n out of m) Multi-Person Control

Deutsche Post CA activates Private Keys for cryptographic operations with multi-person control (using CA activation data) performing duties associated with their trusted roles. The trusted roles permitted to participate in this private key multi-person controls are strongly authenticated (i.e. Token with PIN code). Root Key material is always protected through 3 of 5.

6.2.3 Private Key Escrow

Deutsche Post CA does not escrow Private Keys for any reason.

6.2.4 Private Key Backup

If required for business continuity Deutsche Post CA backs up private keys under the same multi-person control as the original Private Key.

6.2.5 Private Key Archival

Deutsche Post CA does not archive Private Keys.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

Deutsche Post CA Private Keys are generated, activated and stored in Hardware Security Modules. When Private Keys are outside of a Hardware Security Module (either for storage or transfer), they are encrypted. Private Keys never exist in plain text outside of a cryptographic module.

6.2.7 Private Key Storage on Cryptographic Module

Deutsche Post CA stores Private Keys on at least a FIPS 140-2 level 3 device.

6.2.8 Method of Activating Private Key

Deutsche Post CA is responsible for activating the private key in accordance with the instructions and documentation provided by the manufacturer of the hardware security module. Subscribers are responsible

for protecting private keys in line with the obligations that are presented in the form of a Subscriber Agreement or Terms of use Agreement.

6.2.9 Method of Deactivating Private Key

Deutsche Post CA ensures that Hardware Security Modules that have been activated are not left unattended or otherwise available to unauthorized access. During the time a Deutsche Post CA's Cryptographic Module is on-line and operational, it is only used to sign certificates and CRL/OCSPs from an authenticated RA. When a CA is no longer operational, Private Keys are removed from the Hardware Security Module.

6.2.10 Method of Destroying Private Key

Deutsche Post CA private keys are destroyed when they are no longer needed or when the certificates to which they correspond have expired or have been revoked. Destroying Private Keys means that Deutsche Post CA destroys all associated CA secret activation data in such a manner that no information can be used to deduce any part of the private key.

6.2.11 Cryptographic Module Rating

See section 6.2.1

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

Deutsche Post CA archives Public Keys from certificates.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

Deutsche Post CA certificates have a maximum validity period of:-

Type	Private Key Usage	Certificate Term.
SMIME Certificates -	No stipulation	2 years
SSL/TLS Certificates -	No stipulation	1 year

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

Generation and use of Deutsche Post CA activation data used to activate Deutsche Post CA private keys are made during a key ceremony (Refer to section 6.1.1). Activation data is either generated automatically by the appropriate HSM or in such a way that meets the same needs. It is then delivered to a shareholder who is a person in Trusted Role. The delivery method maintains the confidentiality and the integrity of the activation data.

6.4.2 Activation Data Protection

Issue CA activation data is protected from disclosure through a combination of cryptographic and physical access control mechanisms. Deutsche Post CA activation data is stored on smart cards.

6.4.3 Other Aspects of Activation Data

Deutsche Post CA activation data may only be held by Deutsche Post CA personnel in Trusted Roles.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

The following computer security functions are provided by the Operating System, or through a combination of Operating System, software, and Physical Safeguards. The Deutsche Post CA PKI components must include the following functions:

- Require authenticated logins for trusted role;
- Provide Discretionary Access Control;
- Provide security audit capability (protected in integrity);
- Prohibit object re-use;
- Require use of cryptography for session communication;
- Require trusted path for identification and authentication;
- Provide domain isolation for process;
- Provide self-protection for the operating system.

When Deutsche Post CA PKI equipment is hosted on an evaluated platform in support of computer security assurance requirements then the system (Hardware, Software, Operating System), when possible, operates

in an elevated configuration. At a minimum, such platforms use the same version of the computer operating system as that which received the evaluation rating. The computer systems are configured with minimum of the required accounts, network services, and no remote login.

6.5.2 Computer Security Rating

All the Deutsche Post CA PKI component software is compliant with the requirements of the protection profile from a suitable entity.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

The System Development Controls for the Deutsche Post CA are as follows:

- Use software that has been designed and developed under a formal, documented development methodology;
- Hardware and software procured are purchased in a fashion to reduce the likelihood that any particular component was tampered with (e.g., by ensuring the equipment was randomly selected at time of purchase);
- Hardware and software developed are developed in a controlled environment, and the development process are defined and documented. This requirement does not apply to commercial off-the-shelf hardware or software;
- All hardware must be shipped or delivered via controlled methods that provide a continuous chain of accountability, from the purchase location to the operations location;
- The hardware and software are dedicated to performing CA activities. There is no other applications; hardware devices, network connections, or component software installed which are not part of the CA operation;
- Proper care is taken to prevent malicious software from being loaded onto the equipment. Only applications required to perform the CA operations are obtained from sources authorized by local policy. Deutsche Post CA hardware and software are scanned for malicious code on first use and periodically thereafter;
- Hardware and software updates are purchased or developed in the same manner as original equipment; and be installed by trusted and trained personnel in a defined manner.

6.6.2 Security Management Controls

The configuration of the Deutsche Post CA system as well as any modifications and upgrades are documented and controlled by the Deutsche Post CA management. There is a mechanism for detecting unauthorized modification to the Deutsche Post CA software or configuration. A formal configuration management methodology is used for installation and on-going maintenance of the Deutsche Post CA system. The Deutsche Post CA software, when first loaded, is checked as being that supplied from the vendor, with no modifications, and is the version intended for use.

6.6.3 Life Cycle Security Controls

Deutsche Post CA maintains a maintenance scheme to ensure the level of trust of software and hardware that are evaluated and certified,

6.7 Network Security Controls

Deutsche Post CA PKI components implements appropriate security measures to ensure they are guarded against denial of service and intrusion attacks. Such measures include the use of guards, firewalls and filtering routers. Unused network ports and services are turned off. Any boundary control devices used to protect the network on which PKI equipment are hosted deny all but the necessary services to the PKI equipment even if those services are enabled for other devices on the network.

6.8 Time-Stamping

All Deutsche Post CA components are regularly synchronized with a reliable time service. Deutsche Post CA uses non-authenticated NTP source clock to establish the correct time:

- Initial validity time of a CA Certificate;
- Revocation of a CA Certificate;
- Posting of CRL updates;
- Issuance of Subscriber End Entity certificates.

Electronic or manual procedures may be used to maintain system time. Clock adjustments are auditable events.

7.0 Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

7.1.1 Version Number(s)

Deutsche Post CA issues digital certificates in compliance with X.509 Version 3

7.1.2 Certificate Extensions

Deutsche Post CA issues digital certificates in compliance with RFC 5280 and applicable best practice. Criticality also follows best practice to prevent unnecessary risks to relying parties when applied to name constraints.

7.1.3 Algorithm Object Identifiers

Deutsche Post CA issues digital certificates with Algorithms indicated by the following OIDs

- **SHA1WithRSAEncryption** {iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1(1) 5}

7.1.4 Name Forms

Deutsche Post CA issues digital certificates with Name Forms compliant to RFC 5280. Within the domain of each Issuing CA, Deutsche Post CA includes a unique non-sequential Certificate Serial Number that exhibits at least 20 bits of entropy.

7.1.5 Name Constraints

The Deutsche Post CA makes use of the name constraints extension to restrict the issuance of certificates to a list of domains owned by the Deutsche Post AG.

7.1.6 Certificate Policy Object Identifier

No stipulation

7.1.7 Usage of Policy Constraints Extension

No stipulation

7.1.8 Policy Qualifiers Syntax and Semantics

Deutsche Post CA issues digital certificates with a Policy Qualifier and suitable text to aid relying parties determine applicability.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No stipulation

7.2 CRL Profile

7.2.1 Version Number(s)

Deutsche Post CA issues Version 2 CRLs in compliance with RFC 5280. CRLs have the following fields:-

- **Issuer** DPDHL TLS CA I3
- **Effective date** Date and Time
- **Next update** Date and Time
- **Signature Algorithm** sha1RSA
- **Signature Hash Algorithm** sha1
- **Serial Number(s)** List of revoked serial numbers
- **Revocation Date** Date of Revocation

- **Issuer** DPDHL User CA I3
- **Effective date** Date and Time
- **Next update** Date and Time
- **Signature Algorithm** sha1RSA
- **Signature Hash Algorithm** sha1
- **Serial Number(s)** List of revoked serial numbers
- **Revocation Date** Date of Revocation

7.2.2 CRL and CRL Entry Extensions

CRLs have the following extensions:-

- **CRL Number** Sequentially assigned natural number
- **Authority Key Identifier** AKI of the issuing CA for chaining/validation requirements

7.3 OCSP Profile

Deutsche Post CA operates an Online Certificate Status Profile (OCSP) responder in compliance with RFC 2560 or RFC5019 and highlights this within the AIA extension via an OCSP responder URI.

7.3.1 Version Number(s)

Deutsche Post CA issues Version 1 OCSP responses

7.3.2 OCSP Extensions

No stipulation

8.0 Compliance Audit and Other Assessments

The procedures within this CPS encompass all relevant portions of currently applicable PKI standards. Deutsche Post CA is constrained by GlobalSign nv-sa using dNSNameConstraints and therefore external independent auditing is not applicable.

8.1 Frequency and Circumstances of Assessment

The certificates issued by Deutsche Post CA are assessed on an annual basis by GlobalSign nv-sa or an affiliated GlobalSign company as part of the contractual obligation in using TrustedRoot chaining services. The assessment covers all CA related activities as recommended by the CABForum Baseline Requirements.

8.2 Identity/Qualifications of Assessor

GlobalSign nv-sa or an affiliated GlobalSign company determines through an annual assessment that the provisions of the contract and adherence to the CABForum Baseline requirements are maintained using suitably qualified and trained GlobalSign staff members.

8.3 Assessor's Relationship to Assessed Entity

Deutsche Post CA is a cross signed entity under contract with GlobalSign nv-sa or an affiliated company under the TrustedRoot program.

8.4 Topics Covered by Assessment

The Audit meets the requirements of the CABForum Baseline Requirements.

8.5 Actions Taken as a Result of Deficiency

Deutsche Post CA follows the same process if presented with a material non-compliance by GlobalSign nv-sa or an affiliated company. Deutsche Post CA creates a suitable corrective action plan to remove the deficiency. Corrective action plans which directly affect policy and procedure as dictated by GlobalSign's CP and this CPS are highlighted to the GlobalSign Policy Authority for discussion and resolution.

8.6 Communications of Results

Results of the Audit are reported to Deutsche Post CA for analysis and resolution of any deficiency through a subsequent corrective action plan.

9.0 Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

Deutsche Post CA may charge fees for certificate issuance.

9.1.2 Certificate Access Fees

Deutsche Post CA may charge for Access to any Database which stores issued certificates.

9.1.3 Revocation or Status Information Access Fees

Deutsche Post CA may charge fees for Revocation or Status Information.

9.1.4 Fees for Other Services

No stipulation.

9.1.5 Refund Policy

No stipulation.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

Deutsche Post CA maintains Commercial General Liability insurance with policy limits of at least 2 million US dollars in coverage and Errors and Omissions / Professional Liability insurance with a policy limit of at least 5 million US dollars in coverage. GlobalSign's insurance policies include coverage for (1) claims for damages arising out of an act, error, or omission, unintentional breach of contract, or neglect in issuing or maintaining EV Certificates, and (2) claims for damages arising out of infringement of the proprietary rights of any third party (excluding copyright, patent, and trademark infringement), invasion of privacy, and advertising injury. Insurance is carried through companies rated no less than A- as to Policy Holder's Rating in the current edition of Best's Insurance Guide (or with an association of companies, each of the members of which are so rated).

9.2.2 Other Assets

No stipulation

9.2.3 Insurance or Warranty Coverage for End-Entities

No stipulation

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

The following items are classed as being Confidential Information and therefore are subject to reasonable care and attention by Deutsche Post CA staff including Vetting Operators and Administrators.

- Personal Information as detailed in section 9.4
- Audit Logs from CA and RA systems
- Activation Data used to active CA private keys as detailed in section 6.4
- Internal GlobalSign business process documentation including Disaster Recovery Plans (DRP), Business Continuity Plans (BCP)
- Audit reports from an independent auditor as detailed in section 8.0

9.3.2 Information Not Within the Scope of Confidential Information

Any information not defined as confidential within this CPS shall be deemed public. Certificate status information and certificates themselves are deemed public.

9.3.3 Responsibility to Protect Confidential Information

Deutsche Post CA protects confidential information through training and enforcement with employees, agents and contractors.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

Deutsche Post CA protects Personal Information in line with legal requirements where Deutsche Post CA operates through internal policy.

9.4.2 Information Treated as Private

Deutsche Post CA treats all information received from Applicants that will not ordinarily be placed into a certificate as private. This applies both to those Applicants who are successful in being issued a digital certificate and those who are unsuccessful and rejected. Deutsche Post CA periodically trains all RA and Vetting staff as well as anyone who has access to the information about due care and attention that must be applied.

9.4.3 Information Not Deemed Private

Certificate status information and any certificate content is deemed not private.

9.4.4 Responsibility to Protect Private Information

Deutsche Post CA protects Personal Information in line with legal requirements where Deutsche Post CA operates.

9.4.5 Notice and Consent to Use Private Information

Personal Information obtained from Applicants during the application and enrolment process is deemed private and permission is therefore required from the Applicant to allow the use of such information. Deutsche Post CA incorporates the relevant provisions within an appropriate Subscriber Agreement including any additional information obtained from third parties that may be applicable to the validation process for the product or service being offered by Deutsche Post CA.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

Deutsche Post CA may disclose Private Information without notice to Applicants or Subscribers where required to do so by law or regulation.

9.4.7 Other Information Disclosure Circumstances

No Stipulation.

9.5 Intellectual Property rights

Deutsche Post CA does not knowingly violate the Intellectual Property Rights of third parties. Public and Private keys remain the property of Subscribers who legitimately hold them. Deutsche Post CA retains ownership of certificates however, it grants permission to reproduce and distribute certificates on a non-exclusive, royalty free basis, provided that they are reproduced and distributed in full.

GlobalSign and the GlobalSign Logo are the registered trademarks of GMO GlobalSign K.K.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

Deutsche Post CA uses this CPS and applicable Subscriber Agreements to convey legal conditions of usage of issued certificates to Subscribers and Relying Parties. All parties including the Deutsche Post CA, any RAs and subscribers warrant the integrity of their respective private key(s). If any such party suspects that a private key has been compromised they will immediately notify the appropriate RA.

Deutsche Post CA represents and warrants to Certificate Beneficiaries:-

- The Subscriber that is a party to the Subscriber or Terms of Use Agreement for the Certificate;
- All Relying Parties who reasonably rely on a Valid Certificate.

that, during the period when the Certificate is valid, Deutsche Post CA has complied with its Certificate Policy and/or Certification Practice Statement in issuing and managing the Certificate including:-

- **Right to Use Domain Name or IP Address**: That, at the time of issuance, Deutsche Post CA (i) implemented a procedure for verifying that the Applicant either had the right to use, or had control of, the Domain Name(s) and IP address(es) listed in the Certificate's subject field and subjectAltName extension (or, only in the case of Domain Names, was delegated such right or control by someone who had such right to use or control); (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in Deutsche Post CA's Certificate Policy and/or Certification Practice Statement (See section 3.2);
- **Authorization for Certificate:** That, at the time of issuance, Deutsche Post CA (i) implemented a procedure for verifying that the Subject authorized the issuance of the Certificate and that the Applicant Representative is authorized to request the Certificate on behalf of the Subject; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in Deutsche Post CA's Certificate Policy and/or Certification Practice Statement (See section 3.2.5);
- **Accuracy of Information:** That, at the time of issuance, Deutsche Post CA (i) implemented a procedure for verifying the accuracy of all of the information contained in the Certificate (with the exception of the subject:organizationalUnitName attribute); (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in Deutsche Post CA's Certificate Policy and/or Certification Practice Statement (See sections 3.2.3, 3.2.3, 3.2.4);
- **No Misleading Information:** That, at the time of issuance, Deutsche Post CA (i) implemented a procedure for reducing the likelihood that the information contained in the Certificate's subject:organizationalUnitName attribute would be misleading; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in Deutsche Post CA's Certificate Policy and/or Certification Practice Statement (See sections 3.2.3, 3.2.3, 3.2.4);

- **Identity of Applicant:** That, if the Certificate contains Subject Identity Information, the CA (i) implemented a procedure to verify the identity of the Applicant; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in Deutsche Post CA's Certificate Policy and/or Certification Practice Statement (See sections 3.2.3, 3.2.3, 3.2.4);
- **Subscriber Agreement:** That, if Deutsche Post CA and Subscriber are not Affiliated, the Subscriber and CA are parties to a legally valid and enforceable Subscriber Agreement that satisfies these Requirements, or, if Deutsche Post CA and Subscriber are Affiliated, the Applicant Representative acknowledged and accepted the Terms of Use (See section 4.5.1);
- **Status:** That Deutsche Post CA maintains a 24 x 7 publicly-accessible Repository with current information regarding the status (valid or revoked) of all unexpired Certificates; and
- **Revocation:** That Deutsche Post CA will revoke the Certificate for any of the reasons specified in the CABForum Baseline Requirements (See section 4.9.1)

9.6.2 RA Representations and Warranties

RAs warrant that:-

- Issuance processes are in compliance with this CPS and the relevant GlobalSign CP.
- All information provided to Deutsche Post CA does not contain any misleading or false information
- All translated material provided by the RA is accurate

9.6.3 Subscriber Representations and Warranties

Unless otherwise stated in this CPS, subscribers are responsible for:

- Having knowledge and, if necessary, seeking training on using digital certificates.
- Generating securely their private-public key pair, using a trustworthy system.
- Providing correct and accurate information in their communications with Deutsche Post CA.
- Ensuring that the public key submitted to the Deutsche Post CA correctly corresponds to the private key used.
- Accepting all terms and conditions in any subscriber agreement, GlobalSign CP and associated policies published in the Deutsche Post CA repository.
- Refraining from tampering with an issued certificate.
- Using certificates only for legal and authorised purposes in accordance with this CPS.
- Notifying the Deutsche Post CA or RA of any changes in the information submitted.
- Ceasing to use a certificate if any featured information becomes invalid.
- Ceasing to use a certificate when it becomes invalid.
- Removing a certificate when invalid from any applications and/or devices they have been installed on.
- Using a certificate, as it may be reasonable under the circumstances.
- Preventing the compromise, loss, disclosure, modification, or otherwise unauthorised use of their private key.
- For any acts and omissions of partners and agents subscribers use to generate, retain, escrow, or destroy any private keys.
- Refraining from submitting any material that contains statements that violate any law or the rights of any party.
- Requesting the revocation of a certificate in case of an occurrence that materially affects the integrity of a certificate.
- Notifying the appropriate RA immediately, if a subscriber becomes aware of or suspects the compromise of a private key.
- Submit accurate and complete information to Deutsche Post CA in accordance with the requirements of this CPS particularly with regards to registration.
- Only use the key pair for digital signatures and in accordance with any other limitations notified to the subscriber according to this CPS or any Trusted Root CA Chaining agreement.
- Exercise absolute care to avoid unauthorized use of its private key.
- Use a key length and algorithm as indicated in this CPS.
- Notify Deutsche Post CAs without any reasonable delay, if any of the following occur up to the end of the validity period indicated in the certificate:
    - The subscriber's private key has been lost, stolen, potentially compromised; or
    - Control over the subscribers private key has been lost due compromise of activation data (e.g. PIN code or Pass Phrase)
      or
    - Inaccuracy or changes to the certificate content, as notified to the Subscriber.

The Subscriber is ultimately liable for the choices he or she makes when applying for a certificate. The applicant and Deutsche Post CA must designate the usage of a trustworthy device as well as the choice of organizational context.

9.6.4 Relying Party Representations and Warranties

A party relying on a Deutsche Post CA's certificate promises to:

- Have the technical capability to use digital certificates.
- Receive notice of the Deutsche Post CA and associated conditions for relying parties.
- Validate a Deutsche Post CA's certificate by using certificate status information (e.g. a CRL or OCSP) published by the Deutsche Post CA in accordance with the proper certificate path validation procedure.
- Trust a Deutsche Post CA's certificate only if all information featured on such certificate can be verified via such a validation procedure as being correct and up to date.
- Rely on a Deutsche Post CA's certificate, only as it may be reasonable under the circumstances.
- Notify the appropriate RA immediately, if the relying party becomes aware of or suspects that a private key has been compromised.

The obligations of the relying party, if it is to reasonably rely on a certificate, are to:

- Verify the validity or revocation of the CA certificate using current revocation status information as indicated to the relying party.
- Take account of any limitations on the usage of the certificate indicated to the relying party either in the certificate or this CP.
- Take any other precautions prescribed in the Deutsche Post CA's certificate as well as any other policies or terms and conditions made available in the application context a certificate might be used.

Relying parties must at all times establish that it is reasonable to rely on a certificate under the circumstances taking into account circumstances such as the specific application context a certificate is used in.

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimers of Warranties

Deutsche Post CA does not warrant that:-

- The accuracy of any unverifiable piece of information contained in certificates except as it may be stated in the relevant product description below in this CPS and in a Warranty Policy, if available.
- The accuracy, authenticity, completeness or fitness of any information contained in, free, test or demo certificates.

9.8 Limitations of Liability

IN NO EVENT, EXCEPT FOR FRAUD OR WILLFUL MISCONDUCT, SHALL Deutsche Post CA BE LIABLE FOR ANY INDIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGES, OR FOR ANY LOSS OF PROFITS, LOSS OF DATA OR OTHER INDIRECT, INCIDENTAL, CONSEQUENTIAL DAMAGES ARISING FROM OR IN CONNECTION WITH THE USE, DELIVERY, LICENSE, PERFORMANCE OR NON PERFORMANCE OF CERTIFICATES, DIGITAL SIGNATURES OR ANY OTHER TRANSACTIONS OR SERVICES OFFERED OR CONTEMPLATED BY THIS CPS, EXCEPT FOR DAMAGE DUE TO RELIANCE (IN ACCORDANCE WITH THIS CPS) ON THE VERIFIED INFORMATION ON THE MOMENT OF ISSUANCE OF THE CERTIFICATE TILL AN AMOUNT AS INDICATED BY THE WARRANTY COMMUNICATION DOCUMENT IN THE APPROPRIATE LEGAL REPOSITORY OF Deutsche Post CA'S WEB SITE. Deutsche Post CA WILL NOT BE LIABLE IN THIS CASE IF THE FAULT IN THIS VERIFIED INFORMATION IS DUE TO FRAUD OR WILLFUL MISCONDUCT OF THE APPLICANT. Deutsche Post CA WILL NOT BE LIABLE IN THIS CASE IF THE USER HAS NOT RESPECTED HIS OBLIGATIONS MENTIONED IN THIS CPS.

9.9 Indemnities

9.9.1 Indemnification by Deutsche Post CA

Deutsche Post CA shall indemnify each Application Software Vendor against any claim, damage, or loss suffered by the Application Software Vendor related except where the claim, damage, or loss suffered by the Application Software Vendor was directly caused by the Application Software Vendor's software displaying as trustworthy (i) a Certificate that has expired or (ii) a revoked Certificate where the revocation status is available online but the Application Software Vendor's software failed to check or ignored the status.

9.9.2 Indemnification by Subscribers

To the extent permitted by law, each Subscriber shall indemnify Deutsche Post CA, GlobalSign nv-sa and any related entity providing services to Deutsche Post CA, and their respective directors, officers, employees, agents, and contractors against any loss, damage, or expense, including reasonable attorney's fees, related to (i) any misrepresentation or omission of material fact by Subscriber, regardless of whether the misrepresentation or omission was intentional or unintentional; (ii) Subscriber's breach of the Subscriber Agreement, this CPS, or applicable law; (iii) the compromise or unauthorized use of a certificate or Private Key caused by the Subscriber's negligence; or (iv) Subscriber's misuse of the certificate or Private Key.

9.9.3 Indemnification by Relying Parties

To the extent permitted by law, each Relying Party shall indemnify Deutsche Post CA, GlobalSign nv-sa and any related entity providing services to Deutsche Post CA, and their respective directors, officers, employees, agents, and contractors against any loss, damage, or expense, including reasonable attorney's fees, related to the Relying Party's (i) breach of the Relying Party Agreement, an End□User License Agreement, this CPS, or applicable law; (ii) unreasonable reliance on a certificate; or (iii) failure to check the certificate's status prior to use.

9.10 Term and Termination

9.10.1 Term

This CPS remains in force until notice of the opposite is communicated by the Deutsche Post CA on its web site or repository.

9.10.2 Termination

Notified changes are appropriately marked by an indicated version. Following publications, changes become applicable 30 days thereafter.

9.10.3 Effect of Termination and Survival

Deutsche Post CA will communicate the conditions and effect of this CPS termination via their appropriate repository.

9.11 Individual Notices and Communications with Participants

The Deutsche Post CA notifies subscriber representatives via email prior to certificate expiration with sufficient notice to allow for continuity of service.

9.12 Amendments

9.12.1 Procedure for Amendment

Changes to this CPS are indicated by appropriate numbering.

9.12.2 Notification Mechanism and Period

Deutsche Post CA will post appropriate notice on its web sites of any major or significant changes to this CPS as well as any appropriate period by when the revised CPS is deemed to be accepted.

9.12.3 Circumstances Under Which OID Must be Changed

No stipulation

9.13 Dispute Resolution Provisions

No stipulation

9.14 Governing Law

This CPS is governed, construed and interpreted in accordance with the laws of Federal Republic of Germany.

9.15 Compliance with Applicable Law

Deutsche Post CA complies with applicable laws of Federal Republic of Germany. Export of certain types of software used in certain Deutsche Post CA public certificate management products and services may require the approval of appropriate public or private authorities. Parties (including the Deutsche Post CA, subscribers and relying parties) agree to conform to applicable export laws and regulations as pertaining to Federal Republic of Germany.

9.16 Miscellaneous Provisions

9.16.1 Compelled Attacks

Deutsche Post CA is subject to Federal Republic of Germany jurisdiction and regulatory framework. Deutsche Post CA will use all reasonable legal defence against being compelled by a third party to issue certificates in violation of this CPS.

9.16.2 Survival

The obligations and restrictions contained under section “Legal Conditions” survive the termination of this CPS.

9.16.3 Entire Agreement

Deutsche Post CA will contractually obligate every RA involved with Certificate Issuance to comply with this CPS and all applicable Industry guidelines. No third party may rely on or bring action to enforce any such agreement.

9.16.4 Assignment

Entities operating under this CPS cannot assign their rights or obligations without the prior written consent of Deutsche Post CA

9.16.5 Severability

If any provision of this CPS, including limitation of liability clauses, is found to be invalid or unenforceable, the remainder of this CPS will be interpreted in such manner as to effect the original intention of the parties

9.16.6 Enforcement (Attorney’s Fees and Waiver of Rights)

Deutsche Post CA may seek indemnification and attorneys’ fees from a party for damages, losses and expenses related to that party’s conduct. Deutsche Post CA’s failure to enforce a provision of this CPS does not waive Deutsche Post CA’s right to enforce the same provisions later or right to enforce any other provisions of this CPS. To be effective any waivers must be in writing and signed by GlobalSign

9.17 Other Provisions

No Stipulation