Certificate Policy of the Public Key Infrastructure in the Deutsche Forschungsnetz

- Grid -

DFN-Verein

Grid-CP V1.6, January 2012

CONTENTS

1 INTRODUCTION....5
1.1 Overview....5
1.2 Document name and identification....5
1.3 PKI participants....5
1.4 Certificate usage....6
1.5 Policy administration....6
1.6 Definitions and acronyms....6
2 PUBLICATION AND REPOSITORY RESPONSIBILITIES....7
2.1 Repositories....7
2.2 Publication of certification information....7
2.3 Time or frequency of publication....7
2.4 Access controls on repositories....7
3 IDENTIFICATION AND AUTHENTICATION....7
3.1 Naming....7
3.2 Initial identity validation....8
3.3 Identification and authentication for re-key requests....9
3.4 Identification and authentication for revocation request....10
4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS....10
4.1 Certificate application....10
4.2 Certificate application processing....10
4.3 Certificate issuance....11
4.4 Certificate acceptance....11
4.5 Key pair and certificate usage....11
4.6 Certification renewal....13
4.7 Certificate re-key....14
4.8 Certificate modification....14
4.9 Certificate revocation and suspension....14
4.10 Certificate status services....15
4.11 End of subscription....15
4.12 Key escrow and recovery....15
5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS....16
6 TECHNICAL SECURITY CONTROLS....16
7 CERTIFICATE, CRL, AND OCSP PROFILES....16
8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS....16
9 OTHER BUSINESS AND LEGAL MATTERS....16
9.1 Fees....16
9.2 Financial responsibility....16
9.3 Confidentiality of business information....16

9.4 Privacy of personal information....16
9.5 Intellectual property rights....17
9.6 Representations and warranties....17
9.7 Disclaimers of warranties....17
9.8 Limitations of liability....17
9.9 Indemnities....17
9.10 Term and termination....18
9.11 Individual notices and communications with participants....18
9.12 Amendments....18
9.13 Dispute resolution provisions 18
9.14 Governing law....18
9.15 Compliance with applicable law....18
9.16 Miscellaneous provisions 18
10 REFERENCES....20
11 GLOSSARY....21

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 five levels of certification services – SLCS, 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 Certificate Policy (CP) of the DFN-PKI Grid. Associated with this document is the Certification Practice Statement (CPS).

CP and CPS incorporate the requirements of RFC 3647 [RFC3647] and of the *Authentication Profile for Classic X.509 Public Key Certification Authorities with secured infrastructure* version 4.3 of the European Grid Authentication Policy Management Authority [EUGridPMA].

This CP of the DFN-PKI Grid defines the framework conditions for the issuance of certificates for the security level Grid in accordance with the international standard X.509 [X.509].

Certificates for the aforementioned level of security will be solely issued on the basis of this Certificate Policy; the statements made therein are binding on all participants in so far as they do not infringe legal regulations.

1.2 Document name and identification

Identification

- Title: Certificate Policy of the Public Key Infrastructure in the Deutsche Forschungsnetz – Grid –
- Version: 1.6
- Object Identifier (OID) assigned: 1.3.6.1.4.1.22177.300.1.1.3.1.6
- Composition of the OID:

IANA	1.3.6.1.4.1	DFN-Verein	22177	PKI	300	CP	1
X.509	1	Grid	3	Version (major)	1	Version (minor)	6

1.3 PKI participants

Hereinafter the term DFN-site refers to any site that corresponds to the charter ('Satzung') of the DFN-Verein [DFN-Charter], i.e. every site and user related to research and science in Germany.

1.3.1 Certification authorities

A single certification authority (Grid-CA) is used for issuing certificates for natural persons (i.e. user and automated client certificates) and legal persons (i.e. server, service, machine and automated client certificates).

1.3.2 Registration authorities

A single primary registration authority (RA) is associated with the Grid-CA for registration of subordinate RAs. Verification of the identity and authenticity of other subscribers may also be performed by the primary registration authority.

All DFN-sites are enabled to nominate registration authorities for local registration and verification of the identity and authenticity of subscribers. However, such registration authorities are not entitled to register further authorities. The Grid-CA has to be assured of the compliance with the CP in written form. The nomination and revocation of registration authorities is to be documented and made known.

1.3.3 Subscribers

Certificates may be issued for natural persons and legal persons belonging to a DFN-site.

1.3.4 Relying parties

Relying parties are natural persons or organizational entities who rely on certificates issued within the DFN-PKI Grid to verify the identity of a subscriber by receiving or sending information from/to the same.

1.3.5 Other participants

Other participants may be natural or legal persons who are involved in the certification process as service providers. Responsibility for service providers acting on behalf and by order of a DFN site lies with the authorizing DFN-site.

Service agreements with a service provider or the receipt and acceptance of services from a service provider acting on his own behalf can solely and exclusively be undertaken by the DFN-Verein itself.

1.4 Certificate usage

1.4.1 Appropriate certificate usage

Certificates issued within the scope of this CP may be used by subscribers for purposes of authentication, digital signature and data encryption. The Grid-CA or its service providers are not responsible for the deployment of certificates and they will not install any applications or software on systems not owned by themselves.

1.4.2 Prohibited certificate usage

Basically no form of certificate usage is prohibited. With the exception of Proxy-Certificates [RFC3820], the Grid-CA alone may issue further certificates.

1.5 Policy administration

1.5.1 Organization administering the document

This CP is administered by:

DFN-Verein	Tel.: +49 30 884299-955
Alexanderplatz 1	Fax: +49 30 884299-70
10178 Berlin	E-Mail: pki@dfn.de
GERMANY	WWW: http://www.pki.dfn.de

All further regulations are given in the associated CPS.

1.6 Definitions and acronyms

See Glossary.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

The Grid-CA offers a repository allowing online access to the issued certificates which are approved for publication, and to the Certificate Revocation List (CRL). All further regulations are given in the associated CPS.

2.2 Publication of certification information

The Grid-CA makes the following information available:

- Root certificate and its fingerprint
- RAs
- CP and associated CPS

Moreover, information may be offered to subscribers concerning the DFN-PKI Grid, the correct usage of cryptography and the deployment of certificates. If applicable, all further regulations are given in the associated CPS.

2.3 Time or frequency of publication

Newly issued Certificate Revocation Lists (CRLs), Certificate Policies and any other required information will be published promptly. The following frequency of publication applies:

- CRLs: at least every two (2) days and/or within one (1) working day after a revocation request has been approved; the time period between the CRL's *lastUpdate* value and its *nextUpdate* value is at least three (3) days and at most ten (10) days long
- Policies: as required
- Other information: as required

2.4 Access controls on repositories

Access for purposes of reading all information listed in sections 2.1 and 2.2 shall not be subject to any form of control. Access for purposes of writing such information is restricted solely to authorized persons. The repository runs on a best-effort basis, with an intended availability of 24x7.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

Distinguished Names (DN) in end entity certificates will always include C=DE, O=GridGermany.

3.1.1 Types of names

All certificates issued within the DFN-PKI Grid shall be assigned a DN according to the X.500 series of standards. A DN contains a string of unique naming attributes through which all participants in a hierarchy may be referenced. Particulars of the specific types of names are given in the associated CPS.

3.1.2 Need for names to be meaningful

The DN must clearly and unambiguously identify the subscriber and be presented in a form that people can understand. The following basic regulations govern the assignment of names:

- Certificates may only be issued for valid subscriber names.
- Certificates for automated clients must be recognizable as such, i.e. the name of a certificate for an automated client must include a humanly-recognizable and meaningful description of the automated client as well as either the name of a single natural person responsible for the automated client or an email address of a persistent group of people responsible for the automated client's operations.

- Certificates for servers, services and machines must be recognizable as such, i.e. their fully qualified domain name should always be used for naming purposes.

Furthermore, every certificate shall be assigned a unique serial number which allows clear and immutable assignment to the subscriber. All further regulations are given in the associated CPS.

3.1.3 Anonymity or pseudonymity of subscribers

The Grid-CA does not issue certificates that allow the anonymity of subscribers, thus DNs containing a pseudonym are not accepted.

3.1.4 Rules for interpreting various name forms

The character set to be used and the substitution rules for special characters are given in the associated CPS.

3.1.5 Uniqueness of names

Every RA may only assign names within the DN-prefixes allocated to this RA. The Grid-CA takes care, that no DN-prefix is assigned more than once. Before approving a request for certification the correctness and uniqueness of the name assigned within the given DN-prefix must be verified by the RA. The DN of a subscriber must be unique and must not be assigned to a number of different subscribers. Only when a subscriber holds several certificates with disjointed key usage may a DN be used more than once, but only for certificates for this specific subscriber. However, the serial number shall always be unique without reserve or qualification. A single subscriber can have more than one associated DN.

Cases in which the same name has been submitted by different requesters will be settled on a first come, first served basis. Disputes will be decided by the Grid-CA.

3.1.6 Recognition, authentication and role of trademarks

As far as the DN on a certificate explicitly refers solely to a natural person, recognition of trademarks is non-applicable. In all other cases it is the responsibility of the subscriber to ensure that the choice of name does not infringe any law pertaining to trademarks, brand names etc. The Grid-CA and the RAs are not obliged to verify compliance with such legal prescriptions. It is solely incumbent on the subscriber to ensure such compliance. Should a CA be informed of any infringement of such laws, the certificate will be revoked.

3.2 Initial identity validation

Depending on the purposes for which the certificate is to be used, the following regulations apply to the identity verification of a subscriber:

- **Natural persons:** To enable authorization of the data entered in a certificate, appropriate procedures shall be used by the Grid-CA or responsible RA to verify the identity and authenticity of the natural person. Procedures acceptable within the framework of this CP are set forth in section 3.2.3.
- **Legal persons:** Should the subscriber be a legal person, the following matters shall be verified during the registration process:
  a) The existence and identity of the legal person, e.g. by submission of a meaningful document.
  b) Proof of authorization to receive said services (comp. section 3.2.2).
  c) Accreditation of a legal representative or a commissioned service provider by the requesting legal person (comp. section 3.2.5).
  d) Authentication of the legal representative. The verification of the identity and authenticity of the legal representative shall follow in compliance with the provisions of section 3.2.3.

3.2.1 Method to prove possession of private key

When applying for a certificate, the subscriber must furnish proof that he is in possession of a private key. The appropriate methods are given in the associated CPS. No provision is made for key pair generation by the Grid-CA.

3.2.2 Authentication of organizational identity

The DFN-Verein will provide the Grid-CA with a procedure to verify the authorization of an organization to receive services. Further details are given in the associated CPS.

3.2.3 Authentication of individual identity

To validate the identity of a natural person the following procedures are applicable:

a) The subscriber will appear in person at the Grid-CA or the responsible RA where a staff member of the Grid-CA or RA will carry out validation of identity with reference to an official identification document including a photographic likeness (ID card or passport).

b) The authentication of a natural person shall be effected by an appropriate service provider who shall carry out the validation of personal identity with reference to an official identification document including a photographic likeness (ID card or passport). Validation must be documented in an appropriate manner. The service deployed must either have an Attestation of Conformity for the implementation of security concepts by a testing and validation authority recognized by the Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railway [BNetzA] or compliance must be made obligatory through contractual regulation.

Should the requesting person already be in possession of a valid certificate, request for further certificates for this person can also be effected by submission of an encrypted and signed application, in so far as the identity of the requesting person is still the same.

For this type of application to be effective, the period of time between the identification for an issued certificate and the present application for a new certificate must not exceed two years, and the identification documents must still be valid.

3.2.4 Non-verified subscriber information

Only information will be verified which is required for the various authentication procedures for the validation of identity (comp. section 3.2.3). Beyond this requirement, no further information shall be verified.

3.2.5 Validation of authority

Accreditation of a legal representative by the requesting organization will be effected either in writing or through an adequate procedure on the part of an authorized signatory.

Accreditation of an authorized service provider by the requesting organization will be effected either in writing or through an adequate procedure on the part of an authorized signatory. In this case the authorized service provider must accredit a legal representative according to the stipulation of section 3.2. Verification of entitlement to sign accreditations is the responsibility of the requesting organization.

Authority to receive certificates for all names included (i.e. domain names, IP addresses, email addresses, names of organizations, automated clients and natural persons) must be validated. Further details are given in the associated CPS.

3.2.6 Criteria for interoperation

No provision is made for this.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

Re-keying can only take place if the subscriber is in possession of a valid certificate issued by the Grid-CA. Furthermore, before the issuance of a new certificate can occur, the subscriber

must furnish proof of ownership of the private key to the Grid-CA (comp. section 3.2.1) and must confirm the validity of the information contained in the valid certificate.

If the most recent identification of the subscriber (comp. section 3.2.3) is older than five (5) years the subscriber must undergo a new identification as per section 3.2.3.

3.3.2 Identification and authentication for re-key after revocation

Once a certificate has been revoked, it cannot be renewed. A new certificate signing request must be made. In this case the provisions of section 3.2 are applicable. The most recent identification of the subscriber (comp. section 3.2.3) may be reused if it is not older than five (5) years and the verified names have not changed. In any other case the subscriber must undergo a new identification as per section 3.2.3.

3.4 Identification and authentication for revocation request

The subscriber should be furnished with an adequate procedure, should he wish to revoke a certificate at the Grid-CA or responsible RA. The request for revocation of a certificate may be communicated by telephone, with submission of authorization information as agreed with the Grid-CA or RA, or in hand written form. Under certain circumstances, revocation may also be effected by electronic means; details are given in the associated CPS.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate application

4.1.1 Who can submit a certificate application

Within the DFN-PKI Grid certificates can be issued to subscribers who meet the conditions specified in section 1.3.3.

4.1.2 Enrollment process and responsibilities

The Grid-CA can only generate a certificate after the enrollment process at the Grid-CA or appropriate RA has been successfully concluded. The minimum requirement for documentation of the enrollment process for natural persons consists of:

- The certificate application
- The declaration of the sole and exclusive ownership of the private key

Legal persons must furnish further information or documents according to the provisions of section 3.2 (clauses a - c).

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

The appropriate RA or the Grid-CA will perform the identification, authentication and authorization of a subscriber in accordance with the procedures set forth in section 3.2.

4.2.2 Approval or rejection of certificate applications

The certificate application will be accepted by the appropriate RA or the Grid-CA if the following criteria have been met:

- Submission of all requisite documents (comp. section 4.1.2)
- Payment of the fixed fee (if applicable) (comp. section 9.1)

After compliance with the above-mentioned criteria has been ascertained, and after the identification and authentication of the subscriber has been successfully concluded, the Grid-CA will further process the certificate application.

Should compliance with the above-mentioned criteria not be ascertained, or should the identification and authentication of the subscriber not be verified, the certificate application shall not be forwarded for further processing. The subscriber is to be notified of the same with statement of reasons thereto.

4.2.3 Time to process certificate applications

Time to process certificate applications will in principal not exceed one week.

4.3 Certificate issuance

After receipt and successful verification (comp. section 4.3.1) of a certificate application, the Grid-CA will issue a certificate and inform the subscriber of its issuance (comp. section 4.3.2).

4.3.1 CA actions during certificate issuance

The formal conditions on which the issuance of a certificate depend will be verified in the appropriate manner by the Grid-CA. Further verifications will not take place. Details are given in the associated CPS.

4.3.2 Notification to subscriber by the CA of issuance of certificate

Once a certificate has been issued, the Grid-CA will communicate it in a proper manner to the subscriber and/or notify the subscriber about its issuance. Should personal data which are not an integral part of the certificate be electronically stored or transmitted, appropriate measures to protect them must be put in place. Details are given in the associated CPS.

4.4 Certificate acceptance

The subscriber is obliged to verify the correctness of his own certificate and that of the Grid-CA once he has received it.

4.4.1 Conduct constituting certificate acceptance

A certificate is accepted by a subscriber if the certificate is used, or no objection is raised within the time frame specified in the CPS. The Grid-CA shall take immediate action to revoke any certificates that have been issued incorrectly.

4.4.2 Publication of the certificate by the CA

Any certificate issued by the Grid-CA will be published in the public directory. The provisions of section 2.3 apply.

4.4.3 Notification of certificate issuance by the CA to other entities

Normally no provision is made for the notification of other entities. Any provision that is made will be given in the CPS.

4.5 Key pair and certificate usage

The area of application for a certificate issued under this CP is given in section 1.4.

4.5.1 Subscriber private key and certificate usage

By accepting the certificate the subscriber assures all participants of the DFN-PKI Grid and all parties relying on the trustworthiness of the information contained in the certificate that

- a basic understanding exists of the use and purpose of certificates,
- all data and statements given by the subscriber with relation to the information contained in the certificate are truthful and accurate,
- no unauthorized person has or will ever have access to the private key,
- the private key will be maintained in a safe and secure manner, i.e. a private key
    - belonging to a **server, service or machine certificate** may be stored without a password but must be adequately protected by system methods;
    - belonging to a **user certificate** must be stored in accordance with the Guidelines on Private Key Protection [PKP], that is either
        - on a secure hardware token from which it cannot be extracted, protected by a password; or

- on a local file system on an appropriate computer system of which the user is the sole user and administrator, where the key must only ever stored persistently in encrypted form; or
- on a local or networked file system on an appropriate computer system that is administered by the user's home organization, protected by a password. In this case
  - the key must only ever stored persistently in encrypted form,
  - data needed to decrypt or use the private key must not be held by the system on persistent storage, and must not be held by the system administrators. It must only be present in the system as a result of a user action, and only for as long as the user is using the system. The activation data and any plain text private keys should be removed as soon as the user stops using the service, and must not be kept past 24 hours of inactivity,
  - administrative access must be limited to designated individuals who are subject to and aware of applicable privacy rules and a professional code of conduct,
  - the private key shall not be sent in clear text over a network,
  - the password shall not be sent in clear text over a network,
  - the encrypted private key file should not be sent over the network unprotected. Network protections may be via encryption, or by physical control of the network in a trusted environment,
  - the system should not persistently keep passwords or plain text private keys for longer than 24 hours;

  or
- on a local or networked file system on an appropriate computer system that is administered by a third party, provided that
  - the key must only be stored persistently in encrypted form,
  - data needed to decrypt or use the private key must not be held by the system on persistent storage, and must not be held by the system administrators. It must only be present in the system as a result of a user action, and only for as long as the user is using the system. The activation data and any plain text private keys should be removed as soon as the user stops using the service, and must not be kept past 24 hours of inactivity,
  - administrative access to the storage system must be limited to designated individuals. These persons must be subject to and aware of applicable privacy rules and a professional code of conduct,
  - the host organization must have a defined data privacy and security policy,
  - the systems must be located in a secured environment, where access is controlled and limited to only authorized personnel,
  - the private key shall not be sent in clear text over a network,
  - the password shall not be sent in clear text over a network,
  - the encrypted private key file should not be sent over the network unprotected. Network protections may be via encryption, or by physical control of the network in a trusted, access-controlled environment.

  When using software tokens to store the private key it must be protected with a strong password following current practice in choosing high quality passwords;
- belonging to an **automated client certificate** must be stored in accordance with the Guideline on Approved Robots [ROBOTS], that is either
  - inside a Crypto Token or HSM or
  - on a local file system on an appropriate computer system to which only people responsible for the automated client's operations have access and to which no other people have any access, either privileged or unprivileged.

The computer system where a private key belonging to an automated client's certificate is stored must be appropriately secured and actively monitored for security events; and it must be located in a secured room where access is controlled and limited to only authorized personnel.

A private key belonging to an automated client's certificate should not

- be left in plain-text format for extended periods of inactivity,
- be sent over any kind of network unprotected,

and the private key and activation data must not be sent in clear text over any kind of network;

- the certificate will solely and exclusively be put to such uses as are in accordance with this Certificate Policy;
- immediate action will be undertaken on the subscriber's part to revoke the certificate should information in the certificate no longer prove to be correct or should the private key go missing, be stolen, or in any other way be compromised, and
- with exception of proxy-certificates, issuance of further certificates is effected only by the Grid-CA.

4.5.2 Relying party public key and certificate usage

Every person using a certificate issued within the framework of this CP for verification of a signature or for purposes of authentication or encryption

- must verify the validity of the certificate before using it,
- must use the certificate solely and exclusively for authorized and legal purposes in accordance with this CP, and
- should have a basic understanding of the use and purpose of certificates

4.6 Certification renewal

Renewal of certification involves the issuance of a new certificate to the subscriber by the Grid-CA without changing the old key pair, provided that the encryption procedures satisfy the provisions of the associated CPS section 6.1.5. The information contained in the certificate must be without change or modification, and there must be no suspicion of compromise to the private key. Once the new certificate is issued the old certificate will be revoked.

Certificates (and private keys) managed in a software based token should only be re-keyed, not renewed. Certificates associated with a private key restricted solely to a hardware token may be renewed for a period of up to five (5) years (for equivalent RSA key lengths of 2048 bits) or three (3) years (for equivalent RSA key lengths of 1024 bits).

4.6.1 Circumstances for certificate renewal

Application for certificate renewal can only be made when the term of a certificate expires.

4.6.2 Who may request renewal

Renewal of a certificate must always be requested by the subscriber. It is incumbent on the Grid-CA to decide whether it will actively support a renewal of certificate.

4.6.3 Processing certificate renewal requests

The processing of certificate renewal requests is conducted in accordance with the provisions of section 4.3. The provisions of section 3.3 govern the procedures for identification and authentication for certificate renewal.

4.6.4 Notification of new certificate issuance to subscriber

The provisions of section 4.3.2 apply.

4.6.5 Conduct constituting acceptance of a renewal certificate

The provisions of section 4.4.1 apply.

4.6.6 Publication of the renewal certificate by the CA

The provisions of section 4.4.2 apply.

4.6.7 Notification of certificate issuance by the CA to other entities

The provisions of section 4.4.3 apply.

4.7 Certificate re-key

Basically, the provisions of section 4.6 apply here. However, in the case of a re-key a new key pair will be used.

4.8 Certificate modification

Certificate modification may be conducted in the case that information contained in a certificate has changed. Should the name of the subscriber have changed, the procedure is the same as for a new request. However, the provisions of sections 4.6 and 4.7 may be applied, if the characteristics specified in section 3.2.3 are still the same. Once the new certificate has been issued, the old certificate will be revoked.

4.9 Certificate revocation and suspension

This section explains the circumstances under which a certificate should be revoked. No provision is made for the suspension (temporary invalidity) of certificates. Once a certificate has been revoked, it may not be renewed or extended.

4.9.1 Circumstances for revocation

Certificates must be revoked by the Grid-CA should at least one of the following circumstances be known:

- A certificate contains data that is no longer valid.
- The private key of a subscriber has been changed, lost, stolen, published or compromised and/or misused in any other manner.
- The subscriber has lost the grounds for entitlement (comp. section 1.3.3).
- The subscriber does not comply with the terms and conditions of the CP.
- The Grid-CA or RA does not comply with the terms and conditions of the CP or the CPS.
- The subscriber no longer needs a certificate.
- The certification service is discontinued.

4.9.2 Who can request revocation

Generally, revocation of certificates can always only be effected by the Grid-CA. If no limitations are imposed by the CPS, any subscriber may request, without furnishing any reasons for the request, the Grid-CA to revoke the same on his behalf. Acceptance of a revocation of a certificate is predicated on the successful identification and authentication of the subscriber in accordance with section 3.4

4.9.3 Procedure for revocation request

If the conditions precedent to acceptance of the request (comp. section 4.9.2) are met, the certificate will be revoked.

4.9.4 Revocation request grace period

Should circumstances for revocation of a certificate exist (comp. section 4.9.1), the subscriber is obliged to notify the Grid-CA immediately of the same, and to initiate revocation of the certificate.

4.9.5 Time within which CA must process the revocation request

The Grid-CA will process a request for the revocation of a certificate within one working day if the conditions precedent to acceptance of the request (comp. section 4.9.2) are met.

4.9.6 Revocation checking requirement for relying parties

The provisions of section 4.5.2 apply.

4.9.7 CRL issuance frequency

The provisions of section 2.3 apply.

4.9.8 Maximum latency for CRLs

The provisions of section 2.3 apply.

4.9.9 On-line revocation / status checking availability

The Grid-CA must provide an on-line procedure with which the validity of a certificate may be verified. This procedure must cover the whole range of certificates issued by the Grid-CA. CRLs are available from the URL given in the associated CPS section 2.1.

4.9.10 On-line revocation checking requirements

Prior to every usage of the certificate, its validity should be checked. The relevant standards are given in section 7.2 (CRL Profile) and section 7.3 (OCSP Profile) of the CPS.

4.9.11 Other forms of revocation advertisements available

Currently no other forms of revocation advertisements are available.

4.9.12 Special requirements re key compromise

Should a private key become compromised, the certificate so affected shall immediately be revoked. Should the private key of the Grid-CA become compromised, all certificates issued by the same shall be revoked.

4.9.13 Circumstances for suspension

Suspension of certificates is not supported.

4.9.14 Who can request suspension

Not applicable.

4.9.15 Procedure for suspension request

Not applicable.

4.9.16 Limits on suspension period

Not applicable.

4.10 Certificate status services

Certificate status services are not supported by the Grid-CA.

4.11 End of subscription

The term of the contractual relationship is given by the period of validity as indicated in the certificate.

The minimum period for the archiving of documents and certificates corresponds to the period of validity of the certificate of the Grid-CA with the addition of a further period of one year.

4.12 Key escrow and recovery

The Grid-CA does not support key escrow and recovery.

4.12.1 Key escrow recovery and policy practices

Not applicable.

4.12.2 Session key encapsulation and recovery policy and practices

Not applicable.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

Regulation of this is given in the associated CPS. Individual sectors may have their own documentation whose publication is non-mandatory.

6 TECHNICAL SECURITY CONTROLS

Regulation of this is given in the associated CPS.

7 CERTIFICATE, CRL, AND OCSP PROFILES

Regulation of this is given in the associated CPS.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The Grid-CA is obliged to ensure that all its procedures and processes are carried out in compliance with the provisions of this CP and the appropriate CPS. The compliance audit of the Grid-CA will be effected by the DFN-Verein. A compliance audit carried out by a certification authority which is accredited by the EUGridPMA is acceptable.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

If services rendered by the Grid-CA are liable for costs, fees are given in a Price List. This may be downloaded from the contact address indicated in section 1.5.

9.2 Financial responsibility

No provision is made for insurance or warranty coverage.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

All information about participants and requesters which does not fall within the provisions of section 9.3.2 shall be deemed as confidential. Such information also includes business plans, marketing/distribution information, information about business partners and all information disclosed during the enrollment process.

9.3.2 Information not within the scope of confidential information

All information contained in the issued certificates and Certificate Revocation Lists (CRLs) including all information which can be derived from such shall be deemed as non-confidential.

9.3.3 Responsibility to protect confidential information

The Grid-CA bears the responsibility of protecting confidential information and ensuring that it will not be compromised. Data may only be communicated to third parties within a delivery of services if prior to their communication a Non-Disclosure Agreement (NDA) has been signed, and all employees associated herewith have undertaken to comply with legal regulations pertaining to data protection.

9.4 Privacy of personal information

9.4.1 Privacy plan

In the course of its duties the Grid-CA has to electronically store and process personal data. All such actions must be performed in accordance with German laws on data security and privacy [BDSG] and §14 of the German Electronic Signature Act [SigG]. Furthermore, all provisions of section 9.3 apply.

9.4.2 Information treated as private

For personal information the provisions of section 9.3.1 apply respectively.

9.4.3 Information not deemed private

For personal information the provisions of section 9.3.2 apply respectively.

9.4.4 Responsibility to protect private information

For personal information the provisions of section 9.3.3 apply respectively.

9.4.5 Notice and consent to use private information

The subscriber agrees to the usage of personal information by the Grid-CA if required in the course of its operations. Furthermore, all information not treated as confidential may be disclosed (comp. section 9.4.3).

9.4.6 Disclosure pursuant to judicial or administrative process

The Grid-CA governed by the law of the Federal Republic of Germany and are obliged to release confidential and personal information to state authorities upon presentation of appropriate orders in accordance with applicable law.

9.4.7 Other information disclosure circumstances

No provision is made for other information disclosure circumstances.

9.5 Intellectual property rights

The intellectual property rights for the CP and the associated CPS are held by the DFN-Verein.

9.6 Representations and warranties

9.6.1 CA representations and warranties

It is incumbent on the Grid-CA to carry out all duties contained in this CP and its associated CPS with proper diligence.

9.6.2 RA representations and warranties

It is incumbent on the Grid-CA and on every RA acting on its behalf to carry out all duties contained in this CP and its associated CPS with proper diligence.

9.6.3 Subscriber representations and warranties

The provisions of sections 4.5.1 and 9.2 apply.

9.6.4 Relying party representations and warranties

The provisions of sections 4.5.1 and 9.2 apply.

9.6.5 Representations and warranties of other participants

Should other participants be involved in the certification process as service providers, it is incumbent on the Grid-CA to ensure compliance on the part of such other participants with the duties of this CP.

9.7 Disclaimers of warranties

Disclaimers of warranties are regulated in the contractual agreement between the concerned parties.

9.8 Limitations of liability

Limitations of liability are regulated in the contractual agreement between the concerned parties.

9.9 Indemnities

Indemnities are regulated in the contractual agreement between the concerned parties.

9.10 Term and termination

9.10.1 Term

This CP and its associated CPS - in their respective current versions – become effective the day when published via the information service (comp. section 2.2) of the Grid-CA.

9.10.2 Termination

This document will remain in force until it is replaced by a new version, or the Grid-CA ceases operations.

9.10.3 Effect of termination and survival

The termination of the CP and its associated CPS shall be without prejudice to the responsibility to protect confidential and personal information.

9.11 Individual notices and communications with participants

The Grid-CA may distribute individual notices other than those specified in the provisions of this CP.

9.12 Amendments

An amendment to a Policy can only be effected by the DFN-Verein. Details are given in section 1.5 of the associated CPS.

9.13 Dispute resolution provisions

None

9.14 Governing law

The CP, the CPS and the operations of the DFN-PKI Grid are all governed by the law of the Federal Republic of Germany.

9.15 Compliance with applicable law

The DFN-Verein makes no claim either to being a certification service provider in the sense laid down by the German Electronic Signature Act [SigG] or to issuing qualified certificates. The DFN-Verein rather issues certificates with which advanced electronic signatures may be created in accordance with the provisions of the German Electronic Signature Act. Under certain circumstances these could be deemed by the presiding judge as constituting evidence to be presented before the court.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

All provisions made in this CP and the associated CPS apply for the Grid-CA and its subscribers. Agreements or supplementary agreements by word of mouth are not allowed.

9.16.2 Assignment

None

9.16.3 Severability

Should individual provisions of this CP and the associated CPS prove to be ineffective or incomplete, this shall be without prejudice to the effectiveness of all other provisions.

The ineffective provision will be replaced by an effective provision deemed as most closely reflecting the sense and purpose of the ineffective provision. In the case of incomplete provisions, amendment will be agreed as deemed to correspond to what would have reasonably been agreed upon in line with the sense and purposes of this CP and the associated CPS, had the matter been considered beforehand.

9.16.4 Enforcement (attorney's fees and waiver of rights)

Legal disputes arising from the operation of the Grid-CA shall be governed by the law of the Federal Republic of Germany. Place of fulfillment and sole place of jurisdiction is the registered office of the respective operator.

9.17 Other provisions

None

10 REFERENCES

[BDSG] German Data Security and Privacy Act, The Federal Law Gazette I 2003 p. 66 (Datenschutzgesetz, Bundesgesetzblatt I 2003 S.66)

[BNetzA] Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railway (Bundesnetzagentur, BNetzA); Notification in accordance with the Electronic Signatures Act and the Electronic Signatures Ordinance – Suitable Algorithms, Federal Gazette No. 30, p.2537-2538, 13.02.2004 (Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung – Geeignete Algorithmen, Regulierungsbehörde für Telekommunikation und Post, Bundesanzeiger Nr. 30, S.2537-2538, 13.02.2004)

[DFN-Charter] Satzung des DFN-Vereins, http://www.dfn.de/de/verein/

[CP-Grid] Certificate Policy (CP) – Security Level Grid, Version 1.6, DFN-Verein, 2012

[CPS-Grid] Certification Practice Statement of the Certification Authority within the Public Key Infrastructure in the Deutsche Forschungsnetz - Grid -, Version 1.6, DFN-Verein, 2012

[EUGridPMA] Authentication Profile for Classic X.509 Public Key Certification Authorities with secured infrastructure, The European Grid Authentication Policy Management Authority, Version 4.3, 2010, http://www.eugridpma.org/guidelines/

[GFD.125] GFD-C.125 Grid Certificate Profile, CAOPS-WG, Open Grid Forum, 2008

[IT-GSCAT] IT-Grundschutz Catalogues (IT-Grundschutz-Kataloge), German Federal Office for Information Security https://www.bsi.bund.de/ContentBSI/EN/Topics/ITGrundschutz/itgrundschutz.html

[PKP] Protection of private key data for end-users in local and remote systems, Version 1.2, The European Grid Authentication Policy Management Authority, 2011

[PKCS] Public Key Cryptography Standards, RSA Laboratories, RSA Security Inc., http://www.rsa.com/rsalabs/

[PKIX] RFCs and specifications of the IETF Working Group Public Key Infrastructure (X.509)

[RFC3647] Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, Network Working Group, IETF, 2003

[RFC3820] Internet X.509 Public Key Infrastructure, Proxy Certificate Profile, Network Working Group, IETF, 2004

[RFC5280] Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, Network Working Group, IETF, 2008

[ROBOT] Guideline on Approved Robots, Version 1.0, The European Grid Authentication Policy Management Authority, 2010

[SigG] Law Governing Framework Conditions for Electronic Signatures and Amending Other Regulations, The Federal Law Gazette I 2001, p. 876 (Gesetz über Rahmenbedingungen für elektronische Signaturen, Bundesgesetzblatt I 2001, S. 876)

[X.509] Information technology - Open Systems Interconnection - The Directory: authentication framework, Version 3, ITU, 1997

11 GLOSSARY

	Meaning
CA	Certification Authority
Certificate	Certificate – Allocation of a cryptographic key to an identity signed by a CA
CN	Common Name – Part of Distinguished Name (comp. DN)
CRL	Certificate Revocation List
CP	Certificate Policy
CPS	Certification Practice Statement
CSR	Certificate Signing Request
DC	Domain Component
DER	Distinguished Encoding Rules (ASN.1 data)
DFN	The National Research and Education Network in Germany
DN	Distinguished Name
DNS	Domain Name System
DS	Digital Signature
EXT	External
GRP	Group
HSM	Hardware Security Module
I	Issuer
LDAP	Lightweight Directory Access Protocol
O	Organization
OCSP	Online Certification Status Protocol
OID	Object Identifier
OU	Organizational Unit
PCA	Policy Certification Authority
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standard [PKCS]
PKCS#7	Cryptographic Message Syntax Standard
PKCS#10	Certification Request Syntax Standard
PKI	Public Key Infrastructure
PN	Pseudonym
PSE	Personal Secure Environment
PKIX	Public Key Infrastructure (X.509) [PKIX]
RA	Registration Authority
Robot	Robot / Automated client certificate
S	Subject
SSL	Secure Socket Layer
X.509v3	International standard for the definition of electronic certificates (Version 3)