Certificate Policy and Certification Practice Statement of the GÉANT eduPKI CA

Version 1.7

05.02.2016

Abstract

This is the combined Certificate Policy (CP) and Certification Practice Statement (CPS) of the GÉANT eduPKI CA defining the framework conditions for issuing digital Certificates in accordance with the ITU-T recommendation X.509.

Creation and maintenance of this document has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 691567 (GN4-1).

Change History

Version	***Author***	***Date***	***Changes***
1.1	Reimer Karlsen-Masur	19.11.2010	First public version
1.2	Reimer Karlsen-Masur	19.04.2011	Accreditation Review for eduroam TP – in effect for eduPKI CA
1.3	Reimer Karlsen-Masur	01.09.2011	Including TP specifics in regards to GÉANT's Multi-Domain Network Services, wildcard domain Certificates, more variations of organisation names in O attribute
1.4	Reimer Karlsen-Masur	30.11.2011	Refining Multi-Domain Network Services requirements for accreditation under the MDNS Trust Profile
1.5	Reimer Karlsen-Masur	17.06.2013	Support the current Trust Profiles of eduroam and GÉANT's Multi-Domain Network Services; Editorial changes due to transition from GN3 to GN3+
1.6	Reimer Karlsen-Masur	05.06.2014	Added optional SHA256 for digital signatures Including TP specifics in regards to Generic Server- and Client-Machine-Certificates
1.7	Reimer Karlsen-Masur	05.02.2016	Editorial changes due to transition to GN4 and new CD

Table of Contents

1 INTRODUCTION

The eduPKI service being offered from GÉANT aims to ease the adoption of digital Certificates within GÉANT in an efficient way. It creates a service to support other GÉANT services in defining their security requirements, and to provide them with digital Certificates.

1.1 Overview

This document contains the combined Certificate Policy (CP) and Certification Practice Statement (CPS) of GÉANT's eduPKI Certification Authority (CA) which issues X.509 Certificates to users and network entities, i.e. persons, servers and client machines.

This combined CP/CPS incorporates the requirements of RFC 3647 [RFC3647] as well as the requirements stated in the following eduPKI Trust Profiles (TPs):

a) eduPKI Trust Profile for eduroam Certificates Version 1.3; [TP_EDUROAM]; Object Identifier (OID) 1.3.6.1.4.1.27262.1.13.1.1.1.4; [EDUPKI_OID])

b) eduPKI Trust Profile for Certificates for GÉANT's Multi-Domain Network Services Version 1.2; [TP_GN_MDNS]; Object Identifier (OID) 1.3.6.1.4.1.27262.1.13.1.2.1.3; [EDUPKI_OID])

c) eduPKI Trust Profile for Generic Server- and Client-Machine-Certificates Version 1.2; [TP_GSCM]; Object Identifier (OID) 1.3.6.1.4.1.27262.1.13.1.3.1.1; [EDUPKI_OID])

This combined CP/CPS of the eduPKI CA defines the framework conditions for issuing Certificates in accordance with the ITU-T recommendation X.509.

Within this CP/CPS the words 'MUST', 'MUST NOT', 'REQUIRED', 'SHALL', 'SHALL NOT', 'SHOULD', 'SHOULD NOT', 'RECOMMENDED', 'MAY' and 'OPTIONAL' are to be interpreted as in RFC 2119 [RFC2119].

Certificates of the eduPKI CA SHALL be solely issued on the basis of this CP/CPS; the statements made herein are binding on all Subscribers and Registration Authorities within the eduPKI CA in so far as they do not infringe legal regulations.

1.2 Document name and identification

a) Title: Certificate Policy and Certification Practice Statement of the GÉANT eduPKI CA

b) Version: 1.7

c) OID assigned: 1.3.6.1.4.1.27262.1.13.2.1.1.7 [EDUPKI_OID]

d) Composition of the OID: 1.3.6.1.4.1 (IANA-registered Private Enterprises arc) . 27262 (GEANT Ltd.) . 1 (GÉANT) . 13 (eduPKI) . 2 (Policies) . 1 (eduPKI CA) . 1 (Major Version) . 7 (Minor Version)

1.3 PKI participants

Main participants of the PKI induced by the eduPKI CA are users and system administrators of the GÉANT constituency who MAY request a Certificate of the CA.

1.3.1 Certification authorities

A single on-line root CA – the eduPKI CA – is used for issuing Certificates to authenticated and authorised end-entities.

The eduPKI CA issues Certificates that are particularly compliant with none, one or more TPs. The following naming conventions in regards to Certificates compliant with a TP shall be applied:

eduPKI Trust Profile	*Name*
TP for eduroam Certificates	eduroam Certificate
TP for Certificates for GÉANT's Multi-Domain Network Services	Multi-Domain Network Services Certificate
TP for Generic Server- and Client-Machine-Certificates	Generic Server- and Client-Machine-Certificate

Table 1: Naming convention for Certificates

1.3.2 Registration Authorities

Multiple Registration Authorities (RAs) are set up to process and approve Certificate Applications and Certificate revocation requests. Initially a primary RA is installed which will be used to set up secondary RAs that will handle Applications and Requests of specific sub-groups of the GÉANT constituency, e.g. participants and users of a single GÉANT Service.

1.3.3 Subscribers

Subscribers are all Requesters of a Certificate that have successfully obtained a Certificate issued by the eduPKI CA.

Different types of Certificates MUST be requested by different entities:

Type of Certificate	*Requester*
Network Entity Certificate (Organisational Certificate)	administrators and owners of the network entity named in the Certificate's Subject (Organisational Requester)
Personal User Certificate (Personal Certificate)	the person named in the Certificate's Subject (Personal Requester)
Group Certificate (Organisational Certificate)	responsible member of the group named in the Certificate's Subject or their superior staff (Organisational Requester)

Table 2: Shows Requester by Type of Certificate

If a Personal Requester has agreed upfront, his/her actual Certificate Application MAY be initiated and submitted in his/her name by legal representatives of his/her home organisation and their named delegates.

1.3.4 Relying Parties

Relying Parties are individuals or organisations using the Certificates issued by the eduPKI CA to verify the identity of and/or secure electronic communication with Subscribers.

Relying Parties MAY also be Subscribers of the eduPKI CA at the same time.

1.3.5 Other participants

No stipulation.

1.4 Certificate usage

1.4.1 Appropriate Certificate usage

Certificates issued by the eduPKI CA are intended to be used primarily in the realm of the GÉANT constituency.

1.4.2 Prohibited Certificate usage

No form of Certificate usage is prohibited with the exception of issuing further Certificates. The eduPKI CA alone MAY issue further Certificates.

1.5 Policy administration

1.5.1 Organization administering the document

This combined CP/CPS is administered by:

eduPKI
c/o DFN-Verein
Alexanderplatz 1
10178 Berlin
GERMANY

Email: ca@edupki.org
Web: www.edupki.org

Operation of the eduPKI CA is effected by:

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

Phone: +49 40 808077-580
Fax: +49 40 808077-556
Email: dfnpca@dfn-cert.de
Web: www.dfn-cert.de

1.5.2 Contact person

The persons responsible for this CP/CPS are the members of eduPKI within GÉANT.

1.5.3 Person determining CPS suitability for the policy

The persons named in section 1.5.2 are responsible for reviewing and approving the suitability of this CP/CPS.

1.5.4 CPS approval procedures

Approval of the CP/CPS is effected by the responsible persons named in section 1.5.2.

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

a) RFC 3647 [RFC3647]; and

b) the following TPs:

    i. eduPKI Trust Profile for eduroam Certificates Version 1.4 [TP_EDUROAM]

    ii. eduPKI Trust Profile for Certificates for GÉANT's Multi-Domain Network Services Version 1.3 [TP_GN_MDNS]

    i. eduPKI Trust Profile for Generic Server- and Client-Machine-Certificates Version 1.2 [TP_GSCM]

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 this CP/CPS is changed, with the exception of the correction of spelling mistakes, clarifications or editorial changes, the OID of the document MUST change and the major changes as well as changes pertinent to supported TPs MUST be announced to and approved by the PMAs with which the eduPKI CA has sought and successfully obtained accreditation before issuing any Certificates under the updated CP/CPS.

All the CP/CPS documents under which valid Certificates are or have been issued are published via the service named in sections 2.1 and 2.2.

1.6 Definitions and acronyms

See eduPKI glossary https://www.edupki.org/documents/glossary [GLOSSARY].

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

The eduPKI CA offers a repository allowing on-line access to the eduPKI 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 https://www.edupki.org/edupki-ca. The repository runs on a best-effort basis, with an intended availability of 24 hours 7 days a week.

2.2 Publication of certification information

The eduPKI CA makes the following information available:

a) its root CA Certificate and its fingerprint

b) its current CRL

c) its past and current CP/CPS documents

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 eduPKI 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 authorised persons.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

The Subject Distinguished Name (sDN) of an end-entity Certificate issued by the eduPKI CA always starts in Domain Component (DC) style with `/dc=net/dc=geant` followed by a DC describing a GÉANT Service to which the Subscriber relates to or for which the Certificate is intended to be used, optionally followed by further DCs. The sDN is always completed with the X.500-style attributes `C` (Country), `ST` (State, OPTIONAL), `L` (Location, OPTIONAL), `O` (Organisation), `OU` (Organisational Unit, multiple, OPTIONAL) and at least one `CN` (Common Name). Other additional X.500-style attributes including `emailAddress` MAY be present in the sDN.

3.1.1 Types of names

All Certificates issued by the eduPKI CA SHALL be assigned an sDN according to the X.500 series of ITU-T recommendations [X500]. An sDN is a sequence of naming attributes through which all Subjects in a PKI hierarchy SHALL be referenced uniquely.

The Certificate's name of a Subject to which the Certificate is issued by the eduPK CA is always built on the following pattern:

```
/dc=net
/dc=geant
/dc=<name of pertinent GÉANT Service>
```

```
[ /dc=<Domain Component> ]*
/C=<Country>
[ /ST=<State> ]**
[ /L=<Location / City> ]**
/O=<Organisation>
[ /OU=<Organisational Unit> ]*
/CN=<Common Name>
[ /CN=<additional Common Name> ]*
[ /emailAddress=<email address> ]*
```

For an explanation of the meaning of the attributes see section 3.1.2.

Further Certificate names MAY be added to a Certificate by including the Certificate Extension *SubjectAlternativeName* (SaN) which MAY include alternative names of the Certificate as specified by RFC 5280 [RFC5280] and other industry standards such as SaNs of type *rfc822Name* for email addresses, *dNSName* for FQDNs (fully qualified Internet domain names) and wildcard domains, *iPAddress* for IP addresses, *URI* for Uniform Resource Identifiers, *UPN* for Microsoft User Principal Names and *GUID* for Microsoft Globally Unique Identifiers, see section 7.1.2.

It is RECOMMENDED that email addresses are placed in SaNs of type *rfc822Name* and not in the sDN.

3.1.2 Need for names to be meaningful

The value of each single component of the sDN MUST be appropriate and meaningful.

Permissible characters for values of a single component of an sDN are

```
a-z A-Z 0-9 ' ( ) , - . / : @ blank-space
```

with the exception that depending on the type of the component subsets of these characters MAY not be allowed.

Characters with accents such as circumflexes, etc., umlauts and other special characters MUST NOT be used. Characters with accents MUST be used without their respective accents. Umlauts and other special characters SHOULD be substituted by permissible characters in a way that the substitution conveys the sound of the substituted character.

The value of each single component of an sDN MUST NOT be composed of more than 64 characters. If the value of a single component of an sDN would consist of more than 64 characters an appropriate and, if possible, well-known and established abbreviation of that value MUST be used.

The Domain Name *geant.net* is held by a member of the GÉANT consortium for purposes of GÉANT such that the first two DCs `/dc=net/dc=geant` are rightfully used.

The REQUIRED third DC MUST contain GÉANT's formal description of the GÉANT Service the Certificate is used for/within.

Further OPTIONAL DCs, if present, MUST be assigned by the pertinent GÉANT Service.

The REQUIRED `C` attribute MUST be the 2 letter country code – as defined by ISO standard 3166-1 [ISO-3166-1] – of the country where the Subscriber's home organisation is located.

The OPTIONAL `ST` attribute, if present, MUST be the official name – spelled out in an official language of the country named in the `C` attribute or in English language – of the sub-national unit (e.g. state) – as defined by ISO standard 3166-2 [ISO-3166-2] for the country named in the `C` attribute – where the Subscriber's home organisation is located.

The OPTIONAL `L` attribute, if present, MUST be the official name – spelled out in an official

* OPTIONAL, multiple occurrences allowed

** OPTIONAL, single occurrence only

language of the country named in the C attribute or in English language – of the location (e.g. city) where the Subscriber's home organisation is located.

The REQUIRED O attribute MUST be the name of the Subscriber's home organisation as authenticated according to section 3.2.2 – spelled out in an official language of the country named in the C attribute or in English language.

The OPTIONAL OU attributes, if present, MUST contain the names of the Subscriber's organisational units – spelled out in an official language of the country named in the C attribute or in English language – within the organisation named in the O attribute. The ordering of the OU attributes SHOULD be from larger units to smaller units.

Each of the CN attributes (at least one CN attribute is REQUIRED) MUST contain an appropriate presentation of the actual name of the entity represented by the Certificate's sDN belonging to the organisation described in the sDN's O attribute, i.e.

a) the FQDN or IP address of a network entity in case the Certificate is bound to that network entity; or
b) a wildcard domain under a second- or higher level Internet domain name, e.g. **.example.org* or **.sub.example.org* etc., in case the requested Certificate is not an eduroam Certificate or Multi-Domain Network Services Certificate; or
c) a person's name (i.e. given name(s) and surname; at least one given name and the surname MUST be spelled out, additional middle names MAY be abbreviated or left out) in case the Certificate is bound to that person; or
d) the name/description of a well established group within the organisation in case the Certificate is bound to that group of people.

Each of the OPTIONAL email addresses contained in emailAddress attributes of the sDN or SaNs of type *rfc822Name* MUST be a valid RFC 822 formatted email address [RFC822] that is under the control of the Subject or Subscriber.

SaNs of type *dNSName* MUST be FQDNs, or wildcard domains under second- or higher level Internet domain names, e.*g. *.example.org or *.sub.example.org* etc..

SaNs of type *iPAddress* MUST be valid IP addresses.

In particular

a) hostnames without their full Internet domain name; and
b) Internet domain names that are not registered with official Internet Corporation for Assigned Names and Numbers (ICANN) approved Internet domain name registrars or their delegates; and
c) top-level Internet domain names that are not approved by ICANN; and
a) Internet domain names assigned for special use [IANA_SR_DNS] as specified in RFC 6761 [RFC6761] and especially in RFC 2606 [RFC2606]

MUST NOT be part of any issued Certificate.

Furthermore IP addresses from the IP address ranges specified by the IANA Special Purpose Address Registries for IPv4 and IPv6 addresses [IANA_SR_IP4], [IANA_SR_IP6] as described in RFC 6890 [RFC6890] MUST NOT be part of any issued Certificate. This especially includes IPv4 addresses reserved for private use as defined in RFC 1918 [RFC1918].

3.1.3 Anonymity or pseudonymity of Subscribers

The eduPKI CA does not issue Certificates that allow for anonymity of Subscribers and Subjects. Personal User Certificates issued by the eduPKI CA do not allow for pseudonymity of Subscribers and Subjects.

3.1.4 Rules for interpreting various name forms

All Country Codes used in the Certificates MUST comply with the 2-letter country codes as defined by ISO Standard 3166-1 [ISO-3166-1].

All email addresses used in the Certificates MUST comply with RFC 822 – Standard for ARPA

Internet Text Messages [RFC822].

All FQDNs and Internet domain names used in the Certificates MUST comply with RFC 1035 – Domain Names – Implementation and Specification [RFC1035].

All IP addresses used in the Certificates MUST comply with RFC 791 (IPv4) [RFC791] or RFC 4291 (IPv6) [RFC4291] in combination with RFC 5952 [RFC5952].

3.1.5 Uniqueness of names

The name of each Certificate issued by the eduPKI CA, i.e. the sDN, MUST be uniquely and persistently assigned to the entity/Subject the Certificate is bound to. To assist RAs to uniquely assign sDNs to entities/Subjects each RA is assigned a separate name space, i.e. a constant RA-specific prefix of the sDN used in all Requests the RA receives and approves.

In case of a Certificate Application for a renewal or re-key the RA MUST ensure that the newly requested sDN has already been assigned to the same entity/Subject that the Certificate, that is going to be renewed or re-keyed, is bound to.

For Personal and Group Certificates it is RECOMMENDED to build the unique name by either including additional OU attributes in the sDN or extending the CN by additional distinguishing identifiers, e.g. a hash value of some internal identifier that is uniquely assigned to the entity/Subject the Certificate is bound to.

3.1.6 Recognition, authentication and role of trademarks

The Subscriber MUST ensure that the choice of names included in the Subscriber's Certificate does not infringe any law pertaining to trademarks, brand names, etc. The eduPKI CA is not obliged to verify compliance with such legal prescriptions. It is solely incumbent on the Subscriber to ensure such compliance. Should the eduPKI CA be informed of any infringement of such laws, the affected Certificates SHALL be revoked.

3.2 Initial identity validation

A Requester whose identity has not been validated before MUST initially validate his/her identity with the pertaining RA before his/her Certificate Application MAY be approved. The RA MUST document the identity validation according to section 5.5.1 b).

3.2.1 Method to prove possession of private key

To prove that the Requester possesses the private key pertaining to the public key included in a Certificate Signing Request (CSR) pertinent to his/her Certificate Application he/she MUST

a) digitally sign the CSR with that private key and
b) confirm the binding of the public key to the Certificate Application by including the digital fingerprint of the CSR or public key into the submitted Certificate Application form.

The RA MUST

a) verify the digital signature on the CSR and
b) check that its included public key is bound to the Certificate Application by comparing the computed digital fingerprint of the CSR or public key with the digital fingerprint provided by the Certificate Application form

before approving the Certificate Application.

3.2.2 Authentication of organizational identity

Each organisational name included in a Certificate name, i.e. in the O attribute of the sDN, MUST be authenticated. To authenticate the identity of an organisation a Requester of that organisation MUST submit valid and up-to-date information proofing the existence of the organisation to the RA which is processing the Certificate Application.

An appropriate meaningful name of an organisation is

a) its legal name; and
b) the name it's using in business letters (letterhead stationery) when conducting official business with external suppliers, customers, partners, accounting firms, financial institutions, etc.; and
c) the organisation name it's using in the registrant, holder or owner record (according to the WHOIS query result of the pertinent ICANN approved top-level Internet domain name registrar) when it registered its Internet domain name for its main web-site with an official ICANN approved Internet domain name registrar or its delegates.

Once the identity of an organisation has been proven to an RA, the RA MAY omit re-authentication of the organisation's identity for processing of further Certificate Applications if it has sufficient evidence that the organisation's identity has not changed since its last authentication. It is at the discretion of the RA to demand re-authentication of an organisation's identity from the Requester.

3.2.3 Authentication of individual identity

When a Requester submits his/her first Certificate Application to the appropriate RA, the Requester's personal and organisational identity MUST be authenticated.

For all Requesters the RA MUST validate the Requester's

a) registered email address(es), e.g. by using a challenge response procedure including the sending of email to all registered email address(es); and
b) affiliation with his/her registered home organisation (o attribute of sDN).

The Requester's registered home organisation MUST be authenticated according to section 3.2.2.

The RA MAY validate the affiliation of the Requester with his/her registered home organisation via the following methods:

a) The RA checks
    i. that the Requester's full name in combination with one of the registered email address(es) of the Requester are listed in an official staff/affiliate directory (accessible to the RA) of the Requester's registered home organisation and
    ii. that exactly this listed email address of the Requester belongs to an Internet domain name owned by the Requester's registered home organisation.
b) The Requester provides an official document by his/her registered home organisation stating the affiliation with the Requester, e.g. staff ID, staff badge, official letter.

Other suitable methods that prove the Requester's affiliation with his/her registered home organisation are allowed.

For Personal Requesters the RA MUST additionally validate the Requester's full name by checking a valid government issued photo identity document of the Requester which has an expiry date (e.g. passport or national identity card).

3.2.4 Non-verified subscriber information

Only information will be verified which is required for the various authentication and validation procedures for the authentication of identity (see sections 3.2.2 and 3.2.3) and validation of authority (see section 3.2.5). Beyond this requirement, no further information SHALL be verified.

3.2.5 Validation of authority

The Requester MUST be authorised to get the requested Certificate. The Requester MUST provide according information to the RA. The RA MUST check this information.

a) The Requester MUST be affiliated with his/her registered home organisation, see section 3.2.3.
b) The Requester MUST either own/control the requested email addresses or the Requester MUST be authorised to use the requested email addresses in Certificates by the entity who owns/controls the email addresses.

c) The Requester MUST either own/control the requested sDN and SaNs or the Requester MUST be authorised to use the requested sDN and SaNs in Certificates by the entity who owns/controls the requested sDN and SaNs. In particular each Internet domain name that is part of the requested sDN or any requested SaN MUST be either

   i. registered with the official ICANN approved Internet domain name registrar or its delegates for the pertinent top-level Internet domain name by the home organisation of the Requester or

   ii. the Requester MUST be explicitly authorised by the owner of the Internet domain name who registered the Internet domain name with the official ICANN approved Internet domain name registrar or its delegates for the pertinent top-level Internet domain name to use it in the requested Certificate

   and each IP address that is part of the requested sDN or any requested SaN MUST be either

   i. assigned by the official IANA approved Internet registry to the home organisation of the Requester or

   ii. the Requester MUST be explicitly authorised by the officially registered owner of the IP address to use it in the requested Certificate.

   If wildcard domains are part of the requested sDN or SaN the RA MUST check the Requester's authorisation to get a Certificate including these wildcard domains with all due diligence.

d) The Requester MUST provide to the RA appropriate documentation/proof about his/her right to use the requested names.

e) Additional checks MUST be performed for requested Certificates compliant with specific TPs, see table 3.

TP for	***Additional TP specific Requirements***
eduroam Certificates	The RA MUST ensure with the eduroam National Roaming Operator that a) the Requester is authorised to request Certificates for eduroam; and b) the FQDNs requested in the Certificates are registered eduroam Identity/Service Providers for the pertinent home organisations.
Multi-Domain Network Services Certificates	The RA MUST ensure with GÉANT's registry of participating infrastructure nodes in GÉANT's Multi-Domain Network Services or with GÉANT's registry of Multi-Domain Network Services and their management/operations teams that a) the Requester is authorised to request and receive Certificates of the requested profile (see table 6) for the pertinent GÉANT Multi-Domain Network Service; and b) the FQDNs requested in the Certificates are registered infrastructure nodes of the pertinent GÉANT Multi-Domain Network Service for the pertinent home organisation. The RA MUST check the authorisation by either using the information provided by those registries with a secured call-back procedure, i.e. validating a digital signature of an authorisation statement against a pre-registered public key and email address of the pertinent service' management/operations team; or validating a handwritten signature on an authorisation statement against well-known pre-registered signatures of the pertinent service' management/operations team; or checking with pertinent service management/operations team by phone if the voice of team member is well-known to the RA staff performing the check.

TP for	Additional TP specific Requirements
Generic Server- and Client-Machine-Certificates	The RA MUST ensure with its assigned GÉANT Service' registry or management/operations teams that the Requester is authorised to request and receive Certificates of the requested profile (see table 6) and names (i.e. FQDNs, IP addresses, email addresses etc.) for the pertinent GÉANT Service. The RA MUST check the authorisation by either using the information provided by those registries with a secured call-back procedure, i.e. validating a digital signature of an authorisation statement against a pre-registered public key and email address of the pertinent service' management/operations team; or validating a handwritten signature on an authorisation statement against well-known pre-registered signatures of the pertinent service' management/operations team; or checking with pertinent service management/operations team by phone if the voice of team member is well-known to the RA staff performing the check.

Table 3: Additional Checks for TPs

f) In case an Organisational Certificate is requested the Requester MUST be authorised by his/her home organisation to get a Certificate for the requested sDN and SaNs and the Requester MUST submit appropriate documentation issued by his/her home organisation to the RA to prove that he/she is fulfilling the required role, see table 2.

g) In case a Personal Certificate is requested on behalf of the Requester by his/her home organisation the home organisation MUST submit appropriate documentation that it is authorised by the Requester to request a Personal Certificate on his/her behalf.

h) In case a Personal Certificate is requested the Requester MUST be authorised by his/her home organisation to get a Personal Certificate and the Requester MUST submit appropriate documentation issued by his/her home organisation to the RA.

3.2.6 Criteria for interoperation

No stipulation.

3.3 Identification and authentication for re-key requests

An existing Certificate MAY be re-keyed, i.e. a new Certificate MAY be issued under the same sDN with the same included SaNs for a newly generated key, if the re-keying is requested by the original Requester or his/her home organisation acting on behalf of him/her. A re-keying request is submitted in form of a standard Certificate Application.

Re-keying of

a) eduroam Certificates;

b) Multi-Domain Network Services Certificates; and

c) Generic Server- and Client-Machine-Certificates

is not supported. All re-keying requests for

a) eduroam Certificates;

b) Multi-Domain Network Services Certificates; and

c) Generic Server- and Client-Machine-Certificates

SHALL be treated like initial Certificate Applications, see section 3.2.

3.3.1 Identification and authentication for routine re-key

The Requester of a re-keying request MUST be identified and the pertinent Certificate Application MUST be authenticated. Re-keying requests MUST be submitted by the original Requester or his/her home organisation acting on behalf of him/her and for the originally included sDN and SaNs only. The RA MUST ensure that Certificate Application containing the re-keying request is submitted by the original Requester or his/her home organisation acting on behalf of him/her authenticating the Certificate Application by cross checking (digital) signatures from the original Certificate Application and the new Certificate Application containing the re-keying request.

If the Certificate Application containing the re-key request is digitally signed, the pertinent signing Certificate MUST NOT be revoked. Otherwise the Certificate Application MUST be authenticated using hand written signatures.

Furthermore the RA MUST re-validate

a) his/her current authorisation to request Certificates for the entities named in the Request and
b) his/her current ownership/control of the names requested,

see section 3.2.5.

3.3.2 Identification and authentication for re-key after revocation

See section 3.3.1.

3.4 Identification and authentication for revocation request

Revocation of a Certificate is always effected by the pertinent RA which approved the Certificate Application. The Subscriber MUST identify and authenticate himself to that RA to request the revocation of his/her Certificate.

If the entity requesting a revocation of a Certificate proves to the RA or CA that the pertinent private key has been compromised or exposed, no identification nor authentication of that entity is needed.

After successfully requesting the revocation, the RA will forward the approved revocation request to the eduPKI CA.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

All sensitive network communication between the Requester, the RA and the eduPKI CA SHALL be secured by encrypted tunnels e.g. using the transport layer security (TLS) protocol with TLS server authentication and client authentication if applicable.

4.1 Certificate Application

4.1.1 Who can submit a Certificate Application

Any person participating or interacting with GÉANT or a GÉANT Service MAY submit a Certificate Application for this purpose. A Certificate Application MAY be submitted on behalf of the entity named in the requested sDN, see section 1.3.3.

4.1.2 Enrollment process and responsibilities

The enrollment process a Requester MUST adhere to submit a Certificate Application is as follows:

a) The Requester (or his/her home organisation on behalf) creates a key pair and a CSR containing the requested sDNs and SaNs.
b) The Requester submits the CSR and pertinent Certificate Application data like contact details of him/her to the appropriate RA via an online process resulting in a Certificate Application form (as Portable Document Format (PDF) file).
c) The Requester either prints and signs or digitally signs the Certificate Application form and brings/sends it to the RA including truthful documentation about his/her personal and organisational identity as well as authorisation information.

4.2 Certificate Application processing

4.2.1 Performing identification and authentication functions

a) If the Requester has not been identified by the RA before,

   i. the Requester MUST identify himself to the RA or – in case his/her home organisation submits the Certificate Application on his/her behalf – to his/her home organisation, see sections 3.2 and 3.3 and

   ii. the RA MUST validate the Requester's personal and organisational identity.

b) If the Requester has been identified by the RA before, the authenticity of the Certificate Application MUST be validated through the RA by cross-checking its (digital) signature against previously received and validated, i.e. registered, signatures or public cryptographic key material of the Requester.

c) The RA MUST validate the Requester's authorisation to get a Certificate and to use/control the requested sDN and SaNs based on the submitted documents, see section 3.2.5.

If digital signatures are used, the RA MUST ensure, that the pertinent Certificates are valid.

4.2.2 Approval or rejection of Certificate Applications

The RA approves a Certificate Application if the following criteria are met:

a) The personal and organisational identity of the Requester is validated, see sections 3.2.3 and 3.2.2.

b) The Requester is authorised to get a Certificate, see section 3.2.5.

c) The Requester

   i. owns and controls the sDN and SaNs requested in the Certificate Application; or

   ii. is authorised to use the sDN and SaNs requested in the Certificate Application by the registered owner of the names,

   see section 3.2.5.

d) The Certificate Application is (digitally) signed by the Requester.

If digital signatures are used, the RA MUST ensure, that the pertinent Certificate are valid.

If the Requester or his/her Certificate Application fails to adhere to any of the criteria listed above, or in any other way violates the stipulations of this document, the eduPKI CA will reject a Certificate Application.

4.2.3 Time to process Certificate Applications

Certificate Applications MAY be processed at the discretion of the pertinent RA. Once the RA has approved a Certificate Application the Certificate is issued and delivered.

4.3 Certificate issuance

After receipt of an approved Certificate Application the eduPKI CA will issue the pertinent Certificate and deliver it to the Subscriber or his/her home organisation (if requested on behalf of the Subscriber).

4.3.1 CA actions during Certificate issuance

CSRs included in approved Certificate Applications are processed automatically by the eduPKI CA resulting in the issuance of the requested Certificate. All steps of the issuing process are logged.

4.3.2 Notification to Subscriber by the CA of issuance of Certificate

The Subscriber MUST be notified about the issuance of his/her requested Certificate. The notification is sent to the Subscriber or his/her home organisation (if requested on behalf of the Subscriber).

The notification (optionally including the issued Certificated) MAY be emailed to any of the registered email addresses of the Subscriber, any email addresses included in the SaNs and to the approving RA.

If the Certificate has been requested by the Subscriber's home organisation on his/her behalf the home organisation MUST notify the Subscriber and deliver the Certificate.

4.4 Certificate acceptance

The Subscriber MUST verify the correctness of his/her own Certificate and of the issuing CA Certificate once he/she has received it.

4.4.1 Conduct constituting Certificate acceptance

The Subscriber accepts the Certificate once he/she starts using the Certificate or if the eduPKI CA has not received his/her objection within fourteen (14) days after issuance of the Certificate.

4.4.2 Publication of the Certificate by the CA

Certificates issued by the eduPKI CA MAY be published via the CA's Certificate Repositories and Directories if the Subscriber consented to this.

4.4.3 Notification of Certificate issuance by the CA to other entities

The approving RA MAY be notified about the Certificate issuance, see section 4.3.2.

4.5 Key pair and Certificate usage

4.5.1 Subscriber private key and Certificate usage

Subscribers MAY use their Certificates issued by the eduPKI CA as they wish, but SHALL

a) use the Certificates exclusively for legal and authorised intended purposes in accordance with this document;

b) only use a Certificate, if they legitimately are, own or control the entities described by the sDN and SaNs of the Certificate;

c) refrain from using the Subscriber's private key corresponding to the public key of the Certificate to issue other Certificates;

d) realize the importance of properly protecting their private key data (and its password);

e) immediately cease to use the Certificate if any information included in the Certificate change or if changed circumstances make the information in the Certificate misleading or inaccurate, e.g. a change of name(s) or email address(es), and contact the pertinent RA or CA to revoke the affected Certificate;

f) notify the pertinent RA or CA immediately of any suspected or actual compromise of the private key to revoke the affected Certificate;

g) use their own judgement about whether it is appropriate, given the level of security and trust provided by a Certificate issued by the eduPKI CA, to use such a Certificate in any given circumstance;

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 document;

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

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

e) make their own judgement and rely on a Certificate issued by the eduPKI 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 the eduPKI CA and the value of any transaction that MAY involve the use of the aforementioned Certificates.

4.6 Certification renewal

Renewal of an existing Certificate is the issuance of a new Certificate with the same sDN, SaNs and public key as the existing Certificate includes. If any part of the sDN, SaNs or public key has changed the request MUST be treated like an initial Certificate Application, see section 3.2.

The eduPKI CA MAY support Certificate renewal if the renewal request is submitted by the original Requester or his/her home organisation acting on behalf of him/her. Identification and authorisation MUST be checked according to section 3.3.

Renewals of

a) eduroam Certificates;
b) Multi-Domain Network Services Certificates; and
a) Generic Server- and Client-Machine-Certificates

are not supported. All renewal requests for

a) eduroam Certificates;
b) Multi-Domain Network Services Certificates; and
a) Generic Server- and Client-Machine-Certificates

SHALL be treated like initial Certificate Applications, see section 3.2.

4.7 Certificate re-key

Re-keying an existing Certificate is the process where the original Requester or his/her home organisation acting on behalf of him/her generates a new key pair and applies for the issuance of a new Certificate (containing the same sDN and SaNs as in the existing Certificate) that certifies the new public key. If any part of the sDN, SaNs or public key has changed the request MUST be treated like an initial Certificate Application, see section 3.2.

The eduPKI CA MAY support Certificate re-keying if the re-key request is submitted by the original Requester or his/her home organisation acting on behalf of him/her. Identification and authorisation MUST be checked according to section 3.3.

Re-keying of

a) eduroam Certificates;
b) Multi-Domain Network Services Certificates; and
c) Generic Server- and Client-Machine-Certificates

is not supported. All re-keying requests for

a) eduroam Certificates;
b) Multi-Domain Network Services Certificates; and
c) Generic Server- and Client-Machine-Certificates

SHALL be treated like initial Certificate Applications, see section 3.2.

4.8 Certificate modification

The eduPKI CA does not support Certificate modification. The Subscriber MUST submit a new Certificate Application instead.

If the Subscriber wants to change personal or organisational identity information (included in sDN or SaNs) contained in an existing Certificate, he/she MUST contact the pertinent RA to get the changed identity information verified, see section 3.2.

4.9 Certificate revocation and suspension

This section explains the circumstances under which a Certificate SHALL be revoked. Once a Certificate has been revoked, it MUST NOT be renewed.

Suspension of Certificates is not supported.

4.9.1 Circumstances for revocation

A valid end-entity Certificate SHALL be revoked

a) if the private key or its password associated with the Certificate has been compromised or exposed; or
b) if the Subscriber
   i. lost direct ownership/control of the names included in the Certificate's sDN or SaNs; or
   ii. is no longer authorised by the owner of the Certificate's sDN or SaNs to use these in Certificates; or
   iii. is no longer authorised to hold a Certificate issued by the eduPKI CA; or
   iv. has breached his/her obligations.

If a reason for revocation of a Certificate is found after the end of the Certificate's validity period the affected Certificate MAY not be revoked.

4.9.2 Who can request revocation

Any Subscriber MAY request, without furnishing any reasons for the request, the pertinent RA to request the revocation of his/her Certificate by the eduPKI CA on his/her behalf. Acceptance of a revocation request for a Certificate is predicated on the successful identification and authentication of the Subscriber in accordance with section 3.4.

The home organization of the Subscriber acting on behalf of him/her MAY request the pertinent RA to request the revocation of the Subscriber's Certificate by the eduPKI CA.

Additionally an RA MAY request the revocation of end-entity Certificates that were issued based on Certificate Applications approved by that RA.

Others MAY request the revocation of a Certificate issued by the eduPKI CA if and only if they can proof that the private key or its password associated with that Certificate has been compromised or exposed, the content of that Certificate is not representing the truth or the Subscriber or Subject has breached his/her obligations.

4.9.3 Procedure for revocation request

If the conditions precedent to acceptance of the request (see section 4.9.1) are met, the Certificate issued by the eduPKI CA 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 MUST notify his/her pertinent RA immediately, but not later than one working day, of the same, and initiate the revocation of the affected Certificate.

If an RA is aware of circumstances for revocation of Certificates (see section 4.9.1), the RA MUST notify the eduPKI CA immediately of the same, and initiate the revocation of affected Certificates.

4.9.5 Time within which CA must process the revocation request

RAs and the eduPKI CA MUST react to a received revocation request not later than within one working day.

The eduPKI CA will process an approved Certificate revocation request after approval of that request.

4.9.6 Revocation checking requirement for relying parties

The provisions of section 4.5.2 apply.

4.9.7 CRL issuance frequency

A new CRL is issued by the eduPKI CA immediately after an approved revocation request has been processed.

In any case a new CRL is issued by the eduPKI 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 eduPKI 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 chapter 2).

4.9.9 On-line revocation / status checking availability

No stipulation.

4.9.10 On-line revocation checking requirements

No stipulation.

4.9.11 Other forms of revocation advertisements available

No stipulation.

4.9.12 Special requirements re key compromise

Should a private key of a Certificate become compromised or exposed, the affected Certificate SHALL immediately be revoked.

Should the private key of the eduPKI CA become compromised, the PMAs with which eduPKI CA has sought and successfully obtained accreditation and TACAR are notified immediately to remove the affected CA Certificate from its trust anchor distribution. Additionally the available eduPKI CA archive, log and audit trail data are analysed 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 eduPKI CA repository and on-line application services can be reached 24 hours 7 days a week through the Internet, see chapter 2.

4.10.2 Service availability

The organisation operating the eduPKI CA (as named in section 1.5.2) provides all services (registration, certification, directory) on a 24 hours 7 days a week base with a best-effort approach with minimal scheduled interruption. Due to the nature of the Internet, there are no guarantees for these services. Unscheduled interruptions of these services are possible due to circumstances not under the control of the operator of the eduPKI CA.

4.10.3 Optional features

The eduPKI CA Certificate status services do not include or require any additional features.

4.11 End of subscription

Certificate usage is terminated by the Subscriber either by means of revocation or by not requesting a new Certificate once the old one has expired.

4.12 Key escrow and recovery

The eduPKI CA MAY support key escrow and recovery.

Private keys associated with Certificates issued in accordance with the

a) TP for eduroam Certificates; or
b) TP for Certificates for GÉANT's Multi-Domain Network Services
c) TP for Generic Server- and Client-Machine-Certificates

MUST NOT be part of any key escrow and/or recovery plan that the CA MAY offer.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical controls

5.1.1 Site location and construction

The technical systems of the eduPKI CA are located in a computer and data centre on the premises of the operator of the eduPKI CA.

5.1.2 Physical access

The operational areas of the eduPKI CA are protected by appropriate technical and infrastructural measures. Access to the operational areas of the eduPKI CA is restricted to such employees who have been duly authorised by the Information Security Officer of the eduPKI CA. Access for persons not entrusted with a recognised function is regulated by the rules imposed on visitors. Persons external to the eduPKI CA MAY only enter CA service premises when accompanied by at least one authorised eduPKI CA staff.

5.1.3 Power and air conditioning

No stipulations.

5.1.4 Water exposures

No stipulations.

5.1.5 Fire prevention and protection

No stipulations.

5.1.6 Media storage

All media SHALL be stored in locked file cabinets. Media storing sensitive data SHALL be stored in a safe or safe-deposit box.

5.1.7 Waste disposal

Information stored on data carriers SHALL be destroyed in an appropriate manner and subsequently disposed of by a service provider in an appropriate manner. Data stored on paper SHALL 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

Backup media stored externally SHALL be placed in a safety deposit box.

5.2 Procedural controls

All persons with access to the systems hosting the eduPKI CA SHALL be permanently employed personnel of the eduPKI CA operator, which are either trained System and Network Administrators or members of its PKI team.

5.3 Personnel controls

All contracts of employment for employees of the eduPKI CA operator are governed by the law of the Federal Republic of Germany. All employees of the eduPKI CA operator are bound to non-disclosure and data privacy in compliance with applicable legal prescriptions covering data [BDSG].

5.3.1 Qualifications, experience, and clearance requirements

Employees of the eduPKI CA operator 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.

5.3.2 Background check procedures

For all employees with access to the systems hosting the eduPKI CA the operator of the eduPKI CA holds police clearance certificates that are no older than two years.

5.3.3 Training requirements

The eduPKI CA only employs properly qualified and trained staff.

5.3.4 Retraining frequency and requirements

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

5.3.5 Job rotation frequency and sequence

No stipulations.

5.3.6 Sanctions for unauthorised actions

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

5.3.7 Independent contractor requirements

No stipulations.

5.3.8 Documentation supplied to personnel

eduPKI CA employees are supplied with the following documentation:

a) Combined CP/CPS, i.e. this document

b) Instructions manuals (available in German):

   i. Services
   ii. Security concepts
   iii. Process specification and forms for regular operations
   iv. Instructions and procedures for emergencies
   v. Documentation of IT systems
   vi. 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 eduPKI CA, the following measures have been put in place. The following types of events are recorded electronically as log-data or on paper files:

a) Operation of IT components, including

   i. Physical access to the CA systems (log-in and log-out, access to the machine cases)
   ii. Hardware booting and shut-down procedures
   iii. Successful and abortive log-in attempts
   iv. Issuance and withdrawal of authorisations (on paper file)
   v. Installation and configuration of software

b) All CA transactions, including
   i. Certificate Applications
   ii. Certificate Application approvals
   iii. Certificate issuance
   iv. Certificate publication
   v. Certificate revocation
   vi. CRL issuance
   vii. Generation of CA keys
   viii. Creation of CA Certificates
   ix. Activation and deactivation of CA's private keys

c) Modification of the CP/CPS and the operating concept, including
   i. Role definition (on paper file)
   ii. Process specification (on paper file)
   iii. Changes in persons responsible (on paper file)

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 eduPKI CA Certificate or its private key: one (1) year after the CA Certificate expired.

b) For data regarding a specific end-entity Certificate (including the CSR, Requester's name and email address from its Certificate Application): one (1) year after the issuing CA Certificate expired.

c) All sDNs issued in Certificates MUST be recorded and kept until one (1) year after the issuing CA Certificate expired or for the whole lifetime of that name space which ever is longer.

d) For data collected at the RAs:
   i. For Certificate Application forms and supporting documents (paper based or in electronic format): one (1) year after the pertinent end-entity Certificate expired.

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 and Network Administrators.

5.4.5 Audit log backup procedures

In common with all other relevant eduPKI CA 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 Information Security Officer is to be immediately notified in the event of any serious occurrences. In collaboration with System and Network Administrators the Information Security Officer 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 eduPKI CA itself and/or by the vendors of the software deployed.

5.5 Records archival

5.5.1 Types of records archived

The following records relevant to the certification process are archived:

a) The eduPKI CA Certificate
b) All Subscriber's identification and authorisation data as collected by the RAs (see sections 3.2.2, 3.2.3 and 3.2.5)
c) All approved Certificate Applications
d) All Certificates issued by the eduPKI CA
e) All approved Certificate Revocation requests
f) All issued CRLs
g) All versions of this CP/CPS document
h) All audit logs (see section 5.4.1)

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 unauthorised persons.

5.5.4 Archive backup procedures

All electronically recorded 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 full and archive backups are stored in a bank safety deposit box.

5.5.5 Requirements for time-stamping of records

No requirements.

5.5.6 Archive collection system (internal or external)

An internal archive collection system is used.

5.5.7 Procedures to obtain and verify archive information

The Information Security Officer is invested with the authority to authorise the retrieval and verification of archived data.

5.6 Key changeover

The eduPKI CA's private signing key is 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 eduPKI CA's private keys are given in an Emergency Process Instruction manual, see section 5.3.8. 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 eduPKI CA that will have an impact on the proper functioning of the same, the operation of the IT system containing the defect SHALL be immediately terminated.

The IT system SHALL be reset on redundant hardware using backup software and backup data, and SHALL then be checked and put into operation in a safe condition. The defective or modified IT system SHALL 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 SHALL be carried out. If required, additional protective measures SHALL also be put in place to prevent the occurrence of similar incidents in the future. In such cases eduPKI CA employees SHALL work together with experts from the DFN-CERT. Should corrupted data be found in any Certificate, the pertinent Subscriber SHALL be immediately notified and the Certificate immediately revoked.

5.7.3 Entity private key compromise procedures

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

a) Immediate cessation of acceptance of Certificate Applications by the CA

b) Immediate cessation of CA operations

c) Immediate notification of the PMAs with which the eduPKI CA has sought and successfully obtained accreditation and of TACAR to remove the so affected CA Certificate from its trust anchor distributions

d) Immediate notification of all affected Subscribers

e) Immediate revocation of all Certificates (issued by this CA) whose issuance can be acknowledged by available eduPKI CA archive, log or audit trail data. If necessary, the repository will be taken off-line in order to pre-empt incorrect or invalid information being supplied by these services.

f) Publication of a new CRL with the *nextUpdate* field set to a time after the expiration of all issued Certificates

g) Analysis of the events leading to the CA's private key compromise

h) Removal of the cause (based on the analysis) leading to the CA's private key compromise

i) Generation of a new key pair and new Certificate for the CA

j) Publication of the new Certificate of the CA

k) Resumption of CA operations following the instructions of the Information Security Officer

l) Issuance of new end-entity Certificates for Subscribers

5.7.4 Business continuity capabilities after a disaster

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

5.8 CA or RA termination

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

a) Notification of all Subscribers, RAs and Relying Parties, the PMAs with which the eduPKI CA has sought and successfully obtained accreditation, TACAR and concerned organisations in a period at least three months prior to termination.

b) Timely revocation of all Certificates.

c) Generation and publication of a CRL with the *nextUpdate* field set to a time after the expiration of all issued Certificates.

d) Safe destruction of all private keys held by the CA.

The organisation named in section 1.5.1 will ensure the continued existence of the archive records, and of a complete and downloadable CRL, for the stipulated period of retention.

A terminating RA SHALL relay all its archived records (see section 5.5.1 b) to the CA or the RA's organisation MUST keep the RA's archived records for the stipulated period of retention. The CA SHALL disable access of the RA to the CA systems.

6 TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

6.1.1 Key pair generation

Cryptographic key pairs for the eduPKI 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.

Subscribers' cryptographic key pairs MAY be generated by the Subscribers themselves on systems that the Subscribers can access, by the Subscribers' home organisations on behalf of the Subscribers or by the CA or RA in a secure and trustworthy manner.

6.1.2 Private key delivery to Subscriber

If the cryptographic key pair is directly generated on a system that the Subscriber accesses, there is no need to deliver private keys from the CA or RA systems to the Subscriber.

If the cryptographic key pair is generated by the Subscriber's home organisation, the pertinent RA or CA on their systems the private key SHALL be delivered to the Subscriber in a secure and trustworthy manner, using strong passwords to protect the private key and secure procedures to deliver the password to the Subscriber e.g. by a PIN letter handed over to the Subscriber personally or sent asynchronously from the delivery of the private key.

6.1.3 Public key delivery to Certificate issuer

The Certificate Application including the CSR formatted as a self-signed PKCS#10 [PKCS] structure will be submitted to the eduPKI CA using a secure communication channel (e.g. TLS protected web pages). The RA approves the Certificate Application using a mutually authenticated secured communication channel (e.g. TLS protected web pages with client authentication).

6.1.4 CA public key delivery to Relying Parties

All Relying Parties MAY download the eduPKI 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 following cryptographic algorithms and key sizes are used:

a) The RSA algorithm (with SHA1 or SHA256 checksums) is used for signatures.

b) The key size for the eduPKI CA key SHALL be set to a minimum of 2048 bit (RSA).

c) All other keys of issued Certificates MUST have a minimum key size of 2048 bit (RSA), or if non-RSA keys are used, a cryptographically equivalent key size that is at least as strong as that.

6.1.6 Public key parameters generation and quality checking

Parameters for the CA key SHALL be selected with great care and be generated by the eduPKI CA.

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.

A Subscriber's private key MAY be generated and/or stored in a software or hardware token, e.g. in a file or on a cryptographic smart-card.

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

No provision is made for multi-person control of eduPKI 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's private key escrow MAY be supported, see section 4.12.

A Subscriber's private key MAY only be escrowed if the Subscriber gave his/her written consent to the key escrow. In this case the escrowed key MUST always ever be stored in a secure manner using strong encryption on the private key itself. The retrieval/recovery of the escrowed key MUST always ever follow a dual control principle either with the involvement of the Subscriber himself/herself or if that is not possible/desirable with the involvement of the data protection and privacy officer of the Subscriber's home organisation.

CA's private keys SHALL NOT be escrowed.

6.2.4 Private key backup

Private key backup is not supported for individual Subscribers' private keys by the CA. If the Subscriber backs up his/her private key, special care MUST be taken that the backed up private key is encrypted using strong encryption and that only the Subscriber or otherwise authorised personnel can decrypt the backed up private key.

If Subscribers' private keys are escrowed (see section 6.2.3) the escrowed private keys MAY be backed-up (e.g. in form of a database backup of all escrowed private keys) only in a secure manner. Special care MUST be taken that backups containing escrowed private keys are encrypted using strong encryption and that only authorised personnel can access the backups at on-site as well as off-site data storage locations.

Private keys of the CA stored in the HSM are backed up with mechanisms provided by the HSM. The resulting encrypted HSM backup files are stored in on-site vaults and off-site safety deposit boxes. Access to these is strictly regulated.

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

6.2.5 Private key archival

The archiving of individual Subscribers' private keys is not supported by the CA.

If Subscribers' private keys are escrowed (see section 6.2.3) the escrowed private keys MAY be archived (e.g. in form of a database dump of all escrowed private keys) only in a secure manner. Special care MUST be taken that archives containing escrowed private keys are encrypted using strong encryption and that only authorised personnel can access the archives at on-site as well as off-site data storage locations.

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.

A Subscriber's private key MAY be stored in its cryptographic module in unencrypted form, e.g. without password protection. In this case the private key MUST be protected by proper operating system access control mechanisms to prevent unauthorised access.

6.2.8 Method of activating private key

The private key of the eduPKI CA in the HSM is activated by using a SmartCard and entering a pass-phrase to unlock the SmartCard.

6.2.9 Method of deactivating private key

Deactivation of the private key of the CA is automatic. Once the certification process is ended, technical measures prevent any further use of the private key without reactivating it.

6.2.10 Method of destroying private key

The destruction of the eduPKI CA private keys is subject to the dual control principle. The Information Security Officer and the CA Operator are needed to destroy the eduPKI 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 eduPKI CA have the following periods of validity:

a) eduPKI CA root Certificates: a maximum validity period of twenty (20) years

b) All other issued Certificates: a maximum validity period of five (5) years

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 Certificate renewal purposes is permissible if the required algorithms and key sizes allow for it (see section 6.1.5).

6.4 Activation data

Activation data are pass-phrases and/or cryptographic tokens that protect private keys and are entered and/or used to unlock and activate these for the purposes of certification, signature and decryption.

6.4.1 Activation data generation and installation

The quality of the activation data (i.e. length and combination of characters) must be of an appropriate high standard.

The eduPKI CA's activation data for certification purposes is divided into two halves shared by two CA operators.

6.4.2 Activation data protection

Activation data of the private key of the eduPKI CA MUST never be disclosed and MAY only be made known to members of CA staff who require them. The activation data MUST NOT be recorded in writing except for purposes of private key backup as specified in section 6.2.4.

6.4.3 Other aspects of activation data

Activation of the private key of the eduPKI CA is only possible in accordance with the dual control principle needing two CA operators each of them knowing only one half of the pass-phrase.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

All applications within the eduPKI CA are exclusively carried out using hardened operating systems dedicated to CA operations including access control and user authentication.

6.5.2 Computer security rating

No stipulation.

6.6 Life cycle technical controls

6.6.1 System development controls

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) Regular inspection and update of the security concept
b) Checking security measures during on-going operations (see section 5.4)
c) Regular monitoring of the integrity of applications and operating systems in use
    i. Centralized logging of all security processes and procedures
    ii. Collaboration with the Computer Emergency Response Team of the DFN (DFN-CERT)
    iii. Applying upgrades and patches to the CA systems when and if required
    iv. Deployment on a production system only following testing and approval on a test system

6.6.3 Life cycle security controls

No stipulation.

6.7 Network security controls

The network of the eduPKI CA is divided into various security zones which are all separated from one another by firewalls. In addition, Intrusion Prevention 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 the DFN-CERT. On all firewalls rules are activated which only permit CA related 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 eduPKI CA for populating X.509 [X509] end-entity Certificates.

7.1 Certificate profile

All Certificates SHALL follow the PKIX [PKIX] Certificate Profile as defined in RFC 5280 [RFC5280].

7.1.1 Version number(s)

All issued Certificates SHALL be compliant to ITU-T recommendation X.509 version 3 [X509].

7.1.2 Certificate extensions

The eduPKI CA Certificate includes the following extensions:

a) *basicConstraints*: critical; *cA*=true;
b) *keyUsage*: critical; *keyCertSign* and *crlSign* bits are set (any others are unset);
c) *authorityKeyIdentifier*: not critical; value is set to the SHA-1 or SHA-2 hash of the BIT STRING *subjectPublicKey* of the eduPKI CA Certificate;
d) *subjectKeyIdentifier*: not critical; value is set to the SHA-1 or SHA-2 hash of the BIT STRING *subjectPublicKey* of the eduPKI CA Certificate

End-entity Certificates include the following extensions:

a) *basicConstraints*: critical; *cA*=false;
b) *keyUsage*: critical; by default, only the *digitalSignature* and *keyEncipherment* bits are set;
c) *authorityKeyIdentifier*: not critical; value is set to the SHA-1 or SHA-2 hash of the BIT STRING *subjectPublicKey* of the issuing CA's Certificate;
d) *subjectKeyIdentifier*: not critical; value is set to the SHA-1 or SHA-2 hash of the BIT STRING *subjectPublicKey* of the end-entity's Certificate;
e) *certificatePolicies*: not critical; see section 7.1.6;
f) *cRLDistributionPoint*: not critical; includes one or more HTTP URIs for retrieving the CRL of

the issuing CA in DER format;

g) *authorityInfoAccess*: not critical; includes one or more entries (of syntax *id-ad-caIssuers*) with a HTTP URI for retrieving the issuing CA's Certificate in DER format; MAY include one or more entries (of syntax *id-ad-ocsp*) with a HTTP URI to an OCSP responder if the CA supports OCSP;

h) *subjectAlternativeName*: not critical; MUST include at least one entry (suitable for the intended Certificate use case) of type *dNSName*, *rfc822Name* or *iPAddress*; MAY include further entries of these or other types; *subjectAlternativeNames* SHALL be included for requested Certificates compliant with specific TPs, see table 4.

TP for	**subjectAlternativeName *Certificate extension***
eduroam Certificates	a) MUST include entries of type *dNSName* containing the FQDNs of the eduroam Service/Identity Provider entity described by the sDN. b) MUST NOT include wildcard domains in entries of type *dNSName.*
Multi-Domain Network Services Certificates	a) MUST include entries of type *dNSName* containing the FQDNs of the infrastructure node described by the sDN. b) MUST NOT include wildcard domains in entries of type *dNSName.*
Generic Server- and Client-Machine-Certificates	a) MUST include entries of type *dNSName* containing the FQDNs of the machine described by the sDN. b) Additionally MAY include wildcard domains in entries of type *dNSName.*

Table 4: TP specific subjectAlternativeNames

i) *extendedKeyUsage*: not critical; SHOULD include at least one OID out of

   i. TLS client authentication (*id-kp-clientAuth*, OID 1.3.6.1.5.5.7.3.2 [PKIX]); or

   ii. TLS server authentication (*id-kp-serverAuth*, OID 1.3.6.1.5.5.7.3.1 [PKIX]); or

   iii. Code Signing (*id-kp-codeSigning*, OID 1.3.6.1.5.5.7.3.3 [PKIX]); or

   iv. Email Protection (*id-kp-emailProtection*, OID 1.3.6.1.5.5.7.3.4 [PKIX]); or

   v. Microsoft Smartcard Logon, OID 1.3.6.1.4.1.311.20.2.2;

   MAY include other *extededKeyUsage* OIDs; *extendedKeyUsage* OIDs SHALL be included for requested Certificates compliant with specific TPs, see table 5.

TP for	**extendedKeyUsage *Certificate extension***
eduroam Certificates	MUST include the OIDs a) TLS client authentication (*id-kp-clientAuth*, OID 1.3.6.1.5.5.7.3.2 [PKIX]) and b) TLS server authentication (*id-kp-serverAuth*, OID 1.3.6.1.5.5.7.3.1 [PKIX]).
Multi-Domain Network Services Certificates	MUST include the OIDs/OID a) TLS client authentication (*id-kp-clientAuth*, OID 1.3.6.1.5.5.7.3.2 [PKIX]) and/or b) TLS server authentication (*id-kp-serverAuth*, OID 1.3.6.1.5.5.7.3.1 [PKIX]).
Generic Server- and Client-Machine-Certificates	MUST include the OIDs/OID a) TLS client authentication (*id-kp-clientAuth*, OID 1.3.6.1.5.5.7.3.2 [PKIX]) and/or b) TLS server authentication (*id-kp-serverAuth*, OID 1.3.6.1.5.5.7.3.1 [PKIX]).

Table 5: TP specific extendedKeyUsage OIDs

7.1.3 Algorithm object identifiers

The algorithms with OIDs supported by the eduPKI CA are:

a) *rsaEncryption* (OID 1.2.840.113549.1.1.4 [PKIX])

b) *sha1WithRSAEncryption* (OID 1.2.840.113549.1.1.5 [PKIX])

c) *sha256WithRSAEncryption* (OID 1.2.840.113549.1.1.11 [PKIX])

7.1.4 Name forms

All Certificates issued by the eduPKI CA use DC-style distinguished names as described in section 3.1.1.

The subject name of the eduPKI CA Certificate is `/dc=org/dc=edupki/CN=eduPKI CA G 01`.

7.1.5 Name constraints

All end-entity Certificates issued by the eduPKI CA have a subject distinguished name starting with `/dc=net/dc=geant`. No formal name constraints extensions are specified in the issued Certificates.

7.1.6 Certificate policy object identifier

Certificates issued by the eduPKI 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 Certificate issuance as *policyIdentifier* OID.

Additional *policyIdentifier* OIDs SHALL be included for requested Certificates compliant with specific TPs, see table 6.

TP for	***Additional* policyIdentifier *OIDs***
eduroam Certificates	a) 1.3.6.1.4.1.27262.1.13.1.1 (base arc of TP OID) b) 1.3.6.1.4.1.27262.1.13.1.1.1.4 (TP OID) c) 1.3.6.1.4.1.25178.3.1.1 only for Certificates issued to eduroam Service Providers d) 1.3.6.1.4.1.25178.3.1.2 only for Certificates issued to eduroam Identity Providers
Multi-Domain Network Services Certificates	a) 1.3.6.1.4.1.27262.1.13.1.2 (base arc of TP OID) b) 1.3.6.1.4.1.27262.1.13.1.2.1.3 (TP OID) c) 1.3.6.1.4.1.27262.1.13.100.10 only for Certificates issued to any infrastructure nodes from GÉANT's Multi-Domain Network Services d) 1.3.6.1.4.1.27262.1.13.100.10.1.1 only for Certificates issued to infrastructure nodes from GÉANT's Multi-Domain Network Services acting as server e) 1.3.6.1.4.1.27262.1.13.100.10.1.2 only for Certificates issued to infrastructure nodes from GÉANT's Multi-Domain Network Services acting as machine client f) 1.3.6.1.4.1.27262.1.13.100.10.2.1 only for Certificates issued to infrastructure nodes participating in the autoBAHN service g) 1.3.6.1.4.1.27262.1.13.100.10.2.2 only for Certificates issued to infrastructure nodes participating in the perfSONAR service h) 1.3.6.1.4.1.27262.1.13.100.10.2.3 only for Certificates issued to infrastructure nodes participating in the cNIS service i) 1.3.6.1.4.1.27262.1.13.100.10.2.4 only for Certificates issued to infrastructure nodes participating in the I-SHARe service
Generic Server- and Client-Machine-Certificates	a) 1.3.6.1.4.1.27262.1.13.1.3 (base arc of TP OID) b) 1.3.6.1.4.1.27262.1.13.1.3.1.2 (TP OID)

Table 6: Additional policyIdentifier *OIDs for TPs*

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

All CRLs SHALL follow the PKIX CRL Profile as defined in RFC 5280 [RFC5280].

7.2.1 Version number(s)

All issued CRLs SHALL be compliant to ITU-T recommendation X.509 version 2 [X509].

7.2.2 CRL and CRL entry extensions

CRL extensions used:

a) *cRLNumber*: integer value, number of the CRL

b) *authorityKeyIdentifier*: not critical; value is set to the SHA-1 or SHA-2 hash of the BIT STRING *subjectPublicKey* of the issuing CA’s Certificate

7.3 OCSP profile

The eduPKI CA MAY support OCSP.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The eduPKI CA MUST ensure that all its procedures and processes are carried out in compliance with the provisions of this CP/CPS. An audit of the eduPKI CA will be effected by the DFN-Verein. Such audit SHALL be effected during a compromise and disaster recovery exercise (see section 5.7.2) 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 organisation named in section 1.5.1 with the rules and procedures specified in this CP/CPS

b) Current list of CA personnel

PMAs with which the eduPKI CA has sought and successfully obtained accreditation MAY request an audit of the eduPKI CA.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

If services rendered by the eduPKI CA are liable for costs, fees are given in a price list which SHALL be published in the repository (see chapter 2) if applicable.

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 Certificate Requesters 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 and CRLs including all information which MAY be derived from such SHALL be deemed as non-confidential.

9.3.3 Responsibility to protect confidential information

The eduPKI CA bears the responsibility of protecting confidential information and ensuring that it will not be compromised.

9.4 Privacy of personal information

9.4.1 Privacy plan

In the course of its duties the eduPKI CA operator has to electronically store and process personal data. All such actions SHALL be performed in accordance with German laws on data security and privacy. 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 eduPKI CA 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 eduPKI CA 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.

Distribution or reproduction of this CP/CPS document in unchanged form is explicitly allowed.

The distribution of the eduPKI CA Certificate and its CRLs (in unchanged and digitally signed form) as available from the repository (see chapter 2) is explicitly allowed.

eduroam® is a registered trademark of the GÉANT Association.

9.6 Representations and warranties

9.6.1 CA representations and warranties

It is incumbent on the eduPKI CA's personnel 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 RAs' personnel 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 eduPKI CA 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 eduPKI CA.

9.10.2 Termination

This document will remain in force until it is replaced by a new version, or the eduPKI CA 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 eduPKI CA 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 eduPKI, details are given in section 1.5.

Amendments in support of additional TPs MUST consider to add to/update the following sections of this CP/CPS:

Section	***Description***
1.1 Overview	Add TP and its OID to the list of supported TPs.
1.3.1 Certification authorities	Add TP and associated Certificate name to table 1.
1.5.4 CPS approval procedures	Add TP to the list of TPs this CP/CPS adheres to.
3.1.2 Need for names to be meaningful	Specify if TP allows for wildcard domain certificates.
3.2.5 Validation of authority	Amend table 3 by TP's additional requirements for the validation of authority.
3.3 Identification and authentication for re-key requests	Specify TP's requirements in regards to identification and authentication for re-key requests.
4.6 Certification renewal	Specify TP's requirements in regards to certification renewal.
4.7 Certificate re-key	Specify TP's requirements in regards to Certificate re-key.
4.12 Key escrow and recovery	Specify if the TP allows for any key escrow and recovery plan offered by the CA.
7.1.2 Certificate extensions	Specify TP's additional requirements on the Certificate profile, e.g. *keyUsage*, *extendedKeyUsage*, etc.. Amend tables 4 and 5.
7.1.6 Certificate policy object identifier	Specify TP's additional requirements on the policy object identifier extension. Amend table 6.
9.12 Amendments	Amend table 7 by any additional sections – due to the inclusion of a new TP – that include TP dependant requirements.

Table 7: Changes to support additional TPs

Other sections MAY be affected depending on the TP that is to be supported.

9.13 Dispute resolution provisions

In case of any disputes the operator of the CA SHALL decide and implement a resolution of the dispute.

9.14 Governing law

The CP/CPS and the operations of the eduPKI CA are all governed by the law of the Federal Republic of Germany.

9.15 Compliance with applicable law

RAs, Subscribers and Relying Parties MUST adhere to the local law applicable.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

All provisions made in this CP/CPS apply to the eduPKI CA and its participants (see section 1.3). Additional oral agreements 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 eduPKI CA are governed by the law of the Federal Republic of Germany. Place of fulfilment and sole place of jurisdiction is the registered office of the CA operator.

9.16.5 Other provisions

None.

Glossary

The glossary is available online: https://www.edupki.org/documents/glossary

References

[BDSG] Privacy Laws of the Federal Republic of Germany

[EDUPKI_OID] Registry of OIDs assigned by eduPKI, https://www.edupki.org/documents/object-identifiers-oids/

[GLOSSARY] Glossary for eduPKI PMA documents. https://www.edupki.org/documents/glossary

[IANA_SR_DNS] IANA, Special-Use Domain Names, https://www.iana.org/assignments/special-use-domain-names/special-use-domain-names.txt

[IANA_SR_IP4] IANA, IANA IPv4 Special-Purpose Address Registry, https://www.iana.org/assignments/iana-ipv4-special-registry/iana-ipv4-special-registry.txt

[IANA_SR_IP6] IANA, IANA IPv6 Special-Purpose Address Registry, https://www.iana.org/assignments/iana-ipv6-special-registry/iana-ipv6-special-registry.txt

[ISO-3166-1] International Organization for Standardization, ISO 3166-1:2006, Codes for the representation of names of countries and their subdivisions – Part 1: Country codes, http://www.iso.org/iso/country_codes.htm

[ISO-3166-2] International Organization for Standardization, ISO 3166-2:2007, Codes for the representation of names of countries and their subdivisions – Part 2: Country subdivision code, http://www.iso.org/iso/country_codes.htm

[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)

[RFC1035] IETF, Network Working Group, RFC 1035, "Domain Names - Implementation and Specification", P. Mockapetris, 1987

[RFC1918] IETF, Network Working Group, RFC 1918, "Address Allocation for Private Internets", Y. Rekhter, B. Moskowitz, D. Karrenberg, G. J. de Groot, E. Lear, 1996

[RFC2119] IETF, Network Working Group, RFC 2119, "Key words for use in RFCs to Indicate Requirement Levels", S. Bradner, 1997

[RFC2606] IETF, Network Working Group, RFC 2606, "Reserved Top Level DNS Names", D. Eastlake, A. Panitz, 1999

[RFC3647] IETF, Network Working Group, RFC 3647, "Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework", S. Chokhani, W. Ford, R. Sabett, C. Merrill, S. Wu, 2003

[RFC4291] IETF, Network Working Group, RFC 4291, "IP Version 6 Addressing Architecture", R. Hinden, S. Deering, 2006

[RFC5280] IETF, Network Working Group, RFC 5280, "Internet X.509 Public Key Infrastructure, Certificate and Certificate Revocation List (CRL) Profile", D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, W. Polk, 2008

[RFC5952] IETF, RFC 5952, "A Recommendation for IPv6 Address Text Representation", S. Kawamura, M. Kawashima, 2010

[RFC6761] IETF, RFC 6761, "Special-Use Domain Names", S. Cheshire, M. Krochmal, 2013

[RFC6890] IETF, RFC 6890, "Special-Purpose IP Address Registries", M. Cotton, R. Bonica (Ed.), B. Haberman, L. Vegoda, 2013

[RFC791] IETF, RFC 791, "Internet Protocol, DARPA Internet Program, Protocol Specification", University of Southern California, 1981

[RFC822] IETF, RFC 822, "Standard for the Format of ARPA Internet Text Messages", David H. Crocker, 1982

[TP_EDUROAM] eduPKI and eduroam, eduPKI Trust Profile for eduroam Certificates, 2016

[TP_GN_MDNS] eduPKI and GÉANT's Multi-Domain Network Services, eduPKI Trust Profile for Certificates for GÉANT's Multi-Domain Network Services, 2016

[TP_GSCM] eduPKI and GÉANT's Management/IT, eduPKI Trust Profile for Generic Server- and Client-Machine-Certificates, 2016

[X500] ITU-T, X.500, "Information technology – Open Systems Interconnection – The Directory: Overview of concepts, models and services", 2005

[X509] ITU-T, X.509, "Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks”, Version 3, 2005