Amsterdam Office
Singel 468 D
1017 AW Amsterdam
The Netherlands
+31 (0) 20 5304488

www.geant.org
info@geant.org

Trusted Certificate Service (TCS)

TCS Personal CA, eScience Personal CA, and Document Signing CA Certificate Practice Statement

Version 2.0
February 2015
http://www.terena.org/tcs/

Table of Contents

1. Introduction

This document is the Certificate Practice Statement (CPS) for the Trusted Certificate Service (TCS), managed by the GÉANT Association's Amsterdam office (formerly TERENA) for the community of its Members, applicable to the Issuing Authorities for the Personal, eScience Personal, and Document Signing Certificate Profiles – hereafter collectively referred to a 'TCS Personal CAs'.

It outlines the responsibility, operational, and technical principles and practices that TCS employs in providing certificate services that include, but are not limited to, approving, issuing, using and managing Digital Certificates and maintaining a X.509 Certificate based public key infrastructure (PKIX) in accordance with this CPS determined by the GÉANT Association, including the management of a repository and notification of the roles and responsibilities for parties involved in Certificate based practices within the TCS PKI.

The TCS technical implementation is operated on behalf of the GÉANT Association by a CA Operator, which for this CPS is DigiCert, Inc. of Lehi, Utah, USA.

This CPS complies and must comply with the CA Operator's Certificate Policy, and must be interpreted in conjunction with the CPS of the CA Operator. This CPS augments, details, and profiles the CA Operator's CPS for the TCS service. Where no further stipulations are made in this CPS, the stipulations of the CA Operator's CPS apply.

This CPS may be updated and supplemented with amendments in order to provide for additional product offerings, and to comply with certain regulatory or industry standards and requirements.

1.1 Overview

The TCS Personal, eScience Personal, and Document Signing Certificate Authorities (hereafter collectively called 'TCS Personal CAs') is a Certificate Authority (CA) that issues level-2 client certificates, IGTF Classic or MICS Certificates, or LoA1 assurance certificates for signing documents – as defined by the CA Operator's CPS – to Subscribers and their Applicants, where Subscribers are Research and/or Educational organization and/or non-commercial members of an NREN requesting a Certificate through an Account at the CA Operator.

This CPS is only one of many documents that are relevant to the TCS Personal CA's certificate issuance practices. Other pertinent documents include

- The Certificate Terms of Use - the agreement to which authorized Applicants agree on behalf of the Subscriber when submitting a certificate signing request,
- The TCS Consolidated Required Contractual Terms, putting binding requirements on the NREN members and the Subscribers
- the Relying Party agreement,
- other ancillary agreements that are posted on the TCS repository.

These documents obligate parties using or relying on a TCS Personal digital certificate to meet a certain minimum criteria prior to their use or reliance on a TCS Personal Certificate.

The CPS is formatted and maintained in accordance with IETF PKIX RFC 3647, and must be read in conjunction with the Certificate Policy and the Certificate Practice Statements of the CA Operator.

The TCS Personal CAs relate to the following Certificate types issued by the CA Operator:

- 1-3 year Client Encryption Certificate – Level 2 Client Certificates enabled for encryption (Email security plus, Enterprise)
- 1-3 year Client Signing Certificate – Level 2 Client Certificates enabled for signing (Digital Signature Plus, Enterprise)
- 1-3 year Client s/MIME Certificate – Level 2 Client Certificates enabled for both encryption and signing (Client Premium, Enterprise)
- 1-3 year Document Signing Certificate – LOA1 assurance certificate for signing Adobe PDF, Microsoft Office, OpenOffice, and LibreOffice documents complying with the U.S.

Federal ESIGN Act using FIPS 140-2 two factor authentication
- 1-3 year Custom Client Certificates – Created with unique attributes

The TCS eScience Personal CA relates to the following Certificate types issued by the CA Operator:
- 13 month Grid Client Certificate – IGTF MICS and Classic profile certificates containing an email address
- 13 month Grid Robot Certificate – IGTF Classic profile certificate used for M2M communication

1.2 Document Name and Identification

This document is the TCS Personal CAs CPS version 2.0, which was approved for publication in February 2015 by the TCS Policy Management Authority. This document is identified by the following unique registered object identifier: 1.3.6.1.4.1.25178.2.3.2.0.

The CPS is a public statement of the practices of the TCS Personal CAs and the conditions of issuance, revocation and renewal of a certificate issued under the TCS Personal CAs PKI hierarchy. Revisions to this document have been made as follows:

Revision	Version	Date
Changed copyright notice	1.1	11 June 2010
Corrected PMA contact e-mail	1.2	16 December 2011
Align with DigiCert CA Operator operations	2.0	February 2015

Revisions not denoted “significant” are those deemed by the CA’s Policy Management Authority to have minimal or no impact on Subscribers and Relying Parties using certificates, using the CRLs, or using the OCSP responses of the issuing CAs. Insignificant revisions may be made without changing the version number of this CPS.

1.3 PKI Participants

1.3.1 Certification Authorities

The TCS Personal CAs are Chain Certificate Authorities under the DigiCert AssuredID Root CA.

The TCS Personal CAs are part of the Trusted Certificate Service (TCS). The Trusted Certificate Service is managed by the GÉANT Association for the community of its Members.

The CA systems for TCS are hosted and operated by DigiCert, Inc. of Lehi, Utah, USA (hereafter the CA Operator).
The TCS Personal CAs:

- Conform its operations to this CPS as may from time to time be modified by amendments published in the TCS repository (http://www.terena.org/activities/tcs/repository-g3/).
- Conform to the activities as specified in the CA Operator’s CP and CPS for the types of certificates it issues.

1.3.2 Registration Authorities

Registration Authority (RA) functions are undertaken by Subscribers through their Identity Providers. An Identity Provider (IdP) registers and maintains identity related information of Applicants, takes care of authentication, and supplies attributes pertaining to an authenticated Applicant.

Applicants must be registered in the IdP of a Subscriber, and their identity vetted by that Subscriber. Applicants need to be explicitly authorised by the Subscriber to apply for a TCS Personal CA certificate, and must only be authorised if their identity information in the Subscriber’s IdP has been properly validated. The Subscriber must securely communicate the relevant identity attributes and this authorisation to the TCS Personal CA before a certificate

can be issued.

1.3.3 Subscribers

A *Subscriber* is a Research and/or Educational organization and/or non-commercial member of an NREN requesting a Certificate through an Account at the CA Operator.

Subscribers authorise Applicants to apply for a certificate from the TCS Personal CAs, and are identified in issued certificates.

The Subject of the certificate is assigned to the Applicant. Regardless of the Subject listed in the Certificate, the Subscriber always has the responsibility of ensuring that the Certificate is only used appropriately.

1.3.4 Relying Parties

No further stipulations beyond those set forth by the CA Operator.

1.3.5 Other Participants

The TCS Personal CAs comprise a network of Members who authorise Subscribers and their Identity Providers to act as Registration Authorities. Members are National Research and Education Networking organizations who have entered into an agreement with the GÉANT Association to provide TCS services to their Subscribers.

Members must comply with the requirements of this CPS, and ensure the compliance of its Subscribers. The TCS Personal CA, rather than the Member, maintains full control over the certificate lifecycle process, including application, issuance, renewal and revocation.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Usage

No further stipulations beyond those set forth by the CA Operator.

1.4.2 Prohibited Usage

No further stipulations beyond those set forth by the CA Operator.

1.5 Policy Administration

1.5.1 Organisation Administering the Document

This CPS and any related documents, agreements, or policy statements referenced herein are maintained and administered by the TCS Policy Management Authority.

1.5.2 Contact Person

Trusted Certificate Service
GÉANT Association
Singel 468D
1017 AW Amsterdam
The Netherlands

E-mail: tcs-pma@terena.org

1.5.3 Person Determining CPS Suitability for Policy

The suitability and applicability of the TCS Personal CAs CPS is reviewed and approved by the Trusted Certificate Service Policy Management Authority and it shall comply with the requirements of the CP and CPS of the CA Operator as determined by its Policy Management Authority.

1.5.4 CPS Approval Procedures

The TCS Personal CAs CPS and any amendments made to it are reviewed and approved by TCS Policy Management Authority and shall comply with the requirements of the CP and CPS of the CA Operator as determined by its Policy Management Authority.

Amendments to the CPS may be made by reviewing and updating the entire CPS or by publishing an addendum. The current version of the CPS is always made available to the public through TCS' repository which can be accessed online at http://www.terena.org/activities/tcs/repository-g3/.

All updates, amendments and changes are logged in accordance with the logging procedures referenced in Section 5.4 "Audit Logging Procedures" of this CPS.

1.6 Definitions and Acronyms

Acronyms:

CA	Certificate Authority
CPS	Certificate Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
HTTP	Hypertext Transfer Protocol
IdP	Identity Provider
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardization Sector
OCSP	Online Certificate Status Protocol
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure (based on X.509 Digital Certificates)
PKCS	Public Key Cryptography Standard
RA	Registration Authority
RFC	Request for Comments (see http://www.rfc-editor.org/)
SSL	Secure Sockets Layer
TLS	Transport Layer Security
URL	Uniform Resource Locator
X.509	The ITU-T standard for Certificates and their corresponding authentication framework

Definitions:

Applicant:	An Applicant is an individual from the constituency of a Subscriber that - through applying via that Subscriber - is allowed to apply for a Certificate on behalf of the Subscriber.
CA Operator:	The partner contracted by the GÉANT Association to provide certificate services. The CA Operator for this CPS is DigiCert, Inc. of Lehi, Utah, USA.
Certificate:	A certificate is formatted data that cryptographically binds an identified Subject to a public key. It allows the Subject taking part in an electronic transaction to prove its identity to other participants.
End Entity:	An End Entity is an individual or end system that is the subject of a certificate. End entities are not authorized to issue certificates other than Proxy Certificates.
IGTF	Interoperable Global Trust Federation. It defines guidelines and profiles to accredit authorities for use with e-Infrastructure applications.
Identity Provider:	An Identity Provider (IdP) is a service that registers and maintains identity information about individuals, authenticating them, and

	supplying relevant identity information to other services as necessary. An Identity Provider is operated on behalf of a Subscriber.
Member *or* NREN:	A Member is a National Research and Education Networking organization (NREN) that has entered into an agreement with GÉANT Association to provide TCS Personal CA services to its Subscribers.
Proxy Certificate:	A digicat Certificate as defined in RFC 3820
Relying Party:	The Relying Party is an entity that relies upon the information contained within the Certificate.
Relying Party Agreement:	The Relying Party Agreement is an agreement that must be read and accepted by a Relying Party prior to validating, relying on or using a Certificate and is available for reference at the repository of the TCS and/or at the repository of the CA Operator.
Subscriber:	A Research and/or Educational organization and/or non-commercial member of an NREN requesting a Certificate through an Account at the CA Operator. Given the responsibility of a Subscriber for all the certificates of their Applicant this term is often used to include the Subscriber and all its Applicants.
Subscriber Agreement:	A Subscriber Agreement is an agreement between a Member and one of its Subscribers that must be accepted and endorsed by the Subscriber and the Applicant before applying for or requesting a Certificate. The Subscriber Agreement is also acknowledged in the Terms of Use, which is accepted by Subscribers and Applicants.
Subject:	The Subject of a certificate is an entity associated with the use of the private key corresponding to a Certificate.
TCS Personal CAs:	All certificate authorities, being the Personal CA, the eScience Personal CA, and the Document Signing CA, of the TCS service to which this CPS applies.
User	Any individual who uses the certificate application, management, issuance, and monitoring portal(s) or system(s) of the TCS and/or of the CA Operator

References

CA Operator CP	"DigiCert Certificate Policy (CP)" at https://www.digicert.com/ssl-cps-repository.htm
CA Operator CPS	"Certification Practice Statement (CPS)" at https://www.digicert.com/ssl-cps-repository.htm
Relying Party Agreement	"DigiCert Relying Party Agreement" at https://www.digicert.com/ssl-cps-repository.htm
Certificate Terms of Use	as posted in the TCS Repository at http://www.terena.org/activities/tcs/repository-g3/
TCS Consolidated Required	Contractual Terms as posted in the TCS Repository at http://www.terena.org/activities/tcs/repository-g3/
IGTF Classic Profile	https://www.igtf.net/ap/classic, version 4.4
IGTF MICS Profile	https://www.igtf.net/ap/mics, version 1.3

2. Publication and Repository Responsibilities

This CPS is only one of a set of documents relevant to the TCS services. Relevant documents

and/or references thereto are made available through the TCS Repository. The TCS Repository can be found at http://www.terena.org/activities/tcs/repository-g3/.

2.1 Repositories

The TCS Certificate Policy Management Authority maintains the TCS repository. All updates, amendments and changes are logged in accordance with the logging procedures referenced in this CPS. TCS publishes a history of all versions of this CPS that have been in force.

TCS makes all reasonable efforts to ensure that parties accessing its Repositories receive accurate, updated, and correct information. However, TCS cannot accept any liability beyond the limits set forth in this CPS.

All Policies, Practices, and ancillary documents managed by the CA Operator are held in the Repository of the CA Operator, which can be found at https://www.digicert.com/ssl-cps-repository.htm

2.2 Publication of Certificate Information

The certificate of the TCS Personal CAs are published in the TCS repository. End Entity certificates are not published in this repository, but may be published elsewhere in order to fulfil Certificate Transparency requirements.

Root Certificates are published at https://www.digicert.com/digicert-root-certificates.htm

There are no further stipulations beyond those set forth by the CA Operator.

2.3 Time or Frequency of Publication

Updates to the CPS are published in accordance with Section 9.12 “Amendments”.

There are no further stipulations beyond those set forth by the CA Operator.

2.4 Access Controls on Repositories

The information published in the TCS repository is public information and may be accessed freely by anyone visiting the site, provided they agree to the site’s terms and conditions as posted thereon. Read-only access to the information is unrestricted. TCS has implemented logical and physical security measures to prevent unauthorized additions, modification, or deletions of repository entries.

There are no further stipulations beyond those set forth by the CA Operator.

3. Identification and Authentication

3.1 Naming

3.1.1 Types of Names

The Certificates of the TCS Personal CAs are issued with an X.501 compliant non-null Distinguished Name (DN) in the Issuer and Subject Fields.

For the TCS Personal CA the Issuer Distinguished Name is:

/C=NL/ST=Noord-Holland/L=Amsterdam/O=TERENA/CN=TERENA Personal CA 3

The Subject Distinguished Names for Personal certificates consist of the following Components:

Attribute	Abbr.	Value
Country	C	The two letter ISO 3166-1 country code of the relevant Subscriber

State	ST	(optional) State or Province in which the organization is based
Location	L	(optional) City, Town, or Municipality in which the organization is based
Organization	O	The name of the Subscriber
Organizational Unit	OU	(optional) The name of the organizational unit of the Subscriber
Common Name	CN	A reasonable representation of the name of the Applicant
emailAddress		(optional) one or more rfc822 email addresses of the Applicant

For the TCS eScience Personal CA the Issuer Distinguished Name is:

/C=NL/ST=Noord-Holland/L=Amsterdam/O=TERENA/CN=TERENA eScience Personal CA 3

The Subject Distinguished Names for eScience Personal certificates consist of the following Components:

Attribute	**Abbr.**	**Value**
Domain Component	DC	“org”
Domain Component	DC	“terena”
Domain Component	DC	“tcs”
Country	C	The two letter ISO 3166-1 country code of the relevant Subscriber
Organization	O	The name of the Subscriber
Organizational Unit	OU	(optional) The name of the organizational unit of the Subscriber
Common Name	CN	A reasonable representation of the name of the Applicant appended with an Identifier that uniquely and persistently represents the Applicant in the Subscriber's IdP as described in Section 3.1.5 “Uniqueness of Names”; Or: a Robot name in compliance with the specification in this section.

The Common Name (CN) attribute value in the Subject Distinguished Name is obtained from the Subscriber's IdP. For eScience Personal certificates, the CN value will only contain characters that can be encoded in an ASN.1 IA5STRING representation and is a representation of the name as is customary in the best practice for the language and/or country involved.

The Organization (O) attribute value in the Subject Distinguished Name is obtained either from the Subscriber's IdP or directly from the Subscriber during the registration process. For eScience Personal certificates, the O value will be a ASN.1 PrintableString representation thereof as is customary in the best practice for the language involved.

The Organizational Unit (OU) attribute value of the Subject Distinguished Name is obtained from the Subscriber's IdP. For eScience Personal certificates, the OU value will be a PrintableString representation thereof as is customary in the best practice for the language involved.

For the eScience Personal CA a Subscriber may request additional certificates for automated clients (“Robots”). The types of names used in such certificates follow the specification of Subject Distinguished Names for eScience Personal certificates, with the Common Name (CN) attribute set according to the Guidelines for Approved Robots, using “Robot – “ as the unambiguous identifier, followed by either the reasonable representation of the name of the Applicant; or an electronic mail address of a persistent group of people responsible for the robot operations; or the validated fully-qualified domain name of the system from which the robot shall be solely operating. It may be post-pended by further disambiguating name elements. For representations of the name of the Applicant, the value will be a PrintableString representation

thereof as is customary in the best practice for the language involved.

Other subject names in the certificate may be included as stipulated by the CPS of the CA Operator.

For the TCS Document Signer CA the Issuer Distinguished Name is:

C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert Document Signing CA

The Subject Distinguished Names for Document Signer certificates follows the definition of the Personal Certificate subject distinguished name.

There are no further stipulations beyond those set forth by the CA Operator.

3.1.2 Need for Names to be Meaningful

The TCS eScience Personal CA uses non-ambiguous designations and commonly used semantics to identify both the Issuer of the Certificate and the Subject of the Certificate. The CN attribute of an End Entity certificate Subject contains a reasonable representation of the name of the End Entity appended with an Identifier that uniquely and persistently represents the End Entity in the Subscriber's IdP as described in Section 3.1.5 “Uniqueness of Names”.

No further stipulations beyond those set forth by the CA Operator.

3.1.3 Anonymity or Pseudonymity of Subscribers

No further stipulations beyond those set forth by the CA Operator.

3.1.4 Rules for Interpreting Various name Forms

No further stipulations beyond those set forth by the CA Operator.

3.1.5 Uniqueness of Names

The Subject Distinguished Name of a TCS eScience Personal CA-issued Certificate is unique for each Applicant by including an Identifier that uniquely and persistently represents the Applicant in the IdP of its Subscriber. A Subscriber will ensure the persistence and uniqueness of the aforementioned Identifier that its IdP releases to the TCS eScience Personal CA. The Identifier must be traceable to a Applicant for at least as long as the certificate issued to the Applicant is valid. If the traceability from Identifier to Applicant is lost, the Subscriber will ensure the Identifier will not be reused.

There are no further stipulations beyond those set forth by the CA Operator.

3.1.6 Recognition, Authentication, and Role of Trademarks

TCS does not arbitrate, mediate, or otherwise resolve any dispute concerning the ownership of any intellectual property or a domain’s use of any infringing material. TCS in its sole discretion and without any liability may reject an application or revoke a certificate, based on any intellectual property infringement claims or ownership disputes.

There are no further stipulations beyond those set forth by the CA Operator.

3.2 Initial Identity Validation

No further stipulations beyond those set forth by the CA Operator.

3.2.1 Method to Prove Possession of Private Key

No further stipulations beyond those set forth by the CA Operator.

3.2.2 Authentication of Organization Identity

All Personal certificates shall contain Organisation information. This information is validated and authenticated according to the requirements for Level 2 Client Certificates as per the CPS of the

CA Operator. The organization name, address, and legal existence are verified by the CA Operator and associated with the Subscriber and its Applicants.

There are no further stipulations beyond those set forth by the CA Operator.

3.2.3 Authentication of Individual Identity

The identity of a Applicant in a Subscriber's IdP has been validated by the Subscriber in accordance with the requirements set forth by the CA Operator for the certificate product requested. TCS eScience Personal certificates shall be authenticated according to the requirements for IGTF Classic and MICS certificates and as specified by the CA Operator CPS.

When the requesting process is linked to the issuance through electronic means, the Subscriber expresses that an identity has been properly validated by setting a specific value in the *eduPersonEntitlement* attribute of the Applicant's identity in the Subscriber's IdP. The specific value is agreed upon between the Member and the Subscriber.

A Subscriber may link the certificate request to the authenticated individual entity by other means as provided by the CA Operator, as long as all requirements of the CA Operator and those on the Uniqueness of Names as specified in section 3.1.5 are met. In order to meet the requirements, the Subscriber must ensure that the identity vetting is based on data from a identity management system that contains verified content, from which it is clear that the requirements on identity vetting have been met, and where the certificate request process is linked to the entity listed in the identity management system used. For eScience Personal certificates, the unique identifier shall be constructed by the subscriber based on data in the identity management system in a way similar to it having been generated through electronic means. The act of verification must be documented by the Subscriber in either the order system of the CA Operator or through other auditable means. For the validity period of the certificate, the Subscriber shall record in the identity management system or in the order system of the CA operator enough information to enable trace-back to the physical person, and to request revocation in case such traceability is lost.

For Robot certificates based on Name, the Subscriber shall associate the name in a way compatible linking eScience Personal certificates through non-electronic means. It shall ensure uniqueness of the name through either a unique identifier associated with the entity in the identity management system, or through other documented means. The Subscriber and CA Operator shall verify the email address used.
For Robot certificates based on email, the Subscriber and the CA operator shall verify the email address listed in the certificate.
For Robot certificates based on FQDN, the Subscriber shall verify the association of the listed FQDN and the authorized applicant, and the Subscriber and CA operator shall verify the email address listed in the certificate.

There are no further stipulations beyond those set forth by the CA Operator.

3.2.4 Non-Verified Subscriber Information

No further stipulations beyond those set forth by the CA Operator.

3.2.5 Validation of Authority

An Applicant is authorised to request and/or obtain a certificate with the TCS Personal CA and eScience Personal CA by the presence of a specific value in the *eduPersonEntitlement* attribute of that Applicant as released by the Subscriber's IdP, the specific value of which is agreed upon between Member and Subscriber, or by explicit invitation by the Subscriber via means provided by the CA Operator.

The Subscriber shall, on an ongoing basis, control and be responsible for the data that its Applicants supplied to TCS. The Subscriber must promptly notify TCS of any misrepresentations and omissions made by an Applicant.

There are no further stipulations beyond those set forth by the CA Operator, especially for the Document Signing CA.

3.2.6 Criteria for Interoperation

No further stipulations beyond those set forth by the CA Operator.

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication for Routines Re-key

No further stipulations beyond those set forth by the CA Operator.

3.3.2 Identification and Authentication for Re-key After Revocation

No further stipulations beyond those set forth by the CA Operator.

3.4 Identification and Authentication for Revocation Requests

No further stipulations beyond those set forth by the CA Operator.

4. Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

No further stipulations beyond those set forth by the CA Operator.

4.1.1 Who Can Submit a Certificate Application

For the Personal and eScience Personal CA, those who can request certificates are limited to Subscribers that are so configured by the Member NRENs or by the GÉANT Association. Every Subscriber and every Member, by signing the TCS Subscriber Agreement and agreeing to the Certificate Terms of Use, complies with the requirements of this CPS and its supporting documents.
The Subscriber and/or Member shall only link compliant identity management system(s) to the TCS Personal and eScience Personal service. It shall ensure that the entitlement expressing identity vetting and eligibility is only asserted for those entities that are authorized Applicants that meet all requirements, including authentication and vetting requirements, of this CPS. If the Subscriber links an Applicant to certificate request via non-electronic means, the Subscriber shall ensure through such other means comply with this CPS before permitting the submission of certificate applications.
For the Personal and eScience Personal CAs, only those entities that qualify shall have the possibility of certificate applications.

There are no further stipulations beyond those set forth by the CA Operator.

4.1.2 Enrollment Process and Responsibilities

Generally, Applicants will complete the online forms made available by the CA Operator or a Member through its web enrolment application in order to apply for a certificate.

All Applicants using the self-issuance portal must complete the following enrolment process prior to being issued a certificate:

1. The Applicant establishes a secured session with the web enrolment application provided by the CA Operator and/or relevant Member after a successful authentication with its Subscriber's IdP. This authentication is done by a secured transaction.

2. The IdP releases the required attributes to the web enrolment application using a secure transaction within the secure session established in Step 1. The released attributes include:
    - the identity of the Subscriber;
    - optionally, the name of the Organizational unit within the Subscriber;
    - a reasonable representation of the name of the Applicant;

- an Identifier that uniquely and persistently represents the Applicant in the Subscriber's IdP as described in Section 3.1.5 “Uniqueness of Names”;
- the Applicant’s e-mail address(es);
- the eduPersonEntitlement expressing the Applicant’s identity has been properly validated and the Applicant is authorised to request a certificate with the TCS Personal CA or eScience Personal CA.

3. The Applicant submits a Certificate Signing Request (CSR) to the web enrolment application using a secure transaction within the secure session established in Step 1.

The Applicant is responsible for generating a new key pair and the corresponding PKCS#10 CSR.

The Applicant is responsible to make reasonable efforts to prevent the compromise, loss, disclosure, modification or otherwise unauthorised use of his account with the IdP of the Subscriber. The Applicant is responsible to notify the Subscriber in case of an occurrence that materially affects the integrity of his IdP account.

The Applicant is responsible to make reasonable efforts to prevent the compromise, loss, disclosure, modification or otherwise unauthorised use of his private key. The Applicant is responsible to revoke his certificate in case of an occurrence that materially affects the integrity or confidentiality of his private key.

The Subscriber may also issue authenticated invitations to Applicants to apply for a certificate. Such invitations shall only be sent after successful authentication of the identity of the Applicant and validation of any data to be included in the certificate. This process is managed by the CA Operator in accordance with the stipulations set forth by the CA Operator.

There are no further stipulations beyond those set forth by the CA Operator, especially for Document Signing certificates, the enrolment process shall be as defined by the CA Operator.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

The TCS Personal and eScience Personal CA use a Subscriber's Identity Provider to ascertain the identity of an Applicant.

Prior to issuing a Certificate, the TCS Personal and eScience Personal CA employ controls to validate Subscriber and Applicant information featured in the certificate application. The validation process may be an automated process where, upon receiving an application for a Certificate, the receiving web enrolment application:

- ensures that the application has been submitted via a secure session established among the Applicant, its Subscriber's IdP and the enrolment application;
- verifies the identity of the Subscriber's IdP by validating the signature on the delivered attributes;
- verifies the authorization of the Applicant using the method described in Section 3.2.5 “Validation of Authority”.
- verifies the identity of the Applicant based on the secure session parameters;
- verifies that all required attributes pertaining to the Applicant have been released by its Subscriber's IdP and that all the attributes' values comply with the requirements on syntax and semantics;
- verifies the integrity of the PKCS#10 CSR.

There are no further stipulations beyond those set forth by the CA Operator, especially for the Document Signing CA.

4.2.2 Approval or Rejection of Certificate Applications

No further stipulations beyond those set forth by the CA Operator.

4.2.3 Time to Process Certificate Applications

No further stipulations beyond those set forth by the CA Operator.

4.3 Certificate Issuance

4.3.1 CA Actions During Certificate Issuance

No further stipulations beyond those set forth by the CA Operator.

4.3.2 Notification to Requester by the CA of Issuance of Certificate

No further stipulations beyond those set forth by the CA Operator.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

No further stipulations beyond those set forth by the CA Operator.

4.4.2 Publication of the Certificate by the CA

No further stipulations beyond those set forth by the CA Operator.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

No further stipulations beyond those set forth by the CA Operator.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

No further stipulations beyond those set forth by the CA Operator.

4.5.2 Relying Party Public Key and Certificate Usage

No further stipulations beyond those set forth by the CA Operator.

4.6 Certificate Renewal

No further stipulations beyond those set forth by the CA Operator.

4.6.1 Circumstances for Certificate Renewal

No further stipulations beyond those set forth by the CA Operator.

4.6.2 Who May Request Renewal

No further stipulations beyond those set forth by the CA Operator.

4.6.3 Processing Certificate Renewal Requests

No further stipulations beyond those set forth by the CA Operator.

4.6.4 Notification of New Certificate Issuance to Subscriber

No further stipulations beyond those set forth by the CA Operator.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

No further stipulations beyond those set forth by the CA Operator.

4.6.6 Publication of the Renewal Certificate by the CA

No further stipulations beyond those set forth by the CA Operator.

4.6.7 Notification of Certificate Issuance by the CA to other Entities

No further stipulations beyond those set forth by the CA Operator.

4.7 Certificate Re-key

No further stipulations beyond those set forth by the CA Operator.

4.7.1 Circumstances for Certificate Re-Key

No further stipulations beyond those set forth by the CA Operator.

4.7.2 Who May Request Certificate of a New Public Key

No further stipulations beyond those set forth by the CA Operator.

4.7.3 Processing Certificate Re-keying Requests

No further stipulations beyond those set forth by the CA Operator.

4.7.4 Notification of New Certificate Issuance to Subscriber

No further stipulations beyond those set forth by the CA Operator.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

No further stipulations beyond those set forth by the CA Operator.

4.7.6 Publication of the Re-keyed Certificate by the CA

No further stipulations beyond those set forth by the CA Operator.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

No further stipulations beyond those set forth by the CA Operator.

4.8 Certificate Modification

4.8.1 Circumstance for Certificate Modification

No further stipulations beyond those set forth by the CA Operator.

4.8.2 Who May Request Certificate Modification

No further stipulations beyond those set forth by the CA Operator.

4.8.3 Processing Certificate Modification Requests

No further stipulations beyond those set forth by the CA Operator.

4.8.4 Notification of New Certificate Issuance to Subscriber

No further stipulations beyond those set forth by the CA Operator.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

No further stipulations beyond those set forth by the CA Operator.

4.8.6 Publication of the Modified Certificate by the CA

No further stipulations beyond those set forth by the CA Operator.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

No further stipulations beyond those set forth by the CA Operator.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

Revocation of a certificate is the permanent end of the operational period of the certificate prior to reaching the end of its stated validity period.

In addition to the circumstances for revocation as documented in the CP and CPS of the CA Operator, the TCS Personal CAs shall also revoke a digital certificate if it becomes aware of any of the following circumstances:

- For an eScience Personal certificate, there has been loss, theft, modification, unauthorized disclosure, or other compromise of the private key associated with a Proxy Certificate, directly or indirectly derived at any level from the certificate;
- The Applicant's IdP account is compromised, revoked or its password is compromised;
- The Subscriber, the Applicant or the Member has breached a material obligation under this CPS or a relevant agreement;
- Either the Subscriber's, Applicant's, or Member's obligations under this CPS or the relevant Subscriber Agreement are delayed or prevented by a natural disaster, computer or communications failure, or other cause beyond the person's reasonable control, and as a result another person's information is materially threatened or compromised;
- A Digital Certificate has not been issued in accordance with the policies set out in this CPS;
- The Subscriber or Applicant has used the Subscription Service contrary to law, rule or regulation, or TCS reasonably believes that the Subscriber is using the certificate, directly or indirectly, to engage in illegal or fraudulent activity;
- The certificate was issued to persons or entities identified as publishers of malicious software or that impersonated other persons or entities;
- The certificate is being used or is suspected to be used to distribute or sign malware;
- The certificate was issued as a result of fraud or negligence; or
- The certificate, if not revoked, will compromise the trust status of TCS.

When considering whether or not the certificate should be revoked, the TCS Personal CAs will consider:

- The nature and number of complaints received
- The nature of the complaining party
- Relevant legislation and industry standards
- Additional outside input regarding the trust status of the certificate or the nature of the use of the certificate

If a Subscriber cancels its subscription of the TCS Personal CAs, all valid certificates pertaining to that Subscriber shall be revoked on the termination date of the Subscriber Agreement.
If a Member cancels its subscription of the TCS Personal CAs, all valid certificates pertaining to that Member shall be revoked on the termination date of the contract.

There are no further stipulations beyond those set forth by the CA Operator.

4.9.2 Who can Request Revocation

The Subscriber or other appropriately authorized parties can request revocation of a certificate. Prior to the revocation of a certificate the TCS Personal CAs will verify that the revocation request has been made by the properly authorized entity:

- a Member can request the revocation of any certificate within its constituency of Subscribers;

- a Subscriber can request the revocation of any certificate within its constituency of Applicants;
- an Applicant can request the revocation of its own certificate.

A revocation request can be initiated by other entities. Such a revocation request has to be properly and convincingly documented.

There are no further stipulations beyond those set forth by the CA Operator.

4.9.3 Procedure for Revocation Request

The TCS Personal CAs employ the following procedure for authenticating a revocation request depending on the entity who requested the revocation:

- A properly authenticated revocation request made by a Member, Subscriber or Applicant will be automatically accepted without any other checks. The revocation request and the identity of the entity requesting revocation will be logged.
- If the entity requesting revocation can prove his/her ownership of the private key associated with the certificate, the TCS Personal CAs will revoke the certificate without any other checks. The revocation request and the proof of the relevant private key by the entity requesting revocation will be logged.
- If the request has been initiated by entities other than Member, Subscriber or Applicant, the receiving Member or Subscriber will verify that the reasons for the request match those defined in Section 4.9.1 “Circumstances for Revocation”. The Member or Subscriber will revoke the certificate only if it finds reasonable grounds for revocation based on the submitted documentation.

There are no further stipulations beyond those set forth by the CA Operator.

4.9.4 Revocation Request Grace Period

No further stipulations beyond those set forth by the CA Operator.

4.9.5 Time Within Which CA Must Process the Revocation Request

No further stipulations beyond those set forth by the CA Operator.

4.9.6 Revocation Checking Requirement for Relying Parties

No further stipulations beyond those set forth by the CA Operator.

4.9.7 CRL Issuance Frequency

No further stipulations beyond those set forth by the CA Operator.

4.9.8 Maximum Latency for CRLs

No further stipulations beyond those set forth by the CA Operator.

4.9.9 On-line Revocation/Status Checking Availability

No further stipulations beyond those set forth by the CA Operator.

4.9.10 On-line Revocation Checking Requirements

No further stipulations beyond those set forth by the CA Operator.

4.9.11 Other Forms for Revocation Advertisements available

No further stipulations beyond those set forth by the CA Operator.

4.9.12 Special Requirements re Key Compromise

No further stipulations beyond those set forth by the CA Operator.

4.9.13 Circumstances for Suspension

No further stipulations beyond those set forth by the CA Operator.

4.9.14 Who can Request Suspension

No further stipulations beyond those set forth by the CA Operator.

4.9.15 Procedure for Suspension Request

No further stipulations beyond those set forth by the CA Operator.

4.9.16 Limits on Suspension Period

No further stipulations beyond those set forth by the CA Operator.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

No further stipulations beyond those set forth by the CA Operator.

4.10.2 Service Availability

No further stipulations beyond those set forth by the CA Operator.

4.10.3 Optional Features

No further stipulations beyond those set forth by the CA Operator.

4.11 End of Subscription

If a Subscriber cancels its subscription of the TCS Personal CAs, all valid certificates pertaining to that Subscriber shall be revoked on the termination date of the Subscriber Agreement.
If a Member cancels its subscription of the TERENA Personal CAs, all valid certificates pertaining to that Member shall be revoked on the termination date of the contract.

There are no further stipulations beyond those set forth by the CA Operator.

4.12 Key Escrow and Recovery

No further stipulations beyond those set forth by the CA Operator.

5. Facility, Management and Operational Controls

5.1 Physical Security Controls

The TCS Personal CAs make every reasonable effort to detect and prevent material breaches, loss, damage or compromise of assets and interruption to business activities.

5.1.1 Site Location and Construction

No further stipulations beyond those set forth by the CA Operator.

5.1.2 Physical Access

No further stipulations beyond those set forth by the CA Operator.

5.1.3 Power and Air Conditioning

No further stipulations beyond those set forth by the CA Operator.

5.1.4 Water Exposures

No further stipulations beyond those set forth by the CA Operator.

5.1.5 Fire Prevention and Protection

No further stipulations beyond those set forth by the CA Operator.

5.1.6 Media Storage

No further stipulations beyond those set forth by the CA Operator.

5.1.7 Waste Disposal

No further stipulations beyond those set forth by the CA Operator.

5.1.8 Off-site Backup

No further stipulations beyond those set forth by the CA Operator.

5.2 Procedural Controls

5.2.1 Trusted Roles

No further stipulations beyond those set forth by the CA Operator.

5.2.2 Number of Persons Required Per Task

No further stipulations beyond those set forth by the CA Operator.

5.2.3 Identification and Authentication for Each Role

No further stipulations beyond those set forth by the CA Operator.

5.2.4 Roles Requiring Separation of Duties

No further stipulations beyond those set forth by the CA Operator.

5.3 Personnel Security Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

No further stipulations beyond those set forth by the CA Operator.

5.3.2 Background Check Procedures

No further stipulations beyond those set forth by the CA Operator.

5.3.3 Training Requirements

No further stipulations beyond those set forth by the CA Operator.

5.3.4 Retraining Frequency and Requirements

No further stipulations beyond those set forth by the CA Operator.

5.3.5 Job Rotation Frequency and Sequence

No further stipulations beyond those set forth by the CA Operator.

5.3.6 Sanctions for Unauthorized Actions

No further stipulations beyond those set forth by the CA Operator.

5.3.7 Independent Contractor Requirements

No further stipulations beyond those set forth by the CA Operator.

5.3.8 Documentation Supplied to Personnel

No further stipulations beyond those set forth by the CA Operator.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

No further stipulations beyond those set forth by the CA Operator.

5.4.2 Frequency of Processing Log

No further stipulations beyond those set forth by the CA Operator.

5.4.3 Retention Period of Audit Log

No further stipulations beyond those set forth by the CA Operator.

5.4.4 Protection of Audit Log

No further stipulations beyond those set forth by the CA Operator.

5.4.5 Audit Log Backup Procedures

No further stipulations beyond those set forth by the CA Operator.

5.4.6 Audit Collection System

No further stipulations beyond those set forth by the CA Operator.

5.4.7 Notification to Event-Causing Subject

No further stipulations beyond those set forth by the CA Operator.

5.4.8 Vulnerability Assessments

No further stipulations beyond those set forth by the CA Operator.

5.5 Records archival

5.5.1 Types of records archived

No further stipulations beyond those set forth by the CA Operator.

5.5.2 Retention period for archive

Data related to the issuance of certificates shall be held and archived by the CA Operator. For Personal and eScience Personal certificates, the Subscriber shall provide accountability for the identity vetting data contained in the identity management system(s) to enable traceback to the physical person for at least as long as the certificate is valid and in keeping with any additional audit retention requirements. Any necessary supplementary information shall be recorded in the systems provided by the CA Operator.

There are no further stipulations beyond those set forth by the CA Operator.

5.5.3 Protection of archive

No further stipulations beyond those set forth by the CA Operator.

5.5.4 Archive backup procedures

No further stipulations beyond those set forth by the CA Operator.

5.5.5 Requirements for time-stamping of records

No further stipulations beyond those set forth by the CA Operator.

5.5.6 Archive collection system

No further stipulations beyond those set forth by the CA Operator.

5.5.7 Procedures to obtain and verify archive information

No further stipulations beyond those set forth by the CA Operator.

5.6 Key changeover

No further stipulations beyond those set forth by the CA Operator.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

No further stipulations beyond those set forth by the CA Operator..

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

No further stipulations beyond those set forth by the CA Operator.

5.7.3 Business continuity capabilities after a disaster

No further stipulations beyond those set forth by the CA Operator.

5.8 CA termination

In the event that it is necessary for TCS to cease operation, TCS shall make a commercially reasonable effort to notify Participants of such termination in advance of the effective date of the termination. Should TCS cease its CA operations, TCS shall develop a termination plan to minimize the disruption of services to its customers, Subscribers, and Relying Parties.

There are no further stipulations beyond those set forth by the CA Operator.

6. Technical Security Controls

No further stipulations beyond those set forth by the CA Operator.

6.1 Key pair generation and installation

6.1.1 Key pair generation

No further stipulations beyond those set forth by the CA Operator.

6.1.2 Private key delivery to Subscriber

No further stipulations beyond those set forth by the CA Operator.

6.1.3 Public key delivery to certificate issuer

No further stipulations beyond those set forth by the CA Operator.

6.1.4 CA public key delivery to Relying Parties

No further stipulations beyond those set forth by the CA Operator.

6.1.5 Key sizes

No further stipulations beyond those set forth by the CA Operator.

6.1.6 Public key parameters generation and quality checking

No further stipulations beyond those set forth by the CA Operator.

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

No further stipulations beyond those set forth by the CA Operator.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

For eScience Personal certificates, Applicants shall protect any issued certificates according to the IGTF Private Key Protection guidelines as specified at https://www.eugridpma.org/guidelines/pkp/.

There are no further stipulations beyond those set forth by the CA Operator.

6.2.1 Cryptographic module standards and controls

No further stipulations beyond those set forth by the CA Operator.

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

No further stipulations beyond those set forth by the CA Operator.

6.2.3 Private key escrow

No further stipulations beyond those set forth by the CA Operator.

6.2.4 Private key backup

No further stipulations beyond those set forth by the CA Operator.

6.2.5 Private key archival

No further stipulations beyond those set forth by the CA Operator.

6.2.6 Private key transfer into or from a cryptographic module

No further stipulations beyond those set forth by the CA Operator.

6.2.7 Private key storage on cryptographic module

No further stipulations beyond those set forth by the CA Operator.

6.2.8 Method of activating private key

No further stipulations beyond those set forth by the CA Operator.

6.2.9 Method of deactivating private key

No further stipulations beyond those set forth by the CA Operator.

6.2.10 Method of destroying private key

No further stipulations beyond those set forth by the CA Operator.

6.2.11 Cryptographic Module Rating

No further stipulations beyond those set forth by the CA Operator.

6.3 Other aspects of key pair management

No further stipulations beyond those set forth by the CA Operator.

6.3.1 Public key archival

No further stipulations beyond those set forth by the CA Operator.

6.3.2 Certificate operational periods and key pair usage periods

No further stipulations beyond those set forth by the CA Operator.

6.4 Activation data

6.4.1 Activation data generation and installation

No further stipulations beyond those set forth by the CA Operator.

6.4.2 Activation data protection

No further stipulations beyond those set forth by the CA Operator.

6.4.3 Other aspects of activation data

No further stipulations beyond those set forth by the CA Operator.

6.5 Computer security controls

No further stipulations beyond those set forth by the CA Operator.

6.5.1 Specific computer security technical requirements

No further stipulations beyond those set forth by the CA Operator.

6.5.2 Computer security rating

No further stipulations beyond those set forth by the CA Operator.

6.6 Life cycle technical controls

6.6.1 System development controls

No further stipulations beyond those set forth by the CA Operator.

6.6.2 Security management controls

No further stipulations beyond those set forth by the CA Operator.

6.6.3 Life cycle security controls

No further stipulations beyond those set forth by the CA Operator.

6.7 Network security controls

No further stipulations beyond those set forth by the CA Operator.

6.8 Time-stamping

No further stipulations beyond those set forth by the CA Operator.

7. Certificate, CRL and OSCP Profiles

7.1 Certificate profile

7.1.1 Version number(s)

No further stipulations beyond those set forth by the CA Operator.

7.1.2 Certificate extensions

The TCS Personal CAs uses a number of certificate extensions for the purposes intended by X.509v3 as per Amendment 1 to ISO/IEC 9594-8, 1995.

The TCS eScience Personal CA certificate includes the following extensions:

a) ***basicConstraints***: critical; CA=true, pathlen=0

b) ***keyUsage***: critical; 0x60, the keyCertSign, digitalSignature, and cRLSign bits are set (any others are unset)

c) ***authorityKeyIdentifier***: not critical;
keyid:45:EB:A2:AF:F4:92:CB:82:31:2D:51:8B:A7:A7:21:9D:F3:6D:C8:0F

d) ***subjectKeyIdentifier***: not critical;
29:AA:1B:6E:30:F9:30:67:63:A5:87:26:0C:AC:F1:81:9C:69:74:49

e) ***cRLDistributionPoints***: not critical;
URI:http://crl3.digicert.com/DigiCertAssuredIDRootCA.crl
URI:http://crl4.digicert.com/DigiCertAssuredIDRootCA.crl

f) ***authorityInfoAccess***: not critical;
OCSP - URI:http://ocsp.digicert.com
CA Issuers - URI:http://cacerts.digicert.com/DigiCertAssuredIDRootCA.crt

g) **certificatePolicies**
Policy: 2.5.29.32.0 (anyPolicy)
CPS: https://www.digicert.com/CPS

End Entity certificates issued by the eScience Personal CA include the following extensions:

a) ***basicConstraints***: critical; CA=false

b) ***keyUsage***: critical; Digital Signature, Key Encipherment, and Data Encipherment bits are set

c) ***extendedKeyUsage***: not critical;
TLS Web Client Authentication, E-mail Protection

d) ***authorityKeyIdentifier***: not critical;
keyid:8C:9F:11:2E:E6:E3:7A:04:A5:1E:55:8B:46:08:04:A6:ED:97:70:A6

e) ***subjectKeyIdentifier***: not critical;
key-id of the key pair

f) ***certificatePolicies***: not critical;
Policy: 2.16.840.1.114412.4.31.1 (DigiCert Client-public trust), no policy qualifiers
Policy: 1.2.840.113612.5.2.2.1 or Policy: 1.2.840.113612.5.2.2.5 (IGTF Classic or MICS, depending on issuance mode)
Policy: 1.2.840.113612.5.2.3.3.3 (for natural persons), or 1.2.840.113612.5.2.3.3.1 (for Robots)

g) ***subjectAlternativeName***: not critical; includes up to 10 rfc822Name entries with the e-mail addresses of the End Entity

h) ***authorityInfoAccess***: not critical;
OCSP - URI:http://ocsp.digicert.com
CA Issuers - URI:http://cacerts.digicert.com/TERENAeSciencePersonalCA3.crt

i) ***cRLDistributionPoints***: not critical;
URI:http://crl3.digicert.com/TERENAeSciencePersonalCA3.crl
URI:http://crl4.digicert.com/TERENAeSciencePersonalCA3.crl

The TCS eScience Personal certificates and issuing CAs are materially compliant with the Grid Certificate Profile as defined by the Open Grid Forum, document GFD.125 or its relevant updated version(s).

The TCS Personal CA certificate includes the following extensions:

h) ***basicConstraints***: critical; CA=true, pathlen=0

i) ***keyUsage***: critical; 0x60, the keyCertSign, digitalSignature, and cRLSign bits are set (any others are unset)

j) ***authorityKeyIdentifier***: not critical;
keyid:45:EB:A2:AF:F4:92:CB:82:31:2D:51:8B:A7:A7:21:9D:F3:6D:C8:0F

k) ***subjectKeyIdentifier***: not critical;
F0:21:E9:49:77:73:9F:85:AE:18:3B:E8:52:70:14:06:ED:42:EE:CA

l) ***cRLDistributionPoints***: not critical;
URI:http://crl3.digicert.com/DigiCertAssuredIDRootCA.crl
URI:http://crl4.digicert.com/DigiCertAssuredIDRootCA.crl

m) ***authorityInfoAccess***: not critical;
OCSP - URI:http://ocsp.digicert.com
CA Issuers - URI:http://cacerts.digicert.com/DigiCertAssuredIDRootCA.crt

n) **certificatePolicies**
Policy: 2.5.29.32.0 (anyPolicy)
CPS: https://www.digicert.com/CPS

End Entity certificates issued by the Personal CA include the following extensions:

i) ***basicConstraints***: critical; CA=false

j) ***keyUsage***: critical; Digital Signature, Key Encipherment bits are set (Client Premium)

k) ***extendedKeyUsage***: not critical;
TLS Web Client Authentication, E-mail Protection (Client Premium)

l) ***authorityKeyIdentifier***: not critical;
keyid: F0:21:E9:49:77:73:9F:85:AE:18:3B:E8:52:70:14:06:ED:42:EE:CA

m) ***subjectKeyIdentifier***: not critical;
key-id of the key pair

n) ***certificatePolicies***: not critical;
Policy: 2.16.840.1.114412.4.1.2 (Client Level 1 Certificates – Enterprise)
CPS: https://www.digicert.com/CPS

o) ***subjectAlternativeName***: not critical; includes up to 10 rfc822Name entries with the e-mail addresses of the End Entity

p) ***authorityInfoAccess***: not critical;
OCSP - URI:http://ocsp.digicert.com
CA Issuers - URI:http://cacerts.digicert.com/TERENAPersonalCA3.crt

j) ***cRLDistributionPoints***: not critical;
URI:http://crl3.digicert.com/TERENAPersonalCA3.crl
URI:http://crl4.digicert.com/TERENAPersonalCA3.crl

The TCS Document signing certificates issued by the Document Signing CA include the following extensions:

a) ***basicConstraints***: critical; CA=false

b) ***keyUsage***: critical; Digital Signature, Non Repudiation

c) ***extendedKeyUsage***: not critical;
TLS Web Client Authentication, E-mail Protection

d) ***authorityKeyIdentifier***: not critical;
keyid: EF:CE:35:93:CE:F6:86:C5:F8:84:F5:0C:E7:5A:6F:D9:2F:4B:E3:64

e) ***subjectKeyIdentifier***: not critical;
key-id of the key pair

f) ***certificatePolicies***: not critical;
Policy: 2.16.840.1.114412.3.21
Policy: 2.16.840.1.114412.3.21.2
CPS: https://www.digicert.com/CPS
User Notice: Explicit Text: “”

g) ***subjectAlternativeName***: not critical; includes up to 10 rfc822Name entries with the e-mail addresses of the End Entity

h) ***authorityInfoAccess***: not critical;
OCSP - URI:http://ocsp.digicert.com
CA Issuers - URI:http://cacerts.digicert.com/DigiCertDocumentSigningCA.crt

k) ***cRLDistributionPoints***: not critical;
URI: http://crl3.digicert.com/DigiCertDocumentSigningCA-g1.crl
URI: http://crl4.digicert.com/DigiCertDocumentSigningCA-g1.crl

l) ***1.2.840.113583.1.1.9.2*** *(Adobe Archive RevInfo)*
as per Adobe specifications

m) ***1.2.840.113583.1.1.9.1*** *(Adobe Time Stamp)*
as per Adobe specifications, based on http://adobe.timestamp.digicert.com/

There are no further stipulations beyond those set forth by the CA Operator. The CA Operator may define additional profiles, whose specifications and requirements are governed by the CP and CPS of the CA Operator.

There are no further stipulations beyond those set forth by the CA Operator.

7.1.3 Algorithm object identifiers

No further stipulations beyond those set forth by the CA Operator.

7.1.4 Name forms

The subject name of the TERENA Personal CA certificate is *C=NL, ST=Noord-Holland, L=Amsterdam, O=TERENA, CN=TERENA Personal CA 3*

The subject name of the TERENA eScience Personal CA certificate is *C=NL, ST=Noord-Holland, L=Amsterdam, O=TERENA, CN=TERENA eScience Personal CA 3*

The subject name of the Document Signing CA certificate is *C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert Document Signing CA*

Subjects of eScience End Entity Certificates follow the following pattern:

DC: “org”

DC: “terena”

DC: “tcs”

C: ISO 3166 code of the country of the relevant Subscriber

O: Name of the Subscriber

OU: (optional) Name of the organizational unit of the Subscriber

CN: Reasonable representation of the name of the End Entity. For the eScience Personal CA this name shall be appended with a unique identifier assigned persistently to the End Entity by its Subscriber (see Section 3.1.5 ”Uniqueness of Names” and Section 3.1.1 ”Types of Names”). For Robot certificates issued by the eScience Personal CA, the name shall be prepended by “Robot - ” and shall follow the naming convention specified in section 3.1.1.

For certificates issued by the eScience Personal CA all attributes within the certificate subjects contain 7-bit ASCII strings encoded using characters from the IA5STRING subset. For the Personal and Document Signing CAs, the attributes shall use an appropriate encoding sufficient to express the names of the Organisation, Organisational Unit, and CommonName, as specified by the CA Operator.

There are no further stipulations beyond those set forth by the CA Operator

7.1.5 Name constraints

The TCS Personal CAs do not use the nameConstraints extension.

7.1.6 Certificate policy object identifier

No further stipulations beyond those set forth by the CA Operator.

7.1.7 Usage of Policy Constraints extension

No further stipulations beyond those set forth by the CA Operator.

7.1.8 Policy qualifiers syntax and semantics

No further stipulations beyond those set forth by the CA Operator.

7.1.9 Processing semantics for the critical Certificate Policies extension

No further stipulations beyond those set forth by the CA Operator.

7.2 CRL profile

Certificate revocation lists for the TCS issuing CAs are published at least every 24 hours, and are valid for 6 days and 23 hours.

7.2.1 Version number(s)

No further stipulations beyond those set forth by the CA Operator.

7.2.2 CRL and CRL entry extensions

The TCS Personal CA uses the following CRL extensions:

AuthorityKeyIdentifier: F0:21:E9:49:77:73:9F:85:AE:18:3B:E8:52:70:14:06:ED:42:EE:CA

The TCS eScience Personal CA uses the following CRL extensions:

AuthorityKeyIdentifier: 8C:9F:11:2E:E6:E3:7A:04:A5:1E:55:8B:46:08:04:A6:ED:97:70:A6

The Document Signing CA uses the following CRL extensions:

AuthorityKeyIdentifier: EF:CE:35:93:CE:F6:86:C5:F8:84:F5:0C:E7:5A:6F:D9:2F:4B:E3:64

There are no further stipulations beyond those set forth by the CA Operator.

7.3 OCSP profile

There are no further stipulations beyond those set forth by the CA Operator.

8. Compliance Audit and Other Assessments

There are no further stipulations beyond those set forth by the CA Operator.

8.1 Frequency or Circumstances of Assessment

The TCS PMA will, within reasonable limits, accept audit requests on behalf of the EUGridPMA to ensure compliance with relevant accreditation procedures. The entire costs of such audits will be borne by the requesting party.

There are no further stipulations beyond those set forth by the CA Operator.

8.2 Identity/Qualifications of Assessor

There are no further stipulations beyond those set forth by the CA Operator.

8.3 Assessor’s Relationship to Assessed Entity

There are no further stipulations beyond those set forth by the CA Operator.

8.4 Topics Covered by Assessment

There are no further stipulations beyond those set forth by the CA Operator.

8.5 Actions Taken as a Result of Deficiency

There are no further stipulations beyond those set forth by the CA Operator.

8.6 Communication of Results

There are no further stipulations beyond those set forth by the CA Operator.

9. Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

No stipulation.

9.1.2 Certificate Access Fees

No stipulation.

9.1.3 Revocation or Status Information Access Fees

TCS does not charge fees for the revocation of a certificate or for a Relying Party to check the validity status of a TCS issued certificate using its OCSP.

9.1.4 Fees for Other Services

No stipulation.

9.1.5 Refund Policy

No stipulation.

9.2 Financial Responsibility

The final decision concerning whether or not to rely on a verified digital signature is exclusively that of the Relying Party. Reliance on a digital signature should only occur if:

- The digital signature was created during the operational period of a valid certificate and it can be verified by referencing a validated certificate.
- The Relying Party has checked the revocation status of the certificate by referring to the relevant Certificate Revocation Lists and/or the TCS OCSP service and the certificate has not been revoked.
- The Relying Party understands that a digital certificate is issued to a Subscriber for a specific purpose and that the private key associated with the digital certificate may only be used in accordance with the usages suggested in the CPS and specified in the certificate.

Reliance is accepted as reasonable under the provisions made for the Relying Party under this CPS and within the relying party agreement. If the circumstances of reliance exceed the assurances delivered by TCS under the provisions made in this CPS, the Relying Party must obtain additional assurances.

9.2.1 Insurance Coverage

TCS certificates are not covered by GÉANT Association's insurance. The GÉANT Association disclaims all financial liability of any type.

There are no further stipulations beyond those set forth by the CA Operator.

9.2.2 Other Assets

No stipulation.

9.2.3 Insurance or Warranty Coverage for End-Entities

No stipulations beyond those set forth by the CA Operator.

9.3 Confidentiality of Business Information

TCS observes applicable rules on the protection of personal data which by law or the TCS privacy policy are deemed to be confidential.

9.3.1 Scope of Confidential Information

TCS and the CA Operator keep the following types of information confidential and maintain reasonable controls to prevent the exposure of such records to non-trusted personnel.

Executed Subscriber agreements.

Certificate application records and documentation submitted in support of certificate applications whether successful or rejected.

Transaction records and financial audit records.

External or internal audit trail records and reports, except for audit reports that may be published at the discretion of the CA Operator.

Contingency plans and disaster recovery plans.

Internal tracks and records on the operations of TCS infrastructure, certificate management and enrolment services and data.

There are no further stipulations beyond those set forth by the CA Operator.

9.3.2 Information Not Within the Scope of Confidential Information

Subscribers acknowledge that revocation data of all certificates issued by any TCS CA is public information. Subscriber application data marked as “Public” in the relevant Subscriber agreement and submitted as part of a certificate application is published within an issued digital certificate in accordance with this CPS.

9.3.3 Responsibility to Protect Confidential Information

All personnel in trusted positions handle all information in strict confidence. TCS is not required to and does not release any confidential information, unless otherwise required by law, without an authenticated, reasonably specific request by an authorized party specifying:

The party to whom TCS owes a duty to keep information confidential.

The party requesting such information.

A court order, if any.

There are no further stipulations beyond those set forth by the CA Operator.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

The TCS privacy policy is defined by this CPS.

9.4.2 Information Treated as Private

Any information about Subscribers and their Applicants that is not publicly accessible or available through the content of the issued certificate, a CRL, or an OCSP response is treated as private information.

There are no further stipulations beyond those set forth by the CA Operator.

9.4.3 Information Not Deemed Private

Certificates, CRLs, the OCSP, and the information appearing in them are not considered

private.

There are no further stipulations beyond those set forth by the CA Operator.

9.4.4 Responsibility to Protect Private Information

All CA Operator's, Member's, Subscriber's and GÉANT Association 's employees receiving private information are responsible to protect such information from compromise and disclosure to third parties. Each party shall use the same degree of care that it exercises with respect to its own information of similar importance, but in no event shall the degree of care be less than a reasonable degree of care.

There are no further stipulations beyond those set forth by the CA Operator.

9.4.5 Notice and Consent to Use Private Information

Unless otherwise stated in this CPS, a party will not use private information without the subject's express written consent.

There are no further stipulations beyond those set forth by the CA Operator.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

TCS shall be entitled to disclose any confidential or private information, if TCS believes, in good faith, that the disclosure is necessary in response to subpoenas and search warrants or if disclosure is necessary in response to a pending legal proceeding.

There are no further stipulations beyond those set forth by the CA Operator.

9.4.7 Other Information Disclosure Circumstances

No further stipulations beyond those set forth by the CA Operator.

9.5 Intellectual Property Rights

The GÉANT Association or its partners or associates own all intellectual property rights associated with its databases, web sites, and any other publication originating from the GÉANT Association including this CPS.

9.5.1 Certificates

Certificates are the property of the GÉANT Association and/or the CA Operator. The GÉANT Association gives permission to reproduce and distribute certificates on a non-exclusive, royalty-free basis, provided that they are reproduced and distributed in full. The GÉANT Association reserves the right to revoke the certificate at any time. Private and public keys are property of the Subscribers who rightfully issue and hold them.

Subscribers represent and warrant that when submitting to TCS and using a domain and distinguished name (and all other certificate application information), they do not interfere with or infringe any rights of any third parties in any jurisdiction with respect to the third party's trademarks, service marks, trade names, company names, or any other intellectual property right, and that the Subscriber is not seeking to use the domain and distinguished names for any unlawful purpose, including, without limitation, tortuous interference with contract or prospective business advantage, unfair competition, injuring the reputation of another, and confusing or misleading a person, whether natural or incorporated.

There are no further stipulations beyond those set forth by the CA Operator.

9.5.2 Copyright

9.5.3 Trademarks

“Trusted Certificate Service” is and other terms in this CPS are trademarks of TCS and the GÉANT Association and may only be used by permission.

9.5.4 Infringement

Although the GÉANT Association will provide all reasonable assistance, Members and/or Subscribers shall defend, indemnify, and hold the GÉANT Association harmless for any loss or damage resulting from any such interference or infringement and shall be responsible for defending all actions on behalf of the GÉANT Association.

9.6 Representations and Warranties

Applicants, Subscribers, Relying Parties and any other parties shall not interfere with or reverse engineer the technical implementation of TCS, including, but not limited to, the key generation process, the public web site, and the TCS repositories except as explicitly permitted by this CPS or upon prior written approval of the GÉANT Association. Failure to comply with this as a Member will result in the revocation of the Member’s Digital Certificates without further notice to the Member or its Subscribers, and the Member shall pay any charges payable but that have not yet been paid under this Agreement. Failure to comply with this as a Subscriber will result in the revocation of the Subscriber's Digital Certificates without further notice to the Subscriber, and the Subscriber shall pay any charges payable but that have not yet been paid under this Agreement. Failure to comply with this as a Applicant will result in the revocation of the Applicant’s Digital Certificates without further notice to the Applicant. Failure to comply with this as a Relying Party will result in the termination of the agreement with the Relying Party, the removal of permission to use or access the TCS repository and any Digital Certificate or Service provided by TCS.

Parties are solely responsible for having exercised independent judgement and employed adequate training in choosing security software, hardware, and encryption/digital signature algorithms, including their respective parameters, procedures, and techniques as well as PKI as a solution to their security requirements.

There are no further stipulations beyond those set forth by the CA Operator.

9.6.1 CA Representations and Warranties

To the extent specified in this CPS and any Policies and Practices included therein by reference, the GÉANT Association promises to comply with this CPS and any implementation processes thereof.

The Subscriber acknowledges that the GÉANT Association has no further obligations under this CPS.

There are no further stipulations beyond those set forth by the CA Operator.

9.6.2 RA Representations and Warranties

In its role of Registration Authority, the Subscriber represents that:

- The Subscriber’s IdP complies with this CPS.
- All representations made by the Subscriber’s IdP to TCS regarding the information contained in the certificate of its Applicants are accurate and true.
- The Subscriber agrees to provide on request full documentation to the Member and/or the GÉANT Association about the procedures used to populate and maintain the identity related information in its IdP.

Subscribers are exclusively responsible to make reasonable efforts to prevent the compromise, loss, disclosure, modification, or otherwise unauthorized use of its Identity Provider and/or the data contained therein.

There are no further stipulations beyond those set forth by the CA Operator.

9.6.3 Subscriber Representations and Warranties

Upon accepting the Subscriber Agreement, the Subscriber and any authorized Applicants represent to TCS and to Relying Parties that at the time of acceptance and until further notice:

- All representations made by the Subscriber to TCS regarding the information contained in the certificate of its Applicants are accurate and true.
- The Subscriber agrees with the terms and conditions of this CPS and other agreements and policy statements of TCS.
- The Subscriber abides by the laws applicable in its country or territory including those related to intellectual property protection, computer viruses and malware, accessing computer systems etc.
- The Subscriber complies with all export laws and regulations for dual usage goods as may be applicable.
- The Subscriber agrees to give full cooperation to investigations of events that might imperil, put in doubt or reduce the trust associated with the TCS products and services; in particular system security related events.
- The Subscriber agrees, within reasonable limits, to give full cooperation to periodic audits of its IdP and all procedures used for entering and maintaining identity data in its IdP. Audits can be conducted by/on behalf of the relevant Member or the TCS PMA.

Unless otherwise stated in this CPS, Subscribers shall exclusively be responsible:

- To minimize internal risk of private key compromise by ensuring adequate knowledge and training on PKI is provided internally.
- Provide correct and accurate information in its communications with TCS.
- Alert TCS if at any stage whilst a certificate of one of its Applicants is valid, any information originally submitted has changed since it had been submitted to TCS.
- Read, understand and agree with all terms and conditions in this CPS and associated policies published in the TCS Repository at http://www.terena.org/activities/tcs/repository-g3/.
- Refrain from tampering with a TCS certificate.
- Request the revocation of a certificate within one business day in case of an occurrence that materially affects the integrity of a TCS certificate.

When requesting a certificate, at the time of accepting a certificate, and until further notice or until the certificate is revoked, the Applicant – as authorized by the Subscriber – asserts to TCS and to Relying Parties that at the time of acceptance and until further notice:

- any information provided in the request and asserted in the certificate is accurate and true to the best of its knowledge.
- The private key pertaining to the certificate has not been disclosed to unauthorized persons.
- The certificate is used only for permitted purposes, and only in conjunction with the entity named in the organization (O) field of the certificate subject name.
- The Applicant retains control of its private key, uses a trustworthy system, and takes reasonable precautions to prevent its loss, disclosure, modification, or unauthorized use.
- The Applicant will not use the private key corresponding to any public key listed in the certificate for purposes of signing digital certificates, with the exception of Proxy

Certificates, unless expressly agreed in writing between the relevant Subscriber and TCS.

- The Applicant agrees with the terms and conditions of this CPS and other agreements and policy statements of TCS.

Unless otherwise stated in this CPS Applicants shall:

- generate their own private / public key pair to be used in association with the certificate request submitted to TCS.
- ensure that the public key submitted to TCS corresponds with the private key used.
- ensure that the public key submitted to TCS is the correct one.
- provide correct and accurate information in its communications with TCS and/or its Subscriber.
- alert its Subscriber and/or TCS if at any stage whilst the certificate is valid, any information originally submitted has changed since it had been submitted to TCS.
- read, understand and agree with all terms and conditions in this CPS and all associated policies.
- refrain from tampering with a TCS certificate.
- use TCS certificates for legal and authorized purposes in accordance with the suggested usages and practices in this CPS.
- cease using a TCS certificate if any information in it becomes misleading obsolete or invalid.
- refrain from using the private key corresponding to the public key in a TCS issued certificate to issue End Entity digital certificates or subordinate CAs, with the exception of Proxy Certificates.
- make reasonable efforts to prevent the compromise, loss, disclosure, modification, or otherwise unauthorized use of the private key corresponding to the public key published in a TCS certificate.
- request the revocation of a certificate within one business day in case of an occurrence that materially affects the integrity of a TCS certificate.
- The Applicant is responsible to obey the applicable law with respect to each certificate.

There are no further stipulations beyond those set forth by the CA Operator.

9.6.4 Relying Party Representations and Warranties

A party relying on a TCS certificate accepts that in order to reasonably rely on a TCS certificate they must verify that the certificate is valid and has not been revoked. They may only rely on a certificate to the extent warranted by this CPS and any associated documents.

There are no further stipulations beyond those set forth by the CA Operator.

9.6.5 Representations and Warranties of Other Participants

Partners of the TCS network shall not undertake any actions that might imperil, put in doubt or reduce the trust associated with the TCS products and services.

To the extent specified in the relevant sections of the CPS, TCS Members promise to:

Comply with this CPS.

Ensure that the TCS web enrollment application used by the Member complies with this CPS.

Ensure that only authorized Subscribers can access the Member's TCS web enrolment application.

Make reasonable efforts to ensure Subscriber's IdPs are adequately maintained.

Apply adequate organizational and technical safeguards to ensure only authorized IdPs can connect to its web enrollment application.

Conduct or instigate periodic (self-)audits of a sample of its Subscriber's IdPs, and make the results available to the TCS PMA.

Within reasonable limits give full cooperation to periodic audits as described in Section 8 "Compliance Audit and Other Assessements".

There are no further stipulations beyond those set forth by the CA Operator.

9.7 Disclaimers of Warranties

The GÉANT Association disclaims all warranties and obligations of any type, including any warranty of fitness for a particular purpose, and any warranty of the accuracy of unverified information provided, save as contained herein and as cannot be excluded at law.

The GÉANT Association shall not be responsible for non-verified Subscriber information submitted to TCS or otherwise submitted with the intention to be included in a certificate.

In no event (except for fraud or willful misconduct) shall the GÉANT Association be liable for any kind of damages related to the TCS.

There are no further stipulations beyond those set forth by the CA Operator.

9.8 Limitations of Liability

By means of this CPS, TCS has adequately informed Relying Parties on the usage and validation of digital signatures through this CPS and other documentation published in its public repository available at http://www.terena.org/activities/tcs/repository-g3/ or by contacting via out of bands means via the contact address as specified in the Document Control section of this CPS.

The GÉANT Association and the TCS reserve the right to refuse to issue a certificate to any party as it sees fit, without incurring any liability or responsibility for any loss or expenses arising out of such refusal. The GÉANT Association reserves the right not to disclose reasons for such a refusal.

There are no further stipulations beyond those set forth by the CA Operator.

9.9 Indemnities

9.9.1 Indemnification by the GÉANT Association

All provisions specified by the CA Operator in its CP and CPS will hold equally towards TCS and the GÉANT Association.

There are no further stipulations beyond those set forth by the CA Operator.

9.9.2 Indemnification by Subscribers

The Subscriber shall indemnify and hold the GÉANT Association and contractors harmless from any acts or omissions resulting in liability, loss, or damages, and any suits and expenses of any kind, including reasonable attorneys' fees, that the GÉANT Association and the above mentioned parties may incur, that are caused by the use or publication of a certificate, and that arises from data supplied by the Subscriber or by any actions or lack thereof by Subscribers.

All provisions specified by the CA Operator in its CP and CPS will hold equally towards TCS and the GÉANT Association.

There are no further stipulations beyond those set forth by the CA Operator.

9.9.3 Indemnification by Relying Parties

All provisions specified by the CA Operator in its CP and CPS will hold equally towards TCS and the GÉANT Association.

There are no further stipulations beyond those set forth by the CA Operator.

9.10 Term and Termination

9.10.1 Term

This CPS and any amendments hereto shall become effective seven days after being published to the Repository and shall remain effective until terminated in accordance with this section.

9.10.2 Termination

This CPS and any amendments hereto shall remain effective until replaced with a newer version.

9.10.3 Effect of Termination and Survival

In case of termination of CA operations for any reason whatsoever, the GÉANT Association will provide timely notice and transfer of responsibilities to succeeding entities, maintenance of records, and remedies. Before terminating its own CA activities, TCS will take the following steps, where possible:

Providing Members with ninety (90) days notice of its intention to cease acting as a CA.

Revoking all certificates that are still non-revoked or non-expired at the end of the ninety (90) day notice period without consent.

Making reasonable arrangements to preserve its records according to this CPS.

Reserving its right to provide succession arrangements for the re-issuance of certificates by a successor CA that has all relevant permissions to do so and complies with all necessary rules, while its operation is at least as secure as TCS's.

The requirements of this section may be varied by contract, to the extent that such modifications affect only the contracting parties.

9.11 Individual notices and Communications with Participants

The GÉANT Association and TCS accept communications related to this CPS by means of digitally-signed messages or in paper form, addressed as follows:

Trusted Certificate Service
GÉANT Association
Singel 468 D
1017 AW Amsterdam
The Netherlands

And by email at tcs-pma@terena.org.

9.12 Amendments

The TCS Policy Management Authority is responsible for determining the suitability of certificate policies illustrated within the CPS. The Authority is also responsible for determining the suitability of proposed changes to the CPS prior to the publication of an amended edition.

9.12.1 Procedure for Amendment

Amendments to this CPS may be made from time to time by the TCS Policy Management Authority. Amendments shall either be in the form of an amended form of the CPS or made available as a supplemental document on TCS's repository. Updates supersede any designated or conflicting provisions of the referenced version of the CPS and shall be indicated through appropriate revision numbers and publication dates. Revisions that are not deemed significant by TCS Policy Management Authority (those amendments or additions that have minimal or no

impact on Subscribers or Relying Parties), shall be made without notice and without changing the version number of this CPS.

There are no further stipulations beyond those set forth by the CA Operator.

9.12.2 Notification Mechanism and Period

Changes that, according to the TCS PMA, have significant impact will be published at the TCS repository (available at http://www.terena.org/activities/tcs/repository-g3/) with 1 week notice being given of those changes, and by suitably incrementing the version number of the new edition(s).

Major changes affecting accredited certificates are announced and approved by the accrediting agency prior to becoming effective.

There are no further stipulations beyond those set forth by the CA Operator.

9.12.3 Circumstances Under Which OID Must be Changed

If TCS Policy Management Authority decides that a change in TCS's certificate practices warrants a change in the currently specified OID for a particular Certificate type, then the revised CPS or amendment thereto will contain a revised OID for that type of certificate.

If the TCS Policy Management Authority decides that a change in the CA Operators CP or CPS materially affects the certificates issued by TCS, then the revised CPS or amendment thereto will contain a revised OID for the affected type(s) of certificate.

9.13 Dispute Resolution Procedures

Before resorting to any form of dispute resolution all parties will agree to notify the GÉANT Association of the dispute with a view to seek dispute resolution.

9.14 Governing Law

This CPS is governed by, and construed in accordance with the laws of the Netherlands. This choice of law is made to ensure uniform interpretation of this CPS, regardless of the place of residence or place of use of TCS digital certificates or other products and services. The law of the Netherlands applies in all contractual relationships of the GÉANT Association to which this CPS may be pertinent.

9.15 Compliance with Applicable Law

Each party, including TCS partners, Members, Subscribers, Applicants, and Relying Parties must comply with the laws applicable in its country or territory.

9.16 Miscellaneous Provisions

There are no further stipulations beyond those set forth by the CA Operator.

9.17 Other Provisions

There are no further stipulations beyond those set forth by the CA Operator.