DFN-PKI

DFN
Deutsches
Forschungsnetz

Certification Practice Statement

# of the

Public Key Infrastructure in the

Deutsche Forschungsnetz

- Grid -

DFN-Verein

Grid-CPS V1.4, May 2008

Contact: pki@dfn.de

CONTENTS

1 INTRODUCTION

The "Verein zur Förderung eines Deutschen Forschungsnetzes e.V." (The German Association for the Promotion of a National Research and Education Network hereinafter referred to as DFN-Verein) is a non-profit organization that operates the Deutsche Forschungsnetz (Germany's National Research and Education Network hereinafter referred to as DFN) and ensures its further development and usage. This high-performance network for science and research provides network and internet connectivity to universities, technical colleges and research organizations in Germany, and supports the development and testing of new applications using this network. It is the basis on which the DFN-Verein provides services.

The DFN-Verein has established a Public Key Infrastructure in the Deutsche Forschungsnetz (DFN-PKI). Within this DFN-PKI four levels of certification services – Basic, Classic, Global and Grid - are offered, whereby each service displays specific functionalities based on different security requirements.

The DFN-PKI for the security level Grid will hereafter be referred to as DFN-PKI Grid. The certification authority within the DFN-PKI Grid which issues certificates will hereafter be referred to as Grid-CA.

1.1 Overview

This document contains the Certification Practice Statement (CPS) of the DFN-PKI Grid. Associated with this document is the Certificate Policy (CP).

CP and CPS incorporate the requirements of RFC 3647 [RFC 3647] and of the *Authentication Profile for Classic X.509 Public Key Certification Authorities with secured infrastructure* version 4.1 of the *European Grid Authentication Policy Management Authority* [EUGridPMA].

This CPS of the DFN-PKI Grid contains detailed information about specifications, certification authority procedures and security measures for the issuance of certificates for the security level Grid in accordance with the international standard X.509 [X.509].

1.2 Document name and identification

Identification

- Title: Certification Practice Statement of the Public Key Infrastructure in the Deutsche Forschungsnetz - Grid -
- Version: 1.4
- Object Identifier (OID) assigned: 1.3.6.1.4.1.22177.300.2.1.3.1.4
- Composition of the OID:

IANA	1.3.6.1.4.1	DFN-Verein	22177	PKI	300	CPS	2
X.509	1	Grid	3	Version (major)	1	Version (minor)	4

1.3 PKI participants

1.3.1 Certification authorities

Further details are given in the associated CP.

1.3.2 Registration authorities

The primary registration authority (RA) for the Grid-CA is located on the premises of DFN-CERT Services GmbH. In addition, the following registration offices are also available at DFN-Verein (Berlin office and Stuttgart office).

The list of all registration authorities is published on the web server specified in section 2.2.

Verification of subscriber identity may be effected by employees of registration authorities also in locations outside their premises.

1.3.3 Subscribers

Regulation of this is given in the associated CP.

1.3.4 Relying parties

Regulation of this is given in the associated CP.

1.3.5 Other participants

Regulation of this is given in the associated CP.

1.4 Certificate usage

Regulation of this is given in the associated CP.

1.5 Policy administration

1.5.1 Organization administering the document

This CPS is administered by:

DFN-Verein
Alexanderplatz 1
D - 10178 Berlin

Tel.: +49 30 884299-0
Fax: +49 30 884299-70
E-Mail: pki@dfn.de
WWW: http://www.dfn.de/pki

Operation of the Grid-CA is effected by:

DFN-CERT Services GmbH
DFN-PCA
Sachsenstraße 5
D - 20097 Hamburg

Tel.: +49 40 808077-555
Fax: +49 40 808077-556
E-Mail: dfnpca@dfn-cert.de
WWW: https://www.pca.dfn.de

1.5.2 Contact person

The person responsible for the associated CP is "Dr. Marcus Pattloch" (DFN-Verein)". For contact information see section 1.5.1.

1.5.3 Person determining CPS suitability for the policy

The person mentioned in section 1.5.2 is also responsible for this CPS.

1.5.4 CPS approval procedures

Approval of the CP and CPS is effected by the responsible person named in section 1.5.2. There is no dedicated procedure of approval.

1.5.5 Modification of the CP/CPS

Modification of the CP and CPS may be effected at any time in accordance with the procedures specified in section 1.5.4.

Whenever there is a change in the CP or CPS the OID of that document must change and the major changes must be announced to the EUGridPMA and approved before signing any certificates under the new CP and CPS. All the CPs and CPSs under which valid certificates are issued will be available via the service stated in section 2.2.

1.6 Definitions and acronyms

The Glossary is given in the associated CP.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

The Grid-CA repository may be accessed at https://www.pki.dfn.de/grid

2.2 Publication of certification information

The Grid-CA publishes the following information at https://www.pki.dfn.de/grid:

- Root certificate and its fingerprint
- List of registration authorities
- CP
- CPS

2.3 Time or frequency of publication

Regulation of this is given in the associated CP.

2.4 Access controls on repositories

Regulation of this is given in the associated CP.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

The distinguished name (DN) of any end entity subscriber under the Grid-CA contains the attribute "C=<country>"[1], "O=<organization>", and "OU=<organizational entity>".

The name of a Grid-CA end entity subscriber is always modeled on the following pattern:

C=DE,

O=GridGermany,

OU=<official name of the subscriber's organization>,

[OU=<organizational entity/project name>,]

CN=<common name>

The attribute "OU=" may be given one or several times and may contain the organizational entity or a project name allocated to the subscriber. If an email address is used it is included in the "SubjectAlternativeName". Other attributes that may be included in the name are given in section 7.1.

The attribute "OU=" must not be set to "SLCS"; this specific subtree of the namespace (/C=DE/O=GridGermany/OU=SLCS) is reserved.

3.1.2 Need for names to be meaningful

In addition to the regulations given in the associated CP the following accepted usage governs the assignment of names:

- Data processing systems:

  In case of data processing systems, a fully qualified domain name shall be included in the CN as well as a dnsName in the "SubjectAlternativeName". If the hostname contains a hyphen (Globus wildcard feature), the GRID-CA will issue certificates for data processing systems within the namespace (e.g. host.domain and host-*.domain) only to one verified subscriber.

[1] *As given in the ISO country code DIN EN ISO 3166-1.*

- Natural persons

  Affixes to names may only be used if they are included on an official identification document that includes a photographic likeness, e.g.: "CN=John Doe, Dr."

  If the subscriber is associated with the organisation in the OU name component, but not directly employed, the CN must be prefixed by "EXT:", e.g.: "CN=EXT: John Doe".

The order of assignation for clear and unambiguous serial numbers is given in section 7.1.

3.1.3 Anonymity or pseudonymity of subscribers

Not applicable.

3.1.4 Rules for interpreting various name forms

Deployable character sets and substitution rules for special characters:

Permissible characters are: a-z A-Z 0-9 ' ( ) + , - . / : = ? blank spaces.

Substitution rules: Ä (Ae), Ö (Oe), Ü (Ue), ä (ae), ö (oe), ü (ue), ß (ss).

Other special characters with accents such as circumflexes etc., are given without their respective accents. Otherwise, characters from the a-z and A-Z character sets should be used to convey the sound of the accented letter.

Character coding is PrintableString or T61String (neither BMPString nor UTF8String) and IA5String for email addresses.

3.1.5 Uniqueness of names

Regulation of this is given in the associated CP.

3.1.6 Recognition, authentication, and role of trademarks

Regulation of this is given in the associated CP.

3.2 Initial identity validation

Regulation of this is given in the associated CP.

3.2.1 Method to prove possession of private key

When applying for a certificate, a subscriber must guarantee that he is in possession of the private key. The following procedure for validation of possession of the private key applies:

- **Generation of the private key by the subscriber**

  The subscriber generates an asymmetric cryptographic key pair using the appropriate software (e.g. OpenSSL) and communicates the Certificate Signing Request (CSR) with its electronic signature to the relevant RA. Validation and approval of the CSR signature and verification of its authenticity must be effected before a certificate can be issued.

3.2.2 Authentication of organization identity

Authentication of organizational identity if effected during registration by presentation of the appropriate documents. To this end the DFN-Verein will provide the Grid-CA with a list containing the names of all organizations authorized to receive services. The contact person at the DFN-Verein is the person named in section 1.5.2.

3.2.3 Authentication of individual identity

Basic procedures for the authentication of the identity of a natural person are given in the associated CP. A personal meeting with an employee of the RA indicated in section 1.3.2 is required to authenticate the identity of a natural person.

The following information is required:

- Surname, first name(s) and affixes as included in the official identification document
- Address
- Type of identification document, ID number, and issuing authority

For issuing a certificate the following information is also required:

- Email address
- Authorization data for revocation of the certificate
- Intended use of the certificate
- Name components in the certificate
- Evidence of affiliation to an organization authorized to receive services.

3.2.4 Non-verified subscriber information

Regulation of this is given in the associated CP.

3.2.5 Validation of authority

Accreditation of a legal representative will be effected by the requesting organization in written form. In this instance documents having a valid electronic signature may also be used as far as their use has been previously agreed upon with the requesting organization. The following information is required:

- The name of the legal representative
- Email address
- Details of the identification document

The document must be signed by hand by a person from the requesting organization invested with appropriate signatory power (comp. section 3.2.2).

3.2.6 Criteria for interoperation

No provision is made for this.

3.3 Identification and authentication for re-key requests

Regulation of this is given in the associated CP.

3.4 Identification and authentication for revocation request

Revocation of a certificate is always effected by the RA from which the certificate was requested. Revocation can follow by:

- Hand-over of a signed certificate revocation request with details of the authorization information and/or validation of identity as per section 3.2.
- Sending a signed certificate revocation request by surface mail with details of the authorization information.
- Sending a revocation request in the form of a signed email.
- Sending a revocation request in the form of an unsigned email with details of authorization information.
- Telephone call with details of authorization information.

Contact: dfnpca@dfn-cert.de, +49 40 808077-580

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate application

4.1.1 Who can submit a certificate application

Regulation of this is given in the associated CP.

4.1.2 Enrollment process and responsibilities

The enrollment process consists of the following steps in their chronological order:

- Verification of the completeness and correctness of documentation and CSR
- Verification of the uniqueness of the DN in the CSR
- Archiving of documentation in a locked cupboard

- Communication of requisite information for certification to the proper CA either by means of an encrypted and signed email, by means of an encrypted and bi-directionally authenticated network connection, or through postal services.

4.2 Certificate application processing

Regulation of this is given in the associated CP.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

The Grid-CA verifies the authorization of the RA to apply for certificates for the name space entered in the DN of the submitted request.

4.3.2 Notification to subscriber by the CA of issuance of certificate

The certificate will be delivered to the subscriber by email.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

The time frame for objection is 14 days.

4.4.2 Publication of the certificate by the CA

Regulation of this is given in the associated CP.

4.4.3 Notification of certificate issuance by the CA to other entities

No provision is made for notification of other entities.

4.5 Key pair and certificate usage

Regulation of this is given in the associated CP.

4.6 Certificate renewal

Regulation of this is given in the associated CP.

4.7 Certificate re-key

Regulation of this is given in the associated CP.

4.8 Certificate modification

Regulation of this is given in the associated CP.

4.9 Certificate revocation and suspension

Regulation of certificate revocation is given in the associated CP. Suspension of certificates is not supported.

4.10 Certificate status services

Not applicable.

4.11 End of subscription

Regulation of this is given in the associated CP.

4.12 Key escrow and recovery

Not applicable.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

The requirements for infrastructural, organizational and personal security measures of a CA and/or RA are determined by the type of services offered. The precise level of security with regard to basic values such as availability, integrity, confidentiality and authenticity must be established in a security concept. The security concept will not be published but will be made available during validation of conformance.

5.1.1 Site location and construction

The technical systems of the Grid-CA are located on the premises of DFN-CERT Services GmbH. With regard to infrastructural security measures, these premises provide an adequate level of protection appropriate to the level of security required.

5.1.2 Physical access

The operational areas of the Grid-CA are protected by appropriate technical and infrastructural measures. Access to the operational areas of the Grid-CA is restricted to such employees who have been duly authorized by Information Security Officers of the Grid-CA. Access for persons not entrusted with a recognized function is regulated by the rules on visitors.

5.1.3 Power and air conditioning

Installation of the power supply is in compliance with applicable standards, an adequate air conditioning for the premises housing the technical infrastructure has been ensured.

5.1.4 Water exposures

The rooms housing the technical infrastructure are equipped with adequate protection against exposure to water.

5.1.5 Fire prevention and protection

Fire protection requirements are complied with, and an adequate number of fire extinguishers is also in place.

5.1.6 Media storage

The following media storage carriers shall be used:

- Paper
- CD-ROMs
- USB storage modules
- Magnetic tapes
- Hardware tokens

Media storage carriers shall be stored in locked cupboards. Media carriers storing sensitive data shall be stored in a safe.

5.1.7 Waste disposal

Information stored on data carriers will be destroyed in an appropriate manner and subsequently disposed of by a service provider in a proper manner. Data stored on paper will be destroyed by the available document shredders, and subsequently disposed of by a service provider in the appropriate manner.

5.1.8 Off-site backup

Not applicable.

5.2 Procedural controls

5.2.1 Trusted roles

To ensure the proper, correct and orderly operation of a CA, a number of measures need to be put in place, including division of responsibilities and separation of duties.

The table below defines the four categories of security-related roles involved in the certification process. Each role is assigned particular functions. Each role also specifies the degree of knowledge (either whole or split) allowed in relation to PINs and passwords together with access authorization to certain parts of the operational infrastructure (security areas, safes, secure operations rooms).

A member of staff can embody more than one role. However, it should be noted that there are roles requiring separation of duties (see section 5.2.4). It is also permissible for the duties of a certain role to be distributed among a number of staff members.

Role	Function	Code
Registration Service	The subscriber interface. Receives certificate applications, validation of requisite documentation, receipt of revocation requests.	
Customer Service	Receives applications for certificates. Identification, authentication and verification of subscriber authorization. Verification of documentation. Instruction and guidance of subscribers.	CS
Registrar	Verification of the completeness and accuracy of certificate applications. Documentation storage if applicable. Approval of certificate and revocation applications and furtherance to proper CA.	RG
Certification	Issuing certificates and CRLs, generation and safekeeping of the CA keys.	
CA- Employee 1	Responsible for the usage and storage of electronic data carriers on which the CA's private keys are stored. Has knowledge of one half of the PINs (passwords) to the CA's private key.	CAO1
CA- Employee 2	Has knowledge of the second half of the PINs (passwords) for the usage of the private keys of the CA.	CAO2
System Maintenance and Support	Administration of the IT systems and their daily operations (backups etc.).	
System and Network Administrator	Installation, configuration, administration and upkeep of communication systems. Full control of the hardware and software deployed yet without access and special knowledge of the cryptographic keys and their passwords used in the certification process, and in certificate and revocation management. Exclusive knowledge of system boot and administrator passwords.	SA
System Operator	Application support (data backup and recovery, web servers, certificate and revocation management)	SO
Monitoring of Operations	No function in the operational area, responsible for ensuring compliance with baselines stipulated in the CP, CPS and security concept.	
Revisor	Conduct of internal and external audits, monitoring and ensuring compliance with data security regulations.	R
Information Security Officer	Definition and ensuring compliance with the data security regulations. Checks trustworthiness of staff members. Issues authorizations. Liaison officer for all security issues and concerns.	ISO

Table 1: Roles

5.2.2 Number of persons required per task

The following table specifies security-level tasks and assigns them to the proper role. In addition, it also indicates whether compliance with the dual control principle (involving exactly two persons) is necessary for performance of the task.

Task	Role	Dual Control Principle	Comments
Receipt of certificate requests	CS		
Identification and authentication of subscribers	CS		
Verification of subscriber authorization	CS		
Verification of documents	CS		
Instruction of subscribers	CS		
DN verification	CS		
Generation of authorization information	CS		May also be effected by CAO1
Receipt and verification of revocation requests	CS		Receives revocation request and verifies authorization information
Verification of requests in respect of completeness and correctness	RG		
Storage of documents if required	RG		
Clearance and forwarding of certificate and revocation requests to the proper CA	RG		
Generation of cryptographic keys for the Grid-CA	CAO1, CAO2	x	
Certification; initiation of processes for issuance of certificates and revocation lists	CAO1, CAO2	x	
Transfer of certificate requests to certification computer	CAO1		
Publication of certificates and revocation lists	CAO1		
Escrow of private keys of the Grid-CA	CAO1, CAO2	x	
Knowledge of boot and administrator passwords	SA		
Initiation and termination of processes (e.g. webserver, backup)	SO		
Data backup	SO, CAO1		CAO1 allows for physical access
Replacement of soft- and hardware for certification systems	SA, CAO1	x	
Replacement of soft- and hardware for other systems	SA, CAO1		CAO1 allows for physical access
Restoration of backup data for certification systems	SA, CAO1	x	
Restoration of backup data for other systems	SA, CAO1		CAO1 allows for physical access
Verification of protocol data	SA, R		At regular intervals by SA during audit by R
Audit	R		

Task	Role	Dual Control Principle	Comments
Issuance of physical authorizations	ISO		
Technical issuance of authorizations	SA, ISO	x	Monitored by ISO
Development of operational / security concept	ISO		

Table 2: Tasks and assigned roles

5.2.3 Identification and authentication for each role

Identification and authentication for each role is based on the role models as specified in the sections above. Technical access to individual systems is based on user ID and password (provision must be made for rules governing the use of passwords). Physical access to individual systems is regulated by access control measures. Access to the bank safety deposit is restricted to the person holding the key thereto who will also be in possession of personal identification and authentication.

5.2.4 Roles requiring separation of duties

The following table shows roles requiring separation of duties.

Roles	Incompatible with
R - Revision	CS , RG CAO1, CAO2, SA, SO
ISO – Security Officer	CS , RG, CAO1, CA02, SA, SO
CS – Customer Service	R, ISO, SA, SO
RG - Registrar	R, ISO, SA, SO
SA – System Administrator	R, ISO, CS , RG, CAO1
SO – System Operator	R, ISO, CS , RG, CAO1
CAO1 - CA Employee 1	R, ISO, CAO2, SA, SO
CAO2 - CA Employee 2	R, ISO, CAO1

Table 3: Separation of duties

During allocation of roles among staff members, care will be taken to ensure that no two incompatible roles are assigned to the same person.

For the operation of the Grid-CA duties are allocated to the following categories of persons:

Category of persons	Area of activity	Roles
1	Monitoring of operations	R, ISO
2	Registration (Customer Service)	CS
3	Registration (Registrar) and certification	RG, CAO1
4	System support, CA key activation	CAO2, SA, SO

Table 4: Role allocation for the Grid-CA

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

Grid-CA employees meet all requisite requirements with regard to confidentiality, integrity, reliability and professional skills. All employees have general training and qualification in the field of information sciences, and, depending on the role they fulfill, also have in-depth knowledge of the following fields:

- IT security technology, cryptography, electronic signatures, PKI,
- International standards, technical standards,
- National and international law,
- Unix/Linux operating systems, TCP/IP networks and relational databases.

5.3.2 Background check procedures

On entering employment a Grid-CA employee must submit a Certificate of No Criminal Record which is to be renewed and resubmitted every two years.

Persons external to the Grid-CA may only enter CA service premises when accompanied by at least one authorized Grid-CA employee. Background checks on persons external to the Grid-CA are the responsibility of the organizations employing them.

5.3.3 Training requirements

The Grid-CA only employs properly qualified staff. In addition, regular retraining programs for all Grid-CA employees are given by properly qualified trainers. An employee must first furnish proof of holding the necessary professional skills and qualifications before he can be assigned to a specific role.

5.3.4 Retraining frequency and requirements

The frequency of retraining programs is dependent on the requirements of the Grid-CA. In particular, retraining programs will be held in the event of the introduction of a new policy, new IT systems or new security technology.

5.3.5 Job rotation frequency and sequence

Job rotation frequency and sequence depends either on the requirements of the Grid-CA or the requirements of a specific employee. Job rotation takes into account the separation of duties as described in section 5.2.4. Job rotation is not mandatory.

5.3.6 Sanctions for unauthorized actions

Unauthorized actions which endanger the security of the IT systems of the Grid-CA or which violate any provisions of data security regulations will be subject to disciplinary proceedings. In matters of criminal liability the proper authorities will be notified.

5.3.7 Independent contractor requirements

All contracts of employment for employees of the Grid-CA are governed by the law of the Federal Republic of Germany. All employees are bond to non-disclosure in compliance with applicable legal prescriptions covering data protection.

5.3.8 Documentation supplied to personnel

Grid-CA employees are supplied with the following documentation:

- Certificate Policy (CP)
- Certification Practice Statement (CPS)
- Instruction Manual (available in German):
  - Services
  - Security concepts
  - Process specification and forms for regular operations
  - Instructions and procedures for emergencies

    - Documentation of IT systems
    - Instruction manuals for the software in use

5.4 Audit logging procedures

5.4.1 Types of events recorded

To prevent intrusion and to monitor the proper operation of the Grid-CA, the following measures have been put in place. The following types of events are recorded as log-data or paper audits:

- Operation of IT components, including
    - Hardware booting procedures
    - Abortive login attempts
    - Issuance and withdrawal of authorizations
    - Installation and configuration of software
- All CA transactions, including
    - Certificate applications
    - Certificate issuance
    - Certificate publication
    - Certificate revocation
    - Generation of keys
    - Creation of certificates
- Modification of the CP and the operating concept, including
    - Role definition
    - Process specification
    - Changes in persons responsible

5.4.2 Frequency of processing log

Processing data are under regular monitoring and are analyzed at least once a month. Any exceptional events will receive special monitoring.

5.4.3 Retention period for audit log

Security relevant audit logs will be stored in compliance with legal regulations. The retention period for audit logs with regard to the management of keys and certificates corresponds to the term of the certificate of the Grid-CA with the addition of an extra period of two years.

5.4.4 Protection of audit log

Electronic audit logs are protected against intrusion, deletion and manipulation by functions of the operating system. Access to them is restricted to system administrators and network administrators.

5.4.5 Audit log backup procedures

In common with all other relevant Grid-CA data, audit logs are backed-up on a regular basis. Paper audit logs are stored in locked cupboards.

5.4.6 Audit collection system (internal vs. external)

An internal audit collection system is used.

5.4.7 Notification to event-causing subject

The Information Security Officer (ISO) is to be immediately notified in the event of any serious occurrences. In collaboration with System Administrators (SAs) the ISO will evolve a plan of action providing an appropriate response to the occurrence. If necessary, management will also be notified.

5.4.8 Vulnerability assessments

Vulnerability assessment is carried out by the Grid-CA itself and/or by the vendors of the software deployed.

5.5 Records archival

5.5.1 Types of records archived

The following records relevant to the certification process are archived:

- Certificate applications, including personal subscriber data
- All certificates issued by the Grid-CA
- Revocation requests
- Certificate Revocation Lists (CRLs)

5.5.2 Retention period for archive

The provisions of section 5.4.3 apply.

5.5.3 Protection of archive

Appropriate measures are in place to protect data from manipulation and deletion. If archives contain personal data, further measures shall be put in place to ensure that they cannot be read or copied by unauthorized persons.

5.5.4 Archive backup procedures

Data specified in sections 5.4.1 and 5.5.1 receive a regular off-line backup on tape or CD-ROM. The key elements of the archive backup procedure are:

- Incremental backup every working day
- Weekly full backup
- Monthly archive backup

Backup media are stored in an appropriate way outside the server room. The archive backup is stored in a bank safety deposit.

5.5.5 Requirements for time-stamping of records

No requirements.

5.5.6 Archive collection system (internal or external)

An internal archive collection system is used.

5.5.7 Procedures to obtain and verify archive information

The Information Security Officer (ISO) is invested with the authority to authorize the downloading and verification of archived data.

5.6 Key changeover

The Grid-CA's private signing keys are changed periodically. Only the latest key is used for certificate signing purposes. The prior key will still be available to verify signatures and to sign CRLs. The overlap time of the keys is at least the validity period of a subscriber certificate. Certificate operational periods and key pair usage periods are specified in section 6.3.2.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

Procedures for handling breaches of security and the compromising of Grid-CA's private keys are given in an Emergency Process Instruction. These instructions are distributed to all employees. Basic elements of the procedures are given in the following sections.

5.7.2 Computing resources, software, and/or data are corrupted

Should the existence of malfunctioning or manipulated computing resources, software, and/or data be ascertained within a CA that will have an impact on the proper functioning of the same, the operation of the IT system containing the defect will be immediately terminated.

The IT system will be reset on redundant hardware using backup software and backup data, and will then be checked and put into operation in a safe condition. The defective or modified IT system will then be analyzed. Should suspicion arise of malicious intent, legal proceedings may be instigated. In addition, a security check and an audit to detect any vulnerable points will be carried out. If required, additional protective measures will also be put in place to prevent the occurrence of similar incidents in the future. In such cases Grid-CA employees will work together with experts from the DFN-CERT. Should corrupted data be found in any certificate, the certificate subscriber will be immediately notified and the certificate immediately revoked.

5.7.3 Entity private key compromise procedures

Should the private keys of the Grid-CA be compromised, or should reasonable grounds exist for supposing that such compromise has taken place, the Information Security Officer of the Grid-CA is to be notified of the same without delay. The ISO will investigate the comprise or alleged compromise, and, if required, will order the revocation of certificates so affected. In this instance the following measures will be instigated:

- Immediate notification of all affected subscribers
- Revocation of the certificate of the CA and of all certificates certified by it. If necessary, the repository will be taken off-line in order to preempt incorrect or invalid information being supplied by these services.
- Generation of a new key pair and new certificate for the CA
- Publication of the certificate of the CA
- Issuance of new certificates for subscribers following the instructions of the Information Security Officer

5.7.4 Business continuity capabilities after a disaster

The resumption of business operations of a CA following a disaster is part of the case of emergency procedures, and may be effected within a short period of time provided that security for certification services is given. Assessment of the security situation is the responsibility of the Information Security Officer.

5.8 CA or RA termination

Should termination of operations of a CA prove necessary, the following measures will be instigated:

- Notification of all subscribers, RAs, the EUGridPMA, and concerned organizations in a period at least three months prior to termination.
- Timely revocation of all certificates.
- Safe destruction of all private keys held by the CA.

The DFN-Verein will ensure the continued existence of the archive, and of a complete and downloadable Certificate Revocation List (CRL), for the stipulated period of retention.

6 TECHNICAL SECURITY CONTROLS

The requirements for technical security measures of a CA or RA are determined by the type of services offered. The precise level of security with regard to basic values such as availability, integrity, confidentiality and authenticity must be established in a security concept. The security concept will not be published but will be made available during validation of conformance.

As far as requirements for specific security measures are not specified in this CPS, they should be taken from the appropriate catalogue of measures in the IT Baseline Protection Manual [IT-GSHB].

6.1 Key pair generation and installation

6.1.1 Key pair generation

Key pairs for the Grid-CA are generated on a dedicated IT system unequipped with networking capability or directly within a Hardware Security Module (HSM). The keys are stored only on external data storage media and are protected by a PIN or when generated within a HSM the keys are protected by the HSM.

6.1.2 Private key delivery to subscriber

No cryptographic key pairs are generated for subscribers.

6.1.3 Public key delivery to certificate issuer

The subscriber's certificate signing request (CSR) will be communicated to the Grid-CA by the RA using a secure communication channel (e.g. signed emails, SSL protected private web pages that are bi-directionally authenticated).

6.1.4 CA public key delivery to relying parties

All relying parties may download the Grid-CA public key in PEM and PKCS#7 format or in binary (DER) form from the repository (comp. section 2.1).

6.1.5 Key sizes

The cryptographic algorithms deployed and their key sizes are based on publications of the Regulatory Authority for Telecommunications and Posts [RegTP].

- The RSA algorithm (with SHA1 checksums) is used for signature processes.
- Key size for the Grid-CA is set at a minimum of 2048 bit.
- All other keys must have a minimum size of 1024 bit. However, in order to guarantee a long-term security level, it is strongly recommended to use a minimum key size of 2048 bit.

6.1.6 Public key parameters generation and quality checking

Parameters will be generated by the Grid-CA. Great care will be given to the selection of parameters for generation.

6.1.7 Key usage purposes (as per X.509 v3 key usage field)

Key usage purposes and restrictions on the same are stipulated in the appropriate X.509 v3 key usage field (comp. section 7.1.2).

6.2 Private key protection and cryptographic module engineering controls

6.2.1 Cryptographic module standards and controls

If HSMs are used to generate and/or store CA keys these HSMs are certified to the FIPS 140-2 Level 3 standard.

6.2.2 Private key (n out of m) multi-person control

No provision is made for multi-person control of Grid-CA private keys, however PINs for CA keys are split between the roles CAO1 and CAO2.

6.2.3 Private key escrow

Subscriber private key escrow is not supported.

6.2.4 Private key backup

Subscriber private key backup is not supported.

Private CA keys stored in a HSM are backuped with mechanism provided by the HSM. The resulting encrypted HSM backup files are stored in on-site and off-site vaults.

Access to these vaults is strictly regulated.

6.2.5 Private key archival

At present the archiving of subscribers’ private keys is not supported.

6.2.6 Private key transfer into or from a cryptographic module

No stipulation.

6.2.7 Private key storage on cryptographic module

No stipulation.

6.2.8 Method of activating private key

A private key is activated by entering a password or a PIN code.

The PIN of the Grid-CA private keys is divided into two halves. Only one half is known to the CAO1 and CAO2 respectively. Activation of the private key PIN is only possible in accordance with the dual control principle.

6.2.9 Method of deactivating private key

Deactivation of the private key is automatic. Once the certification process (which can also be a batch process) is ended, technical measures prevent any further use of the private key.

6.2.10 Method of destroying private key

The destruction of the Grid-CA private keys is subject to the dual control principle. The roles assigned for the destruction of the private key are "ISO" and "CAO1".

6.2.11 Cryptographic Module Rating

Compare section 6.2.1.

6.3 Other aspects of key pair management

6.3.1 Public key archival

Public keys are archived both in repositories and on data storage media.

6.3.2 Certificate operational periods and key pair usage periods

Certificates issued by the Grid-CA have the following periods of validity:

- Grid-CA root certificates: a maximum of eight (8) years and two (2) month
- All other certificates: a maximum of one (1) year and one (1) month

The period of use for a key pair will correspond to the term of validity of the certificate based on that key pair. Usage of an existing key pair for recertification purposes is permissible should the recommended algorithms and key sizes allow (comp. section 6.1.5).

6.4 Activation data

Common combinations of alphanumerical characters and special characters should not be used for passwords or PINs to activate private keys.

For certification purposes Grid-CA will use activation data composed of a string of at least 15 characters. In all other cases a string of at least 12 characters must be used.

6.4.1 Activation data generation and installation

Not applicable.

6.4.2 Activation data protection

Activation data must never be disclosed and may only be made known to members of staff who require them for the execution of a specific role as specified in section 5.2.1. A record in writing is only permissible in the case of private key backup as specified in section 6.2.4.

6.4.3 Other aspects of activation data

Not applicable.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

All applications within the Grid-CA are exclusively carried out using hardened operating systems. In addition, the following security measures will also be implemented:

- Access controls
- User authentication

6.5.2 Computer security rating

Not specified.

6.6 Life cycle technical controls

6.6.1 System development controls

No specifications. However, software (proprietary or third-party developed) is always only deployed after due inspection and approval.

6.6.2 Security management controls

Security management comprises of the following aspects:

- An annual audit (compliance inspection)
- Regular inspection and upgrading of the security concept
- Checking security measures during on-going operations (comp. section 5.4)
- Regular monitoring of the integrity of applications and operating systems in use
  - Centralized logging of all security processes and procedures
  - Collaboration with DFN-CERT
  - Keying-in upgrades and patches when and if required
  - Deployment on a production system only following testing and approval on a test system

6.6.3 Life cycle security controls

Life cycle security controls are not supported.

6.7 Network security controls

The network of the Grid-CA is divided into various security zones which are all separated from one another by firewalls. In addition, Intrusion Prevention Systems and Detection Systems have been put in place to prevent intrusions from the Internet and/or Intranet. Critical security events will be immediately tracked and processed in collaboration with DFN-CERT. Moreover, all IT systems connected to a network are equipped with a host-based firewall that allows network traffic only on an authorized communication matrix.

6.8 Time-stamping

Certificates issued do not feature time-stamping.

7 CERTIFICATE, CRL, AND OCSP PROFILES

This section describes the profiles, characteristics and extensions that are used in certificates, certificate revocation lists (CRLs) and online certificate status protocols (OCSP).

These are based essentially on syntax and semantics of as laid down in the X.509 [X.509] specification of the IETF working group "Public Key Infrastructure (X.509)" [PKIX] and on widely accepted industry standards such as those used by Netscape (NETS) for its Netscape Certificate Extensions, and by RSA for Public Key Cryptography Standards (PKCS).

7.1 Certificate profile

7.1.1 Version number(s)

Certificates are issued based on PKIX specification X.509 version 3 (X.509v3).

7.1.2 Certificate extensions

The following certificate extensions are used for the issuance of certificates:

	Root	SubCA	Nat. person / role	System-Server	System-Client	Critical	Optional	Mandatory
Identifier of the subscriber key (Subject Key Identifier): KeyID (Hash) of the subscriber public key	x	x	x	x	x			x
Identifier of certificate-issuer key (Authority Key Identifier): KeyID (Hash) of the certificate-issuer public key	x	x	x	x	x			x
URLs for certificate revocation lists (CRL Distribution Points, CDPs): several CDPs in the form of HTTP URIs	x	x	x	x	x			
Basic Constraints: CA=TRUE	x	x				x		x
Basic Constraints: CA=FALSE			x	x	x	x		x
Key Usage: Certificate Sign	x	x				x		x
Key Usage: CRL Sign	x	x				x		x
Key Usage: Digital Signature			x	x	x	x		x
Key Usage: Key Encipherment			x	x	x	x		x
Key Usage: Data Encipherment			x	x	x	x		x
Extended Key Usage clientAuth (according to PKIX)			x		x		x	
Extended Key Usage codeSigning (according to PKIX)			x		x		x	
Extended Key Usage emailProtection (according to PKIX)			x		x		x	
Extended Key Usage serverAuth (according to PKIX)				x			x	
Extended Key Usage ipsecEndSystem (according to PKIX)				x	x		x	
Extended Key Usage ipsecTunnel (according to PKIX)				x	x		x	
Extended Key Usage ipsecUser (according to PKIX)			x				x	
Extended Key Usage smartCardLogin (Microsoft)			x				x	
Netscape Certificate Type: SSL CA	x							x

	Root	SubCA	Nat. person / role	System-Server	System-Client	Critical	Optional	Mandatory
Netscape Certificate Type: S/MIME CA	x							x
Netscape Certificate Type: Object Signing CA	x							x
Netscape Certificate Type: SSL CA		x					x	
Netscape Certificate Type: S/MIME CA		x					x	
Netscape Certificate Type: Object Signing CA		x					x	
Alternative subscriber name (subjectAltName): one or several DNS names				x			x[2]	
Alternative subscriber name (subjectAltName): one or several email addresses			x		x			x
Alternative subscriber name (subjectAltName): one or several IP-numbers				x			x	
Alternative name of certificate issuer (issuerAltName): one or more e-mail addresses		x	x	x	x		x	
Information to locate the certificate of the Grid-CA (authorityInfoAccess, caIssuers): URI		x	x	x	x		x	
Object identifier of the (CP): OID of the CP (comp. section 1.2 of CP) and URIs of CP and CPS			x	x	x			x

Table 5: Certificate Extensions

Further certificate extension:

Further certificate extensions and extended usage of keys may be applied for in so far as they comply with the CP.

Key escrow:

The "non-repudiation flag" may only be set in a certificate if no recovery of private key material is possible either by the Grid-CA or by any third-party.

Serial numbers:

Serial numbers for issued certificates are never issued twice by the Grid-CA and thus are unique in relation to the issuing CA (identified by the DN).

7.1.3 Algorithm object identifiers

Algorithm object identifiers are used in accordance with PKIX.

7.1.4 Name forms

Comp. section 3.1.

7.1.5 Name constraints

Comp. section 3.1.

7.1.6 Certificate policy object identifier

The object identifier of the associated CP is set according to section 1.2 of the same.

[2] *The DNS name shall be contained in the "SubjectAlternativeName".*

7.1.7 Usage of Policy Constraints extension

None.

7.1.8 Policy qualifiers syntax and semantics

None.

7.1.9 Processing semantics for the critical Certificate Policies extension

None.

7.2 CRL profile

7.2.1 Version number(s)

Certificate Revocation Lists are produced in accordance with the international standard X.509 version 2.

7.2.2 CRL and CRL entry extensions

CRL extensions used:

- CRL Number

7.3 OCSP profile

The Grid-CA does not support OCSP.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

Regulation of this is given in the associated CP.

9 OTHER BUSINESS AND LEGAL MATTERS

Regulation of this is given in the associated CP.

10 REFERENCES

References are given in the associated CP.

11 Glossary

The glossary is given in the associated CP.