Trusted Certificate Service Server CAs CPS

TCS OV Server and OV eScience Server CA Certificate Practice Statement

Version 2.1
Published 2020-03-27
http://www.geant.org/tcs/

Table of Contents

1. Introduction

This document is the Certificate Practice Statement (CPS) for the Trusted Certificate Service (TCS), managed by the GEANT Association's Amsterdam office for the community of the association's Members, applicable to the Issuing Authorities for the Server (Organisation-validated, OV) and eScience Server Certificate Profiles – hereafter collectively referred to a 'TCS Server 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 Sectigo Limited of Salford, United Kingdom, for this contract operating from Roseland, New Jersey, 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 Server and eScience Server Certificate Authorities (hereafter collectively called 'TCS Server CAs') are Certificate Authorities (CA) that issue organizationally-validated digital certificates according to industry standards for public trust and for IGTF Classic or MICS Certificates that also have public trust, to Subscribers and their authorized Applicants, where Subscribers are 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 Server CAs' certificate issuance practices. Other pertinent documents include

- The Certificate Subscriber Agreement - the agreement to which authorized applicants agree on behalf of the Subscriber when submitting a certificate signing request,
- 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 Server digital certificate to meet a certain minimum criteria prior to their use or reliance on a TCS Server 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 Server CA relates to the following Certificate types issued by the CA Operator:

- 1-2 year Server SSL certificates– provided in accordance with OV standards under the CABForum Baseline Requirements

The TCS eScience Server CA relates to the following Certificate types issued by the CA Operator:

- 1 year as well as 13 month Grid Server Certificate ("eScience Server Certificate") – IGTF Classic profile certificate containing domain names. The issuance of these

certificates shall in addition follow all requirements set forth for OV SSL Server Certificates.

The TCS may also provide other certificate types, in particular those complaint with the Extended Validation guidelines of the CABForum, which are issued in accordance with the CP/CPS of the CA Operator and of which this CP/CPS does not make any stipulations.

1.2 Document Name and Identification

This document is the TCS Server CAs CPS version 2.1, which was approved for publication on 2020-03-27 by the TCS Policy Management Authority. This document is identified by the following unique registered object identifier: **1.3.6.1.4.1.25178.2.1.2.1**.

The CPS is a public statement of the practices of the TCS Server CAs and the conditions of issuance, revocation and renewal of a certificate issued under the TCS Server 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
Added DCV and reflected OV G2 validation	1.7	February 2013
Added G2 SHA-2 hierarchy	1.8	18 October 2014
Align with DigiCert CA Operator operations	2.0	February 2015
Align with Sectigo CA Operator operations	2.1	March 2020

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 Server CAs are Chain Certificate Authorities under the USERTrust RSA Certification Authority Root CA and (for ECC certificates) the USERTrust ECC Certification Authority Root CA.

The TCS Server 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 Sectigo Limited (hereafter the CA Operator).

The TCS Server CAs:

- Conform its operations to this CPS as may from time to time be modified by amendments published in the TCS repository.
  This repository is accessible at https://wiki.geant.org/display/TCSNT/
- 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, according to all provisions and contractual obligations that exist between NRENs and Subscribers. Registration Authority personnel at the Subscriber organization shall hold an organizational role that includes the management of digital certificates, information security management, management of software distribution, responsibility for organizational identity management, responsibility for relations

with the TCS NREN member(s) involved, responsibility for relations with the TCS, or the representation of the organization in managerial or legal matters. It may also be any role as permitted by the CA Operator.

The identity of Requesters must be vetted by the Subscriber. Requesters need to be explicitly authorised by the Subscriber to apply for TCS Server CA certificates, and their requests must only be authorised if their identity information has been properly validated.

The Subscriber must securely communicate the relevant request information and this authorisation to the TCS Server CA and to CA Operator systems involved 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 Requesters to apply for a certificate from the TCS Server CAs, and are identified in issued certificates.

The Subject of the certificate is assigned to the Requester. 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 Server CAs comprises a network of Members (NRENs) who authorise Subscribers 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 Server CA, rather than the Member, maintains full control over the certificate lifecycle process, including application, issuance, renewal and revocation.

A TCS Member NREN shall:

- maintain a register of organisations within its constituency that are approved as Subscribers.
- verify the accuracy and authenticity of the information provided by the Subscriber at the time of application as specified in the validation guidelines documentation of the TCS and the CA Operator.
- use official, notarized or otherwise indicated documents to evaluate a Subscriber application
- verify the accuracy and authenticity of the information provided by the Subscriber that is used for issuance or reissuance or renewal of certificates as specified in the TCS and CA Operator guidelines documentation.
- use secure channels to communicate with TCS CAs and the CA Operator.

A TCS member NREN acts locally within its own context of geographical or business partnerships on approval and authorisation by the GÉANT Association in accordance with the TCS practices and procedures

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
Hoekenrode 3
1102 BR Amsterdam
The Netherlands

E-mail: tcs-pma@lists.geant.org

1.5.3 Person Determining CPS Suitability for Policy

The suitability and applicability of the TCS Server CAs CPS is reviewed and approved by the TCS 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 Server 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 https://wiki.geant.org/display/TCSNT/

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.
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 eScience Proxy Certificates.
eScience	the qualifier that expresses that the certificate product(s) are intended to be accreditable according to the IGTF requirements.
eScience Server Certificate	the 13-months Grid Host Certificate product of the CA Operator
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 Server and Code Signing CA services to its Subscribers.
Proxy Certificate:	A certificate as defined in RFC 3820
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 Requesters this term is often used to include the Subscriber and all its Requesters.
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 Requester before applying for or requesting a Certificate. The Subscriber Agreement is also acknowledged in the Terms of Use, which is accepted by Subscribers and Requesters.

Subject:	The Subject of a certificate is an entity associated with the use of the private key corresponding to a Certificate.
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.
TCS Server CAs:	All certificate authorities, being the Server CA and the eScience Server 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	WebPKI CP at https://sectigo.com/legal/
CA Operator CPS	Certificate Practice Statement at https://sectigo.com/legal/
Relying Party Agreement	at https://sectigo.com/legal/
Certificate Subscriber Agreement	as posted at https://sectigo.com/legal/
TCS Consolidated Required	Contractual Terms as posted in the TCS Repository
IGTF Classic Profile	https://www.igtf.net/ap/classic, version 5.0
IGTF MICS Profile	https://www.igtf.net/ap/mics, version 2.0

2. Publication and Repository Responsibilities

This CPS is only one of a set of documents relevant to the TCS services. Relevant document and/or references thereto are made available through the TCS Repository. The TCS Repository can be found at https://wiki.geant.org/display/TCSNT/.

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://sectigo.com/legal/

All Root certificate authorities and necessary non-TCS specific intermediates can be found at https://secure.sectigo.com/products/publiclyDisclosedSubCACerts

2.2 Publication of Certificate Information

The certificate of the TCS Server CAs are published in this repository, but may be published elsewhere in order to fulfil Certificate Transparency requirements.

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 (https://wiki.geant.org/display/TCSNT/) 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 Server CAs are issued with an X.501 compliant non-null Distinguished Name (DN) in the Issuer and Subject Fields.

For the TCS Server CA the Issuer Distinguished Name are:

/C=NL/O=GEANT/OU=TCS/CN=GEANT OV RSA CA 4
/C=NL/O=GEANT/OU=TCS/CN=GEANT OV ECC CA 4

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

Attribute	Abbr.	Value
Country	C	The two letter ISO 3166-1 country code of the relevant Member
State	ST	(for organisations where it is defined, optional) State or Province in which the organization is based
Location	L	City, Town, or Municipality in which the organization is based
streetAddress		(for organsiations where it is defined, optional) the street address of the validated organisation
postalCode		(for organisations where it is defined, optional) the postal code of the validared organsiation
Organization	O	The name of the Subscriber
Organizational Unit	OU	(optional) The name of the organizational unit of the Subscriber
Common Name	CN	A subdomain name (FQDN) within a domain managed by the Subscriber

For the TCS eScience Server CA the Issuer Distinguished Name are:

/C=NL/O=GEANT/OU=TCS/CN=GEANT eScience SSL CA 4
/C=NL/O=GEANT/OU=TCS/CN=GEANT eScience SSL ECC CA 4

The Subject Distinguished Names for eScience Server certificates consist of the following Components in an ordered sequence:

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 Member
StateOrProvince	ST	(for organisations where it is defined) State or Province in which the Subscriber is based
Locality	L	City, Town, or Municipality in which the Subscriber is based
Organization	O	Name of the Subscriber (validated organisation)
Organizational Unit	OU	(optional) The name of the organizational unit of the Subscriber
Common Name	CN	A subdomain name (FQDN) within a domain managed by the Subscriber.

The Common Name (CN) attribute value in the Subject Distinguished Name is a validated sub-domain name of a domain controlled or managed by the Subscriber.

The Organization (O) attribute value in the Subject Distinguished Name is obtained directly from the Subscriber during the registration process, and is validated by the CA Operator according to the relevant OV guidelines for the certificate order.
For eScience Server Certificates, the O value will contain a representation thereof with only characters as contained in the PrintableString subset, as is customary in the best practice for the language involved, and in compliance with the OV guidelines.

The Organizational Unit (OU) attribute value the Subject Distinguished Name is set by the Applicant and validated by the Subscriber RA. For eScience Server certificates, the OU value will only contain characters from the PrintableString subset representation thereof as is customary in the best practice for the language involved.

The subjectAlternativeName shall at least contain the sub-domain name listed in the CN subject name element. Other dNSName subject alternative names in the certificate may be included as stipulated by the CPS of the CA Operator.

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

3.1.2 Need for Names to be Meaningful

For TCS eScience Server CA certificates, the Baseline Requirements that are enforced ensure that, before issuing the certificate, the Applicant is appropriately authorized by the owner of the associated sub-domain name(s) (FQDNs) or the responsible administrator of the machine to use the FQDN identifiers asserted in the certificate.

There are 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

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

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

3.2.3 Authentication of Individual Identity

The identity of an Applicant in a Subscriber's IdP, when used to authenticate to the certificate issuance management system, will be validated by the Subscriber in accordance with the requirements set forth by the CA Operator for the certificate product requested.

For eScience Server certificates, the validation process shall comply with the requirements for OV SSL Server Certificates.

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 Server CAs either by having enrolled as a User on behalf of the Subscriber, or by explicit invitation of 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 a Applicant.

The Subscriber, the Member NREN to whom the Subscriber is associated, and the TCS CA reserve the right to reject applications to issue a certificate to Applicants if, on its own assessment, by issuing a certificate to such parties the good and trusted name of TCS might get tarnished, diminished or have its value reduced and under such circumstances may do so without incurring any liability or responsibility for any loss or expenses arising as a result of such refusal. Applicants whose applications have been rejected may subsequently re-apply.

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

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

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, or use the provided programmatic interface (API).

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

The Applicant, as well as any User of the CA Operator or Member systems, are responsible to make reasonable efforts to prevent the compromise, loss, disclosure, modification or otherwise unauthorised use of his account with the CA Operator or Member order request portal. The Applicant or User is responsible to notify the Subscriber and the CA Operator or Member in case of an occurrence that materially affects the integrity of his account.

The Applicant is responsible to make reasonable efforts to prevent the compromise, loss, disclosure, modification or otherwise unauthorised use of all private keys pertaining to submitted requests. The Applicant is responsible to revoke associated certificates in case of an occurrence that materially affects the integrity or confidentiality of a private key.

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

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

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

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 conclusion 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 Server CAs shall also revoke a Digital Certificate if it becomes aware of any of the following circumstances:

- For an eScience Server Certificate, there has been loss, theft, modification, unauthorized disclosure, or other compromise of the private key associated with an eScience Proxy Certificate, directly or indirectly derived at any level from that eScience Service Certificate;
- 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 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 Server 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

The TCS Server CAs will decide based on these factors and make a decision, which is final.

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

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 Server 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

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 Server 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 Requester 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 Server CAs will revoke the certificate without any other checks. The revocation request and the proof of control over 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 itself 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 Server CAs, all valid certificates pertaining to that Subscriber shall be revoked on the termination date of the Subscriber Agreement.

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 Server 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

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

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

There are two independent chains of TCS Server CAs, one based on an RSA keypair used solely for issuing end-entity certificates using RSA key pairs, and one based on an ECC key pair solely used for issuing end-entity certificates using ECC key pairs.

7.1 Certificate profile

All intermediate certificates are valid 13 years after issuance, till February 16, 2033.
End-entity certificates have validity periods according to their product type as indicated in section 1.1.

7.1.1 Version number(s)

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

7.1.2 Certificate extensions

The TCS Server CAs use 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 Server CA certificates includes the following extensions:

X509v3 extensions:
X509v3 Authority Key Identifier:
keyid: *a keyIdentifier generated in accordance with RFC 5280 section 4.2.1.2*

X509v3 Subject Key Identifier:
a keyIdentifier generated in accordance with RFC 5280 section 4.2.1.2
X509v3 Key Usage: critical
Digital Signature, Certificate Sign, CRL Sign
X509v3 Basic Constraints: critical
CA:TRUE, pathlen:0
X509v3 Extended Key Usage:
TLS Web Server Authentication, TLS Web Client Authentication
X509v3 Certificate Policies:
Policy: X509v3 Any Policy

CPS: https://sectigo.com/CPS

X509v3 CRL Distribution Points:

Full Name:
URI:http://crl.usertrust.com/USERTrustRSACertificationAuthority.crl

Authority Information Access:
CA Issuers - URI:http://crt.usertrust.com/USERTrustRSAAddTrustCA.crt
OCSP - URI:http://ocsp.usertrust.com

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

X509v3 extensions:
X509v3 Authority Key Identifier:
keyid:*a keyIdentifier generated in accordance with RFC 5280 section 4.2.1.2*

X509v3 Subject Key Identifier:
a keyIdentifier generated in accordance with RFC5280 section 4.2.1.2
X509v3 Key Usage: critical
Digital Signature, Key Encipherment, and Data Encipherment
X509v3 Basic Constraints: critical
CA:FALSE
X509v3 Extended Key Usage:
TLS Web Server Authentication, TLS Web Client Authentication
X509v3 Certificate Policies: not critical
As described in the listing following
X509v3 CRL Distribution Points:

Full Name:
URI:http://geant.crl.sectigo.com/GEANTeScienceSSLCA4.crl

Authority Information Access:
CA Issuers - URI:http://geant.crt.sectigo.com/GEANTeScienceSSLCA4.crt
OCSP - URI:http://geant.ocsp.sectigo.com
Subject Alternative Name:
dNSName: *one or more fully qualified domain names*

The following policy OIDs are included:
Policy: 1.3.6.1.4.1.6449.1.2.1.3.1 (Secure Server)
Policy: 2.23.140.1.2.2 (OV TLS Organization Server Certificates)
Policy: 1.2.840.113612.5.2.2.1 (IGTF Classic)
Policy: 1.2.840.113612.5.2.3.3.2 (for networked entities)

For the ECC eScience intermediate CA certificate, the CRL and CA Issuers URI are replaced by respectively http://geant.crl.sectigo.com/GEANTeScienceECCSSLCA4.crl and http://geant.crt.sectigo.com/GEANTeScienceECCSSLCA4.crt

The TCS eScience Server certificates and issuing CAs are materially compliant with the Grid Certificate Profile as defined by the Open Grid Forum, document GFD.225 or its relevant updated version(s).

The TCS Server CA certificates include the following extensions:

X509v3 extensions:
X509v3 Authority Key Identifier:
keyid: *a keyIdentifier generated in accordance with RFC 5280 section 4.2.1.2*

X509v3 Subject Key Identifier:

a keyIdentifier generated in accordance with RFC 5280 section 4.2.1.2
X509v3 Key Usage: critical
Digital Signature, Certificate Sign, CRL Sign
X509v3 Basic Constraints: critical
CA:TRUE, pathlen:0
X509v3 Extended Key Usage:
TLS Web Server Authentication, TLS Web Client Authentication
X509v3 Certificate Policies:
Policy: X509v3 Any Policy
CPS: https://sectigo.com/CPS

X509v3 CRL Distribution Points:

Full Name:
URI:http://crl.usertrust.com/USERTrustRSACertificationAuthority.crl

Authority Information Access:
CA Issuers - URI:http://crt.usertrust.com/USERTrustRSAAddTrustCA.crt
OCSP - URI:http://ocsp.usertrust.com

End Entity certificates issued by the TCS Server CA include the following extensions:

X509v3 extensions:
X509v3 Authority Key Identifier:
keyid:*a keyIdentifier generated in accordance with RFC 5280 section 4.2.1.2*

X509v3 Subject Key Identifier:
a keyIdentifier generated in accordance with RFC5280 section 4.2.1.2
X509v3 Key Usage: critical
Digital Signature, Key Encipherment, and Data Encipherment
X509v3 Basic Constraints: critical
CA:FALSE
X509v3 Extended Key Usage:
TLS Web Server Authentication, TLS Web Client Authentication
X509v3 Certificate Policies: not critical
As described in the listing following
X509v3 CRL Distribution Points:

Full Name:
URI:http://geant.crl.sectigo.com/GEANTOVRSACA4.crl

Authority Information Access:
CA Issuers - URI:http://geant.crt.sectigo.com/GEANTOVRSACA4.crt
OCSP - URI:http://geant.ocsp.sectigo.com
Subject Alternative Name:
dNSName: *one or more fully qualified domain names*

The following policy OIDs are included:
Policy: 1.3.6.1.4.1.6449.1.2.1.3.1 (Secure Server)
Policy: 2.23.140.1.2.2 (OV TLS Organization Server Certificates)

For the ECC variant, the “RSA” in the URLs included in the extension is replaced by “ECC”.

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

Specifically, the CA Operator defines additional profiles, e.g. for EV SSL and EV Code Signing certificates, whose specifications and requirements are governed exclusively by the CP and CPS of the CA Operator and outside the scope of this document.

7.1.3 Algorithm object identifiers

There are two independent chains of TCS Server CAs, one based on an RSA keypair used solely for issuing end-entity certificates using RSA key pairs, and one based on an ECC key pair solely used for issuing end-entity certificates using ECC key pairs.

The appropriate identifiers will be included for all roots, intermediate, and end-entity certificates.

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

7.1.4 Name forms

The subject name of the TCS Server and eScience Server CA certificates are

/C=NL/O=GEANT/OU=TCS/CN=GEANT OV RSA CA 4
/C=NL/O=GEANT/OU=TCS/CN=GEANT OV ECC CA 4
/C=NL/O=GEANT/OU=TCS/CN=GEANT eScience SSL CA 4
/C=NL/O=GEANT/OU=TCS/CN=GEANT eScience SSL ECC CA 4

Subjects of TCS eScience Server End Entity Certificates follow the following pattern:

DC: “org”

DC: “terena”

DC: “tcs”

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

ST: State or province in which the Subscriber is based (optional, required if L is absent)

L: Locality (town or city) in which the Subscriber is based (optional, required if ST is absent)

O: Name of the Subscriber

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

CN: A subdomain name (FQDN) within a domain managed by the Subscriber.
It shall follow the naming convention specified in section 3.1.1.

For certificates issued by the eScience Server CAs all attributes within the certificate subjects contain 7-bit ASCII strings encoded using characters from the IA5STRING subset. For the TCS Server 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 Server 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 Server 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 Server CA uses the following CRL extensions:

AuthorityKeyIdentifier:
keyid:6F:1D:35:49:10:6C:32:FA:59:A0:9E:BC:8A:E8:1F:95:BE:71:7A:0CXX:XX

The TCS eScience Server CA uses the following CRL extensions:

AuthorityKeyIdentifier:
keyid:9A:2B:8A:22:D6:8D:0C:C0:2A:A5:6F:64:33:3F:96:60:67:15:1D:B2There are no further stipulations beyond those set forth by the CA Operator.

7.3 OCSP profile

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

8. Compliance Audit and Other Assessments

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

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

8.3 Assessor’s Relationship to Assessed Entity

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

8.4 Topics Covered by Assessment

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

8.5 Actions Taken as a Result of Deficiency

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

8.6 Communication of Results

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 and CRL services.

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 deemed by law or the TCS

privacy policy 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 responses, 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 like 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 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.

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 on request provide full documentation to 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 Certificate Terms of Use, 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 https://wiki.geant.org/display/TCSNT/
- 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 eScience 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 eScience 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.

TCS 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 their trademarks, service marks, trade names, company names, or any other intellectual property right, and that they are 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.

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

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

9.6.4 Relying Party Representations and Warranties

A party relying (Relying Pary) 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 https://wiki.geant.org/display/TCSNT/ 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
Hoekenrode 3
1102 BR Amsterdam
The Netherlands

And by email at tcs-pma@lists.geant.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 https://wiki.geant.org/display/TCSNT/) 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.