TERENA Certificate Service

TERENA Server CA, TERENA eScience Server CA & TERENA Codesigning CA Certificate Practice Statement

Version 1.8
15 October 2014
http://www.terena.org/tcs/

Table of Contents

Terms & Acronyms

Acronyms:

CA	Certification Authority
CPS	Certificate Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DCV	Domain Control Validation
DV	Domain Validated
FQDN	Fully Qualified Domain Name
ITU-T	International Telecommunications Union Telecommunication Standardisation Sector
OSCP	Online Certificate Status Protocol
OV	Organisation Validated
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure (based on X.509 Digital Certificates)
PKCS	Public Key Cryptography Standard
RA	Registration Authority
SSL	Secure Sockets Layer
TCS	TERENA Certificate Service
TLS	Transport Layer Security
URL	Uniform Resource Locator
X.509	The ITU-T standard for Certificates and their corresponding authentication framework

Terms:

Agent:	An entity authorised by another entity to act on its behalf.
Applicant:	An Applicant is a Subscriber applying for a Certificate.
Subscriber:	A Subscriber is an organisation that is part of the education and research community of a country represented by a Member and that is being issued a certificate by TERENA.
Member:	A Member is a National Research and Education Networking organisation (NREN) from a country in Europe or neighbouring regions that is a national member of TERENA, and that will be validating Certificate applications as a Registration Authority for the Member's Subscribers.
Relying Party:	A Relying Party is an entity that relies upon the information contained within the Certificate.
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/
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. It is available for reference at http://www.terena.org/tcs/repository/
Certificate Policy:	The Certificate Policy is a statement of the issuer that corresponds to the prescribed usage of a digital certificate within an issuance context.

1. General

This document is the TERENA Certificate Service (TCS) Certificate Practice Statement (CPS) and 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 the Certificate Policies 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.

1.1 Overview

The TERENA Certificate Service (TCS) is a Chain Subordinate Authority (CA) of UserTrust (AICPA/CICA WebTrust Program for Certification Authorities approved security provider) that issues high quality and highly trusted digital certificates to entities including private and public companies in accordance with this CPS. In its role as a CA, TCS performs functions associated with public key operations that include receiving requests, issuing, revoking and renewing digital certificates and the maintenance, issuance and publication of Certificate Revocation Lists (CRLs) and operating the OCSP service for users within the TCS PKI.

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

TERENA extends, under agreement, membership of TCS to approved third parties known as Registration Authorities. The international network of TCS RAs shares TERENA's policies, practices, and CA infrastructure to issue TCS digital certificates.

The CA system for TCS is hosted and operated by Comodo CA Limited (hereon the CA Operator).

1.2 Certificate Practice Statement

The TCS CPS is a public statement of the practices of TCS and the conditions of issuance, revocation and renewal of a certificate issued under TCS's own hierarchy. Pursuant to the division of the tasks of a CA, this CPS is largely divided in the following sections: Technical, Organisational, Practices and Legal.

The TCS Policy Management Authority maintains this CPS and related agreements referenced within this document. The Policy Management Authority may be contacted by email at: tcs-pma@terena.org.

This CPS, related agreements, TCS PMA description and Certificate policies referenced within this document are available online at http://www.terena.org/tcs/repository.

This CPS is identified by the following unique object identifier (OID): **1.3.6.1.4.1.25178.2.1.1.8**

ISO assigned	1
Organisation acknowledged by ISO	3
US Department of Defense	6
Internet	1
Internet Private	4
IANA registered private enterprises	1
TERENA	25178
TCS	2
CPS	1
Major version	1
Minor version	8

1.3 CPS Suitability, Amendments & Publication

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, consulting relevant external bodies representing Relying Parties when appropriate, prior to the publication of an amended edition. Upon the Policy Management Authority accepting such changes deemed 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 suitable incremental version numbering used to identify new editions. Generally, the TCS Policy Management Authority will post changes thirty days prior to their effective date unless such change is necessitated by a change in industry standards, is required for TCS to maintain its certificate operations, or is required by law or regulation. In those cases, TCS will post the change sufficiently timely to provide reasonable notice in light of the circumstances.

Revisions not denoted “significant” are those deemed by the TCS Policy Management Authority to have minimal or no impact on existing subscribers and relying parties using certificates and CRLs issued by the TCS CA. Such revisions may be made without notice to users of the CPS and without changing the version number of this CPS.

Revisions introducing new TCS products are published within two days after their approval (see 2.4).

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

1.4 Other Practice Statements & Agreements

The CPS is only one of a set of documents relevant to the provision of Certificate Services by TCS. Relevant documents and their status are detailed below:

Document	Status	Location
TCS Certification Practice Statement	Public	TCS Repository: http://www.terena.org/tcs/repository/
Template Subscriber Agreement	Public	TCS Repository: http://www.terena.org/tcs/repository/
NREN-RA Agreement	Confidential	Presented to partners accordingly

1.5 Liability of TCS

For legal liability of TCS under the provisions made in this CPS, please refer to Section 4.

1.6 Compliance with applicable standards

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 and other industry standards related to the operation of CAs including the CA/Browser Forum.

1.7 Digital Certificate Policy Overview

A digital certificate is formatted data that cryptographically binds an identified subscriber with a public key. A digital certificate allows an entity taking part in an electronic transaction to prove its identity to other participants in such transaction.

As detailed in this CPS, TCS offers a range of distinct certificate types. The different certificate types have differing intended usages and differing policies.

Certificate	Applicant	Channels Available	Validation Levels[1]	Suggested Usage
Secure Organisation Validated Server Certificate: *TCS OV Server Certificate*	Company or Organisation	TCS Website, NREN Websites	1. Confirmation of right to use the business name used in the application using third party databases and / or business documentation plus right to use the domain names used in the application. 2. The applicant's name should be the same as the name in the Subscriber Agreement that have its company seal and business license information. 3. The applicant name in the request has to be either its official name, or its English translation, or its transcription into 7-bit ASCII.	Establishes an SSL / TLS session between the server housing the Server Certificate and a client / customer / website visitor. The protocol is designed to authenticate a server to a client and provide confidentiality of data passed through the SSL / TLS session. Can be used for monetary transactions including online payments.
Secure Domain Validated Server Certificate TCS DV Server Certificate	Company or Organisation	TCS Website, NREN Websites	1.Confirmation of the right to use the domain names used in the application by Domain Control Verification (DCV) through Comodo's servers via one of the following means: challenge mail to one of the CA/Browser Forum approved addresses, or use of the HTTP CSR Hash method, or use of the DNS CNAME CSR Hash method. 2. The applicant's Subscriber Agreement uses the Comodo template published in the TERENA repository.	Establishes an SSL / TLS session between the server housing the Server Certificate and a client / customer / website visitor. The protocol is designed to authenticate a server to a client and provide confidentiality of data passed through the SSL / TLS session. Can be used for monetary transactions including online payments.

[1] Validation levels: TCS Registration Authority conducts validation under strict guidelines provided to the Registration Authority. Section 1.10 of this CPS identifies the Registration Authorities and outlines the roles and responsibilities of such entities.

Certificate	Applicant	Channels Available	Validation Levels	Suggested Usage
Secure Organisation Validated Server Certificate: *TCS OV eScience Server Certificate*	Company or Organisation	TCS Website, NREN Websites	1. Confirmation of right to use the business name used in the application using third party databases and / or business documentation plus right to use the domain name used in the application. 2. The applicant's name should be the same as the name in the Subscriber Agreement that has its company seal and business license information. 3. The applicant name in the request has to be either the English translation of its official name or its transcription into 7-bit ASCII.	Authentication of eScience hosts and services. Can be used for monetary transactions including online payments.
Secure Domain Validated Server Certificate: *TCS DV eScience Server Certificate*	Company or Organisation	TCS Website, NREN Websites	1.Confirmation of the right to use the domain names used in the application by Domain Control Verification (DCV) through Comodo's servers via one of the following means: challenge mail to one of the CA/Browser Forum approved addresses, or use of the HTTP CSR Hash method, or use of the DNS CNAME CSR Hash method. 2. The applicant's Subscriber Agreement uses the Comodo template published in the TERENA repository.	Authentication of eScience hosts and services. Can be used for monetary transactions including online payments.

Certificate	Applicant	Channels Available	Validation Levels	Suggested Usage
Object Signing Certificate: TCS Object Signing Certificate	Company or Organisation	NREN objects or code	1. Confirmation of right to use the business name used in the application using third party databases and / or business documentation. 2. The applicant's name should be the same as the name in the Subscriber Agreement that have its company seal and business license information. 3. The applicant name in the request has to be either its official name, or its English translation, or its transcription into 7-bit ASCII.	Signing of objects on behalf of a company or organisation. Examples are executable code in Java, ActiveX, .dll or .exe files and macros in Office documents

As the suggested usage for a digital certificate differs on a per application basis, Subscribers are urged to appropriately study their requirements for their specific application before applying for a specific certificate.

1.8 TCS PKI Hierarchy

TCS uses UserTrust (AICPA/CICA WebTrust Program for Certification Authorities approved security provider) for its Root CA Certificate. The partnership allows TCS to issue highly trusted digital certificates by inheriting the trust level associated with the UserTrust root certificate (named UTN).The following high-level representation of the TCS PKI is used to illustrate the hierarchy utilised.

1.8.1 TCS OV and DV Server Certificates

From the start of the TERENA Certificate Service, the following certificate chain has been in use. Certificates issued with this certificate chain use the SHA-1 algorithm. As of 20 September 2014 the expiration date of End Entity SSL certificates issued using SHA-1 is limited to 31 December 2016 23:59:59 GMT.

AddTrust External CA Root *(serial number = 1, expiry = 30 May 2020)*
↳ UTN-USERFirst-Hardware (*serial number = 48:4b:ac:f1:aa:c7:d7:13:43:d1:a2:74:35:49:97:25, expiry 30 May 2020*)
↳ TERENA SSL CA (*serial number = 4b:c8:14:03:2f:07:fa:6a:a4:f0:da:29:df:61:79:ba, expiry = 30 May 2020)*
• End Entity SSL (*serial number = x, expiry = 1, 2, 3 years from issuance)*

From 8 October 2014 onwards, the following certificate chain is available for issuing certificates that use the SHA2 algorithm.

AddTrust External CA Root *(serial number = 1, expiry = 30 May 2020)*
↳ USERTrust RSA Certification Authority (*serial number = 13:ea:28:70:5b:f4:ec:ed:0c:36:63:09:80:61:43:36, expiry 30 May 2020*)
↳ TERENA SSL CA 2 (*serial number = b0:ff:cf:3a:1d:82:44:98:15:62:9d:64:88:6a:41:65, expiry = 8 Oct 2024)*

- End Entity SSL (*serial number = x, expiry = 1, 2, 3 years from issuance)*

1.8.2 TCS OV and DV eScience Server Certificates

From the start of the TERENA Certificate Service, the following certificate chain has been in use. Certificates issued with this certificate chain use the SHA-1 algorithm. As of 20 September 2014 the expiration date of End Entity SSL certificates issued using SHA-1 is limited to 31 December 2016 23:59:59 GMT.

AddTrust External CA Root *(serial number = 1, expiry = 30 May 2020)*
↳ UTN-USERFirst-Hardware (*serial number = 48:4b:ac:f1:aa:c7:d7:13:43:d1:a2:74:35:49:97:25, expiry 30 May 2020*)
↳ TERENA eScience SSL CA (*serial number = 11:43:9e:af:68:21:02:93:f7:c5:01:1b:5c:17:dc:a0, expiry = 30 May 2020)*
- End Entity eScience SSL (*serial number = x, expiry = max 13 months from issuance)*

From 8 October 2014 onwards, the following certificate chain is available for issuing certificates that use the SHA2 algorithm.

AddTrust External CA Root *(serial number = 1, expiry = 30 May 2020)*
↳ USERTrust RSA Certification Authority (*serial number = 13:ea:28:70:5b:f4:ec:ed:0c:36:63:09:80:61:43:36, expiry 30 May 2020*)
↳ TERENA eScience SSL CA 2 (*serial number = cb:72:4d:c4:85:fd:4f:11:b9:45:a8:f1:38:03:7b:b2, expiry = 8 Oct 2024)*
- End Entity eScience SSL (*serial number = x, expiry = max 13 months from issuance)*

1.8.3 TCS Object Signing Certificates

From the start of the TERENA Certificate Service, the following certificate chain has been in use. Certificates issued with this certificate chain use the SHA-1 algorithm. As of 20 September 2014 the expiration date of End Entity SSL certificates issued using SHA-1 is limited to 31 December 2016 23:59:59 GMT.

AddTrust External CA Root *(serial number = 1, expiry = 30 May 2020)*
↳ UTN-USERFirst-Object (*serial number* = 42:1a:f2:94:09:84:19:1f:52:0a:4b:c6:24:26:a7:4b, expiry = 30 May 2020)
↳ TERENA Codesigning CA (*serial number = 55:1b:68:c7:a6:aa:a4:55:b0:2c:59:e0:73:73:11:da, expiry = 30 May 2020)*
- End Entity eScience SSL (*serial number = x, expiry = max 13 months from issuance)*

From 8 October 2014 onwards, the following certificate chain is available for issuing certificates that use the SHA2 algorithm.

AddTrust External CA Root *(serial number = 1, expiry = 30 May 2020)*
↳ USERTrust RSA Certification Authority (*serial number =* 13:ea:28:70:5b:f4:ec:ed:0c:36:63:09:80:61:43:36, expiry = 30 May 2020)
↳ `TERENA Code Signing CA 2` (*serial number =* `c9:25:e1:df:fb:e3:36:6d:5c:e4:f5:15:c4:76:63:09`*, expiry = 8 Oct 2024)*
- End Entity SSL (*serial number = x, expiry = 1, 2, 3 years from issuance)*

1.9 TCS Certification Authority

In its role as a Certification Authority (CA) TCS provides certificate services within the TCS PKI. The TCS CA will:

- Conform its operations to the CPS (or other CA business practices disclosure), as the same may from time to time be modified by amendments published in the TCS repository (http://www.terena.org/tcs/repository/).
- Issue and publish certificates in a timely manner in accordance with the issuance times set out in this CPS.
- Upon receipt of a valid request to revoke the certificate from a person authorised to request revocation using the revocation methods detailed in this CPS, revoke a certificate issued for use within the TCS PKI.
- Issue and publish CRLs and update the OCSP service data in a timely manner.
- Notify subscribers via email of the imminent expiry of their TCS issued certificate.

1.10 TCS Registration Authorities

TERENA has established the necessary secure infrastructure to fully manage the lifecycle of digital certificates within the TCS PKI. Through a network of Registration Authorities (RA), one for each NREN participating in the TCS, TERENA also makes its certification authority services available to their subscribers. A TCS RA:

- Maintains a register of organisations within its constituency that are approved as Subscribers.
- Accepts, evaluates, approves or rejects certificate applications.
- Verifies the accuracy and authenticity of the information provided by the Subscriber at the time of application as specified in the TCS validation guidelines documentation.
- Uses official, notarized or otherwise indicated documents to evaluate a Subscriber application.
- Verifies the accuracy and authenticity of the information provided by the Subscriber at the time of issuance or reissuance or renewal of certificates as specified in the TCS validation guidelines documentation.
- Uses secure channels to communicate with TCS CAs.

A TCS RA acts locally within its own context of geographical or business partnerships on approval and authorisation by TERENA in accordance with the TCS practices and procedures.

1.11 Subscribers

Subscribers use PKI in relation with TCS supported transactions and communications. Subscribers are identified in a certificate and hold the private key corresponding to the public key listed in the certificate. Each Subscriber must sign and stamp the relevant Subscriber Agreement and deliver it to its RA.

1.12 Relying Parties

Relying parties use PKI services in relation with TCS certificates and reasonably rely on such certificates and/or digital signatures verifiable with reference to a public key listed in a Subscriber's certificate.

To verify the validity of a digital certificate they receive, relying parties must refer to the Certificate Revocation List (CRL) or Online Certificate Status Protocol (OCSP) service prior to relying on information featured in a certificate to ensure that TCS has not revoked the certificate. The CRL location as well as the OCSP responder location are detailed within the certificate.

2. Technology

This section addresses certain technological aspects of the TCS infrastructure and PKI services.

2.1 TCS CA Infrastructure

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. The TCS CA infrastructure is hosted and operated by Comodo CA Limited.

2.1.1 TCS CA Signing Key Protection & Recovery

Protection of the TCS CA signing key pairs is ensured with the use of IBM 4578 cryptographic coprocessor devices, which are certified to FIPS 140-1 Level 4, for key generation, storage and use. The TCS CA signing key pairs are 2048 bit long and were generated within the IBM 4578 device.

CA No.	Description	Usage	Lifetime	Size/hash
1	TERENA SSL CA	Intermediate certificate for Server SSL certificates, Class 3	To 30 May 2020	RSA 2048 SHA-1
2	TERENA eScience SSL CA	Intermediate certificate for Server SSL certificates, Class 3	To 30 May 2020	RSA 2048 SHA-1
3	TERENA Codesigning CA	Intermediate certificate for Object Signing, Class 3	To 30 May 2020	RSA 2048 SHA-1
4	TERENA SSL CA 2	Intermediate certificate for Server SSL certificates, Class 3	To 8 Oct 2024	RSA 2048 SHA384
5	TERENA eScience SSL CA 2	Intermediate certificate for Server SSL certificates, Class 3	To 8 Oct 2024	RSA 2048 SHA384
6	TERENA Code Signing CA 2	Intermediate certificate for Object Signing, Class 3	To 8 Oct 2024	RSA 2048 SHA384

For TCS CA key recovery purposes, the TCS CA signing keys are encrypted and stored within a secure environment. The decryption key is split across five removable media and requires three of five of them to reconstruct the decryption key. Two more authorised custodians are required to physically retrieve the removable media from the distributed physically secure locations.

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

Comodo ensures the protection of the UserTrustRoot signing key pair and the TCS CA signing key pairs in accordance with its AICPA/CICA WebTrust program compliant infrastructure and CPS. Details of Comodo's WebTrust compliancy are available at its official website (http://www.comodo.com/).

2.1.2 TCS CA Signing Key Generation Process

TCS private key(s) are securely generated and protected using a trustworthy system (IBM 4758 accredited to FIPS PUB 140-1 level 4), and takes necessary precautions to prevent the compromise or unauthorised usage of it.

The TCS CA key was generated in a secure manner in a secure facility. The activities undergone and the personnel involved in the root key generation are recorded for audit purposes. Any subsequent key generations will be done in a secure facility.

2.1.3 TCS CA Signing Key Archival

When any TCS CA 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, as detailed in Section 2.1.1 of this CPS.

2.1.4 Procedures employed for TCS CA Signing Key Changeover

The lifetime of TCS CA keys is set out in the table in Section 2.1.1. At least 13 months before expiration of each private key's lifetime, a new CA signing key pair is commissioned and all subsequently issued certificates and CRLs 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 2.1.5 of this CPS.

2.1.5 CA Root Public Key Delivery to Subscribers

TCS makes all its CA certificates and the relevant root certificates available in online repositories at http://www.terena.org/tcs/repository/. The UserTrust Root certificate is present in Internet Explorer 5.00 and above, Netscape 4.x and above and Opera 5.0 and above and is made available to relying parties through these browsers.

TCS provides the full certificate chain (see Section 1.8 of this CPS) to the Subscriber upon issuance and delivery of the Subscriber certificate.

2.1.6 Physical CA Operations

Access to the secure part of CA Operator facilities is limited using physical access control and is only available to appropriately authorised individuals (referred to hereon 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.

The CA Operator has made reasonable efforts to ensure its secure facilities are protected from:

- Fire and smoke damage (fire protection is made in compliance with local fire regulations).
- Flood and water damage.

The CA Operator's 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.

The CA Operator asserts that it makes every reasonable effort to detect and prevent material breaches, loss, damage or compromise of assets and interruption to business activities.

2.2 Digital Certificate Management

TCS certificate management refers to functions that include but are not limited to the following:

- Verification of the identity of an applicant of a certificate.
- Authorising the issuance of certificates.
- Issuance of certificates.
- Revocation of certificates.
- Listing of certificates.
- Distributing certificates.
- Publishing certificates.

- Storing certificates.
- Retrieving certificates in accordance with their particular intended use.

TERENA conducts the overall certification management within the TCS PKI, either directly or through a TERENA approved RA or Comodo. TERENA is not involved in functions associated with the generation, issuance, decommissioning or destruction of a Subscriber key pair.

2.3 TCS Directories, Repository and Certificate Revocation Lists

The CA Operator manages and makes publicly available lists of revoked certificates using Certificate Revocation Lists (CRLs). All CRLs issued on behalf of TCS are X.509v2 CRLs, in particular as profiled in RFC5280. Users and relying parties are strongly urged to consult the lists of revoked certificates at all times prior to relying on information featured in a certificate. The CA operator updates and publishes a new CRL after a certificate revocation. The CRL for end entity certificates using SHA-1 can be accessed via the following URLs:
http://crl.tcs.terena.org/TERENASSLCA.crl
http://crl.tcs.terena.org/TERENAeScienceSSLCA.crl
http://crl.tcs.terena.org/TERENACodeSigningCA.crl

The CRL for end entity certificates using SHA2 can be accessed via the following URL:

http://crl.usertrust.com/USERTrustRSACertificationAuthority.crl

Information about the revocation status of a certificate using SHA-1 may be accessed via Online Certificate Status Protocol (OCSP) responder operated by the CA operator at:

http://ocsp.tcs.terena.org/

Information about the revocation status of a certificate using SHA2 may be accessed via Online Certificate Status Protocol (OCSP) responder operated by the CA operator at:

http://ocsp.usertrust.com/

Revoked intermediate certificates are published in the CRL accessed via:

http://crl.usertrust.com/UTN-USERFirst-Hardware.crl
http://crl.usertrust.com/UTN-USERFirst-Object.crl
http://crl.usertrust.com/USERTrustRSACertificationAuthority.crl

TERENA publishes a repository of legal notices regarding its PKI services, including this CPS, agreements and notices, references within this CPS as well as any other information it considers essential to its services. The TCS legal repository may be accessed at

http://www.terena.org/tcs/repository/

2.4 Types of TCS Certificates

TCS currently offers a portfolio of digital certificates and related products that can be used in a way that addresses the needs of users for secure personal and business communications, including but not limited to protection of online transactions and identification of persons, whether legal or physical, or devices on a network or within a community.

TERENA may update or extend its list of products, including the types of certificates it issues, as it sees fit. The publication or updating of the list of TCS products creates no claims by any third party. Upon the inclusion of a new certificate product in the TCS hierarchy, an amended version of this CPS will be made public within two days in the official TCS repository.

2.4.1 TCS Server Certificates

TCS makes available secure Server Certificates that in combination with a Secure Socket Layer (SSL) or Transport Layer Security (TLS) server attest the public server's identity, providing full

authentication and enabling secure communication with customers and business partners. TCS Server Certificates support multiple domain names with a single certificate. The maximum number of domain names per certificate is 100.

TCS Server Certificates support multiple sub-domains with a single certificate with a wildcard name forms as specified in Section 3.1 of RFC 2818. Starting version 1.7 of this CPS, wildcard name forms MUST be an FQDN that starts with an asterisk immediately followed by a period (*.example.domain.tld), The form f*.com mentioned in RFC 2818, using any character in front of the asterisk is deprecated.

In accordance with Section 4.3 of this CPS, TCS OV and DV Server Certificates validate domain names. Additionally, TCS OV Server Certificates validate the identity of the applying organisation. The organisationName attribute of the TCS OV Server Certificate subject contains:

a) either the official name of the subscribing organisation in its native language encoded as UTF8String, or;

b) the name of the organisation transcribed into 7-bit ASCII, or;

c) the English translation of the name of the organisation.

The official name of the organisation is always known to the respective RA.

From Dec 20th 2010 onwards, TCS no longer issues certificates of less than 2048 bit key length and does not accept Certificate Signing Requests (CSRs) generated with keys of less than 2048 bit.

From Feb 1st 2013 onwards. TCS OV Server Certificates are only issued after an out of band check by Comodo in accordance of the CA/Browser Forum guidelines.

2.4.2 TCS eScience Server Certificates

TCS eScience Server Certificates may be used for authenticating eScience hosts and services.

In accordance with Section 4.3 of this CPS, TCS OV and DV eScience Server Certificates validate domain names. Additionally, TCS OV eScience Server Certificates validate the identity of the applying organisation. The organisationName attribute of the TCS OV eScience Server Certificate subject contains:

a) either the official name of the subscribing organisation in its native language transcribed into 7-bit ASCII, or;

b) the English translation of the name of the organisation.

The official name of the organization is always known to the respective CA.

TCS OV and DV eScience Server Certificates are issued in accordance with IGTF profile “Classic X.509 CAs with secured infrastructure”, namely:

- All TCS eScience Server certificates have subjects within a dedicated namespace defined by the prefix of “dc=org, dc=terena, dc=tcs”.
- Maximum validity period of any TCS eScience Server certificate is 13 months.
- All attribute values within the subject name of any TCS eScience certificate contain only 7-bit ASCII strings.
- The subject of any TCS eScience Server certificate is bound to exactly one end entity.
- The minimum RSA key size from the start of the TCS services was 1024 bits. From Dec 20th 2010 onwards, TCS no longer issues certificates of less than 2048 bit key length and does not accept Certificate Signing Requests (CSRs) generated with keys of less than 2048 bit. From Feb 1st 2013 onwards, TCS OV eScience Server Certificates are

only issued after an out of band check by Comodo in accordance of the CA/Browser Forum guidelines.

2.4.3 TCS Object Signing Certificates

TCS Object Signing Certificates may be used for signing of objects on behalf of a company or organisation.

In accordance with Section 4.3 of this CPS, TCS Object Signing Certificates validate organisation names and the identity of the applying organisation. The commonName attribute of a TCS Object Signing Certificate is set identical to the organisationName. The organisationName attribute of the certificate subject contains:

a) either the official name of the subscribing organisation in its native language encoded as UTF8String, or;

b) the name of the organisation transcribed to 7-bit ASCII, or;

c) the English translation of the name of the organisation.

The official name of the organisation is always known to the respective RA.

From Dec 20th 2010 onwards, TCS no longer issues certificates of less than 2048 bit key length and does not accept Certificate Signing Requests (CSRs) generated with keys of less than 2048 bit.

2.5 Extensions and Naming

TCS uses the standard X.509, version 3, as profiled by RFC 5280 to construct digital certificates for use within the TCS PKI.

2.6 Subscriber Private Key Generation Process

TCS does not provide key generation, escrow, recovery or backup facilities.

Upon making a certificate application, the Subscriber is solely responsible for the generation of an RSA key pair appropriate to the certificate type being applied for. During application, the Subscriber will be required to submit a public key and other personal / corporate details.

Typically, Server Certificate requests are generated using the key generation facilities available in the Subscriber's web server software; typically Object Signing key generation uses a variety of software development kits, a webbrowser or OpenSSL.

2.7 Subscriber Private Key Protection and Backup

Subscribers are solely responsible for protection of their private keys. TCS maintains no involvement in the generation, protection or distribution of such keys.

TCS strongly urges Subscribers to use a strong password or equivalent authentication method to prevent unauthorised access and usage of the Subscriber's private key.

2.8 Subscriber Public Key Delivery to TCS

TCS Server Certificate requests, TCS eScience Server Certificate requests and Object Signing requests are submitted to TCS in the form of a PKCS #10 Certificate Signing Request (CSR). Submission is made electronically via a TERENA approved RA.

2.9 Delivery of Issued Subscriber Certificate to Subscriber

Delivery of Subscriber certificates to the associated Subscriber is dependent on the certificate product type:

2.9.1 TCS Server Certificate

TCS Server Certificates are delivered via email to the Subscriber using the requester's email address provided during the application process.

2.9.2 TCS eScience Server Certificate

TCS eScience Server Certificates are delivered via email to the Subscriber using the requester's email address provided during the application process.

2.9.3 TCS Object Signing Certificate

TCS eScience Server Certificates are delivered via email to the Subscriber using the requester's email address provided during the application process.

2.10 TCS Certificate Profiles

TCS certificates are of general purpose and may be used without restriction on geographical area or industry. In order to use and rely on a TCS certificate the relying party must use X.509v3 compliant software. A Certificate profile contains fields as specified below:

2.10.1 Extension Criticality Field

The Extension Criticality field denotes two possible uses for the respective extension. If the extension is noted as critical, then the key in the certificate is only to be applied to the stated uses. To use the key for another purpose in this case would break the issuer's policy. If the extension is not noted as critical, a certificate using system that does not recognize or implement that extension type may process the remainder of the certificate ignoring the extension.

2.10.2 Key Usage extension field

TCS certificates include a key usage extension field to specify the purposes for which the certificate may be used and to technically limit the functionality of the certificate when used with X.509v3 compliant software. Reliance on key usage extension fields is dependent on correct software implementations of the X.509v3 standard and is outside of the control of TCS.

The possible key purposes identified by the X.509v3 standard are the following:

a) Digital signature, for verifying digital signatures that have purposes other than those identified in b), f) or g), that is, for entity authentication and data origin authentication and/or integrity protection.

b) Non-repudiation, for verifying digital signatures used in providing a non-repudiation service which protects against the signing entity falsely denying some action (excluding certificate or CRL signing, as in f) or g) below).

c) Key encipherment, for enciphering keys or other security information, e.g. for key transport.

d) Data encipherment, for enciphering user data, but not keys or other security information as in c) above.

e) Key agreement, for key agreement, e. g. when a Diffie-Hellman key is to be used for key management.

f) Certificate signing, for verifying a CA's signature on certificates, used in CA-certificates only.

g) CRL signing, for verifying a CA's signature on CRLs.

h) Encipher only, public key agreement key for use only in enciphering data when used with key agreement.

i) Decipher only, public key agreement key for use only in deciphering data when used with key agreement.

2.10.3 Basic Constraints Extension

The Basic Constraints extension specifies whether the subject of the certificate may act as a CA or only as an end-entity. Reliance on the basic constraints extension field is dependent on correct software implementations of the X.509v3 standard and is outside of the control of TERENA.

2.10.4 Certificate Policy (CP)

A Certificate Policy (CP) is a statement of the issuer that corresponds to the prescribed usage of a digital certificate within an issuance context. A policy identifier is a number unique within a specific domain that allows for the unambiguous identification of a policy, including a certificate policy.

2.11 Specific TCS certificate profiles are as per the tables below:

TCS OV Server Certificate using SHA-1		
Signature Algorithm	sha1withRSAEncryption	
Issuer	C	NL
	O	TERENA
	CN	TERENA SSL CA
Validity	1 / 2 / 3 year(s)	
Subject	C	<Country of the Organisation>
	ST	<State of the Organisation> (optional)
	L	<Locality of the Organisation> (optional)
	O	<Organisation Name>
	OU	<Organisational Unit Name> (optional)
	CN	Contains a Fully Qualified Domain Name
	unstructuredName	Contains an FQDN (optional)
Basic Constraint (Critical)	ca: false Path Length Constraint: not included	
Key Usage (Critical)	Digital Signature, Key Encipherment(A0)	
Extended Key Usage	TLS Server Authentication, TLS Client Authentication	
Subject Alternative Name	*1 up to 100 DNS names or IP addresses*	
CRL Distribution Points	[1] CRL Distribution Point Distribution Point Name: Full Name: URL = http://crl.tcs.terena.org/TERENASSLCA.crl	
Authority Information Access	*[1] AccessMethod = CA Issuers* *Location* = http://crt.tcs.terena.org/TERENASSLCA.crt *[2] AccessMethod=OCSP* *Location* = http://ocsp.tcs.terena.org	
Authority Key Identifier	KeyID = <Unique ID of the issuer's public key>	
Subject Key Identifier	<Unique ID of the subject's public key>	
Certificate Policies	[1]Certificate Policy: PolicyIdentifier = 1.3.6.1.4.1.6449.1.2.2.29	

TCS OV Server Certificate using SHA2		
Signature Algorithm	sha256WithRSAEncryption	
Issuer	C	NL
	ST	Noord-Holland
	L	Amsterdam
	O	TERENA
	CN	TERENA SSL CA
Validity	1 / 2 / 3 year(s)	
Subject	C	<Country of the Organisation>
	ST	<State of the Organisation> (optional)
	L	<Locality of the Organisation> (optional)
	O	<Organisation Name>
	OU	<Organisational Unit Name> (optional)
	CN	Contains a Fully Qualified Domain Name
	unstructuredName	Contains an FQDN (optional)
Basic Constraint (Critical)	ca: false Path Length Constraint: not included	
Key Usage (Critical)	Digital Signature, Key Encipherment(A0)	
Extended Key Usage	TLS Server Authentication, TLS Client Authentication	
Subject Alternative Name	*1 up to 100 DNS names or IP addresses*	
CRL Distribution Points	[1] CRL Distribution Point Distribution Point Name: Full Name: URL = http://crl.usertrust.com/TERENASSLCA2.crl	
Authority Information Access	*[1] AccessMethod = CA Issuers* *Location* = http://crt.usertrust.com/TERENASSLCA2.crt *[2] AccessMethod=OCSP* *Location* = http://ocsp.usertrust.com	
Authority Key Identifier	KeyID = <Unique ID of the issuer's public key>	
Subject Key Identifier	<Unique ID of the subject's public key>	
Certificate Policies	[1]Certificate Policy: PolicyIdentifier = 1.3.6.1.4.1.6449.1.2.2.29	

TCS DV Server Certificate using SHA-1		
Signature Algorithm	sha1withRSAEncryption	
Issuer	C	NL
	O	TERENA
	CN	TERENA SSL CA
Validity	1 / 2 / 3 year(s)	
Subject	OU	Domain Control Validated

	CN	Contains a Fully Qualified Domain Name
	unstructuredName	Contains an FQDN(optional)
Basic Constraint (Critical)	ca: false Path Length Constraint: not included	
Key Usage (Critical)	Digital Signature, Key Encipherment(A0)	
Extended Key Usage	TLS Server Authentication, TLS Client Authentication	
Subject Alternative Name	*1 up to 100 DNS names or IP addresses*	
CRL Distribution Points	[1] CRL Distribution Point Distribution Point Name: Full Name: URL = http://crl.tcs.terena.org/TERENASSLCA.crl	
Authority Information Access	*[1] AccessMethod = CA Issuers* *Location* = http://crt.tcs.terena.org/TERENASSLCA.crt *[2] AccessMethod=OCSP* *Location* = http://ocsp.tcs.terena.org	
Authority Key Identifier	KeyID = <Unique ID of the issuer's public key>	
Subject Key Identifier	<Unique ID of the subject's public key>	
Certificate Policies	[1]Certificate Policy: PolicyIdentifier = 1.3.6.1.4.1.6449.1.2.2.29 [2]Certificate Policy: PolicyIdentifier = 2.23.140.1.2.1	

TCS DV Server Certificate using SHA2		
Signature Algorithm	sha256WithRSAEncryption	
Issuer	C	NL
	ST	Noord-Holland
	L	Amsterdam
	O	TERENA
	CN	TERENA SSL CA 2
Validity	1 / 2 / 3 year(s)	
Subject	OU	Domain Control Validated
	CN	Contains a Fully Qualified Domain Name
	unstructuredName	Contains an FQDN(optional)
Basic Constraint (Critical)	ca: false Path Length Constraint: not included	
Key Usage (Critical)	Digital Signature, Key Encipherment(A0)	
Extended Key Usage	TLS Server Authentication, TLS Client Authentication	
Subject Alternative Name	*1 up to 100 DNS names or IP addresses*	

CRL Distribution Points	[1] CRL Distribution Point Distribution Point Name: Full Name: URL = http://crl.usertrust.com/TERENASSLCA2.crl
Authority Information Access	*[1] AccessMethod = CA Issuers* *Location* = URI:http://crt.usertrust.com/TERENASSLCA2.crt *[2] AccessMethod=OCSP* *Location* = http://ocsp.usertrust.com
Authority Key Identifier	KeyID = <Unique ID of the issuer's public key>
Subject Key Identifier	<Unique ID of the subject's public key>
Certificate Policies	[1]Certificate Policy: PolicyIdentifier = 1.3.6.1.4.1.6449.1.2.2.29 [2]Certificate Policy: PolicyIdentifier = 2.23.140.1.2.1

TCS OV eScience Server Certificate using SHA-1		
Signature Algorithm	sha1withRSAEncryption	
Issuer	C	NL
	O	TERENA
	CN	TERENA eScience SSL CA
Validity	Up to 13 months	
Subject	DC	"org"
	DC	"terena"
	DC	"tcs"
	C	<Country of the Organisation>
	O	<Organisation Name>
	OU	<Organisational Unit Name> (optional)
	CN	Contains a fully qualified domain name of the server
Basic Constraint (Critical)	ca: false Path Length Constraint: not included	
Key Usage (Critical)	Digital Signature , Key Encipherment, Data Encipherment(B0)	
Extended Key Usage	TLS Server Authentication, TLS Client Authentication	
Subject Alternative Name	*1 up to 100 DNS names or IP addresses*	
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL = http://crl.tcs.terena.org/TERENAeScienceSSLCA.crl	
Authority Information Access	*[1] AccessMethod = CA Issuers* *Location* = http://crt.tcs.terena.org/TERENAeScienceSSLCA.crt *[2] AccessMethod = OCSP* *Location*=http://ocsp.tcs.terena.org/	
Authority Key Identifier	KeyID= <Unique ID of the issuer's public key>	

Subject Key Identifier	<Unique ID of the subject's public key>
Certificate Policies	[1]Certificate Policy: PolicyIdentifier = 1.3.6.1.4.1.6449.1.2.2.29 [2]Certificate Policy: PolicyIdentifier = 1.2.840.113612.5.2.2.1

TCS OV eScience Server Certificate using SHA2		
Signature Algorithm	sha256WithRSAEncryption	
Issuer	C	NL
	ST	Noord-Holland
	L	Amsterdam
	O	TERENA
	CN	TERENA eScience SSL CA 2
Validity	Up to 13 months	
Subject	DC	"org"
	DC	"terena"
	DC	"tcs"
	C	<Country of the Organisation>
	O	<Organisation Name>
	OU	<Organisational Unit Name> (optional)
	CN	Contains a fully qualified domain name of the server
Basic Constraint (Critical)	ca: false Path Length Constraint: not included	
Key Usage (Critical)	Digital Signature , Key Encipherment, Data Encipherment(B0)	
Extended Key Usage	TLS Server Authentication, TLS Client Authentication	
Subject Alternative Name	*1 up to 100 DNS names or IP addresses*	
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL = http://crt.usertrust.com/TERENASSLCA2.crt	
Authority Information Access	*[1] AccessMethod = CA Issuers* *Location* = http://crt.tcs.terena.org/TERENAeScienceSSLCA.crt *[2] AccessMethod = OCSP* *Location*=http://ocsp.tcs.terena.org	
Authority Key Identifier	KeyID= <Unique ID of the issuer's public key>	
Subject Key Identifier	<Unique ID of the subject's public key>	
Certificate Policies	[1]Certificate Policy: PolicyIdentifier = 1.3.6.1.4.1.6449.1.2.2.29 [2]Certificate Policy: PolicyIdentifier = 1.2.840.113612.5.2.2.1	

TCS DV eScience Server Certificate using SHA-1		
Signature Algorithm	sha1withRSAEncryption	
Issuer	C	NL
	O	TERENA
	CN	TERENA eScience SSL CA
Validity	Up to 13 months	
Subject	DC	"org"
	DC	"terena"
	DC	"tcs"
	OU	Domain Control Validated
	CN	Contains a fully qualified domain name of the server
Basic Constraint (Critical)	ca: false Path Length Constraint: not included	
Key Usage (Critical)	Digital Signature , Key Encipherment (A0)	
Extended Key Usage	TLS Server Authentication, TLS Client Authentication	
Subject Alternative Name	*1 up to 100 DNS names or IP addresses*	
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL = http://crl.tcs.terena.org/TERENAeScienceSSLCA.crl	
Authority Information Access	*[1] AccessMethod = CA Issuers* *Location* = http://crt.tcs.terena.org/TERENAeScienceSSLCA.crt *[2] AccessMethod = OCSP* *Location*=http://ocsp.tcs.terena.org/	
Authority Key Identifier	KeyID= <Unique ID of the issuer's public key>	
Subject Key Identifier	<Unique ID of the subject's public key>	
Certificate Policies	[1]Certificate Policy: PolicyIdentifier = 1.3.6.1.4.1.6449.1.2.2.29 [2]Certificate Policy: PolicyIdentifier = 2.23.140.1.2.1 [3]Certificate Policy: PolicyIdentifier = 1.2.840.113612.5.2.2.1	

TCS DV eScience Server Certificate using SHA2		
Signature Algorithm	sha256WithRSAEncryption	
Issuer	C	NL
	ST	Noord-Holland
	L	Amsterdam
	O	TERENA
	CN	TERENA eScience SSL CA
Validity	Up to 13 months	

Subject	DC	"org"
	DC	"terena"
	DC	"tcs"
	OU	Domain Control Validated
	CN	Contains a fully qualified domain name of the server
Basic Constraint (Critical)	ca: false Path Length Constraint: not included	
Key Usage (Critical)	Digital Signature , Key Encipherment (A0)	
Extended Key Usage	TLS Server Authentication, TLS Client Authentication	
Subject Alternative Name	*1 up to 100 DNS names or IP addresses*	
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL = http://crl.usertrust.com/TERENAeScienceSSLCA2.crl	
Authority Information Access	*[1] AccessMethod = CA Issuers* *Location* = http://crt.usertrust.com/TERENAeScienceSSLCA2.crt *[2] AccessMethod = OCSP* *Location*=http://ocsp.usertrust.com	
Authority Key Identifier	KeyID= <Unique ID of the issuer's public key>	
Subject Key Identifier	<Unique ID of the subject's public key>	
Certificate Policies	[1]Certificate Policy: PolicyIdentifier = 1.3.6.1.4.1.6449.1.2.2.29 [2]Certificate Policy: PolicyIdentifier = 2.23.140.1.2.1 [3]Certificate Policy: PolicyIdentifier = 1.2.840.113612.5.2.2.1	

TCS Object Signing Certificate using SHA-1		
Signature Algorithm	sha1withRSAEncryption	
Issuer	C	NL
	O	TERENA
	CN	TERENA Code Signing CA
Validity	1 / 2 / 3 year(s)	
Subject	C	<Country of the Organisation>
	ST	<State of the Organisation>
	L	<Locality of the Organisation>
	PostalCode	<Postcode of the Organisation>
	Street	<Street Address of the Organisation>
	O	<Organisation Name>
	OU	<Organisational Unit Name> (optional)
	CN	<Organisation Name> (same as O)
Basic Constraint (Critical)	ca: false Path Length Constraint: not included	

Key Usage (Critical)	Digital Signature(80)
Extended Key Usage	Id-kp-codeSigning
Subject Alternative Name	rfc822Name: *Contact e-mail address*
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL = http://crl.tcs.terena.org/crl.tcs.terena.org/TERENACodeSigningCA.crl
Authority Information Access	*[1] AccessMethod=CA Issuers* *Location* = http://crt.tcs.terena.org/TERENACodeSigningCA.crt *[2] AccessMethod=OCSP* *Location*=http://ocsp.tcs.terena.org
Authority Key Identifier	KeyID = <Unique ID of the issuer's public key>
Subject Key Identifier	<Unique ID of the subject's public key>
Certificate Policies	[1]Certificate Policy: PolicyIdentifier = 1.3.6.1.4.1.6449.1.2.2.29

TCS Object Signing Certificate Using SHA2		
Signature Algorithm	sha256WithRSAEncryption	
Issuer	C	NL
	ST	Noord-Holland
	L	Amsterdam
	O	TERENA
	CN	TERENA Code Signing CA 2
Validity	1 / 2 / 3 year(s)	
Subject	C	<Country of the Organisation>/postalCode
	ST	<State of the Organisation>
	L	<Locality of the Organisation>
	PostalCode	<Postcode of the Organisation>
	Street	<Street Address of the Organisation>
	O	<Organisation Name>
	OU	<Organisational Unit Name> (optional)
	CN	<Organisation Name> (same as O)
Basic Constraint (Critical)	ca: false Path Length Constraint: not included	
Key Usage (Critical)	Digital Signature(80)	
Extended Key Usage	Id-kp-codeSigning	
Subject Alternative Name	rfc822Name: *Contact e-mail address*	

CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL = http://crl.usertrust.com/TERENACodeSigningCA2.crl
Authority Information Access	*[1] AccessMethod=CA Issuers* *Location* = http://crt.usertrust.com/TERENACodeSigningCA2.crt *[2] AccessMethod=OCSP* *Location*=http://ocsp.usertrust.com
Authority Key Identifier	KeyID = <Unique ID of the issuer's public key>
Subject Key Identifier	<Unique ID of the subject's public key>
Certificate Policies	[1]Certificate Policy: PolicyIdentifier = 1.3.6.1.4.1.6449.1.2.2.29

2.12 TCS Certificate Revocation List Profile

The profile of the TCS Certificate Revocation List is as per the table below:

Version	[Version 2]	
Issuer Name	<Subject DN of the Issuer>	
This Update	<Date of Issuance>	
Next Update	<Date of Issuance + 96 hours>	
Revoked Certificates	CRL Entries	
	Certificate Serial Number	[Certificate Serial Number]
	Date and Time of Revocation	[Date and Time of Revocation]
Authority Key Identifier	The identifier of Issuer's public key	
CRL Number	Monotonically increasing sequence number	

3. Organisation

TERENA operates within the Netherlands while its PKI infrastructure is hosted by Comodo within the United States. All sites operate under a security policy designed to, within reason, detect, deter and prevent unauthorised 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.

3.1 Conformance to this CPS

TERENA and TCS RAs conform to this CPS and other obligations they undertake through adjacent contracts when they provide the TCS services.

3.2 Termination of CA Operations

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, TERENA will take the following steps, where possible:

- Providing subscribers of valid certificates with ninety (90) days notice of its intention to cease acting as a CA.
- Revoking all certificates that are still un-revoked or un-expired at the end of the ninety (90) day notice period without seeking subscriber's consent.
- Giving timely notice of revocation to each affected subscriber.
- 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'.

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

3.3 Form of Records

TERENA may require Subscribers to submit appropriate documentation in support of a certificate application. In such circumstances, TERENA retains such records in line with the practices of record retention as stated in Section 3.4 of this CPS.

TCS Registration Authorities are required to submit appropriate documentation prior to being validated and successfully accepted as an approved TCS Registration Authority.

In its role as a TCS Registration Authority, RAs may require documentation from subscribers to support certificate applications. In such circumstances, RAs are obliged to retain such records in line with the practices of record retention as stated in Section 3.4 of this CPS.

3.4 Records Retention Period

TERENA or the RAs retain the records of TCS digital certificates and the associated documentation for a term of no less than 3 years after the expiration or revocation of the certificate. Copies of certificates are held, 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 TERENA may see fit.

3.5 Logs for Core Functions

For audit purposes, TERENA, Comodo, or the appropriate RA maintain electronic or manual logs of the following events for core functions. CA Operator's 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 Comodo 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 within the development site, or off-site in a secure storage facility.

An audit log is maintained of each movement of the removable media. Logs are archived by the system administrator on a weekly basis and event journals reviewed on a weekly basis by CA management. Both current and archived logs are maintained in a form that prevents unauthorised 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. RAs' logs are regularly backed up and held at secure location.

All logs include the following elements:

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

3.5.1 CA & Certificate Lifecycle Management

- CA Root signing key functions, including key generation, backup, recovery and destruction; maintained by Comodo.
- Subscriber certificate life cycle management, including successful and unsuccessful certificate applications, certificate issuances, certificate re-issuances and certificate renewals; maintained by the RA that dealt with the event.
- Subscriber certificate revocation requests, including revocation reason; maintained by the RA that dealt with the event.
- Subscriber changes of affiliation that would invalidate the validity of an existing certificate; maintained by the RA that dealt with the event.
- Certificate Revocation List updates, generations and issuances; maintained by Comodo
- Custody of keys and of devices and media holding keys; maintained by Comodo
- Compromise of a private key; maintained by Comodo.

3.5.2 Security Related Events

- System downtime, software crashes and hardware failures; maintained by Comodo
- CA system actions performed by Comodo personnel, including software updates, hardware replacements and upgrades; maintained by Comodo
- Cryptographic hardware security module events, such as usage, de-installation, service or repair and retirement; maintained by Comodo
- Successful and unsuccessful TCS access attempts; maintained by the operator of the accessed system
- Secure CA facility visitor entry and exit; maintained by Comodo

3.5.3 Certificate Application Information

- The documentation and other related information presented by the applicant as part of the application validation process; maintained by the RA that dealt with the event
- Storage locations, whether physical or electronic, of presented documents; maintained by the storage operator

3.5.4 Log Retention Period

TERENA, Comodo and the RAs maintain logs for a period of 3 years, or as necessary to comply with applicable laws.

3.6 Business Continuity Plans and Disaster Recovery

Appropriate contingency and disaster recovery plans and procedures have been implemented, documented and periodically tested to ensure the integrity of TCS services. Such plans are revised and updated as may be required at least once a year.

- TCS's backup CA is readily available in the event that the primary CA should cease operation. All of the 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, allowing a maximum system outage time (in case of critical systems failure) of 1 hour.
- Backup of critical CA software is performed weekly and is stored offsite.
- Backup of critical business information is performed daily and is stored offsite.

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 and

renewal of such certificates.

As well as a fully redundant CA system, there are 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 endeavours to minimise interruptions to TCS CA operations.

3.7 Availability of Revocation Data

Certificate Revocation Lists (CRLs) allow relying parties to verify a digital signature made using a TCS issued digital certificate. Each CRL contains entries for all revoked un-expired certificates issued and is valid for 96 hours. A new CRL is issued by Comodo on TCS's behalf every 24 hours or on at most 1 hour after a certificate revocation. Under special circumstances, a new CRL may be published prior to the expiry of the current CRL. CRLs include a monotonically increasing sequence number for each CRL issued. All expired CRLs are archived (as described in Section 3.4 of this CPS) for a period of 7 years or longer if applicable.

Current revocation status of all non-expired certificates is available via Online Certificate Status Protocol. The OCSP information is updated immediately after every revocation.

3.8 Publication of Critical Information

TERENA publishes this CPS and all its previous versions, certificate terms and conditions, and templates for subscriber agreements in the official TCS repository at http://www.terena.org/tcs/repository/. The TCS Policy Management Authority maintains the repository. All updates, amendments and legal promotions are logged in accordance with the logging procedures referenced in Section 3.5 of this CPS.

Localized templates for subscriber agreements are published by TCS RAs in their repositories.

3.9 Confidential Information

TERENA, Comodo and the RAs observe applicable rules on the protection of personal data deemed by law or this CPS to be confidential.

3.9.1 Types of Information deemed as Confidential

TERENA, Comodo and the RAs keep the following types of information confidential and maintain reasonable controls to prevent the exposure of such records to non-trusted personnel.

j) Signed Subscriber agreements.

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

l) Transaction records and financial audit records.

m) Contingency plans and disaster recovery plans.

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

3.9.2 Types of Information not deemed as Confidential

Subscribers acknowledge that revocation data of all certificates issued by the TCS CA is public information. Subscriber application data marked as "Public" in Section 4.4 of this CPS, and submitted as part of a certificate application is published within an issued digital certificate.

3.9.3 Access to Confidential Information

All personnel in trusted positions handle all information in strict confidence. Personnel of RAs especially must comply with the requirements of the applicable law on the protection of personal data.

3.9.4 Release of Confidential Information

TERENA, Comodo and the RAs are not required to release any confidential information, unless as otherwise required by law, without an authenticated, reasonably specific request by an authorised party specifying:

a) The party to whom TERENA, Comodo and the RAs owe a duty to keep information confidential.

b) The party requesting such information.

c) A court order, if any.

3.10 Personnel Management and Practices

Consistent with this CPS TERENA, Comodo and the RAs follow personnel and management practices that provide reasonable assurance of the trustworthiness and competence of their employees and of the satisfactory performance of their duties.

3.10.1 Trusted roles

Trusted roles relate to access to the TCS account management system, with functional permissions applied on an individual basis. Senior members of the management team decide permissions, with signed authorisations being archived.

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

3.10.2 Personnel controls

All personnel assigned to validation are checked to ensure they are trustworthy before being allowed to validate applicants for Certificates. Personnel are trained on the validation processes found herein prior to assisting in any validation.

3.11 Privacy Policy

TERENA, Comodo and the RAs manage all information in a manner complying with privacy requirements of this CPS.

3.12 Publication of information

All TCS public information is available via the official TCS repository at http://www.terena.org/tcs/repository/.

4. Practice & Procedures

This section describes the certificate application process, including the information required to make and support a successful application.

4.1 Subscriber registration

Prior to requesting any certificate, a Subscriber must submit to an RA:

- All documents and information required to register its organisation with the RA as a Subscriber. These documents should include a proof of identity of the organisation and an appointment of administrative contact(s) to represent the organisation for TCS.
- Subscriber agreement signed by a legal representative of the organisation.
- Optionally, a list of DNS domain names registered by the Subscriber.
- Optionally, a list of IP address ranges assigned to the Subscriber.

After verifying the supplied information, the RA registers the Subscriber and approves it for requesting TCS certificates.

4.1.1 Administrative Contact

An Administrative Contact is a person authorized by the Subscriber to submit certificate applications on behalf of the Subscriber.

An Administrative Contact is also authorized by the Subscriber to approve TCS certificate requests submitted on behalf of the organisation. The requests approved by an Administrative Contact are automatically checked by the RA system to comply with the registered data of the applicant organisation. Namely, the name of the organisation, the DNS name(s), and the IP addresses within the certificate application must match the respective data as registered with the RA. Upon successful check, the application is automatically submitted to the TCS CA for issuance without any further manual intervention of the RA.

By appointing an Administrative Contact, the appointing organisation accepts full responsibility for his/her actions.

An Administrative Contact must operate in compliance with this CPS and other relevant TCS documents.

4.2 Certificate Application Requirements

All Certificate applicants must complete the enrolment process, which includes:

- Generate an RSA key pair and demonstrate to an RA ownership of the private key through the submission of a valid PKCS#10 Certificate Signing Request (CSR).
- Make all reasonable efforts to protect the integrity of their private key.
- Submit to an RA a certificate application, including application information as detailed in this CPS, a public key, and agree to the terms of the relevant subscriber agreement.
- Provide a proof of identity through the submission of official documentation as requested in this CPS.

Certificate applications are submitted to a TERENA approved RA. The following table details the entity(s) involved in the processing of certificate applications. TCS issues all certificates regardless of the processing entity.

Certificate Type	Enrolment Entity	Processing Entity	Issuing Authority
Server Certificate *all types as per Sections 2.4.1 and 2.4.2 of this CPS*	End Entity Subscriber RA	RA	TCS
Object Signing Certificate *as per Section 2.4.3 of this CPS*	End Entity Subscriber RA	RA	TCS

Generally, applicants will complete the online forms made available by TERENA or by approved RAs at their respective official websites. Under special circumstances, the applicant may submit an application via email; however, this process is available at the discretion of the particular RA.

4.3 Application Validation

Prior to issuing a certificate the RA employs controls to validate the subscriber information featured in the certificate application. The product type indicates such controls:

4.3.1 TCS Server Certificate Application Validation Process

TCS RA utilises a validation process prior to the issuance of a secure server certificate of all types.

This process involves TCS RA, automatically or manually, reviewing the application information provided by the applicant (as per Section 4.4 of this CPS) in order to check that:

- The applicant has the right to use the domain name used in the application. This is validated by reviewing domain name ownership records publicly available through the Internet or approved global domain name registrars.
- The application is submitted through the Administrative Contact of the applicant.
- The applicant is an accountable legal entity (organisation) registered with the RA. This is validated by requesting official company documentation, such as Business Licence, Articles of Incorporation, Sales Licence or other relevant documents.
- The applicant has signed a Subscriber Agreement with the RA with its company seal and its officer signed.

The above assertions are reviewed through an automated process when submitted by the Administrative Contact of the applicant or through manual review of supporting documentation and reference to third party official databases in any other case.

4.3.2 TCS Object Signing Certificate Application Validation Process

TCS RA utilises a validation process prior to the issuance of an object signing certificate.

This process involves TCS RA, automatically or manually, reviewing the application information provided by the applicant (as per Section 4.4 of this CPS) in order to check that:

- The application is submitted through the Administrative Contact of the applicant.
- The applicant is an accountable legal entity (organisation) registered with the RA. This is validated by requesting official company documentation, such as Business Licence, Articles of Incorporation, Sales Licence or other relevant documents.
- The applicant has signed a Subscriber Agreement with the RA with its company seal and its officer signed.

The above assertions are reviewed through an automated process when submitted by the Administrative Contact of the applicant or through manual review of supporting documentation and reference to third party official databases in any other case.

4.4 Validation Information for Certificate Applications

Applications for TCS certificates are supported by appropriate documentation to establish the identity of an applicant.

4.4.1 Application Information for Organisational Applicants

The following elements are critical information elements for a TCS certificate issued to an organisation. Those elements marked with PUBLIC might be present within an issued certificate 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 Organisation (PUBLIC)
- Organisational unit – optional (PUBLIC)
- Street, city, postal/zip code, country (PUBLIC)
- Company number (if available)
- Server Software Identification (for server certificates only)

- Administrative contact full name, email address and telephone
- Fully Qualified Domain Name (PUBLIC)
- Public Key (PUBLIC)
- Proof of right to use name
- Proof of existence and organisational status of the Organisation
- Subscriber Agreement (electronically accepted)

4.4.2 Supporting Documentation for Organisational Applicants

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

- Articles of Association
- Business License
- Certificate of Compliance
- Certificate of Incorporation
- Certificate of Authority to Transact Business
- Tax Certification
- Corporate Charter
- Official letter from an authorised representative of a government organisation
- Official letter from office of Dean or Principal (for Educational Institutions)

A TCS RA may accept at its discretion other official organisational documentation supporting an application.

4.5 Validation Requirements for Certificate Applications

Upon receipt of an application for a digital certificate and based on the submitted information, a TCS RA confirms the following information:

- The certificate applicant 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.
- Any agents who apply for a certificate listing the certificate applicant’s public key are duly authorised 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 the TCS RA of any changes that would affect the validity of the certificate. Failure to comply with the obligations as set out in the Subscriber Agreement will result in the revocation of the Subscriber's Digital Certificate without further notice to the Subscriber.

4.5.1 Third-Party Confirmation of Business Entity Information

A TCS RA may use the services of a third party to confirm information on a business entity that applies for a digital certificate. A TCS RA accepts confirmation from third party organisations, other third party databases and government entities.

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

A TCS RA may use any means of communication at its disposal to ascertain the identity of an applicant. TCS RA reserves right of refusal in its absolute discretion.

4.5.2 Serial Number Assignment

TCS assigns certificate serial numbers that appear in TCS certificates. Assigned serial numbers are unique.

4.6 Time to Confirm Submitted Data

A TCS RA makes reasonable efforts to confirm certificate application information and issue a digital certificate within reasonable time frames.

Typically, a TCS RA accepts or rejects certificate requests within 5 working days after the receipt of all required validation information as per this CPS.

4.7 Approval and Rejection of Certificate Applications

Following successful completion of all required validations of a certificate application, the TCS RA approves an application for a digital certificate.

If the validation of a certificate application fails, the TCS RA rejects the certificate application.

A TCS RA 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 TCS might get tarnished, diminished or have its value reduced and under such circumstances may do so without incurring any liability or responsibility for any loss or expenses arising as a result of such refusal.

Applicants whose applications have been rejected may subsequently re-apply.

After the TCS RA approves a certificate application the Comodo CA uses a validation process before issueing or rejecting the application. This process meets or exceeds the requirements of generally accepted and developing industry standards including the AICPA/CICA WebTrust Program for Certification Authorities and other industry standards related to the operation of CAs including the CA/Browser Forum.

From Feb 1st 2013 onwards. TCS OV Server Certificates are only issued after an out of band check by Comodo in accordance of the CA/Browser Forum guidelines.

From Jan 2012 onward, most TCS OV and DV Server Certificates are only issued after a Domain Control Validation for all domain names in an application. From June 1st 2012 all TCS OV and DV Server Certificates use DCV; including all eScience Server certificates and certificates containing names from different domains in the SubjectAlternativeNames.

Domain Control Verification (DCV) is done through Comodo's servers via one of the following means: challenge mail to one of the CA/Browser Forum approved addresses, or use of the HTTP CSR Hash method, or use of the DNS CNAME CSR Hash method.

4.8 Certificate Issuance and Subscriber Consent

TCS 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 4.10 of this CPS). Issuing a digital certificate means that the Comodo CA and TCS RA accept a certificate application.

4.9 Certificate Validity

Certificates are valid upon issuance by TCS and acceptance by the Subscriber. Generally, the certificate validity period will be 1, 2 or 3 years, although TCS reserves the right to offer validity periods outside of this standard validity period.

The maximum validity period for TCS eScience Server Certificate is 13 months.

As of 20 September 2014 the expiration date of End Entity SSL certificates issued using SHA-1

is limited to 31 December 2016 23:59:59 GMT.

4.10 Certificate Acceptance by Subscribers

An issued certificate is either delivered via email or installed on a Subscriber's computer / hardware security module through an online collection method. A Subscriber is deemed to have accepted a certificate when:

- The Subscriber uses the certificate.
- 30 days pass from the date of the issuance of a certificate.

4.11 Verification of Digital Signatures

Verification of a digital signature is used to determine that:

- The private key corresponding to the public key listed in the signer's certificate created the digital signature.
- The signed data associated with this digital signature has not been altered since the digital signature was created.

4.12 Reliance on Digital Signatures

TCS Certificates can be used for online payments. The final decision concerning whether or not to rely on a verified digital signature is exclusively that of the relying party. Reliance on a digital signature should only occur if:

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

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

4.13 Certificate Suspension

TCS does not utilise certificate suspension.

4.14 Certificate Revocation

Revocation of a certificate is to permanently end the operational period of the certificate prior to reaching the end of its stated validity period. TCS will revoke a digital certificate if:

- There has been loss, theft, modification, unauthorised disclosure, or other compromise of the private key associated with the certificate.
- The Subscriber has breached a material obligation under this CPS.
- Either the Subscriber's or TCS' obligations under this CPS 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 Subscriber that is contained within the certificate.
- The certificate is used contrary to law, rule or regulation or was issued as a result of fraud or negligence.
- The certificate, if not revoked, will compromise the ability of TCS to provide certificates.

4.14.1 Request for Revocation

The Subscriber or other appropriately authorised parties such as RAs can request revocation of a certificate. Prior to the revocation of a certificate, the relevant TCS RA will verify that the revocation request has been:

- either made by the organisation that made the certificate application, or;
- made by the RA on behalf of the organisation that used the RA to make the certificate application, or;
- made by an entity that can prove ownership of the private key associated with the certificate

A TCS RA employs the following procedure for processing a revocation request depending on the requester:

- A properly authenticated revocation request made by an Administrative Contact of the Subscriber will be automatically accepted without any other checks. The revocation request and the identity of the Administrative Contact will be logged.
- If the revocation request has been made by a representative of the Subscriber, the RA may require confirmation by telephone or by fax. TCS RA validation personnel will then command the revocation of the certificate and logging of the identity of validation personnel and the reason for revocation will be maintained in accordance with the logging procedures covered in this CPS.
- If the revocation requester can prove its ownership of the private key associated with the certificate, the TCS RA will command the revocation of the certificate without any other checks. The revocation request and the proof of the relevant private key by the requester will be logged.

4.14.2 Effect of Revocation

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 within the Certificate Revocation List (CRL) and remains on the CRL until after the end of the certificate's validity period. After the revocation of each certificate, an updated CRL is published on the TCS repository. For immediate revocation data, the OCSP may be used to obtain real-time validation information. Under special circumstances the CRL may be published more frequently.

The current revocation status of a certificate is also available via the OCSP at http://ocsp.tcs.terena.org/.

4.15 Renewal

Depending on the option selected during application, the validity period of TCS certificates is one year (365 days), two years (730 days), three years (1095 days) or 13 months (396 days) from the date of issuance and is detailed in the relevant field within the certificate. As of 20 September 2014 the expiration date of End Entity SSL certificates issued using SHA-1 is limited to 31 December 2016 23:59:59 GMT.

Renewal application requirements and procedures are the same as those employed for the application validation and issuance requirements detailed for new customers.

4.16 Notice Prior to Expiration

TCS RAs shall make reasonable efforts to notify subscribers via e-mail, of the imminent expiration of a digital certificate. Notice shall ordinarily be provided within a 30-day period prior to the expiry of the certificate.

4.17 TCS Representations

TCS makes to all subscribers and relying parties certain representations regarding its public service, as described below. TCS reserves its right to modify such representations as it sees fit or as required by law.

4.18 Information Incorporated by Reference into a TCS Digital Certificate

TCS incorporates by reference the following information in every digital certificate it issues:

- Terms and conditions of the digital certificate.
- Any other applicable certificate policy as may be stated on an issued TCS certificate, including the location of this CPS.
- The mandatory elements of the standard X.509v3.
- Any non-mandatory but customised elements of the standard X.509v3.
- Any other information inserted into the Certificate.

4.19 Publication of Certificate Revocation Data

TCS publishes OCSP and CRL data as described in Section 2.3.

4.20 Duty to Monitor the Accuracy of Submitted Information

In all cases and for all types of TCS certificates the Subscriber has a continuous obligation to monitor the accuracy of the information submitted with the application and notify the relevant TCS RA about any changes.

4.21 Publication of Information

Published critical information may be updated from time to time as prescribed in this CPS. Such updates shall be indicated through appropriate version numbering and publication date on any new version.

4.22 Interference with TCS Implementation

Subscribers, relying parties and any other parties shall not interfere with, or reverse engineer the technical implementation of TCS PKI services including 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.

4.23 Standards

TCS assumes that user software that is claimed to be compliant with X.509v3 and other applicable standards enforces the requirements set out in this CPS. TERENA, Comodo and the RAs cannot warrant that such user software will support and enforce controls required by TCS, whilst the user should seek appropriate advice.

4.24 RA Limitations

RAs shall not undertake any actions that might imperil, put in doubt or reduce the trust cassociated with TCS' Certificate offering.

4.25 Limitation of Liability for a RA

TERENA warrants that certificates issued through the RAs will be valid as if TERENA itself had issued the Certificate.

4.26 Choice of Cryptographic Methods

Parties are solely responsible for having exercised independent judgment 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.

4.27 Reliance on Unverified Digital Signatures

Parties relying on a digital certificate must verify a digital signature at all times by checking the validity of a digital certificate against the relevant CRL published by TCS and/or OCSP responder operated by TCS. Relying parties are alerted that an unverified digital signature cannot be assigned as a valid signature of the Subscriber.

Relying on an unverifiable digital signature may result in risks that the relying parties, and not TERENA, Comodo and the RAs, assume in whole.

TERENA, Comodo and the RAs have adequately informed relying parties on the usage and validation of digital signatures through this CPS and other documentation published in the 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.

4.28 Rejected Certificate Applications

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. The private key may also not be resubmitted as part of any other certificate application to TCS.

4.29 Refusal to Issue a Certificate

TERENA, Comodo and the RAs reserve the right to refuse to issue a certificate to any party as they sees fit, without incurring any liability or responsibility for any loss or expenses arising out of such refusal. TERENA, Comodo and the RAs reserve the right not to disclose reasons for such a refusal.

4.30 Subscriber Obligations

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

- To minimise internal risk of private key compromise by ensuring adequate knowledge and training on PKI is provided internally.
- To ensure that the public key submitted to a TCS RA corresponds with the private key used.
- To ensure that the public key submitted to a TCS RA is the correct one.
- To provide correct and accurate information in its communications with a TCS RA.
- To alert a TCS RA 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 TCS 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 authorised 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 to sign or encrypt transmissions if such certificate is expired.
- To refrain from using the Subscriber's private key corresponding to the public key in a TCS issued certificate to issue end-entity digital certificates or subordinate CA certificates.
- To make reasonable efforts to prevent the compromise, loss, disclosure, modification, or otherwise unauthorised use of the private key corresponding to the public key published in a TCS certificate.
- To request the revocation of a certificate in case of an occurrence that materially affects the integrity of a TCS certificate as soon as possible, but within one working day after the occurrence.
- For acts and omissions of partners and agents that use to generate, retain, escrow, or destroy their private keys.

4.31 Representations by Subscriber upon Acceptance

Upon accepting a certificate, the Subscriber 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 is the digital signature of the Subscriber and the certificate has been accepted and is properly operational at the time the digital signature is created.
- No unauthorised person has ever had access to the Subscriber's private key.
- All representations made by the Subscriber 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 Subscriber's knowledge or to the extent that the Subscriber had notice of such information whilst the Subscriber shall act promptly to notify TCS of any material inaccuracies in such information.
- The certificate is used exclusively for authorised and legal purposes, consistent with this CPS.
- The Subscriber will use a TCS certificate only in conjunction with the entity named in the organisation field of a digital certificate (if applicable).
- The Subscriber retains control of its private key, uses a trustworthy system, and takes reasonable precautions to prevent its loss, disclosure, modification, or unauthorised use.
- The Subscriber is an end-user Subscriber 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 Subscriber and TERENA.
- 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, viruses, accessing computer systems etc.
- The Subscriber complies with all export laws and regulations for dual usage goods as may be applicable.

4.32 Indemnity by Subscriber

By accepting a certificate, the Subscriber agrees to indemnify and hold TERENA, as well as its RAs, agent(s) 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 agent(s).
- Any failure of the Subscriber 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 the Subscriber's confidential data including their private key, or failure to take reasonable precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorised use of the Subscriber's confidential data.
- Breaking any laws applicable in its country or territory including those related to intellectual property protection, viruses, accessing computer systems etc.

4.33 Obligations of TCS Registration Authorities

A TCS RA operates under the policies and practices detailed in this CPS and the individual agreement with the RA. The RA is bound under contract to:

- Receive applications for TCS certificates in accordance with this CPS.
- Perform all verification actions prescribed by this CPS
- Receive, verify and relay to TCS all requests for revocation of a TCS certificate in accordance with the TCS revocation procedures and the CPS.
- Act according to relevant Law and regulations.

4.34 Obligations of a Relying Party

A party relying on a TCS certificate accepts that in order to reasonably rely on a TCS certificate they must:

- Minimise 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.
- Read and agree with the terms of the TCS CPS.
- Verify a TCS certificate by referring to the relevant CRL and the CRLs of intermediate CA and root CA and/or the relevant OCSP service.
- 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.

4.35 Legality of Information

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.

4.36 Subscriber Liability 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.

4.37 Duty to Monitor Agents

The Subscriber shall control and be responsible for the data that is supplied to TCS for a Certificate, whether by the Subscriber or an agent of the Subscriber.

4.38 Use of Agents

For certificates issued at the request of a Subscriber's agent, both the agent and the Subscriber shall jointly and severally indemnify TCS, and its agents and contractors.

4.39 Conditions of usage of the TCS Repository and Web site

Parties (including subscribers and relying parties) accessing the TCS Repository (http://www.terena.org/tcs/repository/) and official web site(s) agree with the provisions of this CPS and any other conditions of usage that TCS may make available.

Parties demonstrate acceptance of the conditions of usage of the CPS by using a TCS issued certificate.

Failure to comply with the conditions of usage of the TCS Repositories and web site may result in terminating the relationship between TCS and the party.

4.40 Accuracy of Information

TERENA and the RAs, recognising their trusted position, make all reasonable efforts to ensure that parties accessing TCS Repositories receive accurate, updated and correct information. TERENA, Comodo and the RAs however, cannot accept any liability beyond the limits set in this CPS.

4.41 Obligations of TCS

To the extent specified in the relevant sections of the CPS, TERENA and the RAs promise to:

- Comply with this CPS and its internal or published policies and procedures.
- Comply with applicable laws and regulations.
- Provide infrastructure and certificate 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 their private key(s).
- Provide and validate application procedures for the various types of certificates that they may make publicly available.
- Issue digital certificates in accordance with this CPS and fulfil their obligations presented herein.
- Upon receipt of a request from an RA operating within the TCS network act promptly to issue a TCS certificate in accordance with this CPS.
- Upon receipt of a request for revocation from an RA operating within the TCS network act promptly to revoke a TCS certificate in accordance with this CPS. The received revocation request must be reacted upon within one working day.
- 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.

The Subscriber also acknowledges that TERENA and the RAs have no further obligations under this CPS.

4.42 Fitness for a Particular Purpose

TERENA and the RAs disclaim 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.

4.43 Other Warranties

TERENA and the RAs:

- Do not warrant the accuracy, authenticity, completeness or fitness of any unverified information contained in certificates or otherwise compiled, published, or disseminated by or on behalf of TERENA, Comodo and the RAs except as it may be stated in the relevant product description below in this CPS and in the TCS insurance policy.
- 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.
- Do not warrant the quality, functions or performance of any software or hardware device.
- Although being responsible for the revocation of a certificate, cannot be held liable if they cannot execute it for reasons outside their own control.
- Do not warrant the validity, completeness or availability of directories of certificates issued by a third party (including an agent) unless specifically stated by TERENA, Comodo and the RAs.

4.44 Non-Verified Subscriber Information

Notwithstanding limitation warranties under the product section of this CPS, TERENA, Comodo and the RAs shall not be responsible for non-verified Subscriber information submitted to TCS, or the TCS directory or otherwise submitted with the intention to be included in a certificate.

4.45 Exclusion of Certain Elements of Damages

In no event (except for fraud or willful misconduct) shall TERENA and the RAs be liable for:

- Any direct, indirect, incidental or consequential damages.
- Any loss of profits.
- Any loss of data.
- Any other direct, indirect, consequential or punitive damages arising from or in connection with the use, delivery, license, 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.
- 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 uses.
- Any liability that arises from compromise of a Subscriber's private key.
- Any liability that arises from usage of a certificate for monetary transactions including online payments.

4.46 Certificate Insurance Plan

4.47 Financial Limitations on Certificate Usage

This section is deprecated.

4.48 Damage and Loss Limitations

In no event (except for fraud or willful misconduct) will TERENA and the RAs be liable to any party for all digital signatures and transactions related to such certificate

4.49 Conflict of Rules

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.
- Expressly superseding this CPS for which such contract shall govern as to the parties thereto, and to the extent permitted by law.

4.50 TCS 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 TCS including this CPS.

4.51 Infringement and Other Damaging Material

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

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

4.52 Ownership

TCS 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.

4.53 Governing Law

This CPS is governed by, and construed in accordance with the law 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 quoted implicitly or explicitly in relation to TCS products and services where TERENA acts as a provider, supplier, beneficiary receiver or otherwise.

4.54 Jurisdiction

Each party, including TERENA, Comodo and the RAs, partners and relying parties, irrevocably agrees that the courts of the Netherlands have exclusive jurisdiction to hear and decide any suit, action or proceedings, and to settle any disputes, which may arise out of or in connection with this CPS or the provision of TCS PKI services.

4.55 Dispute Resolution

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.

4.56 Successors and Assigns

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's sections 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.

4.57 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.

4.58 Interpretation

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 Registration Authorities 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.

4.59 No Waiver

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.

4.60 Notice

TERENA 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 TERENA, 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:

TCS PMA
TERENA
Singel 468 D
1017 AW Amsterdam
The Netherlands

Email: tcs-pma@terena.org

This CPS, related agreements and Certificate policies referenced within this document are available online at http://www.terena.org/tcs/repository/.

4.61 Fees

Individual NRENs may decide to charge for TCS services to cover their costs.

4.62 Reissue Policy

TCS does not support certificate reissuance. Every application for a certificate is treated as a new one.

4.63 Refund Policy

Individual NRENs may publish their refund policies.

Document Control

This document is version 1.8 of the TCS CPS, created on 18 October 2014 and signed off by the TCS Certificate Policy Authority

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

URL: http://www.terena.org/tcs/
E-mail: tcs-pma@terena.org

Copyright Notice