Fraunhofer

Fraunhofer Corporate PKI

Certificate Policy

Version 1.1

Published in June 2012

Object Identifier of this Document: 1.3.6.1.4.1.778.80.3.1.1

Contact:

Fraunhofer Competence Center PKI
Fraunhofer Str. 1
D-76131 Karlsruhe
Germany

Phone: +49 1802 344 754
E-Mail: servicedesk@fraunhofer.de
WWW: http://www.pki.fraunhofer.de

Table of Contents

List of Tables

List of Figures

1 Introduction

This document specifies the certificate policies of the “Fraunhofer Corporate Public Key Infrastructure (PKI)” referred to as [CP-FhG] in the following. Fraunhofer Corporate PKI provides certification services for all employees of Fraunhofer and machines in order to support security services for integrity, authentication, confidentiality and non-repudiation in applications such as e-mail, web services, VPN communication, and files and device encryption.

1.1 Overview

[CP-FhG] in particular defines the framework requirements for the creation of keys, the issuance of related certificates, their usage, management, renewal, and revocation. The practical implementation of these requirements is described in the associated document "Fraunhofer Corporate PKI Certification Practice Statement“ referred to as [CPS-FhG] in the following.

The documents [CP-FhG]and [CPS-FhG]have the same structure. The following three-layer document referencing scheme has been used: [CP-FhG] --> [CPS-FhG] --> additional internal documents which are listed in section 10.

[CP-FhG] complies with the requirements stated in the international standards “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework” [RFC 3647], “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile)” [RFC 3280], and “Information Technology – Open System Interconnection – The Directory: Authentication Framework” [X.509].

[CP-FhG] is based on a similar approach as made in the ETSI document “Policy Requirements for Certification Authorities Issuing Public Key Certificates” [ETSI TS 102042] that specifies certification requirements for the purpose of advanced electronic signatures, authentication, and encryption. In particular the [CP-FhG] policy requirements both for issuing certificates for employees of Fraunhofer and for machines/services are based upon the ETSI policy requirements referred to as “Normalized Certificate Policy” (NCP). The requirements specified in this [CP-FhG] are expressed in terms of key words such as SHALL, MUST, MAY, OPTIONAL etc. with their meaning as specified in [RFC 2119]. A complete list of references is given in chapter 10.

1.2 Document Name and Identification

This certificate policy document is entitled “Fraunhofer Corporate PKI Certificate Policy” or [CP-FhG] in short notation. This certificate policy is identified by the object identifier (OID) 1.3.6.1.4.1.778.80.3.1.1 whose components have the meaning given in Table 1.

Table 1: CP -OID of Fraunhofer Corporate PKI

OID Component	Meaning of OID Component
1	Iso
3	Org
6	Dod
1	Internet
4	private
1	enterprise
778	778 (Fraunhofer Gesellschaft)
80	80 (Zentrale ZV der Fraunhofer Gesellschaft)[1]
3	Fraunhofer Corporate PKI
1	Certificate Policy
1	Version number (current version: 1.1)

The current version 1.1 has been published, because the Fraunhofer Corporate PKI has to fulfill the « Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.0 » of the CA/Browser Forum with an effective date of 1 July 2012.

The Fraunhofer Corporate PKI conforms to the current version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates published at http://www.cabforum.org. In the event of any inconsistency between this document and those Requirements, those Requirements take precedence over this document.

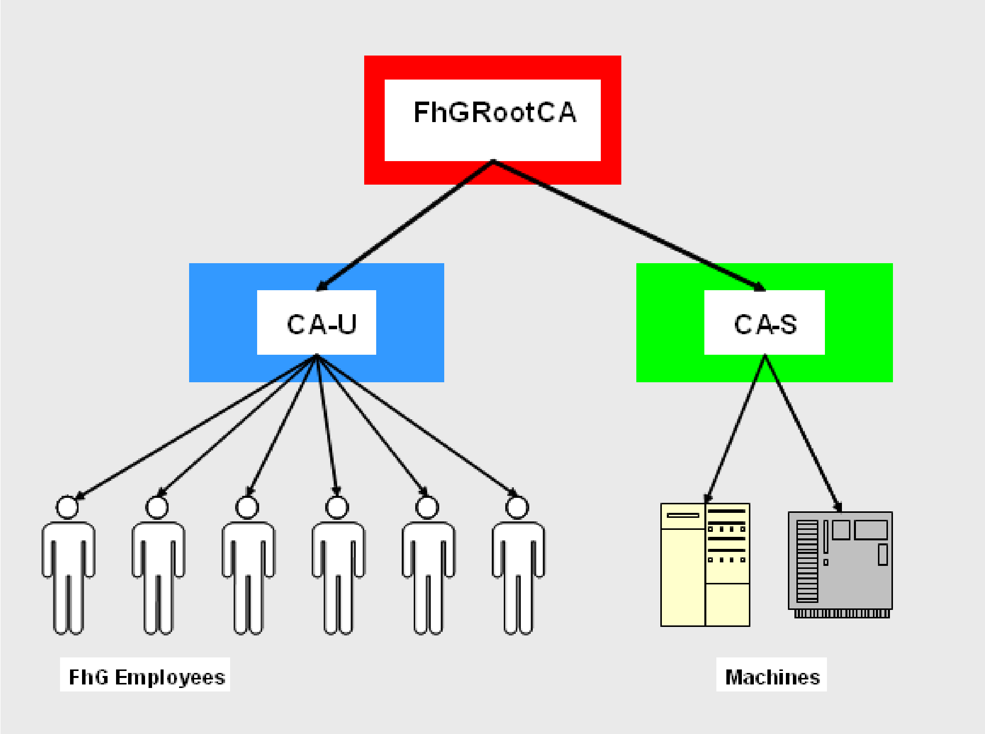
1.3 PKI Participants

1.3.1 Certification Authorities

The architecture of the Fraunhofer Corporate PKI is shown in Figure 1.

[1] Central Office of Fraunhofer Gesellschaft

Figure 1: Architecture of the Fraunhofer Corporate PKI



Fraunhofer Corporate PKI SHALL be based on a two-layer certification hierarchy which SHALL be composed of the following three types of certification authorities (CAs):

- Fraunhofer Root CA (R-CA) is the root certification authority of Fraunhofer Corporate PKI that SHALL be responsible for the issuance of certificates for its directly subordinated CAs.

- Fraunhofer User CA (CA-U) is a certification authority that SHALL be responsible for the issuance of certificates for employees of Fraunhofer. CA-U SHALL support the issuance of the following three types of certificates for natural persons:
  - signature certificates,
  - authentication certificates, and
  - encryption certificates.

  CA-U MAY also be responsible for the issuance of non-personal certificates for OCSP responders.

- Fraunhofer Service CA (CA-S) is a certification authority that SHALL be responsible for the issuance of authentication and encryption certificates for machines, services and other non-personal use.

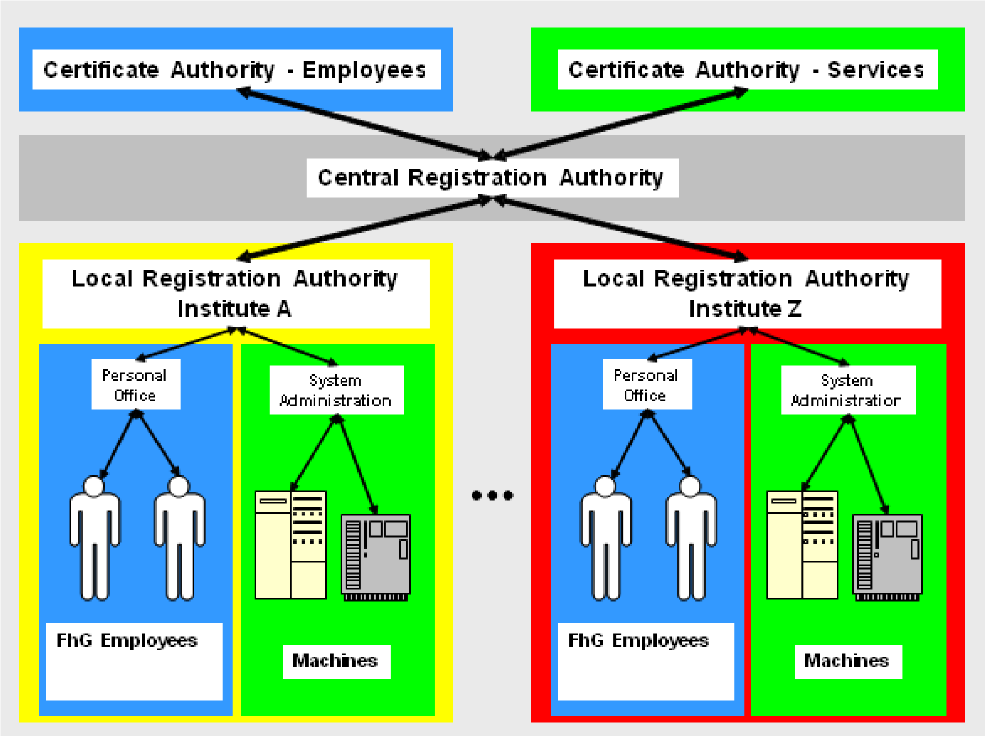
CA-S MAY also be responsible for the issuance of code signing and OCSP responder certificates.

1.3.2 Registration Authorities

The architecture of the registration authorities (RAs) of the Fraunhofer Corporate PKI is illustrated in Figure 2.

The structure of the RAs SHALL be matched with the organizational structure of Fraunhofer. Two kinds of RAs SHALL be distinguished: These are local RAs that SHALL be located at the sites of the different institutes, and a single central RA.

Figure 2: Overview of the RA Architecture of the Fraunhofer Corporate PKI


Certificate Authority - Employees
Certificate Authority - Services
Central Registration Authority
Local Registration Authority Institute A
Local Registration Authority Institute Z
Personal Office
System Administration
FhG Employees
Machines
Personal Office
System Administratior
FhG Employees
Machines

Local RAs SHALL be responsible for the verification of the identity of employees and the authenticity of machines.

The central RA SHALL be responsible for the approval of certification requests from local RAs, employees or system administrators before passing this information to the associated CAs.

1.3.3 Subscribers

Subscribers - also called end entities (EEs) - of the CA-U SHALL be employees of Fraunhofer who have been registered and activated within the Fraunhofer ERP-system SIGMA and furthermore the OCSP responder for which certificates have been or will be issued by CA-U. Subscribers of the CA-S SHALL be services (including code signing services)/machines represented by system administrators or Fraunhofer institutes or organizations within Fraunhofer represented by authorized members, and the OCSP responder for which certificates have been or will be issued by CA-S.

1.3.4 Relying Parties

Relying parties SHALL be communication partners of employees of Fraunhofer and users of services / machines owned or operated by Fraunhofer and its institutes or organizations.

1.3.5 Other Participants

No stipulation.

1.4 Certificate Usage

The issuance, distribution, and usage of all certificates issued by the R-CA, CA-U, or CA-S SHALL comply with this CP.

1.4.1 Appropriate Certificate Usages

Certificates issued by the R-CA SHALL be used by the sub-CAs CA-U and CA-S for issuing certificates and for CRL signing. The certificates issued to the sub-CAs SHALL include the key usage bits for key cert signing and CRL signing. Certificates issued by the CA-R SHALL be used by the related OCSP responder for the purpose of signing OCSP responses. CA-R SHALL NOT issue certificates for any other use, especially not for end entities.

Certificates issued by the CA-U MAY be used by the subscribers for the purposes of non-repudiation, integrity, authentication and confidentiality depending on the particular key usage type specified within the certificates. Certificates issued by the CA-U SHALL be used by the related OCSP responder for the purpose of signing OCSP responses.

Certificates issued by the CA-S MAY be used by services (including code signing services)/machines for the purposes of non-repudiation, integrity, authentication and confidentiality depending on the particular key usage type specified within the certificates. Certificates issued by the CA-S SHALL be used by the related OCSP responder for the purpose of signing OCSP responses.

1.4.2 Prohibited Certificate Usages

R-CA SHALL NOT issue a sub-CA certificate that can be used for Man-in-the-Middle (MitM) or "traffic management" of domain names or IPs that the subscriber does not legitimately own or control.

It is not permitted to use a CA certificate for any kind of MitM scenario.

Certificates issued by CA-S and CA-U to subscribers MUST NOT be used to issue further certificates.

Any other use of certificates not specified in section 1.4.1 SHALL NOT be allowed.

1.5 Policy Administration

See the corresponding section of the certification practice statement [CPS-FhG].

1.6 Definitions and Acronyms

A list of acronyms that are used within this CP is provided in Table 2 of chapter 11. All technical terms used in this document have the same meaning as defined in relevant standards. For this reason a list of definitions of terms that would repeat this information is not provided.

2 Publication and Repository Responsibilities

2.1 Repositories

Fraunhofer Corporate PKI SHALL offer a publicly accessible repository where CA and subscriber encryption certificates are published. The repository MUST be at least available via LDAP or a web interface. CRLs of the Fraunhofer Corporate PKI SHALL be offered on a publicly accessible website. Repositories for revoked certificates are detailed in 4.9.

Access to certificates and CRLs MUST be provided free of charge. Further regulations are provided in the document [CPS-FhG].

2.2 Publication of Certification Information

Fraunhofer Corporate PKI SHALL provide the following publicly available certification information:

- certificate of the R-CA,
- fingerprint of the certificate of the R-CA,
- certificates of the CA-U and CA-S,
- fingerprints of the certificates of the CA-U and CA-S,
- encryption certificates of subscribers, and the
- document [CP-FhG].

Further regulations, if applicable SHALL be provided in section 2.2 of the document [CPS-FhG].

2.3 Time or Frequency of Publication

Requirements related to the time or frequency of publication of certification information SHALL be specified in section 2.3 of the document [CPS-FhG].

2.4 Access Controls on Repositories

Reading access to information mentioned in sections 2.1 and 2.2 SHALL NOT be limited by any form of access control. However, writing access SHALL exclusively be allowed for authorized personal, and SHALL be subject to strong access control.

3 Identification and Authentication

CAs and RAs SHALL use personal data that are provided and managed by the FhG SIGMA system, and that are required for the generation of certificates and the production and personalization of smartcards after the approval of the identity and authenticity of employees. Additional information such as domain user names or photos of employees MAY be provided by other sources. Further details and regulations MAY be provided in the document [CPS-FhG].

3.1 Naming

The identification and authentication of CAs and end entities (EE) SHALL be supported by means of the distinguished names (DN) concept within CA and end entity certificates. This concept allows a unique referencing scheme of members in the directory information tree (DIT). Further details SHALL be provided in the document [CPS-FhG].

3.1.1 Types of Names

All names that occur in X.509 certificates SHALL be DNs compliant with the ITU-T X.500 series of recommendations, and particularly with "The Directory: Models" [X.501], and "The Directory: Selected Attribute Types" [X.520]. DNs included in X.509 certificates SHALL at least include the naming attributes country name (C), organization name (O), organizational unit name (OU), and common name (CN). Specific types of names are specified in section 3.1.1 of the document [CPS-FhG].

3.1.2 Need for Names to be Meaningful

DNs SHALL clearly and unambiguously identify CAs and EEs. The assignment of DNs to CAs and EEs SHALL satisfy the following requirements:

- certificates SHALL only be issued for valid subscribers,
- certificates for machines and services MUST be recognizable as such,
- certificates for employees of Fraunhofer MAY use the pseudonym attribute in DNs,
- subject DNs SHALL be unique within the set of subscribers of a particular CA, and
- any further regulations MAY be specified in the document [CPS-FhG].

3.1.3 Anonymity or Pseudonymity of Subscribers

CAs MUST NOT support the anonymity of EEs. However, CAs MAY issue certificates that support the pseudonymity of EEs provided that the central RA is able to trace back the pseudonym to the corresponding EE.

3.1.4 Rules for Interpreting Various Name Forms

The UTF8 character set SHALL be used as default character set. Further regulations MAY be specified in the document [CPS-FhG].

3.1.5 Uniqueness of Names

The uniqueness of names within the Fraunhofer Corporate PKI SHALL be realized by a hierarchical naming concept with the unique DN-prefix "C=DE, O=Fraunhofer" below which the leaves of the naming tree i.e. the CA and the EE common name component SHALL be assigned. This DN-prefix SHALL be used by RAs in order to assign DNs to subscribers. RAs MUST approve the correctness and uniqueness of new allocated DNs. Subscribers MAY possess several certificates with the same DN, however with a different certificate serial number.

3.1.6 Recognition, Authentication, and Role of Trademarks

Not applicable

3.2 Initial Identity Validation

Local registration authorities SHALL be authorized to perform the initial identity validation of subscribers prior to the issuance of certificates which is required for the purpose of authentication of the data that have to be included in the related certificates.

3.2.1 Method to Prove Possession of Private Key

This section does not apply to key pairs of natural persons since these are generated centrally.

In case where key pairs of EEs certified by CA-S are generated locally a method to prove possession of the private key MUST be implemented.

3.2.2 Authentication of Organization Identity

Fraunhofer Corporate PKI SHALL provide certification services for Fraunhofer institutes and other organizations within Fraunhofer whose authentication

SHALL be verified by RAs. The related authentication procedures SHALL be specified in section 3.2.2 of the document [CPS-FhG].

3.2.3 Authentication of Individual Identity

As a basic principle all employees of Fraunhofer who have been registered within the SIGMA system are automatically authenticated (also called employee in the following). Local registration authorities SHALL perform the identity validation of natural persons when handing-out the smartcards to the subscribers. Subscribers or a duly authorized person with a written authority which is personally signed by the subscriber MUST be personally present at the responsible local RA during the identification procedure. Identity validation of employees of Fraunhofer located at outposts MAY also be performed by alternative methods providing similar strength such as Deutsche Post PostIdent.

The identification of subscribers of CA-U by the local RAs SHALL be based on official documents in German and/or English, namely identity cards or passports. In case the document is not in German and/or English a copy of the document MUST be provided to the local RA. Subscribers whose personal data have been included in SIGMA are registered a-priori. Information such as personal data of employees needed for the issuance of certificates and smartcards SHALL be provided by the SIGMA system to which only authorized RA personnel SHALL have access.

Further details of the authentication procedure are given in section 3.2.3 of the document [CPS-FhG].

3.2.4 Non-Verified Subscriber Information

Not applicable

3.2.5 Validation of Authority

Not applicable

3.2.6 Criteria for Interoperation

The initial identity validation of subscribers is a critical process during which the correct and efficient interoperation between the involved CAs and RAs of the Fraunhofer Corporate PKI SHALL be guaranteed. In order to achieve this goal, the tasks of the CAs and RAs SHALL be clearly specified and separated. Local RAs and the central RA SHALL be responsible for the identity validation and registration of subscribers. The central RA SHALL be responsible for the final approval of data that are required for the issuance of certificates. CA-U SHALL use the approved data produced by the central RA for the generation of key pairs and the issuance of certificates for natural persons. CA-S SHALL use the approved data produced by the central RA for the issuance of certificates for services/machines.

3.3 Identification and Authentication for Re-Key Requests

Every employee of Fraunhofer registered by the Fraunhofer SIGMA system SHALL automatically get a new card with new key pairs and new certificates before the validity of his current certificates expires. For this reason authentication of natural persons for re-key methods is not required since it has been implicitly realized. Consecutive smartcards SHALL be automatically produced at latest a fixed time prior to the expiration of the actual cards. This maximum period SHALL be defined in section 3.3 of the document [CPS-FhG].

3.3.1 Identification and Authentication for Routine Re-key

The identification and authentication methods for routine re-key requests are identical to those used for initial identity validation (see section 3.2.3). Additionally, the identification of subscribers of CA-U MAY also be based on an existent Fraunhofer Smartcard of the subscriber unless his/her name has changed.

3.3.2 Identification and Authentication for Re-key After Revocation

The identification and authentication methods for re-key after revocation are identical to those used for initial identity validation (see section 3.2.3).

3.4 Identification and Authentication for Revocation Requests

The revocation of a subscriber certificate SHALL be initialized by means of an application for revocation by the related employee or an authorized person. A revocation service SHALL be offered that SHALL be responsible for the identification, authentication, and handling of applications for certificate revocation. Further information is provided in section 3.4 of the document [CPS-FhG].

4 Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

The following categories of certificate applications SHALL be supported:

- certificates for employees of Fraunhofer and
- certificates for services (including code signing services)/machines.

Certificate Applications for Employees of Fraunhofer

The following types of certificate applications for employees of Fraunhofer SHALL be supported:

- initial smartcard,
- consecutive smartcard,
- second smartcard,
- backup smartcard,
- emergency smartcard,
- secretary/substitution smartcard, and
- temporary replacement card.

Initial Smartcard

Every employee of Fraunhofer SHALL get an *initial smartcard* that includes certificates and key pairs for signature, authentication and encryption. The submission of the related certificate applications for employees SHALL be done by the assigned personnel offices (local RAs) that have access to the SIGMA personnel administration system of Fraunhofer.

The initial automatic roll-out of smartcards for employees SHALL start in 2007. SIGMA SHALL provide CAs and the central RA with a list of all registered employees and their personal data. The institutes MAY provide additional information to be included within certificates or printed on the cards. The authentication of employees for the initial roll-out is implicitly approved by registration within SIGMA.

CAs and RAs SHALL use personal data that is provided and managed by the SIGMA system of Fraunhofer, and that is required for the generation of certificates and the production and personalization of smartcards after the approval of the identity and authenticity of employees. Additional information such as domain user names or photos of employees MAY be provided by the individual institutes.

Consecutive Smartcard

Every employee registered by SIGMA SHALL automatically get a *consecutive smartcard* that includes new certificates and new key pairs for signature, authentication and encryption as a replacement of his/her initial card a fixed time period prior to the expiration of the validity of his/her certificates. This maximum period SHALL be defined in section 4.1.1 of the document [CPS-FhG]. Additionally, employees registered by SIGMA SHALL get a *consecutive smartcard* in case subscriber information contained in the certificates such as name, affiliation etc. has changed. The submission of the related certificate applications for employees SHALL be done by the assigned personnel offices. Employees MAY submit a certificate application for a *consecutive smartcard* during the course of a certificate revocation request.

Second Smartcard

Employees of Frauhnofer MAY submit a certificate application for a *second smartcard*. The second smartcard SHALL contain new certificates and new key pairs for signature and authentication, and the same key pair and certificate for encryption as of those of the valid (initial or consecutive) smartcard.

Backup Smartcard

Employees of Fraunhofer MAY submit a certificate application for a *backup smartcard*. The *backup smartcard* SHALL contain a key pair and certificate for encryption of a valid or invalid (initial or consecutive) smartcard of the employee. A *backup smartcard* SHALL NOT contain certificates and key pairs for signature or authentication.

Emergency Smartcard

Institutes of Fraunhofer MAY submit a certificate application for an *emergency smartcard* under circumstances agreed with the joint works council of Fraunhofer. The *emergency smartcard* SHALL contain a key pair and certificate for encryption of a valid or invalid (initial or consecutive) smartcard of an employee of Fraunhofer. An *emergency smartcard* SHALL NOT contain certificates and key pairs for signature or authentication.

Secretary/Substitution Smartcard

Employees of Fraunhofer MAY submit a certificate application for a *secretary/substitution smartcard*. The *secretary/substitution smartcard* SHALL contain a key pair and certificate for encryption of a valid (initial or consecutive) smartcard of the employee and SHALL be handed out to another employee of Fraunhofer acting as a substitute for the requesting employee. A *secretary/substitution smartcard* SHALL NOT contain certificates and key pairs for signature or authentication.

Temporary Replacement Cards

Institutes MAY get a set of *temporary replacement cards* for the purpose of authentication of employees who may have forgotten their cards. Local RAs SHALL submit certificate applications for *temporary replacement cards* on behalf of employees. Local RAs SHALL integrate the authentication certificate and keys contained in the certificate responses within the temporary replacement cards. The validity period for temporary replacement cards SHALL be limited to a fixed time which SHALL be defined in section 4.1.1 of the document [CPS-FhG].

Certificate Applications for Services/Machines

Services (including code signing services)/machines MAY be equipped with certificates and key pairs for the purposes of guaranteeing authenticity, integrity and confidentiality in the form of SW-PSEs. The submission of the related certificate applications SHALL be done by the associated authorized system administrators, or service operators who MUST be employees of Fraunhofer.

4.1.2 Enrollment Process and Responsibilities

CAs and the central RA SHALL be responsible for the establishment and operation of the enrollment process. Local RAs are responsible for the identification of subscribers before handing-out the produced smartcards to them.

4.2 Certificate Application Processing

The processing of certification applications by CAs and RAs SHALL be based on proofs of the identity and authenticity of the applicants.

4.2.1 Performing Identification and Authentication Functions

RAs SHALL perform the identification and authentication procedures described in chapter 3 in order to approve the certification applications.

4.2.2 Approval or Rejection of Certificate Applications

RAs SHALL notify the applicants of the approval or rejection of a certificate application. Certificate applications SHALL only be forwarded by the central RA to the CA for further processing if the identification and authentication procedures have been successfully completed.

4.2.3 Time to Process Certificate Applications

The maximum time to process certificate application SHALL be specified in section 4.2.3 of the document [CPS-FhG].

4.3 Certificate Issuance

CAs SHALL issue certificates after the final approval of certificate applications by the central RA, and for CA-U after the generation of key pairs by the card management system (CMS). For CA-S the key pairs SHALL be generated by the subscriber.

The central RA SHALL verify that no known weak keys will be certified by CA-S. Further details MAY be specified in section 4.3 of the document [CPS-FhG].

4.3.1 CA Actions During Certificate Issuance

CA-U SHALL process certification requests coming from the CMS, generate the related certificates and SHALL return the issued certificates to the CMS which in turn SHALL integrate the certificates into the related smartcards. The CMS SHALL also destroy the generated signature and authentication keys, and SHALL store the encryption keys and certificates.

CA-S SHALL process certification requests coming from the central RA, generate the related certificates and SHALL return the issued certificates to the central.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

For CA-U, RAs SHALL notify the subscribers that their smartcards including the certificates have been generated and can be obtained at the related local RA. Local RAs SHALL validate the identity of subscribers before handing-out the smartcards to them.

For CA-S, the central RA SHALL notify the subscribers that their certificates have been issued and can be obtained from the central Fraunhofer directory.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

For CA-U, the handing-out of smartcards to the subscribers by local RAs SHALL indicate the approval and acceptance of the included certificates by both the issuing CA and the subscribers. Subscribers SHALL agree to the actual policy which has been published, and which is also referenced within the certificates.

4.4.2 Publication of the Certificate by the CA

CAs SHALL be responsible for the publication of certificates and revocation information in the central Fraunhofer directory. CA-U SHALL publish subscriber certificates used for the purpose of encryption.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

Not applicable

4.5 Key Pair and Certificate Usage

The scope of certificate usage as described in section 1.4 SHALL apply.

4.5.1 Subscriber Private Key and Certificate Usage

Subscribers of the Fraunhofer Corporate PKI SHALL use the associated private keys of the certificates only for the purposes specified within this policy document (see section 1.4) and included within the key usage extension certificate field.

Subscribers SHALL ensure that their private key is protected appropriately; in particular subscribers of the CA-U SHALL NOT hand over their smartcard to any third party and SHALL only use smartcards that they received personally from their local RAs or via a representative, who is authorized to act on behalf of the subscriber by a signed document.

4.5.2 Relying Party Public Key and Certificate Usage

Relying parties SHOULD verify the validity of a certificate for its intended use prior to using it.

4.6 Certificate Renewal

Certificate renewal, i. e. the issuance of a new certificate for an existing public key SHALL NOT be supported by CAs. Instead for CA-U consecutive smartcards and for CA-S new SW-PSEs respectively including new key pairs and associated new certificates SHALL be produced as specified in section 4.1.

4.6.1 Circumstance for Certificate Renewal

Not applicable

4.6.2 Who May Request Renewal

Not applicable

4.6.3 Processing Certificate Renewal Requests

Not applicable

4.6.4 Notification of New Certificate Issuance to Subscriber

Not applicable

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Not applicable

4.6.6 Publication of the Renewal Certificate by the CA

Not applicable

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

Not applicable

4.7 Certificate Re-Key

Routine certificate re-key leading in case of CA-U to a consecutive smartcard or in case of CA-S to a SW-PSE SHALL be supported by CAs and the central RA. Routine certificate re-key for CA-U subscriber certificates SHALL be initiated by the central RA at least a fixed time prior to the expiration of the validity of a certificate as specified in section 4.1. The maximum period for routine certificate re-key SHALL be defined in section 4.7 of the document [CPS-FhG].

4.7.1 Circumstance for Certificate Re-key

Certificate re-key SHALL be supported within a time range prior to the expiration of the validity of a certificate, during the course of a certificate revocation request or, while processing a request for a second smartcard.

4.7.2 Who May Request Certification of a New Public Key

Certificate re-key leading for CA-U to consecutive smartcards and for CA-S to SW-PSEs respectively MAY be initiated by the subscriber during the course of a certificate revocation request. If in accordance with the description in section 4.9.1 of this document the requirements for a destruction of a damaged valid initial, consecutive or second smartcard are fulfilled, the subscriber MAY opt for a second smartcard instead of a consecutive smartcard. In all other cases certificate re-key SHALL be initiated by the central RA.

4.7.3 Processing Certificate Re-keying Requests

The processing of certificate re-key requests SHALL be performed in accordance with the requirements specified in sections 4.2 and 4.3.

4.7.4 Notification of New Certificate Issuance to Subscriber

For CA-U, RAs SHALL notify the subscribers that their smartcards including the new certificates and key pairs have been generated and can be obtained at the related local RA. Local RAs SHALL proof the identity of subscribers before handing-out the new smartcards to them.

For CA-S, the central RA SHALL notify the subscribers that their new certificates have been issued and can be obtained from the central Fraunhofer directory.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

For CA-U, the handing-out of new smartcards to the subscribers by local RAs SHALL indicate the approval and acceptance of the included certificates by both the issuing CAs and the subscribers.

4.7.6 Publication of the Re-keyed Certificate by the CA

CAs SHALL comply with the requirements on the publication of re-keyed certificates as specified in section 4.4.2.

4.7.7 Notification of certificate issuance by the CA to other entities

Not applicable

4.8 Certificate Modification

Certificate modification SHALL NOT be supported. Instead, if information included in a certificate, such as name or organization of a subscriber has changed, CAs SHALL comply with the procedures for certificate re-key as specified in section 4.7, followed by the revocation of the old certificate or, in case of CA-U by the destruction of the smartcard if in accordance with the description in section 4.9.1 of this document the requirements for a destruction of a smartcard are fulfilled.

4.8.1 Circumstance for Certificate Modification

Certificate re-key instead of certificate modification MAY be required, if subscriber information contained in the certificate such as name, affiliation, e-mail address etc. has changed.

4.8.2 Who May Request Certificate Modification

Certificate re-key instead of certificate modification MAY be requested by subscribers or the central RA which has i. e. knowledge about changed personal data records within SIGMA. See also section 4.7.2.

4.8.3 Processing Certificate Modification Requests

CAs and RAs SHALL process certificate re-key requests instead of certificate modification requests in compliance with the requirements as specified in section 4.7.3.

4.8.4 Notification of New Certificate Issuance to Subscriber

For CA-U, RAs SHALL notify the subscribers that their smartcards including the new (modified) certificates and key pairs have been generated and can be obtained at the related local RA. Local RAs SHALL validate the identity of subscribers before handing-out the new smartcards to them.

For CA-S, the central RA SHALL notify the subscribers that their new certificates have been issued and can be obtained from the central Fraunhofer directory.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

For CA-U, the handing-out of new smartcards to the subscribers by local RAs SHALL indicate the approval and acceptance of the included certificates by both the issuing CAs and the subscribers. Subscribers SHALL agree to the actual policy which has been published, and which is also referenced within the certificates.

4.8.6 Publication of the Modified Certificate by the CA

CAs SHALL comply with the requirements on the publication of new (modified) certificates as specified in section 4.4.2.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

Not applicable

4.9 Certificate Revocation, Suspension and Secure Destruction of Smartcards

CAs SHALL support the revocation of certificates, but SHALL NOT support the suspension of certificates. CA-U MAY support secure destruction of smartcards instead of revocation of the corresponding certificates in defined cases. Secure destruction of smartcards SHALL be confirmed by local RAs.

4.9.1 Circumstances for Revocation or Secure Destruction of Smartcards

CAs SHALL revoke a certificate, if one of the following events has occurred:

- loss, or theft of smartcard or certificate,
- suspicion or knowledge of private key compromise, or
- security-relevant violation of the CP or CPS requirements by subscribers.

CA-U SHALL either revoke a certificate or alternatively securely destroy the smartcards indicated below containing the certificate, in case one of the following events has occurred:

- change of subscriber information contained in the certificate,

  If the destruction of smartcard is chosen, all corresponding smartcards – except for backup smartcards at the most – containing the certificate SHALL be destroyed.

- damage of smartcard.

  If the destruction of smartcard is chosen, the damaged smartcard containing the certificate SHALL be destroyed.

If secure destruction of smartcards cannot be tracked, the certificate MUST be revoked.

4.9.2 Who Can Request Revocation

The revocation of a certificate MAY be requested by the following persons or organizations:

- a subscriber who is the owner of the certificate to be revoked,
- authorized local RA personnel,
- authorized central RA personnel, or
- authorized CA personnel.

4.9.3 Procedure for Revocation Request

Revocation requests SHALL be forwarded to the central RA which in turn SHALL approve the authenticity of the requestor and the reasons for revocation. The central RA SHALL generate for CA-U a signed revocation request and forward it via CMS to the associated CA. For CA-S, the central RA SHALL revoke the certificate directly within the CA or make use of an appropriate tool for passing the revocation request to the CA. After the completion of the revocation the CA SHALL publish this information in the related CRL and SHALL return a confirmation to the certificate owner. CAs and RAs SHALL document and archive all security relevant events that have occurred during the revocation process.

4.9.4 Revocation Request Grace Period

Subscribers or authorized personnel that have observed one of the circumstances for certificate revocation as specified in section 4.9.1 SHALL immediately initiate the revocation of this certificate.

4.9.5 Time Within Which CA Must Process the Revocation Request

The time within which CAs SHALL process revocation requests SHALL be specified in section 4.9.5 of the document [CPS-FhG].

4.9.6 Revocation Checking Requirement for Relying Parties

Relying parties SHOULD perform certificate path validation of a certificate for its intended use prior to using it. This validation procedure SHALL include the checking of the status of all certificates of the certification path. Relying parties MAY perform the checking either against the current CRL from directory publicly accessible website, or against on-line certificate status information from an OCSP responder (see section 2.1).

4.9.7 CRL Issuance Frequency

CAs SHALL issue CRLs with an issuance frequency as specified in section 2.3.

4.9.8 Maximum Latency for CRLs

CAs SHALL issue CRLs within a maximum latency as specified in section 2.3.

4.9.9 On-line Revocation/Status Checking Availability

The availability of the OCSP responders SHALL be defined in section 4.9.9 of the document [CPS-FhG].

4.9.10 On-line Revocation Checking Requirements

The OCSP responders SHALL comply with the requirements as specified in the document [RFC 2560]. Applications MAY use the service of the OCSP responders of Fraunhofer and SHOULD support [RFC 2560]. For further information see sections 7.2 and 7.3 of the document [CPS-FhG].

4.9.11 Other Forms of Revocation Advertisements Available

No stipulation

4.9.12 Special Requirements re Key Compromise

In the case of private key compromise of a subscriber or CA the revocation of the affected certificates SHALL be carried out.

4.9.13 Circumstances for Suspension

Not applicable

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

The OCSP responders of Fraunhofer SHALL comply with the requirements as specified in the document [RFC 2560]. Applications MAY use the service of the OCSP responders of Fraunhofer and SHOULD support [RFC 2560]. For further information see sections 7.2 and 7.3 of the document [CPS-FhG].

4.10.1 Operational Characteristics

Operational aspects of the OCSP SHALL be specified in sections 7.2 and 7.3 of the document [CPS-FhG].

4.10.2 Service Availability

The service availability of the OCSP responders SHALL be continuously controlled by a monitoring system.

Further requirements on service availability SHALL be specified in section 4.10.2 of the document [CPS-FhG].

4.10.3 Optional Features

No stipulation

4.11 End of Subscription

For CA-U, all smartcards containing the subscriber's certificate SHALL be given back to the local RAs and securely be destroyed at the end of subscription. The secure destruction of the smartcards SHALL be documented and confirmed by local RAs. In case the destruction of at least one of the smartcards is not documented accordingly, the corresponding certificate SHALL immediately be revoked.

For CA-S, all certificates SHALL be immediately revoked at the end of subscription.

Further details MAY be specified in section 4.11 of the document [CPS-FhG].

4.12 Key Escrow and Recovery

Key escrow and recovery SHALL be provided for CA keys and encryption keys of employees.

4.12.1 Key Escrow and Recovery Policy and Practices

Key escrow and recovery for CAs private signing keys SHALL be supported.

Key escrow and recovery for CA-U subscriber's private signing keys SHALL NOT be supported.

Key escrow and recovery for CA-U subscriber's private authentication keys SHALL NOT be supported.

Key escrow and recovery for CA-U subscriber’s private encryption keys SHALL be supported.

Key escrow and recovery for CA-S subscriber’s private singing, authentication and encryption keys SHALL NOT be supported.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

No stipulation

5 Facility, Management, and Operational Controls

As a basic principle CAs SHALL consider relevant and applicable requirements on facility, management, and operational controls that are specified in the AICPA/CICA document "WebTrust Program for Certification Authorities" [WT-PCA] and in the BSI document "IT Baseline Protection Manual"[IT-BPM]. The implementation of these requirements SHALL be specified in section 5 of the document [CPS-FhG]. Concrete instructions for CA personnel to fulfill all the requirements specified in this chapter are described in separate non-published documents such as those listed in section 10.

5.1 Physical Controls

CA facilities SHALL provide adequate means of physical security controls. These controls SHALL limit the physical access to the CA facilities to properly authorized personnel only. CA facilities SHALL be protected from environmental hazards.

Further details MAY be specified in section 5.1 of the document [CPS-FhG].

5.1.1 Site Location and Construction

CAs SHALL be located at the sites mentioned in section 1.3.1 of the document [CPS-FhG]. CAs SHALL implement the following security measures related to room construction:

- CA rooms SHALL be designed as closed security area with a single entrance door.
- The security area SHALL at least be structured into the following three security zones:
  - security zone 1 which contains the workplaces for the Service Desk,
  - security zone 2 which contains the workplaces for the CA personnel, and
  - security zone 3 which contains the CA servers.
- Required emergency exits SHALL only be usable from inside the rooms.
- Alarms SHALL be initiated when opening an emergency exit.
- Fire protection requirements and personal security requirements SHALL be regarded.

Further details MAY be specified in section 5.1.1 of the document [CPS-FhG].

5.1.2 Physical Access

Unauthorized access to the security area SHALL be protected by an alarm system and/or constructional security measures. The alarm system SHALL be activated, if the security area is not occupied.

Access to the security area SHALL be protected by high-quality access control mechanisms. Access to the security area SHALL be logged. Inside the security area identification cards SHALL be visibly carried by authorized personnel.

The security zone 1 MAY be accessed by authorized personnel and registered visitors. The access to security zone 1 by visitors SHALL be logged.

The security zone 2 MAY be accessed by authorized personnel and registered visitors with proper justification escorted by authorized persons. The access to security zone 2 by visitors and the associated reasons for their visit SHALL be logged.

Further details MAY be specified in section 5.1.2 of the document [CPS-FhG].

5.1.3 Power and Air Conditioning

CAs SHALL use power and air conditioning facilities that sufficiently support the CA operations. Important CA systems and access control and monitoring systems SHALL protected by UPS.

Further details MAY be specified in section 5.1.3 of the document [CPS-FhG].

5.1.4 Water Exposures

CAs SHALL take appropriate measures to ensure that CA systems are protected from water exposure.

Further details MAY be specified in section 5.1.4 of the document [CPS-FhG].

5.1.5 Fire Prevention and Protection

CAs SHALL use fire suppression facilities and SHALL take appropriate fire prevention measures to ensure that CA systems are protected from fire exposure.

Further details MAY be specified in section 5.1.5 of the document [CPS-FhG].

5.1.6 Media Storage

CAs SHALL take appropriate security measures to ensure that used media storage is protected from environmental effects such as temperature, humidity or magnetism.

CAs SHALL use security safes or security boards in the security zone 2 for the storage of important and sensitive media documents and materials such as sensitive plaintext information, blank smartcards, or HSM for root keys.

Further details MAY be specified in section 5.1.6 of the document [CPS-FhG].

5.1.7 Waste Disposal

CAs SHALL take appropriate security measures to ensure the sanitization or destruction of confidential information on removable media before its release for disposal.

Further details MAY be specified in section 5.1.7 of the document [CPS-FhG].

5.1.8 Off-site Backup

CAs SHALL perform off-site backup using facilities with an appropriate level of security.

Further details MAY be specified in section 5.1.8 of the document [CPS-FhG].

5.2 Procedural Controls

CAs and RAs SHALL provide appropriate organizational measures in order to ensure a proper, secure, and effective operation of their services. These measures SHALL include a clear definition of roles, tasks, assignment of tasks to roles, and a list of incompatible roles.

5.2.1 Trusted Roles

CAs and RAs SHALL make a clear distinction between the following categories of roles:

- supervising roles: e.g. IT security officer, revisor
- administrative roles: e.g. head of CR/RA, contact partner, and
- operative roles: e.g. CA employee, central RA-employee, local RA-employee, directory maintenance, employee, and authorized person.

The related sets of trusted roles SHALL be specified in section 5.2.1 of the document [CPS-FhG].

5.2.2 Number of Persons Required per Task

CAs and the central RA SHALL ensure that at least always two authorized persons are responsible to perform critical CA and RA tasks as for example the production, personalization and rollout of smartcards.

The complete subset of tasks for which this so-called split knowledge and dual control principle has to be realized SHALL be defined in section 5.2.2 of the document [CPS-FhG]. Other tasks that are not included in the selected subset MAY be carried out by single individuals.

5.2.3 Identification and Authentication for Each Role

CAs and RAs SHALL specify the assignment of roles to individual CA and RA employees whose identification and authentication has been verified.

Further details MAY be specified in section 5.2.3 of the document [CPS-FhG].

5.2.4 Roles Requiring Separation of Duties

CAs and RAs SHALL ensure a separation of roles for critical functions in order to prevent any malicious use of CA and RA systems without detection.

The set of roles that require the separation of duties SHALL be given in section 5.2.4 of the document [CPS-FhG].

5.3 Personnel Security Controls

CAs and RAs SHALL maintain personnel security controls to ensure the trustworthiness of CA's and RA's operations.

5.3.1 Qualifications, Experience, and Clearance Requirements

CAs and RAs SHALL ensure that their operations are carried out by personnel with sufficient confidentiality, integrity, reliability, qualification and experience.

Further personnel security requirements MAY be specified in section 5.3.1 of the document [CPS-FhG].

5.3.2 Background Check Procedures

CAs and central RAs MAY require the submission of a "no criminal record" prior to the employment of staff.

Further regulation MAY specified in section 5.3.2 of the document [CPS-FhG].

5.3.3 Training Requirements

CAs and RAs SHALL provide comprehensive regular training for their staff. Prior to the assignment of a specific role to an employee, he or she SHALL receive specialized training or SHALL prove the necessary skills and qualifications.

Further training requirements MAY be specified in section 5.3.3 of the document [CPS-FhG].

5.3.4 Retraining Frequency and Requirements

CAs and RAs SHOULD initiate a retraining program for their staff when introducing new IT systems, new security technologies, or new certificate policies.

Further retraining requirements MAY be specified in section 5.3.4 of the document [CPS-FhG].

5.3.5 Job Rotation Frequency and Sequence

Not applicable

5.3.6 Sanctions for Unauthorized Actions

CAs and RAs SHALL withdraw CA/RA site and system access permission of a person due to known performed unauthorized actions of that person. The related CA SHALL revoke those certificates of that person that are used for CA/RA operations.

5.3.7 Independent Contractor Requirements

Not applicable

5.3.8 Documentation Supplied to Personnel

CAs and RAs SHALL at least make their employees aware of the requirements of the documents [CP-FhG] and [CPS-FhG].

Further documentation SHALL be specified in section 5.3.8 of the document [CPS-FhG].

5.4 Audit Logging Procedures

CAs and RAs SHALL specify and use appropriate audit logging procedures to monitor and record the occurrence of all security relevant events during the operation of the CA/RA systems.

5.4.1 Types of Events Recorded

Log entries SHALL at least contain the date, time and originator of the observed event. Logs MAY be recorded electronically or manually.

CAs and RAs SHALL specify the set of events and additional information that SHALL be logged in section 5.4.1 of the document [CPS-FhG].

5.4.2 Frequency of Processing Log

CAs and RAs SHALL regularly monitor and process the produced logs. Exceptional and significant events and any required actions taken after their occurrence and detection SHALL be documented.

The regular period for analyzing the recorded logs SHALL be specified in section 5.4.2 of the document [CPS-FhG].

5.4.3 Retention Period for Audit Log

CAs and RAs SHALL retain their produced audit logs for a particular retention period in compliance with legal requirements.

The concrete value for the retention period for audit logs SHALL be specified in section 5.4.3 of the document [CPS-FhG].

5.4.4 Protection of Audit Log

Audit logs SHALL be protected from unauthorized viewing, modification or deletion. Access to audit logs SHALL be restricted to system and network administrators.

5.4.5 Audit Log Backup Procedures

Audit logs SHALL be regularly backed up.

5.4.6 Audit Collection System (internal vs. external)

CAs and RAs SHALL identify their audit collection systems in section 5.4.6 of the document [CPS-FhG].

5.4.7 Notification to Event-Causing Subject

Upon the detection of the occurrence of an exceptional and serious event the information security officer SHALL be immediately informed. There is no need to notify the subject that has caused the event.

Further requirements MAY be specified in section 5.4.8 of the document [CPS-FhG].

5.4.8 Vulnerability Assessments

CAs SHOULD use the audit logs to conduct a vulnerability assessment.

Further requirements MAY be specified in section 5.4.8 of the document [CPS-FhG].

5.5 Records Archival

All archiving is carried out by the central RA. Local RAs will send all relevant documentation to the central RA.

5.5.1 Types of Records Archived

CAs and the central RA SHALL at least archive the following type of information:

- certificate applications,
- personal subscriber data,
- issued certificates,
- revocation requests, and
- published CRLs.

CAs and RAs MAY specify further types of information that SHALL be archived in section 5.5.1 of the document [CPS-FhG].

5.5.2 Retention Period for Archive

CAs and the central RA SHALL retain their produced audit logs for a particular retention period in compliance with legal requirements.

The concrete value for the retention period for audit log SHALL be specified in section 5.5.2 of the document [CPS-FhG].

5.5.3 Protection of Archive

CAs and RAs SHALL take measures in order to protect archived data from unauthorized viewing, copying, modification and deletion.

Further requirements MAY be specified in section 5.5.3 of the document [CPS-FhG].

5.5.4 Archive Backup Procedures

CAs and the central RA SHALL use archive backup procedures and SHALL store the archive backup in a safety deposit (e.g. Lampertz Safe). CAs SHALL store confidentiality private keys in HSMs or smartcards.

Requirements on archive backup periods and further requirements SHALL be specified in section 5.5.4 of the document [CPS-FhG].

5.5.5 Requirements for Time-stamping of Records

CAs and the central RA SHALL add the date of archiving records to the archived data. Time-stamping by means of a trusted time stamp authority is NOT MANDATED yet.

Further requirements MAY be specified in section 5.5.5 of the document [CPS-FhG].

5.5.6 Archive Collection System (internal or external)

CAs and the central RA SHALL use an archive collection system.

The type of the archive collection system (internal or external) SHALL be specified in section 5.5.6 of the document [CPS-FhG].

5.5.7 Procedures to Obtain and Verify Archive Information

CAs and the central RA SHALL regularly check the integrity of archive backups. Information security officers and revisors SHALL be authorized to access and to inspect the archived data.

Further requirements MAY be specified in section 5.5.7 of the document [CPS-FhG].

5.6 Key Changeover

The R-CA and CAs SHALL change their private signing keys at least two months prior to the expiration of the validity of associated certificates. It is RECOMMENDED to use a subscriber overlapping key period of at least one month.

Furthermore the following requirements SHALL be fulfilled:

- Latest key SHALL be used for signing certificates or CRLs, and the
- Previous key SHALL only be used for signing CRLs.
- The validity period of CAs SHALL be a subset of the validity period of R-CA.
- The validity period of subscriber certificates SHALL be a subset of the validity period of CAs.

Key changeover for subscribers is identical to certificate re-key as specified in section 4.7.

5.7 Compromise and Disaster Recovery

CAs SHALL maintain controls to provide appropriate assurance of continuity of operations in the event of a disaster and/or of a compromise of the CA's private signing key.

5.7.1 Incident and Compromise Handling Procedures

Incident and compromise handling procedures SHALL be specified in section 5.7.1 of the document [CPS-FhG]. CAs SHALL immediately notify their subscribers upon the occurrence of a key compromise.

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

The operation of an IT system in which the corruption of computing resources, software, and/or data has been observed SHALL immediately be terminated, and further appropriate incident handling procedures SHALL be enacted, such as the

- Analysis of the corrupted IT system, and the
- Conduction of security check and audit in order to find potential points of weakness in the system.

Further details on incident handling procedures MAY be specified in section 5.7.2 of the document [CPS-FhG].

5.7.3 Entity Private Key Compromise Procedures

In the event of a proven or suspected compromise of a subscriber's private key the associated certificate SHALL be immediately revoked.

In the event of a proven or suspected compromise of a CA's private key the following action SHALL be taken: Immediate notification of the information security officer, who SHALL investigate the compromise and SHALL initiate appropriate measures e.g. the ones listed below,

- Immediate notification of all subscribers whose certificates have been signed with the compromised key,
- Revocation of the CA's certificate whose associated private key has been compromised,
- Revocation of all subscriber certificates that have been issued with the compromised private key,
- Removal of CRLs from the on-line repository that have been signed with the compromised private key,
- Generation of a new CA key pair and its associated certificate,
- Publication of the new CA certificate, and the
- Issuance of new subscriber certificates (see section 3.3.2).

Further details on entity private key compromise procedures MAY be provided in section 5.7.3 of the document [CPS-FhG].

5.7.4 Business Continuity Capabilities after a Disaster

In the event of corruption or loss of computing resources, software and/or data CAs SHALL perform required actions in order to enable the resumption of business operations after a disaster.

Further requirements on business continuity capabilities after a disaster MAY be specified in section 5.7.4 of the document [CPS-FhG].

5.8 CA or RA Termination

<u>RA Termination</u>

In case of the termination of a local RA the following actions SHALL be conducted:

- Notification of the affected RA,
- Notification of all affected subscribers,

CA Termination

A CA that terminates its operations SHALL conducts the following actions:

- Notification of the R-CA,
- Notification of all subscribers,
- Notification of all RAs,
- Revocation of all certificates,
- Publication of a CRL that contains all revoked certificates, and the
- Destruction of all private keys of the affected CA.

The R-CA SHALL revoke all certificates of the affected CA, and SHALL publish a CRL that contains the revoked certificates.

R-CA Termination

R-CA termination means the closing of the complete operation of Fraunhofer Corporate PKI, in which case the R-CA SHALL conduct the following actions:

- Initialization of the termination of the sub-CAs CA-U and CA-S,
- Revocation of all certificates of the sub-CAs CA-U and CA-S after the completion of the termination of all sub-CAs,
- Revocation of all R-CA certificates,
- Publication of a CRL that contains all revoked certificates, and the
- Destruction of all private keys of the R-CA.

Data whose continuity SHALL be ensured after R-CA termination include the archive of this R-CA and its issued CRLs.

A custodian of archival records SHALL be identified. Contact address of the custodian SHALL be given in section 5.8 of the document [CPS-FhG].

Further requirements on R-CA termination MAY be specified in section 5.8 of the document [CPS-FhG].

6 Technical Security Controls

As a basic principle CAs SHALL consider relevant and applicable requirements on technical security controls that are specified in the AICPA/CICA document "WebTrust Program for Certification Authorities" [WT-PCA] and in the BSI document "IT Baseline Protection Manual" [IT-BPM]. Further requirements MAY be specified in section 6 of the document [CPS-FhG]. Concrete instructions for CA personnel to fulfill all the requirements specified in this chapter in order to ensure the security targets of availability, integrity, confidentiality and authenticity are described in separate non-published documents such as the CA operations manual and the security concept.

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

R-CA

The generation of key pairs for the R-CA and Sub-CAs SHALL be performed according to the document [FhG-RKC] and securely stored in a Hardware Security Module (HSM). The CAs SHALL perform backups of their key pairs.

OCSP Responders

The generation of signature key pairs for central services such as the OCSP responders SHALL be performed by the related CAs.

Subscribers

The generation of signature, authentication and encryption key pairs for subscribers (natural persons) of CA-U SHALL be carried out within the CMS. Copies of encryption keys SHALL be stored in a secure key backup service within the CMS. All other keys generated by the CMS SHALL be destroyed after their import into the smartcard. The encryption key of subscribers of CA-U MAY be exported to a SW-PSE and conveyed to the subscriber in a secure way.

The generation of key pairs for subscribers of CA-S (machines/services including code signing services) SHALL be performed locally by system administrators. Copies of generated keys SHALL be kept in a secure local storage.

Further requirements MAY be specified in 6.1.1 of the document [CPS-FhG].

6.1.2 Private Key Delivery to Subscriber

The private key delivery to subscribers (natural persons) of CA-U SHALL be done by local RAs that hand out the smartcards (that include the private keys) to the subscribers. The subscribers SHALL identify themselves via valid official pieces of identification (identity card, passport) and SHALL confirm the receipt of the cards. For each generated token CAs SHALL generate a PIN letter and SHALL forward this information to the related subscriber.

When private encryption keys are exported from the smartcard they SHALL be delivered securely to the owner.

Further requirements MAY be specified in section 6.1.2 of the document [CPS-FhG].

6.1.3 Public Key Delivery to Certificate Issuer

The transfer of public keys of subscribers (natural persons) of CA-U is carried out by the CMS during the forwarding of a certificate signing request to CA-U after the generation of the subscriber key pairs.

The transfer of public keys of subscribers (machines and services including code signing services) SHALL be done via signed PKCS10 certificate service requests forwarded from system administrators or the machines/services to the central RA that validates the received information and passes valid certificate service requests to CA-S.

6.1.4 CA Public Key Delivery to Relying Parties

CAs SHALL publish their certificates in a central repository from which relying parties MAY retrieve the associated CA certificate that includes its public key (see also section 2.1).

Further requirements MAY be specified in section 6.1.4 of the document [CPS-FhG].

6.1.5 Key Sizes

The R-CA and CAs SHALL use cryptographic algorithms and key sizes equivalent to at least RSA 2048 bit.

Keys for employees of Fraunhofer stored on smartcards SHALL use cryptographic algorithms and key sizes equivalent to at least RSA 2048 bit.

All other subscribers MUST at least use cryptographic algorithms and key sizes equivalent to at least RSA 1024 bit.

Further requirements MAY be specified in section 6.1.5 of the document [CPS-FhG].

6.1.6 Public Key Parameters Generation and Quality Checking

The R-CA and CAs SHALL conduct a proper selection of parameters to be used for the generation of key pairs. The use of evaluated (e.g. against CC, ITSEC, or FIPS) cryptographic modules for key generation is RECOMMENDED but NOT MANDATED.

Further requirements MAY be specified in section 6.1.6 of the document [CPS-FhG].

6.1.7 Key Usage Purposes

Generated keys and their associated certificates SHALL only be used for the specific purpose (i.e. signature, authentication, or encryption) for which they have been created. CAs SHALL provide the required information on key usage within the certificate extension fields `keyUsage` and `extendedKeyUsage` (see section 7.1.2 of the document [CPS-FhG]). Relying parties SHOULD check the contents of these extension prior to the usage of the certificate.

Further requirements on key usage purposes MAY be specified in section 6.1.7 of the document [CPS-FhG].

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

The R-CA and CAs SHALL conduct cryptographic operations including signature key generation, key storage and certificate signing within HSMs. The use of evaluated (e.g. against CC, ITSEC, or FIPS) cryptographic modules for key generation is MANDATED.

Subscribers (natural persons) of CA-U SHALL conduct cryptographic operations including signature and authentication using smartcards. The use of evaluated (e.g. against CC, ITSEC, or FIPS) smartcards for these operations is RECOMMENDED but NOT MANDATED. Subscribers (natural persons) of CA-U MAY conduct the cryptographic operation decryption within smartcards or based upon SW-PSEs.

Further requirements MAY be specified in section 6.2.1 of the document [CPS-FhG].

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

The R-CA and CAs SHALL apply multiple person control for key generation operations. A minimum requirement is that all critical operations SHALL be carried out based on the "4-eyes principle" which ensured that a single person never can get the sole control over a private signature key.

Further requirements MAY be specified in section 6.2.2 of the document [CPS-FhG].

6.2.3 Private Key Escrow

Private key escrow for R-CA and CAs private singing keys SHALL only be supported for the generation of backups. The storage of the backups and the original HSM SHALL provide the same level of security.

Key escrow for CA-U subscribers' private signing keys SHALL NOT be supported.

Key escrow for CA-U subscribers' private authentication keys SHALL NOT be supported.

Key escrow for CA-U subscribers' private encryption keys SHALL be supported within the CMS.

Further requirements on private key escrow MAY be specified in section 6.2.3 of the document [CPS-FhG].

6.2.4 Private Key Backup

The R-CA and CAs SHALL carry out private key backup in the form of HSM backup tokens (see section 6.2.3) that SHALL be stored in a secure environment, and for which strong access control SHALL apply.

Subscribers of CA-U SHALL NOT carry out private key backup of their signature and authentication keys contained in smartcards.

Private key backup of CA-U subscribers' encryption keys MAY be automatically carried out by the card management system. The access to backup encryption keys SHALL only be allowed via the CMS for the purpose of creating new smartcards and PIN letters and for the purpose of key export to a SW-PSE for the owner of the key complying with the 4-eyes principle.

Further requirements on private key backup MAY be specified in section 6.2.4 of the document [CPS-FhG].

6.2.5 Private Key Archival

Private key archival for encryption keys of subscribers SHALL be done in encrypted format within the CMS.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

Private R-CA and CA keys SHALL be generated according to [FhG-RKC] and stored securely within HSMs. Private CA-U subscribers' keys SHALL be generated within the card management system and stored in smartcards. Private R-CA and CA keys SHALL never leave the HSM. An exception is the procedure used to generate backups (see section 6.2.4). Private CA-U subscribers' authentication and signature keys SHALL never leave the smartcard. Key escrow is performed by the CMS for CA-U subscribers' private encryption keys (see section 6.2.4). CA-U subscribers' private encryption keys MAY be exported as SW-PSEs and securely delivered to their owners.

Further requirements on private key transfer MAY be specified in section 6.2.6 of the document [CPS-FhG].

6.2.7 Private Key Storage on Cryptographic Module

Private R-CA and CA keys SHALL be stored on HSMs. Private CA-U subscriber (natural persons) keys SHALL be stored on smartcards. Private CA-U subscriber (natural person) encryption keys SHALL initially be stored on smartcards. On request of the owner, private CA-U subscriber encryption keys MAY be exported securely be stored in SW-PSEs. Private CA-S subscriber (machines and services including code signing services) keys SHALL be stored in SW-PSEs.

Further requirements on private key storage MAY be specified in section 6.2.7 of the document [CPS-FhG].

6.2.8 Method of Activating Private Key

A private key SHALL NOT be activated prior to the authentication of its owner. The authentication procedure SHALL at least include a PIN or password.

Further requirements on methods for activation of private keys MAY be specified in section 6.2.8 of the document [CPS-FhG].

6.2.9 Method of Deactivating Private Key

The deactivation of a private key MAY be supported via subscriber or CA logging-out.

Further requirements on methods for deactivation of private keys MAY be specified in section 6.2.9 of the document [CPS-FhG].

6.2.10 Method of Destroying Private Key

Private R-CA and CA keys stored on HSMs SHALL be made non-accessible upon the termination of the private key use (end of validity or revocation date of associated certificate). The physical medium SHALL be physically destroyed if it only contains one accessible private key, or in the case of a compromise.

Private CA-U subscriber keys (natural persons) stored on smartcards (except for backup smartcards at the most) SHALL be made non-accessible upon the termination of the private key use (end of validity, revocation date of associated certificate, damage of smartcard, or change of subscriber information contained in the certificate) by physically destroying the smartcards. The affected smartcards SHALL be handed-over to the local RAs and SHALL be physically destroyed at the latest when leaving Fraunhofer. When leaving Fraunhofer the subscriber SHALL also delete CA-U SW-PSEs containing exports of his / her private encryption keys.

Private CA-S subscriber keys (machines and services including code signing services) stored in SW-PSEs SHALL be deleted by system administrators upon the termination of the private key use (end of validity or revocation date of associated certificate).

Further requirements on methods for deactivation of private keys MAY be specified in section 6.2.10 of the document [CPS-FhG].

6.2.11 Cryptographic Module Rating

The use of evaluated cryptographic modules is only RECOMMENDED, but NOT MANDATED.

Further requirements on methods for deactivation of private keys MAY be specified in section 6.2.11 of the document [CPS-FhG].

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

Public keys contained in the basic `subjectPublicKeyInfo` field of X.509 certificates SHALL be archived for the purpose of verification. The requirements on records archival specified in section 5.5 of this document apply.

Further requirements on public key archival MAY be specified in section 6.3.1 of the document [CPS-FhG].

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

Key pair usage periods SHALL correspond to the validity periods of their associated certificates.

Concrete values for certificate validity periods for the R-CA, CAs, and subscribers SHALL be specified in section 6.3.2 of the document [CPS-FhG].

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

Activation data such as tokens, PINs, passwords, or parts of passwords/PINs required to operate private keys SHALL be used.

Further requirements on activation data generation and installation MAY be specified in section 6.4.1 of the document [CPS-FhG].

6.4.2 Activation Data Protection

Activation data SHALL be protected from unauthorized use.

Further requirements on activation data protection MAY be specified in section 6.4.2 of the document [CPS-FhG].

6.4.3 Other Aspects of Activation Data

No stipulation

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

A CA and its attached CMS SHALL provide security measures related to access control for their certification services. The authorization of CMS personnel SHALL be realized by the use of smartcards. Critical CA operations SHALL be performed complying with the 4-eyes principle.

Further technical requirements MAY be specified in section 6.5.1 of the document [CPS-FhG].

6.5.2 Computer Security Rating

The use of evaluated hardware and/or software is RECOMMENDED but NOT MANDATED.

Further technical requirements MAY be specified in section 6.5.2 of the document [CPS-FhG].

6.6 Life Cycle Security Controls

6.6.1 System Development Controls

The R-CA and CAs SHALL deploy hardware and software that has been thoroughly inspected, tested and approved. The use of evaluated hardware and/or software is RECOMMENDED but NOT MANDATED.

Further requirements on system development controls MAY be specified in section 6.6.1 of the document [CPS-FhG].

6.6.2 Security Management Controls

The R-CA and CAs SHALL take the following measures related to security management controls:

- regular monitoring and logging of security processes and procedures,
- periodical verification of the integrity of deployed hardware and software, and
- periodical compliance inspection.

Further requirements on security management controls SHALL be specified in section 6.6.2 of the document [CPS-FhG].

6.6.3 Life Cycle Security Rating

No stipulation

6.7 Network Security Controls

The R-CA SHALL be exclusively run in an off-line mode of operation without any access points to networks. For this reason network security controls are not applicable.

Remote access of "CA network clients" to "CA network server" SHALL be realized via a high-security private network.

"CA network clients" MAY have remote access to the CMS. Only authorized CA personnel SHALL be allowed to use "CA network clients". Adequate network security controls SHALL be provided to protect "CA network server" from unauthorized access.

Further requirements on network security controls MAY be specified in section 6.7 of the document [CPS-FhG].

6.8 Time-Stamping

No stipulation yet.

7 Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

CAs SHALL issue X.509 v3 certificates in compliance with the requirements stated in the document "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile)" [RFC 3280]. EE applications SHALL support all X.509 basic fields, and all extensions that are specified in section 7.1 of the document [CPS-FhG]. The validity period of certificates provided in the X.509 basic field validity SHALL NOT exceed six years and SHALL be presented in the date format UTCTime.

7.1.1 Version Number(s)

The version number of all certificates SHALL be version v3.

7.1.2 Certificate Extensions

Certificate extensions SHALL be issued by CAs in compliance with the requirements stated in the document [RFC 3280]. The set of applicable extension SHALL be specified in section 7.1.2 of the document [CPS-FhG].

7.1.3 Algorithm Object Identifiers

CAs and EEs SHALL use respectively support the algorithm object identifiers that occur in X.509 basic fields *signature* and *signatureAlgorithm* in compliance with the requirements specified in the document "Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile" [RFC 3279]. It is strongly RECOMMENDED to use the signature algorithm *sha1WithRSAEncryption* (OID: 1.2.840.113549.1.1.5).

Further algorithms MAY be selected in section 7.1.3 of the document [CPS-FhG].

7.1.4 Name Forms

CAs SHALL use the name form DistinguishedName (DN) in UTF8 encoding for [X.501] DirectoryString.

7.1.5 Name Constraints

DNs that occur in the X.509 basic fields issuer and subject SHALL comply with [RFC 3280].

7.1.6 Certificate Policy Object Identifier

See section 7.1.6 of the document [CPS-FhG].

7.1.7 Usage of Policy Constraints Extension

See section 7.1.7 of the document [CPS-FhG].

7.1.8 Policy Qualifiers Syntax and Semantics

See section 7.1.8 of the document [CPS-FhG].

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

Not applicable

7.2 CRL Profile

CAs SHALL issue X.509 v2 CRLs in compliance with the requirements stated in the document "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile)" [RFC 3280]. EE applications SHALL support all X.509 basic fields, and all extensions that are specified in section 7.2 of the document [CPS-FhG].

7.2.1 Version Number(s)

The version number of all CRLs SHALL be version v2 (1).

7.2.2 CRL and CRL Entry Extensions

CRL and CRL Entry extensions SHALL be issued by CAs in compliance with the requirements stated in the document [RFC 3280]. The set of applicable extensions SHALL be specified in section 7.2.2 of the document [CPS-FhG].

7.3 OCSP Profile

OCSP responders SHALL comply with the requirements stated in the document "Internet X.509 Public Key Infrastructure Online Certificate Status Protocol" [RFC 2560]. The set of applicable extensions in OCSP requests and OCSP responses SHALL be specified in section 7.3 of the document [CPS-FhG].

7.3.1 Version Number(s)

The version number of the OCSP protocol SHALL be version v1 (0).

7.3.2 OCSP Extensions

CAs and EE applications SHALL support OCSP extensions in compliance with the requirements stated in the document [RFC 2560]. The set of applicable extension SHALL be specified in section 7.3.2 of the document [CPS-FhG].

8 Compliance Audit and other Assessments

CAs SHOULD have compliance audits or other reviews or investigations in order to ensure the trustworthiness of the Fraunhofer Corporate PKI.

8.1 Frequency or Circumstances of Assessment

CAs SHALL at least have an initial compliance audit.

Further requirements MAY be specified in section 8.1 of the document [CPS-FhG].

8.2 Identity/Qualifications of Assessor

Only approved compliance auditors SHALL perform the audits.

Further details MAY be provided in section 8.2 of the document [CPS-FhG].

8.3 Assessor's Relationship to Assessed Entity

Only independent compliance auditors SHALL be in charge of the audit and assessment process.

Further details MAY be provided in section 8.3 of the document [CPS-FhG].

8.4 Topics Covered by Assessment

The compliance audit SHALL prove that a CA under audit complies with the requirements of this certificate policy. The outcome of the audit SHALL be documented in an audit report.

Further details MAY be provided in section 8.4 of the document [CPS-FhG].

8.5 Actions Taken as a Result of Deficiency

The following actions MAY be taken as a result of an observed deficiency:

- determination, if deficiencies can be removed,
- development of an action plan, and removal of deficiencies.

Further details MAY be provided in section 8.5 of the document [CPS-FhG].

8.6 Communication of Results

The results of a compliance audit SHALL be provided by the compliance auditor to the Root CA in the form of an audit report. This report SHALL NOT be published.

9 Other Business and Legal Matters

9.1 Fees

The fees for the initial roll-out of smartcards SHALL be paid by the "Zentralverwaltung ZV" (central FhG office). The fees for all further smartcards SHALL be paid by the institutes.

Further details SHALL be provided in section 9.1 of the document [CPS-FhG].

9.1.1 Certificate Issuance or Renewal Fees

Details on renewal fees SHALL be provided in section 9.1.1 of the document [CPS-FhG].

9.1.2 Certificate Access Fees

Details on certificate access fees SHALL be provided in section 9.1.2 of the document [CPS-FhG].

9.1.3 Revocation or Status Information Access Fees

Details on revocation or status information access fees SHALL be provided in section 9.1.3 of the document [CPS-FhG].

9.1.4 Fees for Other Services

Details on fees for other services SHALL be provided in section 9.1.4 of the document [CPS-FhG].

9.1.5 Refund Policy

No stipulation

9.2 Financial Responsibility

No stipulation

9.2.1 Insurance Coverage

No stipulation

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 scope of confidential information SHALL include all personal and company information that is not covered by section 9.3.2.

9.3.2 Information Not Within the Scope of Confidential Information

Data objects such as certificates, CRLs, OCSP responses, and personal and company information contained in them or in the public directory SHALL NOT be considered as confidential.

9.3.3 Responsibility to Protect Confidential Information

CAs SHALL protect confidential information from unauthorized reading, modification, or deletion.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

CAs and RAs that electronically store and process personal information SHALL perform their tasks in compliance with the German laws on data security and privacy.

9.4.2 Information Treated as Private

Information classified as confidential (see section 9.3.1) SHALL be treated as private information and SHALL NOT be disclosed by CAs or RAs.

9.4.3 Information Not Deemed Private

Information classified as non-confidential (see section 9.3.2) SHALL be treated as public information and MAY be disclosed by CAs or RAs.

9.4.4 Responsibility to Protect Private Information

CAs SHALL protect private information from unauthorized reading, modification, or deletion.

9.4.5 Notice and Consent to Use Private Information

CAs MAY only use private subscriber information that is required for their operations, after the subscribers consent.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

Confidential and private information MAY be disclosed by CAs or RAs, and passed to state authorities, if required by law (see also section 9.4.1).

9.4.7 Other Information Disclosure Circumstances

No stipulation

9.5 Intellectual Property Rights

The Fraunhofer Gesellschaft retains all intellectual property rights in and to the documents [CP-FhG] and [CPS-FhG], issued certificates and CRLs, and produced smartcards.

9.6 Representations and Warranties

[CPS-FhG], all certificates and all documentation that will further detail the documents [CP-FhG]l and [CPS-FhG] SHALL comply with the requirements of this document [CP-FhG].

9.6.1 CA Representations and Warranties

CAs SHALL conduct their tasks complying with the requirements of the documents [CP-FhG] and [CPS-FhG].

9.6.2 RA Representations and Warranties

RAs SHALL conduct their tasks complying with the requirements of the documents [CP-FhG] and [CPS-FhG].

9.6.3 Subscriber Representations and Warranties

Subscribers SHALL use their keys and certificates complying with the requirements specified in section 4.5.1.

9.6.4 Relying Party Representations and Warranties

Subscribers SHALL use certificates complying with the requirements specified in section 4.5.2.

9.6.5 Representations and Warranties of Other Participants

No stipulation

9.7 Disclaimers of Warranties

No stipulation

9.8 Limitations of Liability

No stipulation

9.9 Indemnities

No stipulation

9.10 Term and Termination

9.10.1 Term

The documents [CP-FhG] and [CPS-FhG] come into force after their publication.

9.10.2 Termination

The documents [CP-FhG] and [CPS-FhG] remain in force until their replacement by a new version, or upon termination of CA operation.

9.10.3 Effect of Termination and Survival

The effect of termination and survival of the documents [CP-FhG] and/or [CPS-FhG] SHALL be published on the Fraunhofer Corporate PKI website.

9.11 Individual Notices and Communications With Participants

Additional individual notices MAY published on the Fraunhofer Corporate PKI website.

Further details on individual notices and communications with participants SHALL be provided in section 9.11 of the document [CPS-FhG].

9.12 Amendments

The organization defined in section 1.5 is also responsible for amendments.

9.12.1 Procedure for Amendment

The organization mentioned in section 1.5 SHALL be the responsible administrative board for amendments of the documents [CP-FhG] and [CPS-FhG] (see section 1.5). Further regulations MAY be provided in sections 1.5.2 to 1.5.4 of the document [CPS-FhG].

9.12.2 Notification Mechanism and Period

The organization mentioned in section 1.5 MAY provide notice of any proposed changes to the documents [CP-FhG] or [CPS-FhG].

9.12.3 Circumstances Under Which OID Must be Changed

The organization mentioned in section 1.5 MAY assign new OIDs to the documents [CP-FhG] or [CPS-FhG], if required.

9.13 Dispute Resolution Provisions

The organization mentioned in section 1.5 SHALL be the responsible board for the provision of dispute resolutions related to the documents [CP-FhG] or [CPS-FhG].

9.14 Governing Law

The documents [CP-FhG] and [CPS-FhG], and the operations of the Fraunhofer Corporate PKI are governed by the laws of the Federal Republic of Germany.

9.15 Compliance With Applicable Law

The documents [CP-FhG] and [CPS-FhG], and the operations of the Fraunhofer Corporate PKI SHALL comply with the German laws on data security and privacy.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

No stipulation

9.16.2 Assignment

No stipulation

9.16.3 Severability

No stipulation

9.16.4 Enforcement (Attorneys' Fees and Waiver of Rights)

No stipulation

9.16.5 Force Majeure

No stipulation

9.17 Other Provisions

No stipulation

10 References

[BNetzA-ALG] Overview of suitable algorithms, Federal Gazette No 58, pp 1913-1915 of 23 March 2006

[ETSI TS 102042] Policy Requirements for Certification Authorities Issuing Public Key Certificates, 2007, http://www.etsi.org/deliver/etsi_ts/102000_102099/102042/01.03.04_60/ts_102042v010304p.pdf

[CP-FhG] Certificate Policy of the Fraunhofer Corporate PKI

[CPS-FhG] Certification Practice Statement of the Fraunhofer Corporate PKI

[CS-FhG] General Conditions for handling Code Signing Certificates within the Fraunhofer-Gesellschaft

[IT-BPM] BSI: IT Baseline Protection Manual, 2004

[RFC 2119] S. Bradner: Key Words for Use in RFC's to Indicate Requirement Levels, March 1997

[RFC 2560] W. Polk, R. Housley, and L. Bassham: Internet X.509 Public Key Infrastructure – Online Certificate Status Protocol - OCSP, June 1999

[RFC 3279] W. Polk, R. Housley, and L. Bassham: Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, April 2002

[RFC 3280] R. Housley, W. Polk, W. Ford, and D. Solo: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile), April 2002

[RFC 3647] S. Chokhani, W. Ford, R. Sabett, C. Merrill, and S. Wu: Certificate Policy and Certification Practices Framework, November 2003

[SLA-FhG] Service Level Agreements of the Fraunhofer Corporate PKI

[WT-PCA] AICPA/CICA: WebTrust Program for Certification Authorities, Version 1.0, August 2000

[X.501] ITU-T Recommendation X.501 | ISO/IEC 9594-2: Information Technology – Open System Interconnection – The Directory: Models, 1993

[X.509] ITU-T Recommendation | ISO/IEC 9594-8: Information Technology – Open System Interconnection – The Directory: Authentication Framework, June 1997

[X.520] ITU-T Recommendation X.520 | ISO/IEC 9594-6: "Information Technology – Open Systems Interconnection - The Directory: Selected Attribute Types"

The following internal documents will not be published, but are available for compliance audits, if required:

- Directory Concept
- Emergency Concept,
- Emergency Manual,
- Fraunhofer Corporate PKI Network Concept,
- Fraunhofer Corporate PKI Root Key Ceremony [FhG-RKC]
- Naming Concept,
- Operating Manual,
- Organizational Concept,
- Security Concept, and the
- Training Material for Staff and Operating Personnel.

11 Acronyms

Acronyms used in this document and their meaning are listed in Table 2. All technical terms used in this document have the same meaning as defined in relevant standards. For this reason a list of definitions of terms that would repeat this information is not provided.

Table 2: List of Acronyms

ACRONYM	MEANING
AICPA	**A**merican **I**nstitute of **C**ertified **P**ublic **A**ccountants
BNetzA	Federal Network Agency (**B**undes**NetzA**gentur)
BSI	**B**undesamt für **S**icherheit in der **I**nformationstechnik (Federal Office for Information Security)
C	**C**ountry Name
CA	**C**ertification **A**uthority
CA-U	**CA** for employees of Fraunhofer
CA-S	**CA** for machines / services including code signing services
CC	**C**ommon **C**riteria
CICA	**C**anadian **I**nstitute of **C**hartered **A**ccountants
CMS	**C**ard **M**anagement **S**ystem
CN	**C**ommon **N**ame
CP	**C**ertificate **P**olicy
CP-FhG	**C**ertificate **P**olicy of Fraunhofer Corporate PKI
CPS	**C**ertification **P**ractice **S**tatement
CPS-FhG	**C**ertification **P**ractice *S*tatement of Fraunhofer Corporate PKI
CRL	**C**ertificate **R**evocation **L**ist
DIR	Central FhG **DIR**ectory
DIT	**D**irectory **I**nformation **T**ree
DN	**D**istinguished **N**ame
DNS	**D**omain **N**ame **S**ystem
EE	**E**nd **E**ntity
ETSI	**E**uropean **T**elecommunications **S**tandards **I**nstitute
FhG	**F**raun**h**ofer **G**esellschaft
FIPS	**F**ederal **I**nformation **P**rocessing **S**tandard
HSM	**H**ardware **S**ecurity **M**odule
IT	**I**nformation **T**echnology
ITSEC	**I**nformation **T**echnology **S**ecurity **E**valuation **C**riteria
LDAP	**L**eightweight **D**irectory **A**ccess **P**rotocol

ACRONYM	MEANING
NCP	**N**ormalized **C**ertificate **P**olicy
NCP+	**E**xtended **N**ormalized **C**ertificate **P**olicy
O	**O**rganization Name
OCSP	**O**nline **C**ertificate **S**tatus **P**rotocol
OID	**O**bject **ID**entifier
OU	**O**rganizational **U**nit Name
PIN	**P**ersonal **I**dentification **N**umber
PKI	**P**ublic **K**ey **I**nfrastructure
PSE	**P**ersonal **S**ecurity **E**nvironment
PSE	**P**ersonal **S**ecurity **E**nvironment
PUK	**P**ersonal **U**nblock **K**ey
RA	**R**egistration **A**uthority
R-CA	**R**oot **C**ertification **A**uthority
RFC	**R**equest **F**or **C**omment
RSA	**R**ivest-**S**hamir-**A**dleman
SHA	**S**ecure **H**ash **A**lgorithm
SIGMA	Personnel administration system of Fraunhofer to which only authorized people have access as for example RA and central RA staff
SLA	**S**ervice **L**evel **A**greement
SW-PSE	**S**oft**W**are **PSE**
TSA	**T**ime-**S**tamping **A**uthority
UPS	**U**ninterruptible **P**ower **S**upply
URI	**U**niform **R**esource **I**dentifier
URL	**U**niform **R**esource **L**ocator
UTC	**C**oordinated **U**niversal **T**ime
UTF8	**8**-bit **U**niversal **T**ransformation **F**ormat
VPN	**V**irtual **P**rivate **N**etwork
X509	International Standard that specifies the basic format for digital certificates