Fraunhofer Gesellschaft

Fraunhofer Corporate PKI

Certification Practice Statement

Published in November 2007

Object Identifier of this Document: 1.3.6.1.4.1.778.80.3.2.1

Contact:

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

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

Table of Contents

List of Tables

1 Introduction

This document specifies the certification practice statement of the "Fraunhofer Corporate Public Key Infrastructure (PKI)" referred to as "CPS-FhG" in the following. Fraunhofer Corporate PKI provides certification services for all FhG employees and machines in order to support security services for authentication, confidentiality and non-repudiation in applications such as e-mail, web services, VPN communication, and files and device encryption.

1.1 Overview

CPS-FhG describes the practical implementation of the framework requirements for the creation of keys, the issuance of related certificates, their usage, management, renewal, and revocation that are specified in the associated document "Fraunhofer Corporate PKI Certificate Policy" [FhG-CP].

CPS-FhG provides specific information about relevant Fraunhofer Corporate PKI components, i.e. R-CA, sub CAs, RAs, OCSP responder and the central FhG directory that support the issuance, distribution, usage, renewal, and revocation of certificates in compliance 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]. CPS-FhG in particular includes information about the operational PKI procedures and processes that have been realized and their associated security measures. A complete list of references is given in chapter 10.

1.2 Document Name and Identification

This certification practice statement document is entitled "Fraunhofer Corporate PKI Certification Practice Statement" or CPS-FhG in short notation.

This certification practice statement is identified by the object identifier (OID) 1.3.6.1.4.1.778.80.3.2 whose components have the meaning given in Table 1.

Table 1: CPS-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
2	Certification Practice Statement
1	Version number (current version: 1)

1.3 PKI Participants

1.3.1 Certification Authorities

The architecture of Fraunhofer Corporate PKI and its certification authorities have been realized as required in section 1.3.1 of the document [FhG-CP].

The Root CA is located in the trust center Birlinghoven.

The sub-CA CA-U (certification authority for the issuance of certificates for FhG employees) is located in the trust center Birlinghoven.

The sub-CA CA-S (certification authority for the issuance of authentication and encryption certificates for services/machines) is located in the trust center Birlinghoven.

Both CA-U and CA-S have separate OCSP responders.

1.3.2 Registration Authorities

RAs have been realized in compliance with the requirements specified in section 1.3.2 of the document [FhG-CP].

[1] Central Office of the Fraunhofer Gesellschaft

Local RAs are authorized to perform the following set of tasks:

- authorization and authentication via personalization in the Fraunhofer ERP system SIGMA[2],
- initiation of issuance of smartcards,
- identification and handing out of smartcards,
- performing of PIN reset (if an employee has been forgotten his PIN),
- handing out of replacement cards (if an employee has been forgotten his smartcard), and the
- submission of revocation requests.

For all institutes a list of authorized persons that are in charge of these tasks is defined by the respective head of institute.

The central RA is located at the Fraunhofer Institutes IITB in Karlsruhe and SIT in Birlinghoven. Contact information of the central registration authorities is provided in Table 2.

Table 2: Central RA Contact Information

Mailing Address	Fraunhofer Competence Center PKI Fraunhoferstr. 1 D-76131 Karlsruhe
Phone	+49 180 2 344 754
E-Mail	servicedesk@pki.fraunhofer.de
WWW	http://pki.fraunhofer.de

Service request will be internally dispatched to the related central RA. The central RAs represent the interface to the CAs. A so-called "help desk component" is used to forward incoming service requests to the currently active central RA which provides hotline and support for all employees.

1.3.3 Subscribers

Subscribers of the CA-U are FhG employees. Subscribers of the CA-S are system administrators representing services/machines.

[2] Personnel administration system of the Fraunhofer Gesellschaft to which only authorized people have access as for example RA and central RA staff

1.3.4 Relying Parties

Relying parties are employees of FhG and machines/services.

1.3.5 Other Participants

No stipulation.

1.4 Certificate Usage

Certificate usage has been realized in compliance with the requirements specified in section 1.4 of the document [FhG-CP].

1.5 Policy Administration

1.5.1 Organization Administering the CPS Document

The Fraunhofer Competence Center PKI (CC-PKI) is responsible for maintaining the CP and CPS documents.

1.5.2 Contact Person

Head of CA	Dr. Tobias Straub / Fraunhofer SIT
Mailing Address	Fraunhofer Competence Center PKI Fraunhoferstr. 1 D 76131 Karlsruhe
Phone	+49 1802 344 754
E-Mail	servicedesk@pki.fraunhofer.de
WWW	http://pki.fraunhofer.de

1.5.3 Person Determining CPS Suitability for the Policy

The approval of the Suitability of the related CP document with this CPS document is managed by the same organization mentioned in section 1.5.1.

1.5.4 CP/CPS Approval Procedures

The approval of this CPS and its related CP document is managed by the same organization mentioned in section 1.5.1.

The CP/CPS approval procedures include the approval of any amendments, e.g. additions, deletions and modifications of these documents. Any amendments SHALL be documented, and MAY lead to the publication of a new version with a new OID depending on decisions of the organization mentioned in 1.5.1.

1.6 Definitions and Acronyms

A list of acronyms that are used within this CPS is provided in Table 11 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 offers a publicly accessible LDAP server via *ldap://ldap.fraunhofer.de* and the web site *http://pki.fraunhofer.de*.

Furthermore the CRL distribution point and AIA extension is contained in certificates issued under this CPS.

Subscriber certificates that have been issued for signature and authentication will not be published.

2.2 Publication of Certification Information

The following certification information about Fraunhofer Corporate PKI is publicly available via *http://pki.fraunhofer.de* :

- 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

The document CPS-FhG is available via *http://pki.fraunhofer.de*.

2.3 Time or Frequency of Publication

The time or frequency of publication of certification information is as soon as possible.

- CP and CPS as required by the organization mentioned in 1.5,
- certificates for encryption not later than 2 weeks after their issuance,
- CRLs issued by the R-CA not later than 4 months,
- CRLs issued by the CA-U not later than 1 week, and.
- CRLs issued by the CA-S not later than 1 week.

2.4 Access Controls on Repositories

Publicly accessible LDAP services have been realized that support the retrieval of CA certificates, CRLs, and encryption certificates. Subscriber certificates that

have been issued for the purpose of signature and authentication will not be published. The certificate of the R-CA, the fingerprint of the certificate of the R-CA, the certificates of CA-U and CA-S, the fingerprints of the certificates of CA-U and CA-S, and the documents CP-FhG and CPS-FhG have been published on the web site http://pki.fraunhofer.de.

3 Identification and Authentication

The identification and authentication of subscribers is only performed by authorized local RA and central RA staff. Local RAs and the central RA use personal data that is provided and managed by the FhG SIGMA system. Additional information such as domain user names or photos of employees MAY be provided by the individual institutes.

3.1 Naming

The distinguished names (DN) concept is used within CA and end entity (EE) certificates. Further details MAY have been specified in a separate internal document "Naming Concept" that will not be published as a whole. Parts of the "Naming Concept" will be made available via http://pki.fraunhofer.de.

3.1.1 Types of Names

All names of CAs and EEs that are included in X.509 certificates are constructed as DNs that contain the naming attributes country name (C), organization name (O), organizational unit name (OU), and common name (CN). An overview of the FhG naming concept is provided in Table 3.

Table 3: FhG Naming Concept

TYPE OF ENTITY	NAMING ATTRIBUTES				
	C	O	OU	OU	CN
FhG Root CA	DE	Fraunhofer	Fraunhofer Corporate PKI		Fraunhofer Root CA 2007
CA-U					Fraunhofer User CA 2007
CA-S					Fraunhofer Service CA 2007
OCSP Responder for CA-U					User CA OCSP Responder <no.>
OCSP Responder for CA-S					Service CA OCSP Responder <no.>
Subscriber of CA-U			<Institute Name>	People	<Given name Surname>
Subscriber of CA-S				Services	<Name of service/machine>

3.1.2 Need for Names to be Meaningful

DNs are assigned to CAs and EEs satisfying the requirements specified in section 3.1.2 of the document [FhG-CP].

3.1.3 Anonymity or Pseudonymity of Subscribers

Where pseudonymity of EEs is supported, the pseudonym naming attribute is used.

3.1.4 Rules for Interpreting Various Name Forms

UTF8 is used as default character set. As a basis for name forms the representation of an employee's name in SIGMA is used. Special characters of the German language such as umlauts ä, ö, ü are represented as double vocals ae, oe, ue and ß is substituted by ss. Letters with a diacritic mark such as à, á, â are substituted by the corresponding character without diacritic.

3.1.5 Uniqueness of Names

The requirements specified in section 3.1.5 of the document [FhG-CP] will be regarded when assigning distinguished names (DNs) to subscribers. Further details are specified in the document "Naming Concept" that for example specifies the construction of DNs for guaranteeing unique name.

3.1.6 Recognition, Authentication, and Role of Trademarks

Not applicable

3.2 Initial Identity Validation

The initial identity validation of subscribers is performed by local RAs as specified in section 3.2 of the document [FhG-CP].

3.2.1 Method to Prove Possession of Private Key

Keys for natural persons are generated centrally and stored on hardware devices such as smartcards. As a consequence the method to prove possession of private key is not applicable as specified in section 3.2.1 of the document [FhG-CP].

For keys of EEs certified by CA-S that are generated locally possession of private key is proven by signing the request or by decrypting the corresponding certificate. For key pairs that are generated centrally by CA-S the method to prove possession of private key is not applicable as specified in section 3.2.1 of the document [FhG-CP].

3.2.2 Authentication of Organization Identity

The authentication of Fraunhofer institutes and other organizations within FhG is performed by the central RA that keeps a list of those organizations and their members that are authorized to use the Fraunhofer Corporate PKI certification services.

Only individuals may request such certificates on behalf of their organization by providing meaningful credentials and by going through the authentication procedure defined in 3.2.3.

Administrators may request certificates only for services/machines that are included in the central FhG directory and have to go through the authentication procedure defined in 3.2.3.

3.2.3 Authentication of Individual Identity

The authentication of individual identity is performed by local RAs complying with the requirements for the authentication of individual identity as specified in section 3.2.3 of the document [FhG-CP]. Personal records of employees that are kept by the RAs include the following information:

Information provided by SIGMA

- surname, given name,
- name of FhG institute,
- postal address,
- internal user identification number,
- status of employment,
- begin and end of contract, and
- place of birth and date of birth.

Information provided by FhG institutes

- title,
- e-mail address,
- photo, and optionally
- user domain name for Windows Smartcard Logon.

3.2.4 Non-Verified Subscriber Information

Not applicable

3.2.5 Validation of Authority

Not applicable

3.2.6 Criteria for Interoperation

CAs, local RAs and the central RA interoperate in compliance with the requirements as specified in section 3.2.6 of the document [FhG-CP].

3.3 Identification and Authentication for Re-Key Requests

The identification and authentication of individual identity is performed by local RAs complying with the requirements for the authentication of individual identity as specified in section 3.3 of the document [FhG-CP]. Consecutive smartcards will be automatically produced at latest two months prior to the expiration of the actual smartcard.

3.3.1 Identification and Authentication for Routine Re-key

The identification and authentication for routine re-key has been realized in compliance with the requirements as specified in section 3.3.1 of the document [FhG-CP].

3.3.2 Identification and Authentication for Re-key After Revocation

The identification and authentication for re-key after revocation has been realized in compliance with the requirements as specified in section 3.3.2 of the document [FhG-CP].

3.4 Identification and Authentication for Revocation Requests

The revocation service can be accessed via e-mail, phone, or web service. The identification and authentication of revocation requests is based on the receipt of a

- signed e-mail,
- phone call during which specific authorization information is provided, or a
- completed web form containing specific authorization information

Contact information of the revocation service is provided in Table 4.

Table 4: Revocation Hotline Contact Information

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

4 Certificate Life-Cycle Operational Requirements

All requirements on certificate life-cycle operations specified in the document [FhG-CP] have been fulfilled. Further details on technical and organizational CA processes are provided in the internal non-published document "Fraunhofer Corporate PKI Concept".

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

The submission of certificate applications has been realized in compliance with the requirements specified in section 4.1.1 of the document [FhG-CP].

Consecutive smartcards will be produced at latest two months prior to the expiration of the actual smartcard.

4.1.2 Enrollment Process and Responsibilities

The enrollment process and responsibilities have been realized in compliance with the requirements specified in section 4.1.2 of the document [FhG-CP].

4.2 Certificate Application Processing

Certificate application processing has been realized in compliance with the requirements specified in section 4.2 of the document [FhG-CP].

4.2.1 Performing Identification and Authentication Functions

The performing of identification and authentication functions has been realized in compliance with the requirements specified in section 4.2.1 of the document [FhG-CP].

4.2.2 Approval or Rejection of Certificate Applications

The approval or rejection of certificate applications has been realized in compliance with the requirements specified in section 4.2.2 of the document [FhG-CP].

4.2.3 Time to Process Certificate Applications

The maximum time to process certificate application SHALL NOT exceed one week. Further requirements MAY be specified in the document "Service Level Agreements of Fraunhofer Corporate PKI".

4.3 Certificate Issuance

The issuance of certificates has been realized in compliance with the requirements specified in section 4.3 of the document [FhG-CP].

4.3.1 CA Actions During Certificate Issuance

The CA actions during certificate issuance have been realized in compliance with the requirements specified in section 4.3.1 of the document [FhG-CP].

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

Subscriber notification by the CA of the issuance of certificates has been realized in compliance with the requirements specified in section 4.3.2 of the document [FhG-CP].

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

The procedures for certificate acceptance have been realized in compliance with the requirements specified in section 4.4.1 of the document [FhG-CP].

4.4.2 Publication of the Certificate by the CA

The procedures for the publication of certificates issued by CAs have been realized in compliance with the requirements specified in section 4.4.2 of the document [FhG-CP]. Certificates of employees used for the purpose of signature or authentication will not be published.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

Not applicable

4.5 Key Pair and Certificate Usage

Key pair and certificate usage have been realized in compliance with the requirements specified in section 4.5 of the document [FhG-CP].

4.5.1 Subscriber Private Key and Certificate Usage

Subscriber key pair and certificate usage have been realized in compliance with the requirements specified in section 4.5.1 of the document [FhG-CP].

4.5.2 Relying Party Public Key and Certificate Usage

See section 4.5.2 of the document [FhG-CP].

4.6 Certificate Renewal

Certificate renewal is not supported by CAs. Instead consecutive smartcards including new key pairs and associated certificates will 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

Certificate re-key has been realized in compliance with the requirements specified in section 4.7 of the document [FhG-CP].

Certificate re-key will be initiated by the central RA at latest two months prior to the expiration of the actual certificate.

4.7.1 Circumstance for Certificate Re-key

Certificate re-key will be performed at latest two months prior to the expiration of the validity of a certificate, or during the course of certificate revocation.

4.7.2 Who May Request Certification of a New Public Key

Certification requests will basically be initiated by the central RA or by subscribers during the course of certificate revocation requests.

4.7.3 Processing Certificate Re-keying Requests

The processing of certificate re-keying requests has been realized in compliance with the requirements specified in section 4.7.3 of the document [FhG-CP].

4.7.4 Notification of New Certificate Issuance to Subscriber

The notification of new certificate issuance to subscriber has been realized in compliance with the requirements specified in section 4.7.4 of the document [FhG-CP].

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

The procedure for the acceptance of re-keyed certificates has been realized in compliance with the requirements specified in section 4.7.5 of the document [FhG-CP].

4.7.6 Publication of the Re-keyed Certificate by the CA

The publication of the re-keyed certificates has been realized in compliance with the requirements specified in section 4.7.6 of the document [FhG-CP].

4.7.7 Notification of certificate issuance by the CA to other entities

Not applicable

4.8 Certificate Modification

Certificate modification is not supported. Instead, CAs perform the procedures for certificate re-key as specified in section 4.7, followed by the procedures for certificate revocation (see section 4.9) of the affected certificate, if information contained in the affected certificate needs to be modified.

4.8.1 Circumstance for Certificate Modification

Not applicable

4.8.2 Who May Request Certificate Modification

Not applicable

4.8.3 Processing Certificate Modification Requests

Not applicable

4.8.4 Notification of New Certificate Issuance to Subscriber

Not applicable

4.8.5 Conduct Constituting Acceptance of Modified Certificate

Not applicable

4.8.6 Publication of the Modified Certificate by the CA

Not applicable

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

Not applicable

4.9 Certificate Revocation and Suspension

A revocation service is provided by Fraunhofer Corporate PKI. The suspension of certificates is not supported.

4.9.1 Circumstances for Revocation

Certificate revocation will be performed by CAs if one of the events listed in section 4.9.1 of the document [FhG-CP] has occurred.

4.9.2 Who Can Request Revocation

The revocation of a certificate may be requested by persons listed in section 4.9.2 of the document [FhG-CP].

4.9.3 Procedure for Revocation Request

The procedure for revocation request has been realized in compliance with the requirements specified in section 4.9.3 of the document [FhG-CP].

4.9.4 Revocation Request Grace Period

See corresponding section of [FhG-CP].

4.9.5 Time Within Which CA Must Process the Revocation Request

Revocations SHALL be processed as soon as possible. Exact time limits below which CAs will process revocation requests are specified in the document "Service Level Agreements" [FhG-SLA].

4.9.6 Revocation Checking Requirement for Relying Parties

Revocation checking is supported by the publication of CRLs in the central FhG directory and by the provision of on-line certificate status information by the FhG OCSP responder.

4.9.7 CRL Issuance Frequency

CAs will issue CRLs with an issue frequency defined in section 2.3.

4.9.8 Maximum Latency for CRLs

CAs will issue CRLs within a maximum latency of defined in section 2.3.

4.9.9 On-line Revocation/Status Checking Availability

Service times and the availability of the FhG OCSP responders are published in the document "Service Level Agreements" [FhG-SLA].

4.9.10 On-line Revocation Checking Requirements

On-line revocation checking has been realized in compliance with the requirements specified in section 4.9.10 of the document [FhG-CP].

Further details on CRL and OCSP profiles are provided in sections 7.2 and 7.3

4.9.11 Other Forms of Revocation Advertisements Available

No stipulation

4.9.12 Special Requirements re Key Compromise

The procedures after key compromise have been realized in compliance with the requirements specified in section 4.9.12 of the document [FhG-CP].

Further details are specified in the internal non-published document "Emergency Concept".

4.9.13 Circumstances for Suspension

Not applicable

4.9.14 Who Can Request Suspension

Not applicable

4.9.15 Procedure for Suspension Requestx

Not applicable

4.9.16 Limits on Suspension Period

Not applicable

4.10 Certificate Status Services

Certificate status services are provided by FhG OCSP responders and the central FhG directory. For further information see sections 7.2 and 7.3.

4.10.1 Operational Characteristics

FhG OCSP responders are available under the hostnames contained in the AIA extension of the certificate. They provide status information based on the CRLs of the respective CA.

4.10.2 Service Availability

Concrete data on the service availability of the FhG OCSP responder is provided in the document "Service Level Agreements of Fraunhofer Corporate PKI" [FhG-SLA].

4.10.3 Optional Features

No stipulation

4.11 End of Subscription

The procedures to terminate subscription have been realized in compliance with the requirements specified in section 4.11 of the document [FhG-CP].

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

Key Escrow has been realized in compliance with the requirements specified in section 4.12.1 of the document [FhG-CP].

Key escrow and recovery of private R-CA keys is performed within HSMs.

Key escrow and recovery of private subscriber encryption keys is performed within the CMS.

Further details on key escrow and recovery policy are provided in the internal non-published document "Fraunhofer Corporate PKI Concept" (for subscriber keys) and in the document [FhG-RKC] (for CA keys).

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

No stipulation

5 Facility, Management, and Operational Controls

All requirements on facility, management, operational controls specified in chapter 5 of the document [FhG-CP] have been fulfilled. Further details on these topics are provided in the internal non-published documents "Security Concept", "Operating Manual", "Organizational Concept", and the "Service Level Agreements" [FhG-SLA].

5.1 Physical Controls

Physical controls have been realized in compliance with the requirements specified in section 5.1 of the document [FhG-CP].

5.1.1 Site Location and Construction

Security measures for site location and construction have been realized in compliance with the requirements specified in section 5.1.1 of the document [FhG-CP].

5.1.2 Physical Access

Security measures for physical access have been realized in compliance with the requirements specified in section 5.1.2 of the document [FhG-CP].

5.1.3 Power and Air Conditioning

Security measures for power and air conditioning have been realized in compliance with the requirements specified in section 5.1.3 of the document [FhG-CP].

5.1.4 Water Exposures

Security measures against water exposures have been realized in compliance with the requirements specified in section 5.1.4 of the document [FhG-CP].

5.1.5 Fire Prevention and Protection

Security measures for fire prevention and protection have been realized in compliance with the requirements specified in section 5.1.5 of the document [FhG-CP].

5.1.6 Media Storage

Security measures for the protection of media storage have been realized in compliance with the requirements specified in section 5.1.6 of the document [FhG-CP].

5.1.7 Waste Disposal

Security measures for waste disposals have been realized in compliance with the requirements specified in section 5.1.7 of the document [FhG-CP].

5.1.8 Off-site Backup

Off-site Backup is mutually performed at the other CA site, i.e. backups of the CA-U are kept at the CA-S and vice-versa.

Details of the off-site backup facilities and procedures used are described in the internal non-published document "Backup and Recovery Concept".

5.2 Procedural Controls

Organizational security measures have been realized in compliance with the requirements specified in section 5.2 of the document [FhG-CP].

Further details on procedural controls are described in the internal non-published document "Operating Manual".

5.2.1 Trusted Roles

In general, separation of duties and/or a 4-eyes principles for all security-critical tasks are specified and implemented by the following sets of trusted roles complying with the requirements specified in section 5.2.1 of the document [FhG-CP]):

Table 5: Trusted Roles

Supervising Roles	
Role	**Function**
Information Security Officer	responsibility for ensuring compliance with data security regulations, approval of trustworthiness of CA personal, allocation of authorizations, liaison person for security issues and concerns
Auditor	conduct of audits, monitoring of CA operations, responsibility for ensuring compliance with data security regulations
Administrative Roles	
Role	**Function**

Head of CA	*see section 1.5.2*
Organizational Contact	*see section 1.5.2*
Operational Roles	
Role	**Function**
CA Employee	acquisition and provision of tokens and other products revocation of certificates smartcard/PSE production key recovery of subscriber encryption keys generation of PIN letters
Central RA Employee	approval of certificate, revocation, and key recovery applications approval of authentication and authorization support and contact point for employees revision-secure documentation of procedures maintenance of subscriber data and archiving of original documents distribution of tokens distribution of PIN letters
Local RA Employee	certificate, smartcard and revocation requests for specific groups of employees and/or machines delivery of smartcards to identified employees performing of PIN resets production of temporary replacement cards
Directory Maintenance	maintenance of data integration of certificates integration of CRLs publication
Employee	certificate revocation request for own certificates request for second smartcard request for secretary/substitution smartcard request for temporary replacement smartcard use of PKI support services

5.2.2 Number of Persons Required per Task

The following sets of tasks for which the so-called split knowledge and dual control principle (see also section 5.2.2 of the document [FhG-CP]) has to be realized by at least two persons is given in Table 6:

Table 6: Tasks

Tasks to be performed by at least two authorized persons
All R-CA activities
All critical CA operations
Replacement of CA software and hardware

5.2.3 Identification and Authentication for Each Role

The procedures for the identification and authentication for each role have been realized in compliance with the requirements specified in section 5.2.3 of the document [FhG-CP].

Further details are provided in the internal non-published document "Organizational Concept".

5.2.4 Roles Requiring Separation of Duties

The procedures for roles that requiring a separation of duties have been realized in compliance with the requirements specified in section 5.2.4 of the document [FhG-CP].

Further details on the separation of duties are provided in the internal non-published document "Organizational Concept".

5.3 Personnel Security Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

CA and RA staff with sufficient confidentiality, integrity, reliability, qualification, and experience will be employed. Staff members will receive appropriate technical instructions for performing their tasks.

Employees of CA and central RA will have an IT background and proven knowledge in the following areas:

- IT security in general
- cryptography and PKI in particular
- server administration
- network infrastructure

5.3.2 Background Check Procedures

CA and central RA staff must have a "no criminal record".

5.3.3 Training Requirements

The personal of the IT service management is required to have an ITIL (IT Infrastructure Library) certification.

5.3.4 Retraining Frequency and Requirements

Retraining of CA or central RA staff is initiated depending on major changes in infrastructure, IT systems or CP/CPS or any other security-critical component.

Retraining for decentral RA staff is provided periodically, at least once a year.

5.3.5 Job Rotation Frequency and Sequence

No stipulation

5.3.6 Sanctions for Unauthorized Actions

Sanctions for unauthorized actions complying with the requirements specified in section 5.3.6 of the document [FhG-CP] are defined.

5.3.7 Independent Contractor Requirements

Not applicable

5.3.8 Documentation Supplied to Personnel

In addition to the requirements specified in section 5.3.8 of the document [FhG-CP] the training documents referred to by the internal non-published documents "Operating Concept", "Emergency Concept", and "Training Material for Staff and Operating Personnel" is supplied to the personnel.

5.4 Audit Logging Procedures

A ticket system is used for the logging of all events in the lifecycle of the certificates. The monitoring of the technical systems is specified in the internal non-published document [Monitoring].

5.4.1 Types of Events Recorded

The sets of events and additional information that will be logged are

- request and approval of the certificate request
- creation and shipment of smartcards and pin-letters
- receipt of the handover protocol of the smartcard
- revocation of certificate

- PIN reset of smartcards

5.4.2 Frequency of Processing Log

The regular period for analyzing the recorded logs is at least once a month. In case of suspicious or exceptional events additional analyzing of the recorded logs will be applicable.

5.4.3 Retention Period for Audit Log

The retention period for audit logs is at least 10 years.

5.4.4 Protection of Audit Log

The protection of audit log has been realized within the ticket system and the underlaying database. Logged entries are protected from modification and deletion.

5.4.5 Audit Log Backup Procedures

The database of the ticket system will be daily backuped according the internal non-pulished document [Datenhaltung und Backup].

5.4.6 Audit Collection System (internal vs. external)

The audit collection system used is internal.

5.4.7 Notification to Event-Causing Subject

Upon the detection of the occurrence of an exceptional and serious event the information security officer will be immediately informed.

5.4.8 Vulnerability Assessments

Audit logs will be used for performing vulnerability assessment.

5.5 Records Archival

5.5.1 Types of Records Archived

CAs and RAs archive the following types of information:

- certificate applications,
- personal subscriber data,
- issued certificates,

- revocation requests, and
- published CRLs.

5.5.2 Retention Period for Archive

The retention period for archived records is at least 10 years.

5.5.3 Protection of Archive

The Archive is protected against unauthorized modification and deletion of data using the mechanism of the operation system of the filer.

5.5.4 Archive Backup Procedures

The archive is backuped daily to an off-site mirror-system. Incremental Backups to tape are scheduled each buisiness-day. A full Backup of the Archive is scheduled once a week.

5.5.5 Requirements for Time-stamping of Records

CAs and RAs add the date of archiving records to the archived data.

5.5.6 Archive Collection System (internal or external)

The archive collection system used is internal.

5.5.7 Procedures to Obtain and Verify Archive Information

CAs and RAs regularly prove the integrity of archive backups.

5.6 Key Changeover

Key Changeover is implemented according to section 5.6 of [FhG-CP].

5.7 Compromise and Disaster Recovery

In addition to the requirements specified in section 5.7 of the document [FhG-CP] the requirements specified in the internal non-published documents "Emergency Concept" and "Emergency Manual" will be satisfied.

5.7.1 Incident and Compromise Handling Procedures

The incident and compromise handling procedures specified in the emergency concept and emergency manual have been realized.

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

Security measures with regard to computing resources, software, and/or data that are corrupted have been realized in compliance with the requirements specified in section 5.7.2 of the document [FhG-CP].

Further details are provided in the internal non-published documents "Emergency Concept" and "Emergency Manual".

5.7.3 Entity Private Key Compromise Procedures

The procedures to be performed after an entity private key compromise have been realized in compliance with the requirements specified in section 5.7.3 of the document [FhG-CP].

Further details are provided in the internal non-published documents "Emergency Concept" and "Emergency Manual".

5.7.4 Business Continuity Capabilities after a Disaster

The procedures to be performed after a disaster in order to provide business continuity capabilities have been realized in compliance with the requirements specified in section 5.7.4 of the document [FhG-CP].

Further details are provided in the internal non-published documents "Emergency Concept" and "Emergency Manual".

5.8 CA or RA Termination

CAs and RAs will perform the set of actions that has been listed in section 5.8 of the document [FhG-CP].

Further details are provided in the internal non-published documents "Emergency Concept" and "Emergency Manual".

6 Technical Security Controls

All requirements on technical security controls specified in chapter 6 of the document [FhG-CP] have been fulfilled.

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

Key pair generation will be performed in compliance with the requirements specified in section 6.1 of the document [FhG-CP].

6.1.2 Private Key Delivery to Subscriber

Private key delivery to subscribers will be performed in compliance with the requirements specified in section 6.2 of the document [FhG-CP].

6.1.3 Public Key Delivery to Certificate Issuer

Not applicable

6.1.4 CA Public Key Delivery to Relying Parties

CAs publish their certificates in the central FhG directory from which relying parties can retrieve public CA keys.

6.1.5 Key Sizes

The selection key sizes will be done in compliance with the requirements specified in section 6.1.5 of the document [FhG-CP].

6.1.6 Public Key Parameters Generation and Quality Checking

Public key parameters generation and quality checking will be in compliance with the requirements specified in section 6.1.6 of the document [FhG-CP].

6.1.7 Key Usage Purposes

CAs will provide information on key usage with the issued certificates in compliance with the requirements specified in section 6.1.7 of the document [FhG-CP].

Further details on key usage purposes are provided in section 7.1.2.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

Cryptographic module standards and controls will be used in compliance with the requirements specified in section 6.2.1 of the document [FhG-CP].

Cryptographic operations are performed by the R-CA within HSMs that have been approved according to FIPS 140-2 Level 3.

Cryptographic operations are performed by the CAs within HSMs that have been approved according to FIPS 140-2 Level 3.

Cryptographic operations are performed by the subscribers (natural persons) within smartcards.

Further details are specified in the internal non-published document "CA Operating Manual".

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

Private keys of R-CA and CAs SHALL be stored on the HSM. The technical implementation of the "n out of m multi-personal control" has been realized by token- and PIN-based authentication of two authorized persons versus the HSM.

6.2.3 Private Key Escrow

Private key escrow has been realized in compliance with the requirements specified in section 6.2.3 of the document [FhG-CP].

Key escrow for R-CA and CAs private signing keys is supported for the generation of backups. The key material is handed over to a notary, and the activation data are handed over to another notary.

Key escrow for subscriber's private signing keys is not supported.

Key escrow for subscriber's private authentication keys is not supported.

Key escrow for subscriber's private encryption keys is supported. Escrowed encryption keys are stored in encrypted form within the CMS. The recovery of escrowed private keys is based on the "4-eyes-principle".

6.2.4 Private Key Backup

Private key backup has been realized as described in [FhG-RKC] and in compliance with the requirements specified in section 6.2.4 of the document [FhG-CP].

Private key backup of R-CA keys is supported in the form of HSM Backup Tokens.

Private key backup of CA keys is supported in the form of HSM Backup Tokens

Private key backup of subscriber signature and authentication keys is not supported.

Private key backup of subscriber encryption is automatically performed by the CMS. The access to backup encryption keys is only allowed via the CMS for the purpose of creating new smartcards and PIN letters complying with the 4-eyes principle.

6.2.5 Private Key Archival

Private key archival has been realized in compliance with the requirements specified in section 5.5 of the document [FhG-CP].

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

6.2.6 Private Key Transfer Into or From a Cryptographic Module

Private key transfer into or from a cryptographic module may occur according to the document [FhG-RKC] and in compliance with the requirements specified in section 6.2.6 of the document [FhG-CP].

The only exception were private R-CA and CA keys may leave the HSM is during the procedure used to generate private key backups (see section 6.2.4) within the CMS. Backup private keys are stored in HSM Backup Tokens.

The only exception were duplicates of private subscriber encryption keys may occur is during the procedure used to generate private encryption key backups (see section 6.2.4) within the CMS.

6.2.7 Private Key Storage on Cryptographic Module

Private key storage on cryptographic module has been realized in compliance with the requirements specified in section 6.2.7 of the document [FhG-CP].

Private R-CA and CA keys SHALL be stored on HSMs. Private subscriber (employees) keys will be stored on smartcards. For the initial rollout smartcards with Starcos operating system are used. Other smartcards MAY be used if they provide a similar level of security. Private subscriber (services/machines) keys will be stored in SW-PSEs.

6.2.8 Method of Activating Private Key

The method of activating a private key has been realized in compliance with the requirements specified in section 6.2.8 of the document [FhG-CP].

The PIN authentication procedure is used as method for activating the private key.

6.2.9 Method of Deactivating Private Key

The method of deactivating a private key has been realized in compliance with the requirements specified in section 6.2.9 of the document [FhG-CP].

The deactivation of a private key is supported via subscriber or CA log-out.

6.2.10 Method of Destroying Private Key

The method of destroying a private key has been realized in compliance with the requirements specified in section 6.2.10 of the document [FhG-CP].

6.2.11 Cryptographic Module Rating

The cryptographic modules (HSMs) used by the R-CA have been evaluated versus [FIPS 140-2].

The cryptographic modules (HSMs) used by the CAs have been evaluated versus [FIPS 140-2].

The cryptographic modules used within smartcards by the subscribers have been evaluated and have been considered appropriately secure for the use within Fraunhofer-Gesellschaft by the organization mentioned in 1.5.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

Public key archival has been realized in compliance with the requirements specified in section 6.3.1 of the document [FhG-CP].

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The following certificate validity periods are used:

- R-CA certificates have a validity period of at most 12 years,
- CA certificates have a validity period of at most 12 years,
- OCSP certificates for signing OCSP responses have a validity period of at most 3 months,
- subscriber certificates for signature stored on smartcards have a validity period of at most 6 years,
- subscriber certificates for authentication stored on smartcards have a validity period of at most 6 years,
- subscriber temporary certificates for authentication have a validity period of at most 1month,
- subscriber certificates for encryption stored on smartcards have a validity period of at most 6 years, and
- service/machine certificates have a validity period of at most 3 years.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

The generation and installation of activation data has been realized in compliance with the requirements specified in section 6.4.1 of the document [FhG-CP].

Subscribers and RA staff use PINs as activation data for their smartcards. The signing keys of R-CA and CAs require a 4-eyes principle implemented by the use of passwords, tokens and PINs.

Further details on activation data generation and installation are provided in the internal non-published document [FhG-RKC].

6.4.2 Activation Data Protection

The protection of activation data has been realized in compliance with the requirements specified in section 6.4.2 of the document [FhG-CP].

Further details on activation data protection is provided in the internal non-published document [FhG-RKC].

6.4.3 Other Aspects of Activation Data

No stipulation

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

Security measures related to access control for certification services have been realized in compliance with the requirements specified in section 6.5.1 of the document [FhG-CP].

The set of technical functional components that is used by CAs is described in the internal non-published document "Operating Manual".

6.5.2 Computer Security Rating

Details on computer security rating of technical functional components are provided in the internal non-published document "Operating Manual".

6.6 Life Cycle Security Controls

6.6.1 System Development Controls

The deployment of hardware and software is performed in compliance with the requirements specified in section 6.6.1 of the document [FhG-CP].

The R-CA and CAs only use hardware and software that has been thoroughly inspected, tested and approved.

6.6.2 Security Management Controls

Security management controls will be performed in compliance with the requirements specified in section 6.6.2 of the document [FhG-CP].

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

- regular monitoring and logging of security processes is performed by CA staff,
- the integrity of deployed hardware and software is periodically verified by CA staff, and
- compliance inspection is regularly performed by CA staff.

6.6.3 Life Cycle Security Controls

No stipulation

6.7 Network Security Controls

Network Security Controls will be performed in compliance with the requirements specified in section 6.7 of the document [FhG-CP].

The R-CA is exclusively run in an off-line mode of operation without any access points to networks.

Remote access of CA network clients to CA network server has been realized via a high-security private network.

Remote access of authorized CA personnel to the CMS has been realized for CA network clients.

Strong network security controls have been provided to protect CA network server from unauthorized access. These security measures are specified in the internal document "Fraunhofer Corporate PKI Network Concept".

6.8 Time-Stamping

No stipulation

7 Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

Certificates of Fraunhofer Corporate PKI are issued in compliance with the "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile" [RFC 3280].

7.1.1 Version Number(s)

The version of all issued certificates is version 3 (2).

7.1.2 Certificate Extensions

Extensions that are used in X.509 certificates are shown below. Background color is used in this table to visualize the following characteristics of extensions:

+	mandatory extension
-	prohibited extension
	optional extension

Table 7: Extensions Used in Certificates

Extensions	PKI-Components			Users			Services/Machines
	Root-CA	CA	OCSP	Signature	Encryption	Authentication	
authorityKeyIdentifier.keyIdentifier (non-critical) [3]	[4]	+	+	+	+	+	+
subjectKeyIdentifier (non-critical) [5]	+	+					
keyUsage (critical)							
digitalSignature	-		+	+	-	+	
nonRepudiation	-	-		+	-	-	
keyEncipherment	-	-	-	-	+	-	
dataEncipherment	-	-	-	-	+	-	
keyAgreement	-	-	-	-		-	
keyCertSign	+	+	-	-	-	-	-
cRLSign	+	+	-	-	-	-	-
encipherOnly	-	-	-	-		-	
decipherOnly	-	-	-	-		-	
certificatePolicies (non-critical) [6]				+	+	+	+
subjectAltName (non-critical) [7]							
issuerAltName (non-critical) [8]							
basicConstraints (critical)							
cA=TRUE [9]	+[10]	+	-	-	-	-	-
cA=FALSE or omitted [11]	-	-	+	+	+	+	+

[3] Identification of the associated public signature key of the CA that has issued this certificate.
[4] In a self-signed certificate this extension MAY be omitted or, if present, it SHALL contain the value of the R-CA subjectKeyIdentifier.
[5] Identification of certificates that contain a specific public key used for the construction of the certification path.
[6] OID (1.3.6.4.1.778.80.3.1.1) of the certificate policy of Fraunhofer Corporate PKI and URI to CP-documents
[7] Alternative names for the certificate subject of the type GeneralName: e.g. E-Mail address in the format RFC822, which may contain the naming attribute domain component (DC) in server certificates.
[8] Alternative names for the certificate issuer of the type GeneralName: E-Mail address in the format RFC822, Web-link to general CA-information in the URI format
[9] Indication of a CA certificate
[10] Component pathLenConstraints used with value 1
[11] Indication of an EE certificate

Extensions	PKI-Components			Users			Services/Machines
	Root-CA	CA	OCSP	Signature	Encryption	Authentication	
extendedKeyUsage (non-critical)							
serverAuth	-	-	-	-	-	-	
clientAuth	-	-	-	-	-	+	
codeSigning	-	-	-				
emailProtection	-	-	-	+	+		
ipsecEndSystem	-	-	-	-	-	-	
ipsecTunnel	-	-	-	-	-	-	
ipsecUser	-	-	-	-	-	-	
timeStamping	-	-	-				
OCSPSigning[12]	-	-	+	-	-	-	-
cRLDistributionPoints (non-critical)							
distributionPoint.fullName [13]	+	+		+	+	+	+
cRLIssuer [14]	-	-	-	-	-	-	-
authorityInfoAccess (non-critical)							
method: OCSP [15]			-	+	+	+	+
method: calssuers [16]							
Private Extensions							
smartCardLogon (extended key usage)[17]	-	-	-	-	-		
Microsoft Encrypting File System (extended key usage) [18]	-	-	-	-		-	
other extended key usages or non-critical extensions	-	-					

[12] OID (1.3.6.1.5.5.7.3.9)
[13] Format GeneralNames: URI to the CRL
[14] This component SHALL NOT be used since indirect CRLs are not supported
[15] Access method OCSP: OID (1.3.6.1.5.5.7.48.1) and URL as OCSP responder address
[16] Access method calssuers: OID (1.3.6.1.5.5.7.48.2) and URL to issuer certificates
[17] In the case of certificate-based system and SmartCard-Logon the user principal name (UPN, OID: 1.3.6.1.4.1.311.20.2.3) has to be included in the subjectAltName extension in addition to the extended key usage smartCardLogon (OID: 1.3.6.1.4.1.311.20.2.)
[18] OID: 1.3.6.1.4.1.311.10.3.4

7.1.3 Algorithm Object Identifiers

Algorithm object identifiers will be selected complying with the requirements specified in section 7.1.3 of the document [FhG-CP].

7.1.4 Name Forms

Name forms will be used in compliance with the requirements specified in section 7.1.4 of the document [FhG-CP].

7.1.5 Name Constraints

Name constraints will be used in compliance with the requirements specified in section 7.1.5 of the document [FhG-CP].

7.1.6 Certificate Policy Object Identifier

See section 1.2.

7.1.7 Usage of Policy Constraints Extension

Not Applicable

7.1.8 Policy Qualifiers Syntax and Semantics

Not Applicable

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

Not Applicable.

7.2 CRL Profile

Certificate Revocation Lists of Fraunhofer Corporate PKI are issued in compliance with the "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile" [RFC 3280].

7.2.1 Version Number(s)

The version of all issued CRLs is version 2(1).

7.2.2 CRL and CRL Entry Extensions

CRL and CRL Entry Extensions that are used in X.509 CRLs are shown below. The same color-coding scheme as in section 7.1.2 is used.

Table 8: CRL and CRL Entry Extensions

	CRL Entry Extensions	
	reasonCode	non-critical extension, reason for revocation
	invalidityDate	non-critical extension, date on which private key compromise is known or suspected in the date format UTCTime
-	**certificateIssuer**	critical extension, identification of CA that has issued an associated certificate, naming format GeneralNames, to be used for indirect CRL
	CRL Extensions	
	authorityKeyIdentifier	non-critical extension, identification of the public CRL signing key
	issuerAltName	non-critical extension, alternative names for the CRL issuer of type GeneralName, E-Mail address in the format RFC822, Web links in the URI format
+	**CRLNumber**	non-critical extension, CRL-sequence number
	deltaCRLIndicator	critical extension, identification of delta CRLs
-	**issuingDistributionPoint.indirectCRL**	critical extension, identification of indirect CRLs
	freshestCRL	non-critical extension, information in complete CRL to obtain delta CRLs

7.3 OCSP Profile

The OCSP responder of Fraunhofer Corporate PKI complies with the requirements stated in the document "Internet X.509 Public Key Infrastructure – Online Certificate Status Protocol" [RFC 2560].

7.3.1 Version Number(s)

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

7.3.2 OCSP Extensions

OCSP request extensions that are used in OCSP requests are shown in Table 9. OCSP response extensions that are used in OCSP responses are shown in Table 10. The same color-coding scheme as in section 7.1.2 is used.

Table 9: OCSP Request Extensions

	OCSP Request Extensions	
	Nonce	non-critical extension, prevention of replay attacks
	AcceptableResponses	non-critical extension, kind of expected response type
	ServiceLocator	non-critical extension, forwarding of request to another responder

Table 10: OCSP Response Extensions

	OCSP Response Extensions	
	Nonce	non-critical extension, prevention of replay attacks
	CrlID	non-critical extension, reference to CRL used by the responder to obtain status information
	ArchiveCutoff	non-critical extension, cutoff date as difference between retention period and current time of response
	CRL Entry Extensions Within OCSP Single Response Extensions	
	ReasonCode	non-critical CRL entry extension, reason for revocation
	InvalidityDate	non-critical CRL entry extension, date on which private key compromise is known or suspected in the date format UTCTime
-	**CertificateIssuer**	critical CRL entry extension, identification of CA that has issued an associated certificate, naming format GeneralNames, to be used for indirect CRL

8 Compliance Audit and other Assessments

The initial compliance audit will follow the requirements of Fraunhofer-Gesellschaft.

8.1 Frequency or Circumstances of Assessment

Compliance audits will be initiated by Fraunhofer-Gesellschaft.

8.2 Identity/Qualifications of Assessor

Audits will be performed by approved compliance auditors.

8.3 Assessor's Relationship to Assessed Entity

Audits will be performed by independent external compliance auditors.

8.4 Topics Covered by Assessment

The assessment will be performed in compliance with the requirements specified in section 8.4 of the document [FhG-CP].

8.5 Actions Taken as a Result of Deficiency

The actions specified in section 8.5 of the document [FhG-CP] will be taken as a result of deficiency.

8.6 Communication of Results

The result of an audit will be described by the auditor in the form of a non-published report and communicated to the head of the audited CA.

9 Other Business and Legal Matters

9.1 Fees

Concrete fees are provided in the document "Service Level Agreements of Fraunhofer Corporate PKI" [FhG-SLA].

9.1.1 Certificate Issuance or Renewal Fees

Concrete renewal fees are provided in the document "Service Level Agreements of Fraunhofer Corporate PKI" [FhG-SLA].

9.1.2 Certificate Access Fees

Concrete certificate access fees are provided in the document "Service Level Agreements of Fraunhofer Corporate PKI" [FhG-SLA].

9.1.3 Revocation or Status Information Access Fees

Concrete revocation or status information access fees are provided in the document "Service Level Agreements of Fraunhofer Corporate PKI" [FhG-SLA].

9.1.4 Fees for Other Services

Concrete fees for other services such as express service SHALL be specified in the document [FhG-SLA].

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

Information specified in section 9.3.1 of the document [FhG-CP] will be treated as confidential information.

9.3.2 Information Not Within the Scope of Confidential Information

Information specified in section 9.3.2 of the document [FhG-CP] will be treated as non-confidential information.

9.3.3 Responsibility to Protect Confidential Information

CAs provide security measures in order to protect confidential information from unauthorized reading, modification, or deletion.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

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

9.4.2 Information Treated as Private

RAs and CAs will treat confidential information as private information and will not disclose this information.

9.4.3 Information Not Deemed Private

RAs and CAs will treat non-confidential information as public information that may be disclosed.

9.4.4 Responsibility to Protect Private Information

RAs and CAs will perform security measures in order to protect private information from unauthorized reading, modification, or deletion.

9.4.5 Notice and Consent to Use Private Information

Notice and consent to use private information is performed in compliance with the requirements specified in section 9.4.5 of the document [FhG-CP].

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

RAs and CAs will only disclose confidential and private information to state authorities upon judicial requests.

9.4.7 Other Information Disclosure Circumstances

No stipulation

9.5 Intellectual Property Rights

See section 9.5 of the document [FhG-CP].

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

CAs will perform their tasks in compliance with the requirements specified in section 9.6.1 of the document [FhG-CP].

9.6.2 RA Representations and Warranties

RAs will perform their tasks in compliance with the requirements specified in section 9.6.2 of the document [FhG-CP].

9.6.3 Subscriber Representations and Warranties

See section 9.6.3 of the document [FhG-CP].

9.6.4 Relying Party Representations and Warranties

See section 9.6.4 of the document [FhG-CP].

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 [FhG-CP] and [FhG-CPS] have been published on the Fraunhofer Corporate PKI webpage *http://pki.fraunhofer.de*.

9.10.2 Termination

See section 9.10.2 of the document [FhG-CP].

9.10.3 Effect of Termination and Survival

See section 9.10.3 of the document [FhG-CP].

9.11 Individual Notices and Communications With Participants

This kind of information includes FAQs, user instructions and a blog that is published on the Fraunhofer Corporate PKI webpage *http://pki.fraunhofer.de*.

9.12 Amendments

9.12.1 Procedure for Amendment

See sections 1.5.2 to 1.5.4 of this document.

9.12.2 Notification Mechanism and Period

Currently no stipulation

9.12.3 Circumstances Under Which OID Must be Changed

See section 9.12.3 of this document [FhG-CP].

9.13 Dispute Resolution Provisions

See section 9.13 of this document [FhG-CP].

9.14 Governing Law

See section 9.14 of this document [FhG-CP].

9.15 Compliance With Applicable Law

The documents [FhG-CP] and [FhG-CPS], and the operations of Fraunhofer Corporate PKI 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

[FhG-CP] Fraunhofer Corporate PKI Certificate Policy

[FhG-CPS] Fraunhofer Corporate PKI Certification Practice Statement

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

[FIPS 140-2] NIST: Security Requirements for Cryptographic Modules

[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

[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 have not been published, but are available for compliance audits, if required:

- Backup and Recovery Concept
- Directory Concept
- Emergency Concept,
- Emergency Manual,
- Fraunhofer Corporate PKI Network Concept
- Fraunhofer Corporate PKI 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 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.

Table 11: 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 FhG Employees
CA-S	**CA** for Services / Machines
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
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
ITIL	**IT In**frastructure **L**ibrary
ITSEC	**I**nformation **T**echnology **S**ecurity **E**valuation **C**riteria
LDAP	**L**eightweight **D**irectory **A**ccess **P**rotocol

ACRONYM	MEANING
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 the FhG to which only authorized people have access as for example RA and central RA staff
SLA	**S**ervice **L**evel **A**greements
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