DFN-PKI

DFN
Deutsches
Forschungsnetz

Certificate Policy and Certification Practice Statement of the

Public Key Infrastructure in the

Deutsche Forschungsnetz

- SLCS -

DFN-Verein

DFN-SLCS CP/CPS
Version 1.1
Mai 2009

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.

Besides other services the DFN-Verein has established a Public Key Infrastructure in the Deutsche Forschungsnetz (DFN-PKI) and a Shibboleth [SHIBBOLETH] based federated Authentication and Authorisation Infrastructure in the Deutsche Forschungsnetz (DFN-AAI).

Within the DFN-PKI several security levels are offered. The DFN-PKI for the security level "Short-Lived Credential Service" (SLCS) will hereinafter be referred to as DFN-PKI SLCS or shorter DFN-SLCS. The certification authority within the DFN-SLCS which issues X.509 [X.509] short-lived certificates with a lifetime of less than one million seconds (roughly 11.5 days) will hereinafter be referred to as DFN-SLCS-CA.

The DFN-SLCS-CA is a Shibboleth service provider within the DFN-AAI federation, delivering short-lived certificates to authenticated and authorized users of the DFN-AAI federation.

1.1 Overview

This document contains the combined Certificate Policy (CP) and Certification Practice Statement (CPS) of the DFN-SLCS with its DFN-SLCS-CA.

This combined CP/CPS incorporates the requirements of RFC 3647 [RFC3647] and of the *Authentication Profile for SLCS X.509 Public Key Certification Authorities with Secured Infrastructure* version 2.1 - Object Identifier 1.2.840.113612.5.2.2.3.2.1 - of the International Grid Trust Federation [IGTF-AP-SLCS].

This combined CP/CPS of the DFN-SLCS defines the framework conditions for the issuance of certificates for the security level SLCS in accordance with the international standard X.509.

Certificates for the security level SLCS will be solely issued on the basis of this CP/CPS; the statements made herein are binding on all subscribers and registration authorities within the DFN-SLCS and the DFN-SLCS-CA in so far as they do not infringe legal regulations.

1.2 Document name and identification

Identification

a) Title: Certificate Policy and Certificate Practice Statement of the Public Key Infrastructure in the Deutsche Forschungsnetz – SLCS –
b) Version: 1.1
c) Object Identifier (OID) assigned: 1.3.6.1.4.1.22177.300.3.1.6.1.1 [DFN-SLCS-CP-CPS-OID]
d) Composition of the OID:

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

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 related to research and science in Germany.

The term "DFN-SLCS participant" refers to a DFN-site already participating in the DFN-AAI that subscribes to the DFN-SLCS by signing the DFN-SLCS agreement and therefore agreeing and accepting this CP/CPS document.

The term "user" refers to an individual person who is a member of a DFN-site.

The term "SLCS registration authority" or "SLCS-RA" refers to a registration authority (RA) of a DFN-SLCS participant. Staff members of the SLCS-RA perform identity vetting and authorisation checking of users, and based on that, the creation of users' DFN-AAI accounts by registering the users' identity and authorization data in the underlying Identity Management System (IDMS) according to the requirements stated in this CP/CPS. The SLCS-RA is also responsible to maintain this data over time. See section 1.3.2.

The term "registered user" refers to a user with a valid DFN-AAI account who is allowed to request certificates from the DFN-SLCS-CA, see section 4.1. Identity vetting and maintenance of the registered user's DFN-AAI account and identity data in the underlying IDMS must be performed by the SLCS-RA responsible.

The term "subscriber" refers to a registered user who has obtained a certificate from the DFN-SLCS-CA, see section 1.3.3.

1.3.1 Certification authorities

A single on-line root certification authority (DFN-SLCS-CA) is used for issuing short-lived certificates with a maximum lifetime of one million (1000000) seconds (which is about 11.5 days) for registered users of the DFN-AAI. The DFN-SLCS-CA is set up as Shibboleth service provider within the DFN-AAI federation, delivering short-lived certificates to authenticated and authorized users of the DFN-AAI federation.

1.3.2 Registration authorities

Any DFN-site that participates in the DFN-AAI may subscribe to the DFN-SLCS by signing the DFN-SLCS participants agreement accepting this DFN-SLCS CP/CPS document.

A DFN-SLCS participant must establish, staff and operate a SLCS-RA which is typically located within the DFN-SLCS participant's organization.

DFN-AAI account and authorization data of registered users in the DFN-SLCS participant's Identity Provider and the underlying IDMS must be well maintained by staff members of the SLCS-RA.

The DFN-SLCS participant and its SLCS-RA must ensure that the quality and maintenance level of the IDMS, its servers and its contained data is high.

To ensure that this high quality and maintenance level is in the best interest of the DFN-SLCS participant itself, the DFN-SLCS participant must use the underlying IDMS for on-line authentication and authorisation purposes to protect valuable resources of the organization like e.g. access to internal human resources (HR) databases, student grant management application processing systems or student on-line exam registration and marking systems or user log-ons.

For users of DFN-sites that are not DFN-SLCS participants the DFN-Verein operates the "DFN-SLCS Virtual Home Organization" SLCS-RA (short DFN-SLCS-VO-RA) and its associated Shibboleth based Identity Provider within the DFN-AAI federation. Staff members of the DFN-SLCS-VO-RA are specifically trained and appointed employees of the DFN-Verein or organizations named in section 1.5.1.

The DFN-SLCS-CA supports multiple SLCS-RAs with their associated Shibboleth based Identity Providers which are adhering to the minimum requirement in regards to the registration of users set forth in this CP/CPS document, see section 3.2.

The DFN-SLCS-CA will automatically issue short-lived user certificates to registered users based on an on-line application for such a short-lived user certificate after a successful authentication and authorisation of that registered user at his Identity Provider within the DFN-AAI federation (see section 3.2 d).

1.3.3 Subscribers

Subscribers are all registered users who have obtained a short-lived certificate from the DFN-SLCS-CA.

1.3.4 Relying parties

Relying parties are individuals or organizations using the certificates to verify the identity of subscribers and to secure communication with these subscribers.

Relying parties may or may not be subscribers of the DFN-SLCS-CA.

1.3.5 Other participants

No stipulation.

1.4 Certificate usage

1.4.1 Appropriate certificate usage

Certificates issued by the DFN-SLCS-CA are intended to be used primarily by users in the Grid and e-Science environment.

1.4.2 Prohibited certificate usage

Basically no form of certificate usage is prohibited.

With the exception of proxy certificates [RFC3820], the DFN-SLCS-CA alone may issue further certificates.

1.5 Policy administration

1.5.1 Organization administering the document

This CP is administered by:

DFN-Verein	Phone: +49 30 884299-955
Alexanderplatz 1	Fax: +49 30 884299-70
10178 Berlin	Email: pki@dfn.de
GERMANY	Web: www.pki.dfn.de

Operation of the DFN-SLCS-CA is effected by:

DFN-CERT Services GmbH	Phone: +49 40 808077-580
DFN-PCA	Fax: +49 40 808077-556
Sachsenstraße 5	Email: dfnpca@dfn-cert.de
20097 Hamburg	Web: www.dfn-cert.de
GERMANY	

1.5.2 Contact person

The person responsible for this CP/CPS 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 responsible for reviewing and approving this CP/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.

The review and approval process must assure that this CP/CPS adheres to:

a) Authentication Profile for SLCS X.509 Public Key Certification Authorities with Secured Infrastructure of the IGTF [IGTF-AP-SLCS] and

b) RFC 3647 [RFC3647]

1.5.5 Modification of the CP/CPS

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

Whenever there is a change in this CP/CPS the OID of the document must change and the major changes must be announced to the EUGridPMA [EUGridPMA] and approved before issuing any certificates under the new CP/CPS. All the CP/CPS documents under which valid certificates are or have been issued will be available via the service stated in section 2.2.

1.6 Definitions and acronyms

See Glossary.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

The DFN-SLCS-CA offers a repository allowing on-line access to the DFN-SLCS-CA certificate and its fingerprint, the most currently issued Certificate Revocation List (CRL) and to all CP/CPS documents under which valid certificates are or have been issued. The repository can be reached at http://www.pki.dfn.de.

2.2 Publication of certification information

The DFN-SLCS-CA makes the following information available:

a) root CA certificate and its fingerprint

b) current CRL

c) past and current CP/CPS documents

Moreover, information may be offered to subscribers concerning the DFN-SLCS, the correct usage of cryptography and the deployment of certificates.

2.3 Time or frequency of publication

Newly issued CRLs, CP/CPS and any other required information will be published promptly. The following frequency of publication applies:

a) CRLs: immediately after the DFN-SLCS-CA issues a new CRL

b) CP/CPS: as required

c) 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 access 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 short-lived end entity certificates issued by the DFN-SLCS-CA will always start with C=DE, O=GridGermany, OU=SLCS.

3.1.1 Types of names

All certificates issued by the DFN-SLCS-CA 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 subscribers in a PKI hierarchy may be referenced.

The subject name in certificates issued by this CA is constructed based on the registered user's attributes as provided by his Identity Provider responsible.

The certificate's name of a DFN-SLCS-CA subscriber is always modelled on the following pattern:

C=DE

O=GridGermany

OU=SLCS

OU=<unique representation of the name of the DFN-SLCS participant
assigned to the Identity Provider of the registered user>

[OU=<additional unique organizational unit name
assigned to the Identity Provider of the registered user> ...]

CN=<common name>

All organizational unit (OU) attribute values are assigned per Identity Provider by the DFN-SLCS-CA ensuring a unique name space.

The optional OU attribute may be present one or several times and if present contains further organizational unit entity name(s) assigned by the DFN-SLCS-CA to the DFN-SLCS participant's IdP.

If the Identity Provider of the registered user is the DFN-SLCS Virtual Home Organization, the second OU attribute is set to "DFN-SLCS Virtual Home Organization" and no further OU attributes are set.

The common name (CN) is composed of the given name(s) and the surname(s) as provided by the Identity Provider of the registered user, a hyphen character "-" and the eduPersonPrincipalName (epPN) attribute [EDUPERSON] of the registered user as provided by his Identity Provider: CN="<given name(s)> <surname(s)> - <epPN>".

The epPN attribute definition of the DFN-AAI is described in the attribute specification document available at http://www.aai.dfn.de:

DFN-AAI attribute specification of eduPersonPrincipalName

DFN-AAI attribute name:	eduPersonPrincipalName (epPN)
Description:	a person's net ID
Inherits from object class:	eduPerson [EDUPERSON]
Semantic:	The value consists of a left and a right part separated by an @ character, e.g. user@pki.dfn.de, where the right part describes a domain, which is usually officially registered in the DNS and the left part describes the unique ID within this domain

LDAP syntax (RFC 2252):	DirectoryString [RFC2252]
Numbers of values:	1
Classification:	essential for DFN-AAI Identity Providers
Comments:	Unlike the mail attribute the value of the epPN attribute does not necessarily need to be a working email address which is assigned to the person described in this directory entry. This is the place to implement a persistant ID - subject to the sale of the domain.
Example:	eduPersonPrincipalName: john.doe@pki.dfn.de eduPersonPrincipalName: jhdo123@pki.dfn.de
Usage:	The eduPersonPrincipalName is often used in (internal) applications if the user must be uniquely identified and a pseudonym is not a strong enough identification, e.g. for writing access to wikis, forums or repositories.

The epPN attribute value is constructed from a user-id part and a domain part separated by an @ character: <user-id>@<domain>, e.g. john.doe@pki.dfn.de.

An email address is included in the certificate extension "SubjectAlternativeName", see section 7.1.

3.1.2 Need for names to be meaningful

The subject name is meaningful in the sense that it is obtained from the registered user's attribute "eduPersonPrincipalName" and the assigned name of the DFN-SLCS participant.

The SLCS-RA is able to name and identify the registered user it assigned these "eduPersonPrincipalName" attribute values.

3.1.3 Anonymity or pseudonymity of subscribers

The DFN-SLCS-CA does not issue certificates that allow for anonymity or pseudonymity of subscribers.

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.

Email addresses and epPN attributes contain an "@" character to separate the user part from the domain part.

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.

3.1.5 Uniqueness of names

The uniqueness of the subject name (SubjectDN) of valid certificates is guaranteed by a combination of:

a) The assigned unique name of the DFN-SLCS participant as well as optionally further unique organizational unit names are present in the subject field. These parts of the subject name are assigned and administered by the DFN-SLCS-CA providing the DFN-SLCS participant with an unique name space prefix consisting of C, O, OU, OU [, OU ...] attributes as described in section 3.1.1.

b) The CN attribute which is part of the subject name is filled with the given name(s), the surname(s) and the value of the eduPersonPrincipalName attribute of the registered user's DFN-AAI account provided by his Identity Provider. The DFN-SLCS participant and its SLCS-RA are guaranteeing that the eduPersonPrincipalName attribute values are assigned persistently and uniquely to a single registered user over the lifetime of their assigned name space prefix.

3.1.6 Recognition, authentication and role of trademarks

It is the responsibility of the subscriber and the DFN-SLCS participant responsible to ensure that the choice of name (OU and CN attributes) does not infringe any law pertaining to trademarks, brand names etc. The DFN-SLCS-CA is not obliged to verify compliance with such legal prescriptions. It is solely incumbent on the subscriber and the DFN-SLCS participant responsible to ensure such compliance. Should the DFN-SLCS-CA be informed of any infringement of such laws, the affected certificates will be revoked.

3.2 Initial identity validation

A staff member of the SLCS-RA responsible must meet the requesting user in person to perform the initial identity vetting.

Performing a registration of an user the SLCS-RA must ensure that

a) the identity vetting of the user and identity data thereof recorded meet the requirements specified in section 3.2.3

b) the user has or gets a valid DFN-AAI account within the Identity Provider/IDMS of the SLCS-RA

c) it has included or includes the given name(s) and the surname(s) values of the registering user into the appropriate attributes (givenName, surName) of the registering user's DFN-AAI account

d) it has assigned or assigns and includes a unique and persistent value of the form <user-id>@<domain> into the eduPersonPrincipalName (epPN) attribute [EDUPERSON] of the registering user's DFN-AAI account

e) it assigns and includes the value "urn:geant:dfn.de:dfn-pki:slcs" [SLCS-URN] into the eduPersonEntitlement attribute [EDUPERSON] of the registering user's DFN-AAI account, to generally allow the user access to the DFN-SLCS.

The epPN attribute value assigned to a registered user must be unique during the whole lifetime of the assigned DFN-SLCS participant's name space of the DFN-SLCS-CA. The epPN must not be reused in any other user's identity and authorization data within his DFN-site.

In due course staff members of the SLCS-RA ensure that the DFN-AAI account's identity and authorization data and validity is kept up-to-date up to the standards set forth in section 1.3.2.

3.2.1 Method to prove possession of private key

Possession of the private key is verified for certificates issued by the DFN-SLCS-CA through the verification of the digital signature on the certificate signing request (CSR) as the registered user always generates his own key pair when requesting a certificate.

3.2.2 Authentication of organizational identity

DFN-sites that participate in the DFN-AAI requesting to participate with the DFN-SLCS must prove their organizational identity to the DFN-SLCS during the subscription process. Based

on the authenticated organizational identity a unique name value for the second organizational unit (OU) and further OU attributes, see section 3.1, of issued certificates will be assigned by the DFN-SLCS-CA to the DFN-SLCS participant's Identity Provider.

3.2.3 Authentication of individual identity

When a user first registers with his SLCS-RA responsible which is not the DFN-SLCS-VO-RA the registering user must submit his own official and valid photo ID documents (passport or national ID card with photo) to prove his identity to the SLCS-RA during a personal identification meeting.

In this case the following information details must be recorded:

a) Given name(s) and surname(s) as included in the official identification document
b) Email address
c) Evidence of affiliation to the DFN-SLCS participant

The SLCS-RA may request and record further information of the registering user as it deems appropriate to meet IDMS quality requirements stated in section 1.3.2.

When a user first registers with the DFN-SLCS-VO-RA the registering user must submit his own official and valid photo ID documents (passport or national ID card with photo) to prove his identity to the DFN-SLCS-VO-RA during a personal identification meeting with a staff member of DFN-SLCS-VO-RA.

In this case the following information details must be recorded:

a) Given name(s) and surname(s) as included in the official identification document
b) User registration form with agreement and acceptance of this CP/CPS by handwritten signature
c) Type of official identification document, last five (5) digits of the ID documents serial number
d) Email address

Users who are requesting a DFN-AAI account at the DFN-SLCS-VO-RA do not need to prove their affiliation with an organization to the DFN-SLCS-VO-RA because organizational information is not part of certificates issued for registered users of the DFN-SLCS-VO-RA.

In any case the SLCS-RA responsible can make use of Deutsche Post PostIdent [PostIdent] services to confirm name and photo ID document details as well as to retrieve a handwritten signature from the registering user.

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 (see section 3.2.3). Beyond this requirement, no further information shall be verified.

3.2.5 Validation of authority

DFN-SLCS participants, SLCS-RAs and their Identity Providers must have procedures in place that guarantee the requirements as stated in section 3.2.

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

Certificates issued by the DFN-SLCS-CA are not re-keyed. Thus every certificate request is treated as an initial request.

3.3.2 Identification and authentication for re-key after revocation

Once a certificate has been revoked, it cannot be renewed. A new CSR must be made. In this case the provisions of section 3.2 are applicable.

3.4 Identification and authentication for revocation request

Revocation of a certificate is always effected by the SLCS-RA responsible. The subscriber needs to identify and authenticate himself to his SLCS-RA responsible to request the revocation of his certificate. After successful requesting the revocation the SLCS-RA will forward the revocation request to the DFN-SLCS-CA.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate application

4.1.1 Who can submit a certificate application

Any registered user with a valid DFN-AAI account with an eduPersonEntitlement attribute containing the value "urn:geant:dfn.de:dfn-pki:slcs" at an DFN-SLCS participant can submit a certificate request, see section 3.2.

4.1.2 Enrollment process and responsibilities

The enrollment process used by a user to submit a certificate application is as follows:

a) The user registers with his SLCS-RA responsible to get a DFN-AAI account, see section 3.2.

b) The user logs into the DFN-SLCS with his DFN-AAI account. The DFN-SLCS grants access and sets up a Shibboleth authenticated session if the user is successfully authenticated by his Identity Provider and his DFN-AAI account's eduPersonEntitlement attribute contains the value "urn:geant:dfn.de:dfn-pki:slcs".

c) The user creates a key pair and a CSR and submits the CSR to the DFN-SLCS using the Shibboleth authenticated session.

d) The DFN-SLCS builds the subject DN from the assigned namespace and the attributes provided and assured by the Identity Provider, see section 3.1.1.

All sensitive network communication between the registered users' client, his DFN-site's Identity Provider and the DFN-SLCS are secured by encrypted tunnels using the transport layer security (TLS) protocol with TLS server authentication and Shibboleth authenticated sessions.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

The DFN-SLCS will identify and authenticate the certificate requester based on his successful DFN-AAI login with his DFN-AAI account.

4.2.2 Approval or rejection of certificate applications

DFN-SLCS will approve a CSR automatically if the following criteria are met:

a) The requester has been granted access to the DFN-SLCS after successful authentication at his Identity Provider responsible.

b) The requester's organisation is a DFN-SLCS participant.

c) The requester's DFN-AAI account's eduPersonEntitlement attribute contains the value "urn:geant:dfn.de:dfn-pki:slcs", see section 3.2.

If the requester fails to adhere to any of the above, or in any other way violates the stipulations of this document, the DFN-SLCS will reject the access to request certificates from the DFN-SLCS-CA.

4.2.3 Time to process certificate applications

Certificate requests are processed automatically and in real time.

4.3 Certificate issuance

After receipt and successful verification (see section 4.3.1) of a certificate application, the DFN-SLCS-CA will issue a certificate and deliver it to the subscriber.

4.3.1 CA actions during certificate issuance

CSRs are processed automatically by the DFN-SLCS if the registered user has authenticated himself successfully at his Identity Provider responsible. All steps of this process are logged in real time.

4.3.2 Notification to subscriber by the CA of issuance of certificate

The registered user receives the certificates through the application they are using to request them.

4.4 Certificate acceptance

The subscriber is obliged to verify the correctness of his own certificate once he has received it.

4.4.1 Conduct constituting certificate acceptance

The subscriber accepts the certificate by invoking the application, which requests it in first place.

4.4.2 Publication of the certificate by the CA

Certificates issued by the DFN-SLCS-CA are not published.

4.4.3 Notification of certificate issuance by the CA to other entities

DFN-SLCS may perform notifications.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

Subscribers may use their certificates as they wish, but must observe the following rules:

a) use DFN-SLCS certificates exclusively for legal and authorized intended purposes in accordance with this CP/CPS;

b) only use a DFN-SLCS certificate on behalf of the person, entity or organization listed as the Subject of such a certificate – the Subject describes the only legitimate user of the certificate;

c) refrain from using the subscriber's private key corresponding to the public key certificate to sign other certificates, with the exception of proxy certificates as described in RFC 3820 [RFC3820];

d) realize the importance of properly protecting their private key data as well as their Shibboleth account log-on credentials;

e) immediately cease to use the certificate if any information included in the certificate or if any change in any circumstances would make the information in the certificate misleading or inaccurate, e.g. a change of name(s) or email address(es), and contact the SLCS-RA responsible to get the DFN-AAI account information updated accordingly;

f) notify the SLCS-RA responsible immediately of any suspected or actual compromise of the DFN-AAI account that is used to authenticate against the DFN-SLCS;

g) immediately cease to use the certificate upon (i) expiration of such certificate, or (ii) any suspected or actual compromise of the private key corresponding to the public key in such certificate, or (iii) any suspected or actual compromise of private keys corresponding to public keys in proxy certificates directly or indirectly derived at any level from the DFN-SLCS certificate and remove such certificate from the devices and/or software in which it has been installed;

h) use their own judgement about whether it is appropriate, given the level of security and trust provided by a certificate issued by the DFN-SLCS-CA, to use such a certificate in any given circumstance;

i) comply with all laws and regulations applicable to a subscriber's right to export, import, and/or use a certificate issued by the DFN-SLCS-CA and/or related information. Subscribers shall be responsible for procuring all required licenses and permissions for any export, import, and/or use of a certificate issued by this CA and/or related information.

4.5.2 Relying party public key and certificate usage

Relying parties shall:

a) be held responsible to understand the proper use of public key cryptography and certificates;

b) read and agree to all terms and conditions of this CP/CPS;

c) verify certificates issued by the DFN-SLCS-CA, including use of CRLs, in accordance with the certification path validation procedure as specified in RFC 5280 [RFC5280], taking into account any critical extensions, key usage, and approved technical corrigenda as appropriate;

d) trust and make use of a certificate issued by the DFN-SLCS-CA only if such certificate has not expired and if a proper chain of trust can be established to a trustworthy issuing party;

e) make their own judgement and rely on a certificate issued by the DFN-SLCS-CA only if such reliance is reasonable in the circumstances, including determining whether such reliance is reasonable given the nature of the security and trust provided by a certificate issued by this CA and the value of any transaction that may involve the use of the aforementioned certificates.

4.6 Certification renewal

DFN-SLCS does not support certificate renewal. The subscriber requests a new certificate instead.

4.7 Certificate re-key

Re-keying a certificate is the process where a subscriber or other party generates a new key pair and applies for the issuance of a new certificate that certifies the new public key.

DFN-SLCS does not support certificate re-key. The subscriber requests a new certificate instead.

4.8 Certificate modification

DFN-SLCS does not support certificate modification. The subscriber requests a new certificate instead.

If the subscriber wants to change identity information contained in certificate data, he/she must contact his SLCS-RA responsible to get the changed information verified and updated in the underlying IDMS by his SLCS-RA responsible before requesting a new certificate from the DFN-SLCS.

4.9 Certificate revocation and suspension

This section explains the circumstances under which a certificate should be revoked. Once a certificate has been revoked, it must not be renewed or extended.

Suspension of certificates is not supported.

4.9.1 Circumstances for revocation

A valid certificate should be revoked if the key material it is based on or its password is compromised or if the DFN-AAI account it is based on got compromised.

A valid certificate should also be revoked if key material or the password of a proxy certificate directly or indirectly derived at any level from the DFN-SLCS certificate got compromised.

If the SLCS-RA gets aware of circumstances that its organization's Identity Provider or the underlying IDMS got compromised, it shall initiate the revocation of all valid certificates that were issued based on DFN-AAI accounts relying on data from the compromised Identity Provider and/or IDMS. In this case the SLCS-RA shall request the suspension of its organization's Identity Provider from the DFN-SLCS until the affected Identity Provider and IDMS are back up in a safe, trusted and secured state.

If a reason for revocation of a certificate is found after the end of the certificates validity period the affected certificate may not be revoked.

4.9.2 Who can request revocation

Generally, revocation of certificates can always only be effected by the DFN-SLCS-CA.

Any subscriber may request, without furnishing any reasons for the request, the SLCS-RA responsible to request the revocation of his certificate by the DFN-SLCS-CA 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.

Additionally a SLCS-RA may request the revocation of certificates which were issued using the Identity Provider of its organization.

Others may request the revocation of a certificate by the DFN-SLCS-CA if and only if they can proof that the DFN-SLCS certificate, the DFN-AAI account it is based on or a derived proxy certificate is compromised.

4.9.3 Procedure for revocation request

If the conditions precedent to acceptance of the request are met, the DFN-SLCS certificate will be revoked.

4.9.4 Revocation request grace period

Should circumstances for revocation of a certificate exist (see section 4.9.1), the subscriber is obliged to notify his SLCS-RA immediately of the same, and to initiate revocation of the certificate.

If a SLCS-RA is aware of circumstances for revocation of certificates based on DFN-AAI accounts of its organization's Identity Provider (see section 4.9.1), the SLCS-RA is obliged to notify the DFN-SLCS-CA immediately of the same, and to initiate revocation of affected certificates.

4.9.5 Time within which CA must process the revocation request

The DFN-SLCS-CA will process a request for the revocation of a certificate within one working day if the conditions precedent to acceptance of the request (see 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

An initial empty CRL is issued by the DFN-SLCS-CA at setup time of this CA.

A new CRL is issued by this CA immediately after a revocation request has been processed.

In any case a new CRL is issued by this CA at the latest five (5) days before the date indicated by the nextUpdate field of the most current CRL.

4.9.8 Maximum latency for CRLs

All CRLs issued by the DFN-SLCS-CA are valid for a maximum of thirty (30) days, as indicated by the time difference of the date values of the lastUpdate and nextUpdate fields of the CRL.

Once a new CRL is issued (see section 4.9.7) it will be published in the repository immediately (see section 2.3).

4.9.9 On-line revocation / status checking availability

The DFN-SLCS-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 DFN-SLCS-CA. CRLs are available via the URL given in 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).

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 of a short-lived end entity certificate become compromised, the certificate so affected shall immediately be revoked.

Should the private key of the DFN-SLCS-CA become compromised, the EUGridPMA is notified immediately to remove the so affected CA certificate from its trust anchor distribution. Additionally available DFN-SLCS-CA archive, log and audit trail data are analyzed to identify as many certificates as possible which have been issued by this CA to revoke these possibly erroneously issued certificates immediately.

4.10 Certificate status services

4.10.1 Operational characteristics

The DFN-SLCS-CA can be reached 24x7 through the Internet.

4.10.2 Service availability

The DFN-Verein provides all services (registration, certification, directory) as 24x7 services with a best-effort approach with minimal scheduled interruption. Due to the nature of the Internet, the DFN-Verein is in no position to guarantee such services. Unscheduled interruptions of these services are possible due to circumstances not under the control of the DFN-Verein.

4.10.3 Optional features

The DFN-SLCS-CA certificate status services do not include or require any additional features.

4.11 End of subscription

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

4.12 Key escrow and recovery

The DFN-SLCS-CA does not support key escrow and recovery.

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 Physical controls

5.1.1 Site location and construction

The technical systems of the DFN-SLCS 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 DFN-SLCS are protected by appropriate technical and infrastructural measures. Access to the operational areas of the DFN-SCLS is restricted to such employees who have been duly authorized by Information Security Officers (ISOs) of the DFN-SLCS. 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

All media shall be stored in locked file cabinets. Media 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

Externally stored backup media is stored in a safe deposit box.

5.2 Procedural controls

All persons with access to the systems hosting the DFN-SLCS will be permanently employed DFN-CERT Services GmbH personnel, which are either trained system administrators or members of its PKI team.

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

DFN-SLCS 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 fulfil, also have in-depth knowledge of the following fields:

a) IT security technology, cryptography, electronic signatures, PKI,

b) International standards, technical standards,

c) National and international law,

d) Unix/Linux operating systems, TCP/IP networks and relational databases.

5.3.2 Background check procedures

For all employees with access to the systems hosting the DFN-SLCS DFN-CERT Services GmbH holds police clearance certificates that are no older than two years.

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

5.3.3 Training requirements

The DFN-SLCS only employs properly qualified staff. In addition, regular retraining programs for all DFN-SLCS 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 DFN-SLCS. 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 DFN-SLCS or the requirements of a specific employee. Job rotation is not mandatory.

5.3.6 Sanctions for unauthorized actions

Unauthorized actions which endanger the security of the IT systems of the DFN-SLCS 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 DFN-SLCS 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 [BDSG].

5.3.8 Documentation supplied to personnel

DFN-SLCS employees are supplied with the following documentation:

a) Combined Certificate Policy (CP) and Certification Practice Statement (CPS)

b) Instruction Manual (available in German):

    a) Services

    b) Security concepts

    c) Process specification and forms for regular operations

    d) Instructions and procedures for emergencies

e) Documentation of IT systems

f) 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 DFN-SLCS, the following measures have been put in place. The following types of events are recorded as log-data or paper audits:

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

5.4.2 Frequency of processing log

Processing data are under regular monitoring and are analysed 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 is set as follows:

a) For data affecting the DFN-SLCS-CA certificate or its private key: three (3) years after the CA certificate expired

b) For data regarding a specific short-lived end entity certificate: three (3) years after the issuing CA certificate expired

c) For data incurring from the IDMSs, Identity Providers and SLCS-RAs at the DFN-SLCS participants:

    a) For data and identification documentation affecting a registered user: three (3) years after the user's DFN-AAI account got deleted or its attribute value "urn:geant:dfn.de:dfn-pki:slcs" permanently removed from its eduPersonEntitlement attribute

    b) For a complete list of ever assigned epPN attribute values to a single registered user: three (3) years after the user's DFN-AAI account got deleted or its attribute value "urn:geant:dfn.de:dfn-pki:slcs" permanently removed from its eduPersonEntitlement attribute

c) All plain epPN attribute values of DFN-AAI accounts of all registered users must be recorded and kept over the whole lifetime of the DFN-SLCS participant's assigned name space

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 (SA).

5.4.5 Audit log backup procedures

In common with all other relevant DFN-SLCS data, audit logs are backed-up on a regular basis. Paper audit logs are stored in locked file cabinets.

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 ISO is to be immediately notified in the event of any serious occurrences. In collaboration with 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 DFN-SLCS 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:

a) Personal data of registered users including their identification details and a complete list of ever assigned epPN attribute values per registered user as provided and archived by the SLCS-RAs
b) Electronic certificate applications, including personal subscriber data as provided by the subscriber's Identity Provider
c) All certificates issued by the DFN-SLCS-CA
d) Revocation requests
e) 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. The key elements of the archive backup procedure are:

a) Incremental backup every working day
b) Weekly full backup
c) 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 ISO is invested with the authority to authorize the downloading and verification of archived data.

5.6 Key changeover

The DFN-SLCS-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 DFN-SLCS-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 the DFN-SLCS-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 analysed. 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 DFN-SLCS 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 DFN-SLCS-CA be compromised, or should reasonable grounds exist for supposing that such compromise has taken place, the ISO of the DFN-SLCS-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:

a) Immediate notification of the EUGridPMA to remove the so affected CA certificate from its trust anchor distribution
b) Immediate notification of all affected subscribers
c) Immediate revocation of all certificates (issued by this CA) whose issuance can be acknowledged by available DFN-SLCS-CA archive, log or audit trail data. If necessary, the repository will be taken off-line in order to preempt incorrect or invalid information being supplied by these services.
d) Generation of a new key pair and new certificate for the CA
e) Publication of the new certificate of the CA
f) Issuance of new certificates for subscribers following the instructions of the ISO

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 ISO.

5.8 CA or RA termination

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

a) Notification of all subscribers, SLCS-RAs and DFN-SLCS participants, the EUGridPMA, and concerned organizations in a period at least three months prior to termination.
b) Timely revocation of all certificates.
c) 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 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 CP/CPS, they should be taken from the appropriate catalog of measures in the IT Baseline Protection Manual [IT-GSHB].

6.1 Key pair generation and installation

6.1.1 Key pair generation

Cryptographic key pairs for the DFN-SLCS-CA are generated on a dedicated IT system directly by and within a Hardware Security Module (HSM). The CA keys are always protected by the HSM.

Cryptographic key pairs for subscribers are generated by the subscribers themselves on systems that the subscribers can access.

6.1.2 Private key delivery to subscriber

Cryptographic key pairs are directly generated on a system that the subscriber accesses. Thus, there is no need to deliver private keys from central DFN-SLCS systems to the subscriber.

6.1.3 Public key delivery to certificate issuer

The certificate requester's CSR formatted as a self-signed PKCS#10 structure will be communicated to the DFN-SLCS-CA by the DFN-SLCS using a secure communication channel (e.g. SSL protected private web pages) after successful authentication by the requester's Identity Provider.

6.1.4 CA public key delivery to relying parties

All relying parties may download the DFN-SLCS-CA public key in Privacy Enhanced Mail (PEM) and PKCS#7 format or in binary (DER) form from the repository (see section 2.1).

6.1.5 Key sizes

The cryptographic algorithms deployed and their key sizes are based on publications of the Federal Network Agency [BNetzA].

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

6.1.6 Public key parameters generation and quality checking

Parameters will be generated by the DFN-SLCS-CA. Great care will especially be given to the selection of parameters for generation of the CA key.

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 (see section 7.1.2).

6.2 Private key protection and cryptographic module engineering controls

6.2.1 Cryptographic module standards and controls

The HSMs used to generate and store CA keys are certified and operated according 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 DFN-SLCS-CA private keys, however PINs for CA keys are split between two distinct CA operator roles to facilitate the dual control principle, see section 6.2.8.

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 the HSM are backed up with mechanisms 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.

Private CA keys or copies thereof can't leave the HSM in unencrypted form.

6.2.5 Private key archival

The archiving of subscribers' private keys is not supported.

6.2.6 Private key transfer into or from a cryptographic module

The CA's private key is generated by and within the HSM and never leaves the HSM activated or unencrypted, see sections 6.1.1 and 6.2.4. Thus the CA's private key is always protected by the HSM.

6.2.7 Private key storage on cryptographic module

The CA's private key never leaves the HSM in unencrypted form, see sections 6.1.1 and 6.2.4. Thus the CA's private key is always protected by the HSM.

6.2.8 Method of activating private key

The private key of the DFN-SLCS-CA is activated by entering a password or a PIN code.

The PIN of the DFN-SLCS-CA private keys is divided into two halves. Activation of the private key of the DFN-SLCS-CA is only possible in accordance with the dual control principle needing two CA operators each of them knowing only one half of the PIN.

6.2.9 Method of deactivating private key

Deactivation of the private key is automatic. Once the certification 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 DFN-SLCS-CA private keys is subject to the dual control principle. The ISO and the CA Operator are needed to destroy the DFN-SLCS-CA private keys.

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 DFN-SLCS-CA have the following periods of validity:

a) DFN-SLCS-CA root certificates: a maximum of ten (10) years

b) All other issued certificates: a maximum of one million (1000000) seconds

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 (see 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 the DFN-SLCS-CA will use activation data composed of a string of at least 15 characters.

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. 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 DFN-SLCS-CA are exclusively carried out using hardened operating systems. In addition, the following security measures will also be implemented:

a) Access controls

b) 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:

a) An annual audit (compliance inspection)

b) Regular inspection and upgrading of the security concept

c) Checking security measures during on-going operations (see section 5.4)

d) Regular monitoring of the integrity of applications and operating systems in use

    a) Centralized logging of all security processes and procedures

    b) Collaboration with DFN-CERT

    c) Applying upgrades and patches when and if required

    d) 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 DFN-SLCS 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. On all firewalls rules are activated which only permit network traffic that is permitted in a defined communication matrix.

6.8 Time-stamping

Not applicable.

7 CERTIFICATE, CRL, AND OCSP PROFILES

This section contains the rules and guidelines followed by the DFN-SLCS-CA for populating X.509 end-entity certificates.

7.1 Certificate profile

7.1.1 Version number(s)

Version of X.509 certificates: Version 3

7.1.2 Certificate extensions

The DFN-SLCS-CA certificate includes the following extensions:

a) basicConstraints: critical; CA=true

b) keyUsage: critical; keyCertSign crlSign bits are set (any others are unset)

c) authorityKeyIdentifier: not critical; value is set to the SHA-1 hash of the BIT STRING subjectPublicKey of the DFN-SLCS-CA certificate

d) subjectKeyIdentifier: not critical; value is set to the SHA-1 hash of the BIT STRING subjectPublicKey of the DFN-SLCS-CA certificate

End-entity certificates include the following extensions:

a) keyUsage: critical; by default, only the digitalSignature, keyEncipherment and dataEncipherment bits are set

b) extendedKeyUsage: not critical; by default, contains the OID for TLS client authentication (id-kp-clientAuth, OID 1.3.6.1.5.5.7.3.2 [PKIX]); may contain other OIDs

c) authorityKeyIdentifier: not critical; value is set to the SHA-1 hash of the BIT STRING subjectPublicKey of the issuing CA's certificate

d) subjectKeyIdentifier: not critical; value is set to the SHA-1 hash of the BIT STRING subjectPublicKey of the end-entity's certificate

e) certificatePolicies: not critical; see section 7.1.6.

f) subjectAlternativeName: not critical; for user certificates, includes an rfc822Name entry with the email address of the end-entity

g) cRLDistributionPoint: not critical; includes one or more HTTP URIs for retrieving the CRL of the issuing CA

h) authorityInfoAccess: not critical; includes one or more entries (of syntax id-ad-caIssuers) with a HTTP URI for retrieving the issuing CA's certificate

i) sAMLX509CertificateExtension (OID 1.3.6.1.4.1.3536.1.1.1.12 [GLOBUS-OID]): not critical; optional; contains SAML assertions as received from the subscriber's Identity Provider responsible.

7.1.3 Algorithm object identifiers

The algorithms with OIDs supported by the DFN-SLCS-CA are:

a) rsaEncryption (OID 1.2.840.113549.1.1.4 [PKIX])

b) sha1WithRSAEncryption (OID 1.2.840.113549.1.1.5 [PKIX])

7.1.4 Name forms

All certificates issued by the DFN-SLCS-CA use X.500 distinguished names as described in section 3.1.1.

The subject name of the CA certificate is /C=DE/O=DFN-Verein/OU=DFN-PKI/CN=DFN SLCS-CA.

7.1.5 Name constraints

All certificates issued by the DFN-SLCS-CA have a subject distinguished name starting with /C=DE/O=GridGermany/OU=SLCS.

7.1.6 Certificate policy object identifier

Certificates issued by the DFN-SLCS-CA include a certificatePolicies extension containing at least the then current OID of this CP/CPS document (as defined in section 1.2) at the time of SLCS certificate issuance as policyIdentifier OID and additionally the OID 1.2.840.113612.5.2.2.3 (Short-lived Credential Services (SLCS) as assigned by the IGTF [IGTF-OID]) as second policyIdentifier OID. Certificates may contain additional policyIdentifier OIDs.

7.1.7 Usage of Policy Constraints extension

No stipulation.

7.1.8 Policy qualifiers syntax and semantics

No stipulation.

7.1.9 Processing semantics for the critical Certificate Policies extension

No stipulation.

7.2 CRL profile

7.2.1 Version number(s)

CRLs are produced in accordance with CRL version 2 format as defined in the international standard X.509 version 3.

7.2.2 CRL and CRL entry extensions

CRL extensions used:

a) CRL Number: integer value, number of the CRL

b) authorityKeyIdentifier: not critical; value is set to the SHA-1 hash of the BIT STRING subjectPublicKey of the issuing CA's certificate

7.3 OCSP profile

This CA does not support the On-line Certificate Status Protocol (OCSP).

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The DFN-SLCS-CA is obliged to ensure that all its procedures and processes are carried out in compliance with the provisions of this CP/CPS. The compliance audit of the DFN-SLCS-CA will be effected by the DFN-Verein. Such compliance audit shall be effected at least once a year and shall check and include the following topics:

a) operational compliance of the CA staff and the CA's IT systems and network operated by the organization named in section 1.5.1 with the rules and procedures specified in this CP/CPS

b) current list of CA personnel

The results of such audits shall be made available to the EUGridPMA on request.

A compliance audit carried out by a certification authority which is accredited by the EUGridPMA is acceptable. The entire costs of such a requested audit must be covered by the requester.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

If services rendered by the DFN-SLCS 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 DFN-SLCS participants, registered users and subscribers 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 (including any contained attribute data submitted by the Identity Provider) and 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 DFN-SLCS-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 [BDSG].

9.4 Privacy of personal information

9.4.1 Privacy plan

In the course of its duties the DFN-SLCS-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 DFN-SLCS if required in the course of its operations. Furthermore, all information not treated as confidential may be disclosed (see section 9.4.3).

9.4.6 Disclosure pursuant to judicial or administrative process

The DFN-SLCS is governed by the law of the Federal Republic of Germany and is 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 this CP/CPS are held by the DFN-Verein. Parts of this document are inspired by the "SWITCHslcs CA Certificate Policy and Certification Practice Statement".

Distribution or reproduction of this CP/CPS document in unchanged form is explicitly allowed. No transfer of this document, either in whole or in part, into modifiable electronic formats is allowed without permission of the DFN-Verein.

The distribution of the DFN-SLCS-CA certificate and its CRLs (in unchanged and digitally signed form) as available from the repository (see section 2) is explicitly allowed.

9.6 Representations and warranties

9.6.1 CA representations and warranties

It is incumbent on the DFN-SLCS to carry out all duties contained in this CP/CPS with proper diligence.

9.6.2 RA representations and warranties

It is incumbent on the DFN-SLCS and on every SLCS-RA including their Identity Provider and IDMS acting on its behalf to carry out all duties contained in this CP/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 4.5.2 and 9.2 apply.

9.6.5 Representations and warranties of other participants

Should other parties be involved in the certification process as service providers, it is incumbent on the DFN-SLCS to ensure compliance on the part of such other parties with the duties of this CP/CPS.

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/CPS - in their respective current versions – becomes effective the day when published via the information service (see section 2.2) of the DFN-SLCS.

9.10.2 Termination

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

9.10.3 Effect of termination and survival

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

9.11 Individual notices and communications with participants

The DFN-SLCS may distribute individual notices other than those specified in the provisions of this CP/CPS.

9.12 Amendments

An amendment to this CP/CPS can only be effected by the DFN-Verein. Details are given in section 1.5.

9.13 Dispute resolution provisions

None

9.14 Governing law

The CP/CPS and the operations of the DFN-SLCS are all governed by the law of the Federal Republic of Germany.

9.15 Compliance with applicable law

The DFN-Verein issues certificates with which advanced electronic signatures may be created in accordance with the provisions of the German Electronic Signature Act [SigG]. 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/CPS apply for the DFN-SLCS-CA, DFN-SLCS participants 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/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/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 DFN-SLCS shall be governed by the law of the Federal Republic of Germany. Place of fulfilment and sole place of jurisdiction is the registered office of the respective operator.

9.16.5 Other provisions

None

10 REFERENCES

[BDSG] German Data Security and Privacy Act, The Federal Law Gazette I 2003 p. 66

[BNetzA] Notification in accordance with the Electronic Signatures Act and the Electronic Signatures Ordinance - Suitable Algorithms, German Regulatory Authority for Telecommunications and Posts (BNetzA), Federal Gazette No. 19, p.376, 05.02.2008

[DFN-Charter] Charter of the DFN-Verein, http://www.dfn.de/organisation/

[EDUPERSON] eduPerson object class specification defined by the National Science Foundation (NSF) under the NSF Middleware Initiative (Internet 2 consortium) http://www.nmi-edit.org

[EUGridPMA] European Grid Policy Management Authority http://www.eugridpma.org

[EU-RL] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, Official Journal L 013 , 19/01/2000 p. 0012 – 0020

[GLOBUS-OID] OID assignments by The Globus Alliance http://dev.globus.org/wiki/Infrastructure/OIDs

[IGTF] The International Grid Trust Federation (IGTF), http://www.igtf.net

[IGTF-AP-SLCS] Authentication Profile for SLCS X.509 Public Key Certification Authorities with Secured Infrastructure version 2.1 as defined by the [IGTF] http://www.tagpma.org/authn_profiles/slcs

[IGTF-OID] OIDs assigned by the IGTF, http://www.eugridpma.org/objectid/

[IT-GSHB] IT Baseline Protection Manual (*IT-Grundschutzhandbuch), German Fed. Office for Information Security http://www.bsi.de/english/gshb/*

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

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

[PostIdent] Deutsche Post PostIdent identity check services, http://www.deutschepost.de/dpag?lang=de_EN&xmlFile=1016309

[RFC2252] Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions, Network Working Group, IETF, 1997

[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

[SigG] Law Governing Framework Conditions for Electronic Signatures and Amending Other Regulations, The Federal Law Gazette I 2001, p. 876

[SLCS-CP-CPS-OID] DFN-PKI OID registry, http://www.pki.dfn.de/oid

[SLCS-URN] DFN URN registry, https://registry.dfn.de/delegationen/dfn-pki.html

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

11 GLOSSARY

	Meaning
C	Country
CA	Certification Authority
Certificate	Certificate – Allocation of a cryptographic key to an identity signed by a CA
CN	Common Name – Part of Distinguished Name (see DN)
CRL	Certificate Revocation List
CP	Certificate Policy
CPS	Certification Practice Statement
CSR	Certificate Signing Request
DER	Distinguished Encoding Rules (ASN.1 data)
DFN	The National Research and Education Network in Germany
DFN-AAI	Shibboleth based Authentication and Authorization Infrastructure provided and operated by DFN
DFN-AAI account	Shibboleth account of a user in his DFN-site's Identity Provider and underlying IDMS that holds identity and authentication information and authorisation attributes of the user
DFN-PKI	Public Key Infrastructure provided and operated by DFN
DFN-site	Any site that corresponds to the charter ("Satzung") of the DFN-Verein [DFN-Charter], i.e. every site related to research and science in Germany
DFN-PKI SLCS	See DFN-SLCS
DFN-SLCS	Short-lived Credential Service of the DFN-PKI Security level "SLCS"
DFN-SLCS-CA	CA of the DFN-SLCS
DFN-SLCS participant	A DFN-site already participating in the DFN-AAI that subscribes to the DFN-SLCS by signing the DFN-SLCS agreement and therefore agreeing and accepting this CP/CPS document
DFN-SLCS Virtual Home Organization	Virtual home organization for users of various organizations which are not DFN-SLCS participants. Operates its own SLCS-RA and Identity Provider for these users
DFN-SLCS-VO-RA	SLCS-RA of the DFN-SLCS Virtual Home Organization, operated by the DFN-Verein
DN	Distinguished Name
eduPerson	LDAP attribute schema for educational organization defined by the MACE-Dir working group of the Middleware Architecture Committee for Education (MACE) of the Internet2 consortium, http://middleware.internet2.edu/eduperson/
HSM	Hardware Security Module
IDMS	Identity Management System, defined processes and a database system to store user's identity, authentication and authorisation attribute information
Identity Provider	Shibboleth based service to authenticate users of one organization via various authentication mechanisms, like e.g. username/password, client certificates, etc and to provide user's attribute information
ISO	Role of the Information Security Officer
LDAP	Lightweight Directory Access Protocol
O	Organization
OCSP	Online Certification Status Protocol

	Meaning
OID	Object Identifier
OU	Organizational Unit
PCA	Policy Certification Authority
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standard
PKCS#7	Cryptographic Message Syntax Standard
PKCS#10	Certification Request Syntax Standard
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure (X.509)
RA	Registration Authority
Registered user	A user with a valid DFN-AAI account who is allowed to request certificates from the DFN-SLCS-CA, see section 4.1; identity vetting and maintenance of the registered user's DFN-AAI account and identity data in the underlying IDMS must be performed by the SLCS-RA responsible.
SA	Role of System and Network Administrators
SAML	Security Assertion Markup Language defined by the OASIS (Organization for the Advancement of Structured Information Standards) consortium, http://www.oasis-open.org/
SHA-1	Secure Hash Algorithm 1, specified by U.S. National Institute of Standards and Technology (NIST)
Shibboleth	Shibboleth is a standards based, open source software system for federated web single sign-on across or within organizational boundaries, http://shibboleth.internet2.edu
SLCS	Short-Lived Credential Service including web-frontends and online CA issuing short-lived certificates
SLCS-RA	An RA of a DFN-SLCS participant; staff members of the SLCS-RA perform identity vetting and authorisation checking of users, and based on that, the creation of users' DFN-AAI accounts by registering the users' identity and authorization data in the underlying IDMS according to the requirements stated in this CP/CPS; the SLCS-RA is also responsible to maintain this data over time; see section 1.3.2
SLCS registration authority	See SLCS-RA
SSL	Secure Socket Layer, earlier protocol version of TLS
Subscriber	A registered user who has obtained a certificate from the DFN-SLCS-CA, see section 1.3.3
TLS	Transport Layer Security Protocol as defined in RFC 5246
URN	Uniform Resource Name
User	An individual person who is a member of a DFN-site
X.509v3	International standard for the definition of electronic certificates (Version 3)