TERENA Certificate Service

TERENA eScience Personal CA Certificate Practice Statement

Version 1.0
1 February 2010
http://www.terena.org/activities/tcs/

Table of Contents

1. Introduction

This document is the Certificate Practice Statement (CPS) for the TERENA (TERENA Trans-European Research and Education Networking Association) Certificate Service (TCS) eScience Personal Certificate Authority. It outlines the legal, commercial 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 TERENA. It also defines the underlying certification processes for Subscribers and describes TCS's repository operations. The CPS is also a means of notification of roles and responsibilities for parties involved in Certificate based practices within the TCS PKI.

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 TERENA eScience Personal Certificate Authority ('TERENA eScience Personal CA') is a Certificate Authority (CA) that issues personal digital certificates for use in the eScience community. The TERENA eScience Personal CA performs functions associated with public key operations which include receiving application requests for, issuing, revoking and renewing digital certificates and the maintenance, issuance, and publication of Certificate Revocation Lists ("CRLs") and operating an Online Certificate Status Protocol ("OCSP") responder.

The TERENA Certificate Service is operated by TERENA for the community of its Members.

This CPS describes the TERENA eScience Personal CA's certification processes, business operations, and repository operations. The CPS is only one of many documents that are relevant to the TERENA eScience Personal CA's certificate issuance practices. Other important documents include TCS Subscriber Agreements (between Members and Subscribers), the Relying Party agreement, and other ancillary agreements that are posted on the TCS repository. These documents obligate parties using or relying on a TCS eScience Personal digital certificate to meet a certain minimum criteria prior to their use or reliance on a TCS eScience Personal Certificate.

The TERENA eScience Personal CA's CPS is also a means to notify the public and relevant parties of the roles and responsibilities involved in Certificate based practices within the TCS PKI. The CPS is formatted and maintained in accordance with IETF PKIX RFC 3647 and is divided into separate sections that cover the practices and procedures for applying for, identifying, issuing, and revoking certificates along with information about the TERENA eScience Personal CA's security controls and auditing process. To preserve the format of RFC 3647, some section headings do not apply. Those sections will contain the text "Not applicable" or "No stipulation". The format is preserved to assist the reader in comparing and contrasting the various CPS documents provided by various CAs.

1.2 Document Name and Identification

This document is the TERENA eScience Personal CA CPS version 1.0, which was approved for publication on 1 February 2010 by the TCS Policy Management Authority. This document is identified by the following unique registered object identifier: 1.3.6.1.4.1.25178.2.3.1.0.

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

Revision	Version	Date

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, the CRLs and the OCSP response used by the TERENA eScience Personal CA. Insignificant revisions may be made without changing the version number of this CPS.

1.3 PKI Participants

1.3.1 Certification Authorities

The TERENA eScience Personal CA is a Chain Certificate Authority of the UserTrust PKI hierarchy that issues personal certificates for use in the eScience community.

The TERENA eScience Personal CA is part of the TERENA Certificate Service (TCS). The TERENA Certificate Service is operated by TERENA for the community of its Members.

The CA systems for TCS are hosted and operated by Comodo (hereafter the CA Operator). The TERENA eScience Personal CA:

- Conforms its operations to this CPS as may from time to time be modified by amendments published in the TCS repository (http://www.terena.org/tcs/repository/).
- Issues and publishes certificates in a timely manner in accordance with the issuance times set forth in this CPS.
- Distributes issued certificates in accordance with the methods detailed in this CPS.
- Revokes certificates upon receipt of a valid revocation request from a person authorized to request revocation.
- Maintains and updates its OCSP service on a regular basis and in a timely manner, in accordance with in this CPS.
- Issues and updates CRLs in a timely manner as detailed in this CPS.
- Publishes CRLs on a regular basis, in accordance with this CPS.
- Notifies Subscribers via e-mail of expiring TERENA eScience Personal CA issued certificates (for a period disclosed in this CPS).

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 users, takes care of user authentication, and supplies attributes pertaining to an authenticated user.

Requesters must be registered in the IdP of a Subscriber, and their identity vetted by that Subscriber. Requesters need to be explicitly authorised by the Subscriber to apply for a TERENA eScience 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 TERENA eScience Personal CA before a certificate can be issued.

1.3.3 Subscribers

A *Subscriber* is an organisation that is part of the educational and research community of a country represented by a Member. Subscribers authorise Requesters to apply for a certificate from the TERENA eScience Personal CA, 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

Relying Parties use the TERENA eScience Personal CA's PKI services to perform certain transactions, communications, or functions and may reasonably rely on issued certificates and/or digital signatures that contain a verifiable reference to a public key that is listed in the Subscriber certificate. None of the TERENA eScience Personal CA's certificate products are intended to be used in e-commerce transactions or environments, and parties who rely on such certificates do not qualify as a Relying Party.

1.3.5 Other Participants

The TERENA eScience Personal CA operates through 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 TERENA to provide TERENA eScience Personal CA services to their Subscribers.

Members must comply with the requirements of this CPS, and ensure the compliance of its Subscribers. The TERENA eScience Personal CA, rather than 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

The certificates issued from the TERENA eScience Personal CA are intended to be used by individuals in eScience infrastructure environments.

1.4.2 Prohibited Usage

Certificates may only be used in accordance with their intended purpose and in compliance with all applicable laws and regulations. Certificates may not be used to complete or assist in performing any transaction that is prohibited by law.

Each party using or relying on a certificate shall be bound by and comply with the terms and conditions set forth in the applicable agreement between the party and TERENA. Digital certificates do not guarantee that a certificate holder has good intentions or that the certificate holder will be an ethical business operator.

Certificates must not be used for any application requiring fail-safe performance systems such as the operation of nuclear power facilities, air traffic control systems, weapon control systems, or any other system where a failure of the system could cause any form of damage.

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

TERENA Certificate Service
TERENA
Singel 468D
1017 AW Amsterdam
The Netherlands

E-mail: tcs_pcs@terena.org

1.5.3 Person Determining CPS Suitability for Policy

The suitability and applicability of the TERENA eScience Personal CA's CPS is reviewed and approved by both the TERENA Certificate Service Policy Management Authority and Comodo's legal department.

1.5.4 CPS Approval Procedures

The TERENA eScience Personal CA's CPS and any amendments made to it are reviewed and approved by TCS Policy Management Authority and Comodo's legal department. 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's repository which can be accessed online at http://www.terena.org/tcs/repository/. All updates, amendments and legal promotions 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
FTP	File Transfer Protocol
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:

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.
EUGridPMA	The European Policy Management Authority for Grid Authentication in eScience. This accredits Certificates Authorities for use with Grid authentication middleware.
Identity Provider:	An Identity Provider 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:	A Member is a National Research and Education Networking organisation that has entered into an agreement with TERENA to provide TERENA eScience Personal CA services to its Subscribers.
Proxy Certificate:	As defined in RFC 3820
Subscriber:	A Subscriber is an organisation that is part of the educational and research community of a country represented by a Member, that has subscribed to the TERENA eScience Personal CA service by signing a Subscriber Agreement. A Subscriber authorises Requesters to apply for a Certificate. 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 signed by the Subscriber before applying for a Certificate. A template for a Subscriber Agreement is available for reference at http://www.terena.org/tcs/repository/.
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 http://www.terena.org/tcs/repository/
Requester:	A Requester is an individual from the constituency of a Subscriber applying for a Certificate.

2. Publication and Repository Responsibilities

This CPS is only one of a set of documents relevant to the TERENA eScience Personal CA's certification services. The list of documents below is a list of other documents that this CPS will from time to time mention. The list is not exhaustive. The document names, location of, and status, whether public or private, are detailed below. The TCS Repository can be found at http://www.terena.org/tcs/repository/.

Document Status	Status	Location
TERENA eScience Personal CA Certificate Practice Statement	Public	TCS Repository
TCS Subscriber Agreement Template	Public	TCS Repository
TCS Relying Party Agreement	Public	TCS Repository

2.1 Repositories

TCS publishes this CPS, its Subscriber Agreements template, and the Relying Party Agreement in the official TCS repository. The TCS Certificate Policy Management Authority maintains the TCS repository. All updates, amendments and legal promotions 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.

2.2 Publication of Certificate Information

The certificate of the TERENA eScience Personal CA is published in the TCS repository. End Entity certificates are not published.

Information about the revocation status of End Entity certificates is published through the TERENA eScience Personal CA CRL and the TERENA eScience Personal CA's OCSP service.

2.3 Time or Frequency of Publication

Updates to the CPS are published in accordance with Section 9.12 "Amendments". Updates to the Subscriber Agreement template, Relying Party Agreements, and other agreements posted on the repository are published as often as necessary.

CRLs are issued every 24 hours or at most 1 hour after a certificate revocation. Under special circumstances, the TERENA eScience Personal CA may publish new CRLs more frequently. Each CRL is valid for the 96 hours following its publication or until an updated CRL has been published, whichever comes first.

Typically, the TERENA eScience Personal CA updates its OCSP Responder every 24 hours or immediately after a certificate revocation. Under special circumstances the OCSP Responder may be updated more frequently. All parties are strongly recommended to always consult the OCSP Responder prior to relying on information featured in a certificate.

2.4 Access Controls on Repositories

The information published in the TCS repository (http://www.terena.org/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.

The CRL and the OCSP service are publicly available.

3. Identification and Authentication

3.1 Naming

3.1.1 Types of Names

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

Attribute	Abbr.	Value
Country	C	"NL"
Organization	O	"TERENA"
Common Name	CN	"TERENA eScience Personal CA"

The Subject Distinguished Names 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 Member
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 Requester appended with an Identifier that uniquely and persistently represents the Requester in the Subscriber's IdP as described in Section 3.1.5 “Uniqueness of Names”.

All attribute values within certificate Subject and Issuer fields are 7-bit ASCII strings encoded as PrintableStrings.

The Common Name (CN) attribute value in the Subject Distinguished Name is obtained from the Subscriber's IdP.

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.

The Organizational Unit (OU) attribute value the Subject Distinguished Name is obtained from the Subscriber's IdP.

A certificate issued by the TERENA eScience Personal CA may contain e-mail addresses of the Requester as provided and guaranteed by the Subscriber’s IdP. The e-mail addresses are stored in the rfc822Name of the subjectAltName extension. The format of the e-mail addresses is a “Mailbox” as defined in RFC 2821, Section 4.1.2.

3.1.2 Need for Names to be Meaningful

The TERENA 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”.

The O attribute of an End Entity certificate Subject contains either the English translation of the Subscriber's name or its transcription into 7-bit ASCII. If the official Subscriber's name is longer than 64 characters, the Subscriber provides its abbreviated version for inclusion in the certificates.

3.1.3 Anonymity or Pseudonymity of Subscribers

The TERENA eScience Personal CA does not support anonymous names or pseudonyms.

3.1.4 Rules for Interpreting Various name Forms

Distinguished Names in Certificates are X.501 compliant. For information on how X.501 Distinguished Names are interpreted, please see RFC 4514.

rfc822names in Certificates are RFC 2821 compliant. For information on how rfc822Names are interpreted, please see RFC 2821 and RFC 2822.

3.1.5 Uniqueness of Names

The Subject Distinguished Name of a TERENA eScience Personal CA-issued Certificate is unique for each Requester by including an Identifier that uniquely and persistently represents the Requester in the IdP of its Subscriber. A Subscriber will ensure the persistence and uniqueness

of the aforementioned Identifier that its IdP releases to the TERENA eScience Personal CA. The Identifier must be traceable to a Requester for at least as long as the certificate issued to the Requester is valid. If the traceability from Identifier to Requester is lost, the Subscriber will ensure the Identifier will not be reused.

3.1.6 Recognition, Authentication, and Role of Trademarks

The TERENA eScience Personal CA prohibits the use of a name or symbol that infringes upon the Intellectual Property Rights of another. However, the TERENA eScience Personal CA does not verify or check the name appearing in a Certificate for non-infringement. Subscribers are solely responsible for ensuring the legality of any information presented for use in a TERENA eScience Personal CA-issued Certificate. TERENA eScience Personal CA Subscribers represent and warrant that applications to the TERENA eScience Personal CA from Requesters and when using a domain and distinguished name (and all other certificate application information) that they are not interfering with or infringing 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.

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.

3.2 Initial Identity Validation

Upon receipt of an application for a digital certificate and based on the submitted information, the TERENA eScience Personal CA confirms the following information:

- The Requester is the same person as the person identified in the certificate application.
- The Requester holds the private key corresponding to the public key to be included in the certificate.
- The information to be published in the certificate is accurate, except for non-verified Subscriber information.
- Any Requester who applies for a certificate is duly authorized to do so.

In all types of TCS certificates, the Subscriber has a continuous obligation to monitor the accuracy of the submitted information and notify TCS of any changes that would affect the validity of the certificate. Failure to comply with the obligations as set out in this CPS will result in the revocation of the Subscriber's Digital Certificate without further notice to the Subscriber.

3.2.1 Method to Prove Possession of Private Key

Every Requester must demonstrate that he/she holds the private key corresponding to the public key that will be included in the Certificate. To prove possession, the Requester must submit a digitally signed PKCS#10 to the TERENA eScience Personal CA or provide another cryptographically equivalent demonstration.

3.2.2 Authentication of Organization Identity

The following elements are critical information elements for registering an organization as a Subscriber by a Member. Those elements marked with PUBLIC are present within issued certificates and are therefore within the public domain. Those elements not marked with PUBLIC remain confidential in line with the privacy and protection of data provisions outlined in this CPS.

- Legal Name of the Organization (PUBLIC)
- Organizational unit; optional (PUBLIC)

- Street, city, postal/zip code, country
- Company registration number (if available)
- Administrator contact full name, e-mail address and telephone
- Proof of right to use name of the Organization
- Proof of existence and organizational status of the Organization
- Subscriber agreement, signed

Documentation requirements for organizational applicants include any / all of the following:

- Articles of Association
- Corporate Charter
- Official letter from an authorized representative of a government organization
- Official letter from office of Dean or Principal (for Educational Institutions)

A Member may accept at its discretion other official organizational documentation supporting registration of a Subscriber.

A Member may use the services of a third party to confirm information on an entity that applies to register as a Subscriber. A Member accepts confirmation from third party organizations, other third party databases and government entities.

A Member's controls may also include Trade Registry transcripts that confirm the registration of the applicant organization and state the members of the board, the management and Directors representing the company.

Subscribers shall solely be responsible for the legality of the information they present for use in certificates issued under this CPS, in any jurisdiction in which such content may be used or viewed.

3.2.3 Authentication of Individual Identity

The following elements are critical information elements for a TCS eScience Personal certificate issued to an individual:

- Name of the Individual (PUBLIC)
- Organizational unit; optional (PUBLIC)
- Public Key (PUBLIC)
- Proof of right to use name

Documentation requirements for Individual applicants shall include identification elements such as:

- Passport
- National Identification Document
- Driving Licence

The identity of a Requester in a Subscriber's IdP has been validated by the Subscriber. During the validation process or during processes supporting that validation process the identity of the Requester was confirmed with a face-to-face meeting and valid photo identification and/or similar official documents. The TERENA eScience Personal CA may approve, at its discretion, the use of other official documentation to support an application. The Requesters identity is stored and maintained within the Subscriber's IdP.

The Subscriber expresses that an identity has been properly validated by setting a specific value in the *eduPersonEntitlement* attribute of the Requester's identity in the Subscriber's IdP. The specific value is agreed upon between the Member and the Subscriber.

3.2.4 Non-Verified Subscriber Information

TCS does not validate any information not listed as being validated under Section 4.2 "Certificate Application Processing".

3.2.5 Validation of Authority

A Requester is authorised to request a certificate with the TERENA eScience Personal CA by the presence of a specific value in the *eduPersonEntitlement* attribute of that Requester as released by the Subscriber's IdP. The specific value is agreed upon between Member and Subscriber.

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

3.2.6 Criteria for Interoperation

The TERENA eScience Personal CA does not interoperate with third party PKIs.

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication for Routines Re-key

The TERENA eScience Personal CA does not support certificate re-keying. Every certificate request is treated as an initial request, and requires the verification procedure to be followed.

3.3.2 Identification and Authentication for Re-key After Revocation

The TERENA eScience Personal CA does not support certificate re-keying. Every certificate request is treated as an initial request, and requires the verification procedure to be followed.

3.4 Identification and Authentication for Revocation Requests

Prior to revoking a certificate, the TERENA eScience Personal CA verifies that the revocation was requested by an authorized entity:

- *Member*: Authorized personnel of a Member are authenticated using their credentials for accessing the TCS management system. A Member can revoke a certificate of an End Entity belonging to any of its Subscribers.
- *Subscriber:* Authorized personnel of a Subscriber are authenticated using their credentials for accessing the TCS management system. A Subscriber can revoke a certificate of an End Entity registered with its IdP.
- *End Entity:* An End Entity can revoke its own certificate after successfully authenticating with their IdP.

Upon receipt of the revocation request, TCS may request confirmation from authorized personnel of a Subscriber by telephone or fax.

4. Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

TCS eScience Personal certificates are issued to Subscribers for Requesters from their Constituency. Prior to the issuance of a certificate, the TERENA eScience Personal CA will validate an application in accordance with this CPS.

4.1.1 Who Can Submit a Certificate Application

Certificate applications may be submitted by an individual who is the subject of the certificate.

The Requester must have a valid account with an Identity Provider of a Subscriber and be authorised according to the mechanism described in Section 3.2.5 “Validation of Authority”.

4.1.2 Enrollment Process and Responsibilities

The TERENA eScience Personal CA enrolment process is accessible through a Member operated web enrolment application. Members can share the web enrolment application.

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

All Requesters must complete the following enrolment process prior to being issued a certificate:

1. The Requester establishes a secured session with the web enrolment application provided by the 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 Requester;
   - an Identifier that uniquely and persistently represents the Requester in the Subscriber's IdP as described in Section 3.1.5 “Uniqueness of Names”;
   - the Requester's e-mail address(es);
   - the eduPersonEntitlement expressing the Requester's identity has been properly validated and the Requester is authorised to request a certificate with the TERENA eScience Personal CA.
3. The Requester submits the Certificate Signing Request (CSR) to the web enrolment application using a secure transaction within the secure session established in Step 1.

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

The Requester 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 Requester is responsible to notify the Subscriber in case of an occurrence that materially affects the integrity of his IdP account.

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

4.2 Certificate Application Processing

An application for a Certificate consists of the PKCS#10 Certificate Signing Request and a set of signed attributes released by the Requester's IdP.

Prior to the issuance of a certificate the TERENA eScience Personal CA will validate an application in accordance with this CPS which involves verifying the identity and authorization of the Subscriber, verifying the identity and authorization of the Requester and the validity of the Certificate Signing Request.

From time to time, TCS may modify the requirements related to application information for

individuals, to respond to TCS's requirements, the business context of the usage of a digital certificate, or as prescribed by law.

4.2.1 Performing Identification and Authentication Functions

The TERENA eScience Personal CA uses a Subscriber's Identity Provider to ascertain the identity of a Requester.

Prior to issuing a Certificate, the TERENA eScience Personal CA employs controls to validate Subscriber and Requester information featured in the certificate application. The validation process is 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 Requester, 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 Requester using the method described in Section 3.2.5 "Validation of Authority".
- verifies the identity of the Requester based on the secure session parameters;
- verifies that all required attributes pertaining to the Requester 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.

4.2.2 Approval or Rejection of Certificate Applications

Following successful completion of all required validations of a certificate application as described in Section 4.2.1 "Performing Identification and Authentication Functions", the TERENA eScience Personal CA will automatically approve an application for a digital certificate and issue the certificate.

If the validation of a certificate application fails, the TERENA eScience Personal CA will reject the certificate application. The TERENA eScience Personal CA reserves its 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 TERENA Certificate Services 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.

The private key associated with a public key, which has been submitted as part of a rejected certificate application, may not under any circumstances be used to create a digital signature if the effect of the signature is to create conditions of reliance upon the rejected certificate application.

4.2.3 Time to Process Certificate Applications

Certificate applications are processed automatically and in real time.

From time to time, events outside of the control of the TERENA eScience Personal CA may delay the issuance process. However, the TERENA eScience Personal CA will make every reasonable effort to meet issuance times and to make applicants aware of any factors that may affect issuance times in a timely manner.

4.3 Certificate Issuance

4.3.1 CA Actions During Certificate Issuance

The TERENA eScience Personal CA issues a certificate upon approval of a certificate application. A digital certificate is deemed to be valid at the moment a Subscriber accepts it (refer to Section 4.4 "Certificate Acceptance"). Issuing a digital certificate means that the TERENA eScience Personal CA accepts a certificate application.

4.3.2 Notification to Requester by the CA of Issuance of Certificate

The TERENA eScience Personal CA notifies the Requester of the issuance of a certificate within a reasonable amount of time after the certificate is created by sending a message to his e-mail address(es) provided by his IdP. Issued certificates may be installed by the Requester directly from the TERENA eScience Personal CA web enrolment application.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

A Requester is deemed to have accepted a certificate when:

- the Requester uses the certificate, or
- 7 days pass from the date of notification of a certificate and the Requester has not explicitly rejected the certificate by requesting its revocation.

4.4.2 Publication of the Certificate by the CA

An issued certificate is published solely by delivering the certificate to the Requester.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

Other parties involved in the issuance and approval of the Certificate may receive notification of the issuance of a certificate to their customer or client.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

Certificates may only be used for lawful and appropriate purposes as set forth in this CPS. End Entities are responsible for protecting their private keys from unauthorized use and agree to immediately cease using the private key following the expiration or revocation of the Certificate.

4.5.2 Relying Party Public Key and Certificate Usage

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 OCSP service and/or CRL 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 allowed in the CPS and named as Object Identifiers in the certificate profile.

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 the TERENA eScience Personal CA under the provisions made in this CPS, the Relying Party must obtain additional assurances.

Warranties are only valid if the steps detailed above have been carried out.

4.6 Certificate Renewal

The TERENA eScience Personal CA does not support certificate renewal. Every certificate application is treated as a new certificate application.

4.6.1 Circumstances for Certificate Renewal

Not applicable.

4.6.2 Who May Request Renewal

Not applicable.

4.6.3 Processing Certificate Renewal Requests

Not applicable.

4.6.4 Notification of New Certificate Issuance to Subscriber

Not applicable.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Not applicable.

4.6.6 Publication of the Renewal Certificate by the CA

Not applicable.

4.6.7 Notification of Certificate Issuance by the CA to other Entities

Not applicable.

4.7 Certificate Re-key

The TERENA eScience Personal CA does not support certificate re-keying. Every certificate application is treated as a new certificate application.

4.7.1 Circumstances for Certificate Re-Key

Not applicable.

4.7.2 Who May Request Certificate of a New Public Key

Not applicable.

4.7.3 Processing Certificate Re-keying Requests

Not applicable.

4.7.4 Notification of New Certificate Issuance to Subscriber

Not applicable.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

Not applicable.

4.7.6 Publication of the Re-keyed Certificate by the CA

Not applicable.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

Not applicable.

4.8 Certificate Modification

4.8.1 Circumstance for Certificate Modification

The TERENA eScience Personal CA does not support certificate modification. Every certificate application is treated as a new certificate application.

4.8.2 Who May Request Certificate Modification

Not applicable.

4.8.3 Processing Certificate Modification Requests

Not applicable.

4.8.4 Notification of New Certificate Issuance to Subscriber

Not applicable.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

Not applicable.

4.8.6 Publication of the Modified Certificate by the CA

Not applicable.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

Not applicable.

4.9 Certificate Revocation and Suspension

Upon revocation of a certificate, the operational period of that certificate is immediately considered terminated. The serial number of the revoked certificate will be placed in the CRL and within the OCSP Responder and remains in the CRL and on the OCSP Responder until some time after the end of the certificate's validity period.

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. The TERENA eScience Personal CA shall revoke a digital certificate if it becomes aware of any of the following circumstances:

- There has been loss, theft, modification, unauthorized disclosure, or other compromise of the private key associated with the 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 Requester's IdP account is compromised, revoked or its password is compromised;
- The Subscriber, the Requester or the Member has breached a material obligation under this CPS or a relevant agreement;
- Either the Subscriber's, Requester'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;

- There has been a modification of the information pertaining to the Requester that is contained within the certificate;
- A private Key or password has, or is likely to become known to someone not authorized to use it, or is being or is likely to be used in an unauthorized way;
- A Digital Certificate has not been issued in accordance with the policies set out in this CPS;
- The Subscriber or Requester 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 information contained in the certificate is incorrect or has changed;
- 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 TERENA eScience Personal CA 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 TERENA eScience Personal CA, all valid certificates pertaining to that Subscriber shall be revoked on the termination date of the Subscriber Agreement.

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 TERENA eScience Personal CA 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 Requesters;
- a Requester 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.

4.9.3 Procedure for Revocation Request

The TERENA eScience Personal CA employs 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 revocation requester will be logged.
- If the revocation requester can prove his/her ownership of the private key associated with the certificate, the TERENA eScience Personal CA will revoke the certificate

without any other checks. The revocation request and the proof of the relevant private key by the Requester will be logged.

- If the request has been initiated by entities other then Member, Subscriber or Requester, 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.

4.9.4 Revocation Request Grace Period

Any of the parties defined in Section 4.9.2 "Who can Request Revocation" that becomes aware of circumstances that require revocation of a certificate is obliged to initiate a revocation request as soon as possible.

4.9.5 Time Within Which CA Must Process the Revocation Request

The TERENA eScience Personal CA processes all revocation requests without delay. The amount of time required depends on the nature of the revocation request, the party requesting the revocation, and other factors surrounding the revocation request. Ordinary certificate revocation requests are processed automatically upon receipt within one business day.

4.9.6 Revocation Checking Requirement for Relying Parties

Relying Parties must always check the status of the Certificate on which they are relying. Relying Parties should check the OCSP service and/or CRL or use the applicable web-based repository to confirm that the certificate has not been revoked.

The TERENA eScience Personal CA will revoke the certificate, place the certificate in the CRL and mark it as revoked in the OCSP service once it has determined, to the TERENA eScience Personal CA's satisfaction, that the revocation request was proper.

4.9.7 CRL Issuance Frequency

An updated CRL is published on the TCS website every 24 hours or at most 1 hour after a certificate revocation. Under special circumstances the CRL may be published more frequently.

4.9.8 Maximum Latency for CRLs

CRLs are posted to the online repository within a commercially reasonable time after their generation. Usually, this is within a minute of the CRL's generation.

4.9.9 On-line Revocation/Status Checking Availability

TCS manages and makes publicly available an OCSP service for on-line checking of certificate status. The service is available at http://ocsp.tcs.terena.org/.

4.9.10 On-line Revocation Checking Requirements

Relying Parties must confirm the validity of a certificate via the CRL and/or OCSP prior to relying on the Certificate.

4.9.11 Other Forms for Revocation Advertisements available

Not applicable.

4.9.12 Special Requirements re Key Compromise

TCS uses commercially reasonable efforts to notify Relying Parties if it believes or has reason to believe that one of its private keys has been compromised.

4.9.13 Circumstances for Suspension

The TERENA eScience Personal CA does not utilize certificate suspension.

4.9.14 Who can Request Suspension

Not applicable.

4.9.15 Procedure for Suspension Request

Not applicable.

4.9.16 Limits on Suspension Period

Not applicable.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

The TERENA eScience Personal CA utilizes both CRLs and an OCSP service to allow Relying Parties to verify the validity of a digital signature made using a TERENA eScience Personal CA issued digital certificate. Each CRL and the OCSP Responder contain information for all of TERENA eScience Personal CA's revoked non-expired certificates.

Each CRL contains entries for all revoked non-expired certificates issued and is valid for 96 hours. The TERENA eScience Personal CA issues a new CRL every 24 hours or at most 1 hour after a certificate revocation and includes a monotonically increasing sequence number for each CRL issued. All expired CRLs are archived (as described in Section 5.5 "Records Archival") for a period of 3 years or longer if applicable.

Individual entries in the OCSP service can be requested using the TCS OCSP responder. Revoked certificates are affected in the OCSP Responder immediately after their revocation.

4.10.2 Service Availability

The OCSP Responder provides access to certificate status information 24x7. CRLs are open to public inspection 24x7.

4.10.3 Optional Features

No stipulation.

4.11 End of Subscription

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

4.12 Key Escrow and Recovery

The TERENA eScience Personal CA does not escrow Subscriber private keys.

5. Facility, Management and Operational Controls

5.1 Physical Security Controls

The TERENA eScience Personal CA makes 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

The TERENA eScience Personal CA performs its CA operations in a secure data centre located in the United States. The building is a secure structure. The data centre is operated under a security policy to ensure that no unauthorized logical or physical access is allowed. Most records

are archived at a secure off-site location and are maintained in a form that prevents unauthorized modification, substitution or destruction.

5.1.2 Physical Access

Access to the secure part of the TCS facilities is limited using physical access control and is only accessible to appropriately authorized individuals (referred to here-on as Trusted Personnel). Card access systems are in place to control, monitor and log access to all areas of the facility. Access to the TCS CA physical machinery within the secure facility is protected with locked cabinets and logical access control.

5.1.3 Power and Air Conditioning

TCS secure facilities have a primary and secondary power supply and ensure continuous, uninterrupted access to electric power. Heating / air ventilation systems are used to prevent overheating and to maintain a suitable humidity level.

5.1.4 Water Exposures

TCS has taken commercially reasonable efforts to ensure that its CA system is secure and protected from flood and water damage.

5.1.5 Fire Prevention and Protection

Fire protection and prevention is made in compliance with local fire regulations

5.1.6 Media Storage

All media storing TCS data or information, including media containing audit logs, archived records, software, Subscriber information, and other information pertinent to the CA's operation is stored in a secure facility that has implemented both logical and physical controls that limit potential harm to the data.

5.1.7 Waste Disposal

Sensitive documents are shredded prior to disposal. Electronic Media is wiped clean by a trusted party upon the expiration of the data. All media is rendered unreadable prior to its disposal and, where possible, is physically destroyed.

5.1.8 Off-site Backup

TCS performs routine backups of all sensitive information. Off-site backups are stored in a separate secure location using a third party data centre.

5.2 Procedural Controls

5.2.1 Trusted Roles

Trusted roles are parties allowed to access the TCS CA management system. Persons acting in a trusted role are granted functional permissions to the account management system. All permissions are applied on an individual basis and are assigned by senior members of the management team. All signed authorizations are archived. The roles and responsibilities of each personnel are assigned in such a manner that one person alone cannot circumvent the TCS CA security measures.

5.2.2 Number of Persons Required Per Task

Internal policy and operational procedures require multiple trusted personnel to take part in the CA's operations. This provides an added layer of security. All of the CA's most sensitive tasks require the involvement of multiple trusted personnel. At least two trusted individuals are required to handle the CA's private keys.

5.2.3 Identification and Authentication for Each Role

Trusted personnel must identify and authenticate themselves before system access is granted. Identification is via a username, with authentication requiring a password and a digital certificate.

5.2.4 Roles Requiring Separation of Duties

Roles requiring the separation of duties include the management of the CA key, including issuance or destruction of a CA certificate.

5.3 Personnel Security Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

TCS follows personnel and management practices that provide reasonable assurance of the trustworthiness and competence of their employees and of the satisfactory performance of their duties. All TCS employees must have the necessary qualifications or experience to fulfill their job descriptions.

5.3.2 Background Check Procedures

Background checks are performed on all trusted personnel of the CA operator before access is granted to TCS's systems. These checks include, but are not limited to, credit history, employment history (for references), and a company registry cross-reference to disqualified directors.

5.3.3 Training Requirements

Personnel training occurs via a mentoring process involving senior members of the team to which the employee is attached. The CA operator periodically reviews and enhances its training programs as necessary.

Training programs are tailored toward each individual's job responsibilities and include training on PKI concepts, job responsibilities, operational policies and procedures, incident handling and reporting, and disaster recovery procedures.

5.3.4 Retraining Frequency and Requirements

The CA Operator provides refresher training courses to its personnel in order to ensure that all such personnel can competently and satisfactorily perform their job responsibilities.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

Any personnel found violating a CA Operator's policy or procedure is subject to disciplinary action. The action taken by the CA Operator depends on the circumstances surrounding the action, the severity of the violation, and the personnel's past performance. In some cases, disciplinary action may include the personnel's termination of employment.

5.3.7 Independent Contractor Requirements

If an independent contractor or consultant is used, the CA Operator shall initially ensure that each such contractor or consultant is first obligated to abide by the same functional and security criteria that are set forth herein. Contractors and consultants are subject to the same sanctions as other personnel as set forth in Section 5.3.6 "Sanctions for Unauthorized Actions".

5.3.8 Documentation Supplied to Personnel

TCS supplies its personnel with the training and documentation needed to perform their job responsibilities. The CA Operator's personnel understand and are obligated and required to safe

guard and protect all private and confidential information to which they might have access.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

For audit purposes, TCS maintains electronic or manual logs of the following events for core functions.

CA & Certificate Lifecycle Management

- CA Root signing key functions, including key generation, backup, recovery and destruction.
- Certificate life cycle management, including successful and unsuccessful certificate applications and certificate issuances.
- Certificate revocation requests, including the reason for the revocation.
- Certificate Revocation List updates, generations and issuances.
- Custody of keys and of devices and media holding keys.
- Compromise of a private key.
- Security Related Events.
- System downtime, software crashes, and hardware failures.
- CA system actions performed by CA Operator personnel, including software updates, hardware replacements, and upgrades.
- Cryptographic hardware security module events, such as usage, de-installation, service, or repair and retirement.
- Successful and unsuccessful TCS PKI access attempts.
- Secure CA facility visitor entry and exit.

Subscription Application Information

- The documentation and other related information pertaining to a Subscriber subscribing to the TERENA eScience Personal CA

5.4.2 Frequency of Processing Log

Logs are reviewed on a weekly basis by CA management.

5.4.3 Retention Period of Audit Log

Logs are archived by the system administrator on a weekly basis. Logs are thereafter retained as part of the record archive as set forth in Section 5.5 “Records Archival”.

5.4.4 Protection of Audit Log

All logs are backed up on removable media and the media held at a secure off-site location on a daily basis. These media are only removed by the CA Operator staff on a visit to the data centre, and when not in the data centre are held either in a safe in a locked office on site, or off-site in a secure storage facility.

5.4.5 Audit Log Backup Procedures

Logs are archived on a weekly basis by the system administrator. Both current and archived logs are maintained in a form that prevents unauthorized modification, substitution or destruction. When the removable media reaches the end of its life it is wiped by a third party secure data destruction facility and the certificates of destruction are archived.

5.4.6 Audit Collection System

Audit data is generated both automatically and manually. Automatic logs are computer-generated and are based on a set of security protocols, scans, and alerts. Manual audits are recorded and stored by the CA Operator's personnel.

All logs include the following elements:

- Date and time of entry
- Serial or sequence number of entry
- Method of entry
- Source of entry
- Identity of entity making log entry

5.4.7 Notification to Event-Causing Subject

Notices of audited events are confidential information and no notice is given to individuals or organizations unless required by law or agreement.

5.4.8 Vulnerability Assessments

Events in the audit process are logged to monitor vulnerabilities. TCS periodically reevaluates its security procedures and updates them as may be required.

5.5 Records archival

5.5.1 Types of records archived

The following information must be archived:

- Information or documentation submitted by Subscribers in support of a certificate application.
- Copies of certificates, regardless of their status (such as expired or revoked). Such records may be retained in electronic, in paper-based format or any other format that TCS may see fit.
- Audit logs
- Other records deemed important and valuable to the TCS business operations

5.5.2 Retention period for archive

TCS retains the records of TCS eScience Personal digital certificates and the associated documentation for a term of at least 3 years, or as necessary to comply with applicable laws. The retention term begins on the date of expiration or revocation.

5.5.3 Protection of archive

Records are archived at a secure off-site location and are maintained in a form that prevents unauthorized modification, substitution or destruction.

5.5.4 Archive backup procedures

The CA Operator regularly backs up electronic archives. Copies are maintained of paper files.

5.5.5 Requirements for time-stamping of records

Certificates, CRLs, and other archived information shall contain time and date information.

5.5.6 Archive collection system

The CA's Operator archive collection system is an internal system.

5.5.7 Procedures to obtain and verify archive information

Only authorized trusted personnel are permitted access to the archive. Subscribers may obtain copies of archived information related to their Certificate upon written request and payment of any associated costs.

5.6 Key changeover

Towards the end of each CA private key's lifetime, a new CA signing key pair is commissioned and all subsequently issued certificates are signed with the new private signing key. Both keys may be concurrently active. The corresponding new CA public key certificate is provided to Subscribers and Relying Parties through the delivery methods detailed in Section 6.1 "Key pair generation and installation".

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

To maintain its CA operations when an incident occurs, the CA Operator makes a backup of critical CA software. The backup is performed weekly and is stored off-site. The CA Operator also performs a backup of critical business information. The backup is performed daily and is stored off-site. Further, TCS operations are distributed across several sites world wide. All sites offer facilities to manage the lifecycle of a certificate, including but not limited to the application, issuance, revocation of such certificates.

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

The CA Operator operates a fully redundant CA system. The backup CA is readily available in the event that the primary CA should cease operation. All of TCS's critical computer equipment is housed in a co-location facility run by a commercial data-centre, and all of the critical computer equipment is duplicated within the facility. Incoming power and connectivity feeds are duplicated. The duplicate equipment is ready to take over the role of providing the implementation of the CA, and allows TCS to specify a maximum system outage time (in case of critical systems failure) of 1 hour.

As well as a fully redundant CA system, the CA Operator maintains provisions for the activation of a backup CA and a secondary site should the primary site suffer a total loss of systems. This disaster recovery plan states that the CA Operator will endeavour to minimize interruptions to its CA operations.

5.7.3 Business continuity capabilities after a disaster

To maintain the integrity of its services the CA Operator implements, documents and periodically tests appropriate contingency and disaster recovery plans and procedures. Such plans are revised and updated as may be required at least once a year.

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. The plan shall provide for:

- Revocation of Certificates issued to the CA
- Revocation of non-expired and non-revoked Certificates as may be necessary
- Preservation of the CA's archives and records as required by this CPS

- Continuation of customer support services
- Providing to affected parties how to address the cost of such notice
- Transition of the services to the CA's successor
- Disposition of the CA's private key
- Refunds (if necessary)
- Continuation of revocation services

6. Technical Security Controls

TCS's operational sites operate under a security policy designed to, within reason, detect, deter and prevent unauthorized logical or physical access to CA related facilities. This section of the CPS outlines the security policy, physical and logical access control mechanisms, service levels and personnel policy in use to provide trustworthy and reliable CA operations.

6.1 Key pair generation and installation

6.1.1 Key pair generation

The CA Operator securely generates and protects TCS's private key(s), using a trustworthy system (IBM 4758 accredited to FIPS PUB 140-1 level 4, operating in at least FIPS PUB 140-1 level 3), and takes necessary precautions to prevent the compromise or unauthorized usage of it.

The TERENA eScience Personal CA key was generated in accordance with the guidelines detailed in the Root Key Generation Ceremony Reference. The activities undergone and the personnel involved in the Root Key Generation Ceremony are recorded for audit purposes. Subsequent Root Key Generation Ceremonies are to follow the documented reference guide also.

The Requester is solely responsible for the generation of the private key used in the certificate request. The TERENA eScience Personal CA does not provide key generation, escrow, recovery or backup facilities.

6.1.2 Private key delivery to Subscriber

The End Entity private key is generated directly by the Requester.

6.1.3 Public key delivery to certificate issuer

Requester's public key is delivered to the TERENA eScience Personal CA via a Member's web enrolment application using a secured session.

6.1.4 CA public key delivery to Relying Parties

TCS makes all its CA Certificates available in online repositories at http://crt.tcs.terena.org/.

6.1.5 Key sizes

The TERENA eScience Personal CA RSA signing key is 2048 bits long.

End Entity RSA keys must be at least 1024 bits long.

6.1.6 Public key parameters generation and quality checking

TCS securely generates and protects its own private key(s), using a trustworthy system (IBM 4758 accredited to FIPS PUB 140-1 level 4), and takes necessary precautions to prevent the compromise or unauthorized usage of it.

See 6.1.1

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

The key usage field extension in the TCS eScience Personal Certificates specifies the purpose for which the Certificate may be used. Enforcement of the limitations of use found in this field is beyond TCS's control as its correct use is highly dependent on using the correct software.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

The TERENA eScience Personal CA protects its signing key in accordance with this CPS.

6.2.1 Cryptographic module standards and controls

TCS private keys are generated and stored on an IBM 4758 accredited to FIPS PUB 140-1 level 4.

End Entities' private keys may be stored in software tokens in which case the access to the private key must be protected with a strong pass phrase, i.e. at least 12 characters long and following current best practice in choosing high-quality passwords.

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

For CA Root key recovery purposes, the Root CA signing keys are encrypted and stored within a secure environment. The decryption key is split across 5 removable media and it requires 3 of 5 of those media to reconstruct the decryption key. Custodians in the form of two or more authorized CA Operator's officers are required to physically retrieve the removable media from the distributed physically secure locations.

6.2.3 Private key escrow

TCS does not escrow private keys.

6.2.4 Private key backup

TCS's CA keys are generated and stored inside cryptographic hardware. The keys are backed up and transferred in an encrypted form.

The End Entities are solely responsible for maintenance and protection of their private keys backup. The private keys must never be backed up and transferred in an unencrypted form.

6.2.5 Private key archival

When any CA Root Signing Key pair expires, they will be archived for at least 7 years. The keys will be archived in a secure cryptographic hardware module, as per their secure storage prior to expiration.

End Entities private keys are not archived.

6.2.6 Private key transfer into or from a cryptographic module

Where CA Root signing keys are backed up to another cryptographic hardware security module, such keys are transferred between devices in encrypted format only.

6.2.7 Private key storage on cryptographic module

TCS private keys are generated and stored on an IBM 4758 HSM accredited to FIPS PUB 140-1 level 4.

6.2.8 Method of activating private key

TCS's private keys are activated according to the specifications of the cryptographic hardware

manufacturer.

An End Entities' private key is typically activated by the End Entity providing the software token pass phrase. The pass phrase must never be transferred over an unencrypted channel.

6.2.9 Method of deactivating private key

All deactivated private keys should be kept in an encrypted form only. Keys are deactivated by logging off their system. Root keys are further deactivated by removing them from their storage partition.

6.2.10 Method of destroying private key

Private keys are destroyed by deleting them from all known storage partitions and then by zeroing or by physically destroying the hardware on which they were stored. All CA key destruction activities are logged.

6.2.11 Cryptographic Module Rating

See Section 6.2.1 "Cryptographic module standards and controls".

6.3 Other aspects of key pair management

TCS conducts the overall certification management within the TCS PKI. TCS is not involved in functions associated with the generation, issuance, decommissioning or destruction of an End Entity key pair.

6.3.1 Public key archival

TCS retains copies of all Public Keys in its archive via its routine backup procedures and as described in Section 5.5 "Records archival".

6.3.2 Certificate operational periods and key pair usage periods

The operational period of each Certificate generated ends upon its revocation or expiration. The validity period of the End Entity certificates is at most 395 days.

The operational period of the CA key is 18 May 2009 until 31 December 2028.

6.4 Activation data

6.4.1 Activation data generation and installation

The CA Operator activates the cryptographic module containing TCS private keys according the specifications set forth by the hardware manufacture and meets the requirements of FIPS 140-2 Level 4. All cryptographic hardware is under dual person control.

All CA Operator's personnel are required to use strong passwords (non-dictionary alphanumeric passwords with a minimum length that are changed on a regular basis) to protect sensitive information.

6.4.2 Activation data protection

TCS activation data is protected using strong passwords as described in Section 6.4.1 "Activation data generation and installation".

6.4.3 Other aspects of activation data

All activation data is transmitted, stored, and destroyed using methods and procedures that protect against loss, theft, modification, or any other unauthorized access, loss, or use.

6.5 Computer security controls

The TCS CA Infrastructure uses trustworthy systems to provide certificate services. A trustworthy system is computer hardware, software and procedures that provide an acceptable resilience against security risks, provide a reasonable level of availability, reliability and correct operation, and enforce a security policy.

6.5.1 Specific computer security technical requirements

The CA Operator's computer systems are set up and maintained in a secure manner that prevents unauthorized access. The CA Operator uses software and hardware that constitute the industry's best practice in security measures.

Computers are password protected and require a strong password for access. All passwords are changed on a regular basis. Computers are firewalled and scanned regularly for viruses, spyware, Trojans, and other malware.

6.5.2 Computer security rating

No stipulation.

6.6 Life cycle technical controls

6.6.1 System development controls

The CA Operator closely controls and monitors TCS CA systems and software development. All systems and software are developed and implemented in accordance with industry standards. All systems and software are routinely checked for malware and security issues.

6.6.2 Security management controls

The CA Operator controls and monitors the configuration and operation of TCS CA systems. Security-related changes are logged and processed. TCS periodically reviews and updates its security policy and controls to ensure that no unauthorized access is allowed.

6.6.3 Life cycle security controls

No stipulation.

6.7 Network security controls

TCS performs all of its CA functions on secured networks to prevent unauthorized access and other malicious activity.

6.8 Time-stamping

Certificates, CRLs, OCSP responses and log entries shall contain time and date information about the Certificate, CRL, OCSP response or event information.

7. Certificate, CRL and OSCP Profiles

7.1 Certificate profile

The TCS eScience Personal certificates may be used in eScience infrastructure environments. In order to use and rely on a TCS eScience Personal certificate, the Relying Party must use X.509v3 compliant software.

7.1.1 Version number(s)

All TCS eScience Personal certificates are X.509 version 3 certificates.

7.1.2 Certificate extensions

The TERENA eScience Personal CA uses the standard X.509, version 3 to construct digital certificates for use within the TCS PKI. X.509v3 allows a CA to add certain certificate extensions to the basic certificate structure. The TERENA eScience Personal CA uses a number of certificate extensions for the purposes intended by X.509v3 as per Amendment 1 to ISO/IEC 9594-8, 1995. X.509v3 is the standard of the International Telecommunications Union for digital certificates.

The TERENA eScience Personal CA certificate includes the following extensions:

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

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

c) ***authorityKeyIdentifier***: not critical;
89:82:67:7D:C4:9D:26:70:00:4B:B4:50:48:7C:DE:3D:AE:04:6E:7D

d) ***subjectKeyIdentifier***: not critical;
C8:89:73:99:A7:5D:51:16:53:45:54:7C:A3:C2:39:7C:CB:D7:AA:81

e) ***cRLDistributionPoints***: not critical;
http://crl.usertrust.com/UTN-USERFirst-ClientAuthenticationandEmail.crl - URI for retrieving the CRL of the issuing CA

f) ***authorityInfoAccess***: not critical;

- CA Issuers: URI = http://crt.usertrust.com/UTNAAAClient_CA.crt - a URI for retrieving the issuing CA's certificate
- OCSP: URI = http://ocsp.usertrust.com/ - a URI to access the issuing CA's OCSP responder

g) **certificatePolicies**

- Policy ID: 1.3.6.1.4.1.6449.1.2.2.29 (Comodo CP), no policy qualifiers
- Policy ID: 1.2.840.113612.5.2.2.5 (IGTF Member Integrated X.509 Credential Services with Secured Infrastructure profile), no policy qualifiers

End Entity certificates include the following extensions:

- ***basicConstraints***: critical; CA=false
- ***keyUsage***: critical; 0xD, the digitalSignature, keyEncipherment and dataEncipherment bits are set
- ***extendedKeyUsage***: not critical;
TLS client authentication (1.3.6.1.5.5.7.3.2), e-mail protection (1.3.6.1.5.5.7.3.4)
- ***authorityKeyIdentifier***: not critical;
C8:89:73:99:A7:5D:51:16:53:45:54:7C:A3:C2:39:7C:CB:D7:AA:81
- ***subjectKeyIdentifier***: not critical;
- ***certificatePolicies***: not critical;
  - Policy ID: 1.3.6.1.4.1.6449.1.2.2.29 (Comodo CP), no policy qualifiers
  - Policy ID: 1.2.840.113612.5.2.2.5 (IGTF Member Integrated X.509 Credential Services with Secured Infrastructure profile), no policy qualifiers

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

h) ***authorityInfoAccess***: not critical;

- CA Issuers: URI = http://crt.tcs.terena.org/TERENAeSciencePersonalCA.crt
  - a URI for retrieving the issuing CA's certificate
- OCSP: URI = http://ocsp.tcs.terena.org/
  - a URI to access the issuing CA's OCSP responder

i) ***cRLDistributionPoints***: not critical;
URI = http://crl.tcs.terena.org/TERENAeSciencePersonalCA.crl
HTTP URI for retrieving the CRL of the issuing CA

7.1.3 Algorithm object identifiers

The TERENA eScience Personal CA issues certificates using the following algorithms:

- rsaEncryption (OID 1.2.840.113549.1.1.4)
- sha1WithRSAEncryption (OID 1.2.840.113549.1.1.5)

7.1.4 Name forms

The subject name of the TERENA eScience Personal CA certificate is *C=NL, O=TERENA, CN=TERENA eScience Personal CA*

Subjects of End Entity certificates follow the following pattern:

- DC: "org"
- DC: "terena"
- DC: "tcs"
- C: ISO 3166 code of the country of the relevant Member
- 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 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")
- unstructuredName: (optional) further identification of the End Entity

All attributes within the certificate subjects contain 7-bit ASCII strings encoded as PrintableStrings.

7.1.5 Name constraints

The TERENA eScience Personal CA does not use the nameConstraints extension.

7.1.6 Certificate policy object identifier

See Section 7.1.2 "Certificate extensions".

7.1.7 Usage of Policy Constraints extension

Not used.

7.1.8 Policy qualifiers syntax and semantics

Not used.

7.1.9 Processing semantics for the critical Certificate Policies extension

No Stipulation.

7.2 CRL profile

7.2.1 Version number(s)

The TERENA eScience Personal CA issues CRLs in accordance with CRL version 2 format as defined in the international standard X.509 version 3.

7.2.2 CRL and CRL entry extensions

The TERENA eScience Personal CA uses the following CRL extensions:

- ***AuthorityKeyIdentifier***: C8:89:73:99:A7:5D:51:16:53:45:54:7C:A3:C2:39:7C:CB:D7:AA:81
- ***CRL Number***: sequence number of the issued CRL

7.3 OCSP profile

The TERENA eScience Personal CA OCSP responder uses the BasicOCSPResponse version 1 as defined in RFC 2560.

The response is signed by the TCS eScience CA signing key identified by its keyID: responderID.byKey = C8:89:73:99:A7:5D:51:16:53:45:54:7C:A3:C2:39:7C:CB:D7:AA:81.

A response is signed every 24 hours or immediately after a certificate revocation. The *nextUpdate* field of a response is set to the time of its *thisUpdate* field increased by 96 hours.

The TERENA eScience Personal CA OCSP responder does not support any OCSP extensions. In particular, the TERENA eScience Personal CA does not use a cryptographic nonce in connection with its OCSP services. Instead, local time should be used by participants to ensure the freshness of the OCSP response.

8. Compliance Audit and Other Assessments

The practices specified in this CPS have been designed to meet or exceed the requirements of generally accepted and developing industry standards including the AICPA/CICA WebTrust Program for Certification Authorities, ANS X9.79:2001 PKI Practices and Policy Framework, and other industry standards related to the operation of CAs.

8.1 Frequency or Circumstances of Assessment

An annual audit is performed to assess TCS's compliance with the AICPA/CICA WebTrust programme for Certification Authorities.

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.

8.2 Identity/Qualifications of Assessor

Audits of the PKI system housing TCS's roots are performed by a public accounting firm. Audits of TCS are performed by either a public accounting firm or representative of the EUGridPMA. In both cases, the auditor:

- Has significant quality assurance mechanisms, including peer review, competency testing, and other measures.
- Abides by and conforms with the applicable standards and best practices as set forth by the relevant standards committees.

- Is knowledgeable about the operations of the CA and has an expertise in public key security technology, data centres, personnel controls, and other relevant fields of interest.
- Is knowledgeable about the operations of the CA and has an expertise in public key security technology.

8.3 Assessor's Relationship to Assessed Entity

The Assessor is independent of TCS and does not have any financial interest or course of dealings with TCS that could foreseeably create a significant bias in the Assessor's evaluation.

8.4 Topics Covered by Assessment

Topics covered by the annual audit include but are not limited to the following:

- CA practices disclosure
- Service integrity
- User data integrity

8.5 Actions Taken as a Result of Deficiency

If any material noncompliance or deficiencies are discovered during an audit, then TCS shall create and implement a plan to cure such deficiencies or noncompliance. The plan shall be created by TCS management with input from the auditing agent. In the event that the deficiency cannot be resolved, TCS may revoke any certificates affected by deficiency or noncompliance.

8.6 Communication of Results

The results of each audit are reported directly to TCS management and any other appropriate entities that may be entitled to a copy of the results by law, regulation, or agreement. Audit results may also be published by TCS at its sole and absolute discretion.

9. Other Business and Legal Matters

This part of the CPS describes the business matters of TCS and legal representations, warranties and limitations associated with TCS digital certificates.

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

9.2.1 Insurance Coverage

Because TCS Certificates are not intended to be used in financial transactions, the use of TCS certificates is not covered by TERENA's insurance.

9.2.2 Other Assets

No stipulation.

9.2.3 Insurance or Warranty Coverage for End-Entities

Not applicable.

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 keeps the following types of information confidential and maintains 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.

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.

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 Requesters 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.

9.4.3 Information Not Deemed Private

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

9.4.4 Responsibility to Protect Private Information

All CA Operator's, Member's, Subscriber's and TERENA'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.

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.

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.

9.4.7 Other Information Disclosure Circumstances

No stipulation.

9.5 Intellectual Property Rights

TERENA or its partners or associates own all intellectual property rights associated with its databases, web sites, TCS digital certificates and any other publication originating from TERENA including this CPS.

9.5.1 Certificates

Certificates are the property of TERENA. TERENA gives permission to reproduce and distribute certificates on a non-exclusive, royalty-free basis, provided that they are reproduced and distributed in full. TERENA 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. All secret shares (distributed elements) of a TCS private key remain the property of TERENA.

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.

9.5.2 Copyright

reproduce this TERENA document (as well as requests for copies from TERENA) must be addressed to: tcs-pma@terena.org.

9.5.3 Trademarks

“TERENA Certificate Service” is and other terms in this CPS are trademarks of TERENA and may only be used by permission.

9.5.4 Infringement

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

9.6 Representations and Warranties

Requesters, Subscribers, Relying Parties and any other parties shall not interfere with or reverse engineer the technical implementation of TCS PKI services, 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 TERENA. 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 Requester will result in the revocation of the Requester Digital Certificates without further notice to the Requester. 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.

9.6.1 CA Representations and Warranties

To the extent specified in the relevant sections of the CPS, TERENA promises to:

- Comply with this CPS and its internal or published policies and procedures.
- Comply with applicable laws and regulations.
- Provide infrastructure and certification services, including but not limited to the establishment and operation of the TCS Repository and web site for the operation of PKI services.
- Provide Trust mechanisms, including a key generation mechanism, key protection, and secret sharing procedures regarding its own infrastructure.
- Provide prompt notice in case of compromise of its private key(s).
- Provide and validate application procedures for the various types of certificates that it may make publicly available.
- Issue digital certificates in accordance with this CPS and fulfill its obligations presented herein.
- Publish accepted certificates in accordance with this CPS.
- Provide support to Subscribers and Relying Parties as described in this CPS.
- Revoke certificates according to this CPS.
- Provide for the expiration and renewal of certificates according to this CPS.
- Make available a copy of this CPS and applicable policies to requesting parties.

- Ensure only Members with authorized web enrollment applications can connect to the TERENA eScience Personal CA.

The Subscriber also acknowledges that TERENA has no further obligations under this CPS.

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 Requesters are accurate and true.
- The Subscriber agrees to on request provide full documentation to Member and/or TERENA 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.

9.6.3 Subscriber Representations and Warranties

Upon signing and accepting the Subscriber Agreement, the Subscriber represents 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 Requesters 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 Requesters 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/tcs/repository/.
- 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.

Upon accepting a certificate, the Requester represents to TCS and to Relying Parties that at the time of acceptance and until further notice:

- Digital signatures created using the private key corresponding to the public key included in the certificate are the digital signatures of the Requester and the certificate has been accepted and is properly operational at the time the digital signature are created.
- No unauthorized person has ever had access to the Requester's private key.
- All representations made by the Requester to TCS regarding the information contained in the certificate are accurate and true.
- All information contained in the certificate is accurate and true to the best of the Requester's knowledge or to the extent that the Requester had notice of such information whilst the Requester shall act promptly to notify TCS and/or its Subscriber of any material inaccuracies in such information.
- The certificate is used exclusively for authorized and legal purposes, consistent with this CPS.
- It will use a TCS certificate only in conjunction with the entity named in the organization field of a digital certificate (if applicable).
- The Requester retains control of its private key, uses a trustworthy system, and takes reasonable precautions to prevent its loss, disclosure, modification, or unauthorized use.
- The Requester is an end-user and not a CA, and will not use the private key corresponding to any public key listed in the certificate for purposes of signing any certificate (or any other format of certified public key) or CRL, as a CA or otherwise, with the exception of proxy certificates as defined in RFC 3820, unless expressly agreed in writing between the relevant Subscriber and TCS.
- The Requester agrees with the terms and conditions of this CPS and other agreements and policy statements of TCS.
- The Requester abides by the laws applicable in his/her country or territory including those related to intellectual property protection, computer viruses and malware, accessing computer systems etc.
- The Requester complies with all export laws and regulations for dual usage goods as may be applicable.

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

- To generate their own private / public key pair to be used in association with the certificate request submitted to TCS.
- To ensure that the public key submitted to TCS corresponds with the private key used.
- To ensure that the public key submitted to TCS is the correct one.
- To provide correct and accurate information in its communications with TCS and/or its Subscriber.
- To 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.
- To 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/tcs/repository/.
- To refrain from tampering with a TCS certificate.
- To use TCS certificates for legal and authorized purposes in accordance with the suggested usages and practices in this CPS.
- To cease using a TCS certificate if any information in it becomes misleading obsolete or invalid.
- To cease using a TCS certificate if such certificate is expired.

- To 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 as described in RFC 3820.
- To 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.
- To 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 Requester is responsible to obey the applicable law with respect to each certificate.

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:

- Minimize the risk of relying on a digital signature created by an invalid, revoked, expired or rejected certificate; the Relying Party must have reasonably made the effort to acquire sufficient knowledge on using digital certificates and PKI.
- Study the limitations to the usage of digital certificates and be aware through the Relying Party agreement the maximum value of the transactions that can be made using a TCS digital certificate.
- Read and agree with the terms of the relevant TCS CPS and Relying Party agreement.
- Verify a TCS certificate by examining the information available through TCS's OCSP service or the relevant CRL.
- Trust a TCS certificate only if it is valid and has not been revoked or has expired.
- Rely on a TCS certificate, only as may be reasonable under the circumstances listed in this section and other relevant sections of this CPS.

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 eScience Personal Certificates 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".

9.7 Disclaimers of Warranties

TERENA 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.

TERENA does not warrant:

- The accuracy, authenticity, completeness or fitness of any non-verified information contained in certificates or otherwise compiled, published, or disseminated by or on behalf of TCS except as it may be stated in the relevant product description below in this CPS.
- In addition, shall not incur liability for representations of information contained in a certificate except as it may be stated in the relevant product description in this CPS.
- Does not warrant the quality, functions or performance of any software or hardware device.
- Although TCS is responsible for the revocation of a certificate, it cannot be held liable if it cannot execute it for reasons outside its own control.
- The validity, completeness or availability of directories of certificates issued by a third party unless specifically authorised by TERENA.

Notwithstanding limitation warranties under the product section of this CPS, TERENA 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 TERENA be liable for:

- Any indirect, incidental or consequential damages.
- Any loss of profits.
- Any loss of data.
- Any other indirect, consequential or punitive damages arising from or in connection with the use, delivery, licence, performance or non-performance of certificates or digital signatures.
- Any other transactions or services offered within the framework of this CPS.
- Any other damages except for those due to reliance, on the information featured on a certificate, on the verified information in a certificate.
- Any liability incurred in this case or any other case if the fault in this verified information is due to fraud or willful misconduct of the applicant.
- Any liability that arises from the usage of a certificate that has not been issued or used in conformance with this CPS or the intended use of the ordered certificate as described on the TCS website or elsewhere.
- Any liability that arises from the usage of a certificate that is not valid.
- Any liability that arises from usage of a certificate that exceeds the limitations in usage and value and transactions stated upon it or on the CPS.
- Any liability that arises from security, usability, integrity of products, including hardware and software a Subscriber or Requester uses.
- Any liability that arises from compromise of a private key.

9.8 Limitations of Liability

In no event (except for fraud or willful misconduct) will the aggregate liability of TERENA to all parties including without any limitation a Subscriber, Requester, End Entity or Relying Party for all digital signatures and transactions related to such certificate exceed the cumulative maximum liability for such certificate as stated in the TCS insurance plan detailed in Section 9.

Parties relying on a digital certificate must verify a digital signature at all times by checking the

validity of a digital certificate through the OCSP services or the CRL provided by TCS. Relying Parties are alerted that an unverified digital signature cannot be assigned as a valid signature.

Relying on an unverifiable digital signature may result in risks that the Relying Party, and not TERENA, assumes in whole.

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/tcs/repository/ or by contacting via out of bands means via the contact address as specified in the Document Control section of this CPS.

TCS reserves its 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. TCS reserves the right not to disclose reasons for such a refusal.

9.9 Indemnities

9.9.1 Subscriber Indemnity to TERENA

By signing the Subscriber Agreement, the Subscriber agrees to indemnify and hold TERENA and contractors harmless from any acts or omissions resulting in liability, any loss or damage, and any suits and expenses of any kind, including reasonable attorneys' fees, that TERENA, and the above mentioned parties may incur, that are caused by the use or publication of a certificate, and that arises from:

- Any false or misrepresented data supplied by the Subscriber or Requester.
- Any failure of the Subscriber and Requester to disclose a material fact, if the misrepresentation or omission was made negligently or with intent to deceive the CA, TERENA, or any person receiving or relying on the certificate.
- Failure to protect their Requester's confidential data including their private key, or failure to take reasonable precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorized use of the Subscriber's confidential data.
- Breaking any laws applicable in his/her country or territory including those related to intellectual property protection, computer viruses and malware, accessing computer systems etc.

9.9.2 Subscriber Indemnity to Relying Parties

Without limiting other Subscriber obligations stated in this CPS, Subscribers are liable for any misrepresentations they make in certificates to third parties that reasonably rely on the representations contained therein and have verified one or more digital signatures with the certificate.

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, TERENA 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

TCS accepts notices related to this CPS by means of digitally-signed messages or in paper form. Upon receipt of a valid digitally-signed acknowledgment of receipt from TCS, the sender of the notice shall deem their communication effective. The sender must receive such acknowledgment within five (5) days, or else written notice must then be sent in paper form through a courier service that confirms delivery or via certified or registered mail, postage prepaid, return receipt requested, addressed as follows:

TERENA Certificate Service
TERENA
Singel 468 D
1017 AW Amsterdam
The Netherlands

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.

Controls are in place to reasonably ensure that a TCS CPS is not amended and published without the prior authorization of the TCS Policy Management Authority.

9.12.2 Notification Mechanism and Period

Upon the TCS Policy Management Authority accepting changes deemed by the CA's Policy Authority to have significant impact on the users of this CPS an updated edition of the CPS will be published at the TCS repository (available at http://www.terena.org/tcs/repository/), with seven (7) days notice given of upcoming changes and suitable incremental version numbering used to identify new editions.

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.

9.13 Dispute Resolution Procedures

Before resorting to any dispute resolution mechanism including adjudication or any type of Alternative Dispute Resolution (including without exception mini-trial, arbitration, binding expert's advice, co-operation monitoring and normal expert's advice) parties agree to notify TERENA 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 TERENA commercial or contractual relationships in which this CPS may apply or be quoted implicitly or explicitly in relation to TCS products and services where TERENA acts as a provider, supplier, beneficiary receiver or otherwise.

9.15 Compliance with Applicable Law

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

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

This CPS shall be interpreted consistently within the boundaries of business customs, commercial reasonableness under the circumstances and intended usage of a product or service. In interpreting this CPS, parties shall also take into account the international scope and application of the services and products of TCS and its international network of Members and Subscribers as well as the principle of good faith as it is applied in commercial transactions. The headings, subheadings, and other captions in this CPS are intended for convenience and reference only and shall not be used in interpreting, construing, or enforcing any of the provisions of this CPS.

Appendices and definitions to this CPS are for all purposes an integral and binding part of the CPS. When this CPS conflicts with other rules, guidelines, or contracts, this CPS shall prevail and bind the Subscriber and other parties except as to other contracts either:

- Predating the first public release of the present version of this CPS, or;
- Expressly superseding this CPS for which such contract shall govern as to the parties thereto, and to the extent permitted by law.

9.16.2 Assignment

This CPS shall be binding upon the successors, executors, heirs, representatives, administrators, and assigns, whether express, implied, or apparent, of the parties. The rights and obligations detailed in this CPS are assignable by the parties, by operation of law (including as a result of merger or a transfer of a controlling interest in voting securities) or otherwise, provided such assignment is undertaken consistent with this CPS articles on termination or cessation of operations, and provided that such assignment does not effect a novation of any other debts or obligations the assigning party owes to other parties at the time of such assignment.

9.16.3 Severability

If any provision of this CPS or the application thereof, is for any reason and to any extent found to be invalid or unenforceable, the remainder of this CPS (and the application of the invalid or

unenforceable provision to other persons or circumstances) shall be interpreted in such manner as to affect the original intention of the parties.

Each and every provision of this CPS that provides for a limitation of liability, disclaimer of or limitation upon any warranties or other obligations, or exclusion of damages is intended to be severable and independent of any other provision and is to be enforced as such.

9.16.4 Enforcement

This CPS shall be enforced as a whole, whilst failure by any person to enforce any provision of this CPS shall not be deemed a waiver of future enforcement of that or any other provision. Agreements between TERENA and the parties detailed in this CPS may contain additional provisions governing enforcement and shall be enforced according to the terms and conditions set forth within each respective agreement.

TERENA may seek indemnification and attorneys' fees from any party that violates their individual agreements with TERENA or whose conduct is in violation of this CPS. Except where an express time frame is set forth in this CPS any delay or omission by any party shall not impair or be construed as a waiver of such right, remedy or power.

9.16.5 Force Majeure

TERENA shall not be liable for any breach of its obligations, representations, warranties, or for its failure to perform where such failure or breach is as a result of a Force Majeure Event, including, but not limited to, fire, flood, earthquake, storm, hurricane or other natural disaster), war, invasion, act of foreign enemies, hostilities (whether war is declared or not), civil war, rebellion, revolution, insurrection, military or usurped power or confiscation, terrorist activities, nationalization, government sanction, blockage, embargo, labour dispute, strike, lockout or interruption or failure of electricity or telephone service or any other system operated by any other party over which TERENA has no control, or other similar causes beyond TERENA’s reasonable control where TERENA is without fault or negligence.

9.17 Other Provisions

No stipulation.

Appendix A – PKI Hierarchy

The TERENA (eScience) Personal CA is available in two PKI hierarchies:

1) **UTN-USERFirst-Client Authentication and Email**
(serial number = 44 be 0c 8b 50 00 24 b4 11 d3 36 25 25 67 c9 89,
expiry = 09/07/2019 17:36:58 GMT)
↳ **TERENA eScience Personal CA**
(serial number = 5d ff 50 ea fe 0f 53 46 88 9f 80 41 8f e7 42 c8,
expiry = 31/12/2028 23:59:59 GMT)
↳ *End Entity*
(serial number = x, expiry = up to 395 days from issuance)

2) **AAA Certificate Services**
(serial number = 01,expiry = 31/12/2028 23:59:59 GMT)
↳ **UTN-USERFirst-Client Authentication and Email**
(serial number = 7c 7c 5d bd fd 82 11 1a 73 be cd fc 27 01 b8 f0,
expiry = 31/12/2028 23:59:59 GMT)
↳ **TERENA eScience Personal CA**
(serial number = 5d ff 50 ea fe 0f 53 46 88 9f 80 41 8f e7 42 c8, expiry = 31/12/2028 23:59:59 GMT)
↳ *End Entity*
(serial number = x, expiry = up to 395 days from issuance)

Appendix B – Certificate Profiles

TCS eScience Personal		
Signature Algorithm	Sha1	
Issuer	C	"NL"
	O	"TERENA"
	CN	"TERENA eScience Personal CA"
Validity	395 days	
Subject	DC	"org"
	DC	"terena"
	DC	"tcs"
	C	ISO 3166-1 code of the country of the relevant Member
	O	Name of the Subscriber
	OU	(optional) Name of the organizational unit ofthe Subscriber
	CN	A reasonable representation of the name of the End Entity appended with an Identifier that uniquely and persistently represents the Requester in the Subscriber's IdP as described in Section 3.1.5 "Uniqueness of Names".
Authority Key Identifier	C8 89 73 99 A7 5D 51 16 53 45 54 7C A3 C2 39 7C CB D7 AA 81	

Subject Key Identifier	Public key identifier
Key Usage (Critical)	0xD (digitalSignature, keyEncipherment and dataEncipherment)
Extended Key Usage	TLS client authentication (1.3.6.1.5.5.7.3.2) E-mail protection (1.3.6.1.5.5.7.3.4)
Basic Constraint	CA = false Path Length Constraint = None
Certificate Policies	[1] Certificate Policy: PolicyIdentifier = 1.3.6.1.4.1.6449.1.2.2.29, no policy qualifiers [2] Certificate Policy: PolicyIdentifier = 1.2.840.113612.5.2.2.5, no policy qualifiers [3] Certificate Policy: PolicyIdentifier =
Subject Alternative Name	up to 10 RFC 822 name entries with e-mail addresses of the End Entity
Authority Information Access	CA Issuers: URI = http://crt.tcs.terena.org/TERENAeSciencePersonalCA.crt OCSP: URI = http://ocsp.tcs.terena.org
CRL Distribution Policies	[1] CRL Distribution Point URI = http://crl.tcs.terena.org/TERENAeSciencePersonalCA.crl