TRUST ITALIA SPA Certification Practice Statement

Version 4.2

Related to
DigiCert CP v5.4 (29/09/2020) and DigiCert CPS v5.4 (29/09/20)

Effective Date: 17/06/2022

TRUST ITALIA SPA
Via Po 22, 00198 Roma - ITALY
+39 06 332287
www.trustitalia.it

TRUST ITALIA SPA Certification Practices Statement

Published date: 21/10/2020

Important – Acquisition Notice

On October 31, 2017, DigiCert, Inc. completed the acquisition of Symantec Corporation's Website Security business unit. As a result, DigiCert is now the registered owner of this Certification Practices Statement document and the PKI Services described within this document.

However, a hybrid of references to "VeriSign," "Symantec" and "DigiCert" shall be evident within this document for a period of time until it is operationally practical to complete the re-branding of the Certification Authorities and services. Any references to VeriSign or Symantec as a corporate entity should be strictly considered to be legacy language that solely reflects the history of ownership.

At the same time , any referral to STN CPS should be intended as this CPS, and referral to STN intended as TRUST ITALIA SPA sub-domain.

Trademark Notices

1. INTRODUCTION

This document is the **TRUST ITALIA SPA** Certification Practice Statement ("CPS"). It states the practices that **TRUST ITALIA SPA** certification authorities ("CAs") employ in providing certification services that include, but are not limited to, issuing, managing, revoking, and renewing certificates in accordance with the specific requirements of the DigiCert Certificate Policies ("CP").

The CP is the principal statement of policy and establishes the business, legal, and technical requirements for approving, issuing, managing, using, revoking, and renewing, digital Certificates and providing associated trust services.

TRUST ITALIA SPA has authority over End-Entity Certificates and Sub-CAs chained to his Intermediate CAs, in turn chained up to DigiCert Primary CAs (herein referred as Sub-Domain) **TRUST ITALIA SPA**'s Sub-domain includes entities subordinate to it such as its Customers, Subscribers, and Relying Parties.

While the CP sets forth requirements that **TRUST ITALIA SPA** meet, this CPS describes how **TRUST ITALIA SPA** meets these requirements within **TRUST ITALIA SPA**'s Sub-domain. More specifically, this CPS describes the practices that **TRUST ITALIA SPA** employs for:

- securely managing the core infrastructure ,
- and issuing, managing, revoking, and renewing Certificates

within **TRUST ITALIA SPA**'s Sub-domain , in accordance with the requirements of the CP.

This CPS conforms to the Internet Engineering Task Force (IETF) RFC 3647 for Certificate Policy and Certification Practice Statement construction.

1.1 Overview

TRUST ITALIA SPA is a Service Center which means **TRUST ITALIA SPA** can approve or reject Certificate Applications in the case of Retail Certificates or, in the case of Enterprise Certificates, arrange with a Processing Center to provide Enterprise Customers with back-end Certificate lifecycle services.

TRUST ITALIA SPA is a "Processing Center which means **TRUST ITALIA SPA** has established a secure facility housing, among other things, CA systems, including the cryptographic modules holding the private keys used for the issuance of Certificates. **TRUST ITALIA SPA** acts as a CA and performs all Certificate lifecycle services of issuing, managing, revoking, and renewing Certificates. It also provides CA key management and Certificate lifecycle services on behalf of its Enterprise Customers or the Enterprise Customers of the Service Centers subordinate to **TRUST ITALIA SPA**. **TRUST ITALIA SPA** also offers Certificates in all three lines of business, Consumer (Level 1 and 2 client Retail Certificates), and Enterprise (providing Managed PKI services). The practices relating to services provided by Affiliates or services provided by DigiCert to Affiliates are beyond the scope of this CPS.

This CPS is specifically applicable to:

- **TRUST ITALIA SPA** Infrastructure CAs, and **TRUST ITALIA SPA** Administrative CAs
- **TRUST ITALIA SPA**'s Public CAs and the CAs of enterprise Customers, who issue Certificates within **TRUST ITALIA SPA's** sub-domain.More generally, the CPS also governs the use of **TRUST ITALIA SPA**'s Sub-domain by all individuals and entities within **TRUST ITALIA SPA**'s Sub-domain (collectively, **TRUST ITALIA SPA** Sub-domain Participants"). Unless specifically noted within this CPS, Private CAs and hierarchies managed by **TRUST ITALIA SPA** are outside the scope of this CPS.

TRUST ITALIA SPA offers two Levels of Certificates within its Sub-domain. This CPS describes how **TRUST ITALIA SPA** meets the CP requirements for each Level within its Sub-domain. Thus, the CPS, as a single document, covers practices and procedures concerning the issuance and management of all two Certificate Levels.

TRUST ITALIA SPA may publish Certificate Practices Statements that are supplemental to this CPS in order comply with the specific policy requirements of Government, or other industry standards and requirements.

These supplemental certificate policies shall be made available to subscribers for the certificates issued under the supplemental policies and their relying parties.

This CPS describes the practices used to comply with the current versions of the following policies, guidelines, and requirements:

Name of Policy/Guideline/Requirement Standard	**Location of Source Document/Language**
DigiCert Certificate Policy version 5.4	https://www.digicert.com/legal-repository/
the Certification Authority / Browser Forum ("CAB Forum") Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates ("Baseline Requirements")	https://cabforum.org/baseline-requirements-document/
the CAB Forum Network and Certificate System Security Requirements	https://cabforum.org/network-security-requirements/
Microsoft Trusted Root Store (Program Requirements)	https://docs.microsoft.com/en-us/security/trusted-root/program-requirements
Mozilla Root Store Policy	https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/
Mozilla CA/Forbidden or Problematic Practices	https://wiki.mozilla.org/CA/Forbidden_or_Problematic_Practices
Apple Root Store Program	https://www.apple.com/certificateauthority/ca_program.html
360 Browser CA Policy	https://caprogram.360.cn/#strategy
Chromium Project Root Store Certificate Policy	https://www.chromium.org/Home/chromium-security/root-ca-policy

- The CPS is only one of a set of documents relevant to **TRUST ITALIA SPA**'s Sub-domain. These other documents include both private and public documents, such as the DigiCert's CP, Relying Party agreements, and agreements imposed by **TRUST ITALIA SPA** such as Subscribers and Customers Agreement**.**

Pursuant to the IETF PKIX RFC 3647 CP/CPS framework, this CPS is divided into nine parts that cover the security controls and practices and procedures for certificate. To preserve the outline specified by RFC 3647, section headings that do not apply are accompanied with the statement "Not applicable" or "No stipulation."

1.2 Document name and Identification

This document is the **TRUST ITALIA SPA** Certification Practice Statement. Issued Certificates contain object identifier values corresponding to the applicable Level of Certificate. Therefore, **TRUST ITALIA SPA** has not assigned this CPS an object identifier value. Certificate Policy Object Identifiers are used in accordance with Section 7.1.6.

The following revisions have been made:

Date	Changes	Version
01/04/2020	This version 4.0 replaces the **TRUST ITALIA SPA** Certification Practices Statement, Version 3.9.2, dated December 23, 2019	4.0
19/10/2020	Renamed Class1-2 to Level1-2; Update referral to policies, guidelines and requirements as per SC31; Specified information about OCSP services Updated Certificate Extensions (7.1.2) Updated information about CRL minor editorial changes throughout the document for consistency and accuracy.	4.1

1.3 PKI Participants

1.3.1 Certification Authorities

DigiCert operates certification authorities (CAs) that issue digital certificates. The CA term encompasses a subcategory of issuers called Primary Certification Authorities (PCA).

[2] Although these documents are not publicly available their specifications are included in DigiCert's Annual WebTrust for Certification authorities audit and may be made available to customer under special Agreement

Each PCA is a DigiCert entity. Subordinate to the PCAs are **TRUST ITALIA SPA** Certification Authorities that issue Certificates to end-user Subscribers or other CAs.

TRUST ITALIA SPA enterprise customers may operate their own CAs as a subordinate CA to a **TRUST ITALIA SPA** CA. Such a customer enters into a contractual relationship with **TRUST ITALIA SPA** to abide by all the requirements of the DigiCert CP and the **TRUST ITALIA SPA** CPS. These subordinate CAs may, however implement a more restrictive practices based on their internal requirements.

1.3.2 Registration Authorities

A Registration Authority is an entity that performs identification and authentication of certificate applicants for end-user certificates, initiates or passes along revocation requests for certificates for end-user certificates, and approves applications for renewal or re-keying certificates on behalf of a Issuer CA. **TRUST ITALIA SPA** may act as an RA for certificates it issues. Validation of domains or Email Control for S/MIME Certificates cannot be delegated to a third party and is only validated by the RA of the Issuer CA.

Third parties, who enter into a contractual relationship with **TRUST ITALIA SPA**, may operate their own RA and authorize the issuance of certificates by a **TRUST ITALIA SPA** CA. Third party RAs must abide by all the requirements of the DigiCert CP, the **TRUST ITALIA SPA** CPS and the terms of their enterprise services agreement with **TRUST ITALIA SPA**. RAs may, however implement more restrictive practices based on
their internal requirements.[4]

1.3.3 Subscribers

Subscribers under this CPS include all end users (including entities) of certificates issued by an issuerCA. A subscriber is the entity named as the end-user Subscriber of a certificate. End-user Subscribers may be individuals, organizations or, infrastructure components such as firewalls, routers, trusted servers or other devices used to secure communications within an Organization.

In some cases certificates are issued directly to individuals or entities for their own use. However, there commonly exist other situations where the party requiring a certificate is different from the subject to whom the credential applies. For example, an organization may require certificates for its employees to allow them to represent the organization in electronic transactions/business. In such situations the entity subscribing for the issuance of certificates (i.e. paying for them, either through subscription to a specific service, or as the issuer itself) is different from the entity which is the subject of the certificate (generally, the holder of the credential). Two different terms are used in this CPS to distinguish between these two roles: "Subscriber", is the entity which contracts with TRUST ITALIA SPA for the issuance of credentials and; “Subject", is the person to whom the credential is bound. The Subscriber bears ultimate responsibility for the use of the credential but the Subject is the individual that is authenticated when the credential is presented.

When ‘Subject’ is used, it is to indicate a distinction from the Subscriber. When “Subscriber” is used it may mean just the Subscriber as a distinct entity but may also use the term to embrace the two. The context of its use in this CPS will invoke the correct understanding.

CAs are technically also subscribers of certificates within this CPS, either as a PCA issuing a self signed Certificate to itself, or as a CA issued a Certificate by a superior CA. References to “end entities” and “subscribers” in this CPS, however, apply only to end-user Subscribers.

[4] An example of a third party RA is a customer of Managed PKI services customer.

1.3.4 Relying Parties

A Relying Party is an individual or entity that acts in reliance of a certificate and/or a digital signature issued under this CPS. A Relying party may, or may not also be a Subscriber within this CPS.

1.3.5 Other Participants

No stipulation

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

1.4.1.1 Certificates Issued to Individuals

Individual Certificates are normally used by individuals to sign and encrypt e-mail and to authenticate to applications (client authentication). While the most common usages for individual certificates are included in Table 1 below, an individual certificate may be used for other purposes, provided that a Relying Party is able to reasonably rely on that certificate and the usage is not otherwise prohibited by law, the DigiCert CP, the CPS under which the certificate has been issued and any agreements with Subscribers.

Certificate .evel	Assurance Level			Usage		
	Low assurance level	Medium assurance level	High assurance Level	Signing	Encryption	Client Authentication
Level 1 Certificates	●			●	●	●
Level 2 Certificates		●		●	●	●

Table 1. Individual Certificate Usage

1.4.1.2 Assurance levels

Low assurance certificates are certificates that should not be used for authentication purposes or to support Non-repudiation. The digital signature provides modest assurances that the e-mail originated from a sender with a certain e-mail address. The Certificate, however, provides no proof of the identity of the Subscriber. The encryption application enables a Relying Party to use the Subscriber's Certificate to encrypt messages to the Subscriber, although the sending Relying Party cannot be sure that the recipient is in fact the person named in the Certificate.

Medium assurance certificates are certificates that are suitable for securing some inter- and intra-organizational, commercial, and personal e-mail requiring a medium level of assurances of the Subscriber identity, in relation to Level 1 and 2.

1.4.2 Prohibited Certificate Uses

Certificates shall be used only to the extent the use is consistent with applicable law, and in particular shall be used only to the extent permitted by applicable export or import laws.

DigiCert and **TRUST ITALIA SPA** Certificates are not designed, intended, or authorized for use or resale as control equipment in hazardous circumstances or for uses requiring fail-safe performance such as the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control systems, or weapons control systems, where failure could lead directly to death, personal injury, or severe environmental damage. Also, Level 1 Certificates shall not be used as proof of identity or as support of non repudiation of identity or authority. Client Certificates are intended for client applications and shall not be used as server or organizational Certificates.

CA Certificates may not be used for any functions except CA functions. In addition, end-user Subscriber Certificates shall not be used as CA Certificates.

DigiCert and **TRUST ITALIA SPA** periodically rekey Intermediate CAs. Third party applications or platforms that have an Intermediate CA embedded as a root certificate may not operate as

[5] "In limited circumstances Level 2 certificates may be issued by a Managed MPKI customer to an affiliated organization (and not an individual within the organization). Such certificate may be used for organization authentication and application signing only. Except as expressly authorized by Symantec through an Enterprise Service Agreement imposing authentication and practice requirements consistent with the security standards of this CPS, Subscribers are prohibited from using this certificate for code and content signing, SSL encryption and S/mime signing and such key usage will be disabled for these certificates."

designed after the Intermediate CA has been rekeyed. **TRUST ITALIA SPA** therefore does not warrant the use of Intermediate CAs as root certificates and recommends that Intermediate CAs not be embedded into applications and/or platforms as root certificates. **TRUST ITALIA SPA** recommends the use of PCA Roots as root certificates.

1.5 Policy Administration

1.5.1 Organization Administering the Document

TRUST ITALIA SPA
Via Po 22
00198 – Roma
Tel. +39 06 332287

1.5.2 Contact Person

Trust ItaliaCertificate Policy Manager

TRUST ITALIA SPA
Via Po 22
00198 – Roma
Tel. +39 06 332287
infosec@trustitalia.it

1.5.2.1 Revocation Reporting Contact Person

Trust Italia Technical Support

TRUST ITALIA SPA
Via Po 22
00198 – Roma
Tel. +39 06 332287
supporto@trustitalia.it

1.5.3 Person Determining CP Suitability for the Policy

The organization identified in Section 1.5.2 is responsible for determining whether this CPS and other documents in the nature of certification practice statements that supplement or are subordinate to this CPS are suitable under the CP and this CPS.

1.5.4 CPS Approval Procedure

Approval of this CPS and subsequent amendments shall be made by the PMA. Amendments shall either be in the form of a document containing an amended form of the CPS or an update notice. Amended versions or updates shall be linked to the Practices Updates and Notices section of the TRUST ITALIA SPA Repository located at: https://www.trustitalia.it. Updates supersede any designated or conflicting provisions of the referenced version of the CPS.

1.6 Definitions and Acronyms

1.6.1 Definitions

See Appendix A for a table of acronyms and definitions

1.6.2 Acronyms

See Appendix A for a table of acronyms and definitions

1.6.3 References

If not listed in section 1.1:

- CA/Browser Forum Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates ("Baseline Requirements")
- Mozilla Root Store Policy v.2.7

2. Publication and Repository Responsibilities

2.1 Repositories

TRUST ITALIA SPA is responsible for the repository functions for its own CAs and the CAs of its Enterprise Customers (Managed PKI customers). **TRUST ITALIA SPA** issuing Certificates to end-user Subscribers publish Certificates they issue in public repository

TRUST ITALIA SPA develops, implements, enforces, and annually updates this CPS to meet the compliance standards of the documents listed in Sections 1.1 and 1.6.3. As Baseline Requirements are updated, **TRUST ITALIA SPA** reviews the changes to determine their impact on these practices.

Upon revocation of an end-user Subscriber's Certificate, **TRUST ITALIA SPA** publishes notice of such revocation in the repository**. TRUST ITALIA SPA** issues CRLs for its own CAs and the CAs of Service Centers and Enterprise Customers within its Sub-domain, pursuant to the provisions of this CPS. In addition, Enterprise Customers who have contracted for Online Certificate Status Protocol ("OCSP") services, **TRUST ITALIA SPA** provides OCSP services pursuant to the provisions of this CPS.

2.2 Publication of Certificate Information

The **TRUST ITALIA SPA** certificate services and the repository are accessible through several means of communication:
1. On the web: https://www.trustitalia.it (and via URIs included in the certificates themselves)
2. By email to supporto@trustitalia.it
3. By mail addressed to: Trust Italia SpA, Via Po 22, 00198, Roma, Italy
4. By telephone Tel: +39 06 332287

TRUST ITALIA SPA maintains a web-based repository that permits Relying Parties to make online inquiries regarding revocation and other Certificate status information. **TRUST ITALIA SPA** provides Relying Parties with information on how to find the appropriate repository to check Certificate status and, if OCSP (Online Certificate Status Protocol) is available, how to find the right OCSP responder.

TRUST ITALIA SPA publishes the Certificates it issues on behalf of its own CAs, and the CAs of Client Service Centers in their Sub-domain. Upon revocation of an end-user Subscriber's Certificate, **TRUST ITALIA SPA** shall publish notice of such revocation in the repository. In addition, **TRUST ITALIA SPA** issues Certificate Revocation Lists (CRLs) and, if available, provide OCSP services (Online Certificate Status Protocol) for its own CAs and the CAs of Service Centers within its Sub-domain.

TRUST ITALIA SPA will at all times publish a current version of:
- The **TRUST ITALIA SPA** CPS,
- Subscriber Agreements, o
  Relying Party Agreements

TRUST ITALIA SPA is responsible for the repository function for **TRUST ITALIA SPA** CAs and Enterprise Customers' CAs that issue Certificates within **TRUST ITALIA SPA**'s Sub-domain.
TRUST ITALIA SPA publishes certain CA information in the repository section of **TRUST ITALIA SPA**'s web site at http://www.trustitalia.it as described below.

TRUST ITALIA SPA publishes this CPS, Subscriber Agreements, and Relying Party Agreements in the repository section of **TRUST ITALIA SPA**'s web site.
TRUST ITALIA SPA publishes Certificates in accordance with Table 3 below.

Certificate Type	*Publication Requirements*
DigiCert PCA and DigiCert Issuing Root CA Certificates	Available to Relying Parties through inclusion in current browser software and as part of a Certificate Chain that can be obtained with the end-user Subscriber Certificate through the

	query functions described below.
TRUST ITALIA SPA Issuing CA Certificates	Available to Relying Parties as part of a Certificate Chain that can be obtained with the end-user Subscriber Certificate through the query functions described below.
Certificate of the **TRUST ITALIA SPA** CA supporting Managed PKI Lite Certificates and CA Certificates of Managed PKI Customers	Available through query of the **TRUST ITALIA SPA** LDAP directory server at *directory.trustitalia.it*.
TRUST ITALIA SPA OCSP Responder Certificates	Available through query of the TRUST ITALIA SPA OCSP responder at onsite-ocsp.trustitalia.it
End-User Subscriber Certificates depending on usage.	Optionally published and available to relying parties through query functions in the **TRUST ITALIA SPA** repository at: https://onsite.trustitalia.it and query of the TRUST ITALIA SPA LDAP directory server at *directory.trustitalia.it*

Certificate Type	***Publication Requirements***
End-User Subscriber Certificates issued through Managed PKI Customers	Made available through the query functions listed above, although at the discretion of the Managed PKI Customer, the Certificate may be accessible only via a search using the Certificate's common name or email address.

Table 3 – Certificate Publication Requirements

2.3 Time or Frequency of Publication

Updates to this CPS are published in accordance Section 9.12. Updates to Subscriber Agreements and Relying Party Agreements are published as necessary. Certificates are published upon issuance. Certificate status information is published in accordance with the provisions of this CPS.

New or modified versions of CPS, Subscriber Agreements, or Relying Party Warranties are typically published within seven days after their approval.

Trust Italia develops, implements, enforces, and annually updates this CPS to describe in detail how Trust Italia complies with the CA/Browser Baseline Requirements and other documents as listed in section 1.1 and 1.6.3 of this CPS. Those updates indicate conformance by incrementing the version number and adding a dated changelog entry even if no other changes are made to the document as specified in section 1.2 of this CPS.

2.4 Access Controls on Repositories

Information published in the repository portion of the **TRUST ITALIA SPA** web site is publicly-accessible information. Read only access to such information is unrestricted. **TRUST ITALIA SPA** requires persons to agree to a Relying Party Agreement or CRL Usage Agreement as a condition to accessing Certificates, Certificate status information, or CRLs. **TRUST ITALIA SPA** has implemented logical and physical security measures to prevent unauthorized persons from adding, deleting, or modifying repository entries.

3. Identification and Authentication

3.1 Naming

Unless where indicated otherwise in the DigiCert CP, this CPS or the content of the digital certificate, names appearing in Certificates issued under sub-domain are authenticated.

3.1.1 Type of Names

While the STN is currently owned by DigiCert, legacy certificates have been issued in the name of the former owner. Any legacy certificate that indicates the Organization (O) as "VeriSign, Inc." or "Symantec Corporation" and Organizational Unit (OU) as "VeriSign Trust Network" shall mean DigiCert Inc. and the Symantec Trust Network, respectively.

TRUST ITALIA SPA CA Certificates contain X.501 Distinguished Names in the Issuer and Subject fields.
TRUST ITALIA SPA CA Distinguished Names consist of the components specified in Table 4 below.

Attribute	***Value***
Country (C) =	2-letter ISO country code or not used.
Organization (O) =	"DigiCert Inc." "Symantec Corporation" or "Trust Italia S.p.A."[6] or <organization name>
Organizational Unit (OU) =	**TRUST ITALIA SPA** CA Certificates may contain multiple OU attributes. Such attributes may contain one or more of the following: • CA Name • Symantec Trust Network • VeriSign Trust Network • A statement referencing the applicable Relying Party Agreement governing terms of use of the Certificate • A copyright notice • Text to describe the type of Certificate.
State or Province (S) =	Not used.
Locality (L) =	Not used

6 For a CA dedicated to a customer organization, the (o=) component shall be the legal name of the organization.

Attribute	*Value*
Common Name (CN) =	This attribute includes the CA Name (if the CA Name is not specified in an OU attribute) or is not used.

Table 4 – Distinguished Name Attributes in CA Certificates

End-user Subscriber Certificates contain an X.501 distinguished name in the Subject name field and consist of the components specified in Table 5 below.

Attribute	*Value*
Country (C) =	2-letter ISO country code or not used
Organization (O) = "Trust Italia S.p.A.	The Organization attribute is used as follows: • " for **TRUST ITALIA SPA** OCSP Responder and optionally for individual Certificates that do not have an organization affiliation. • Subscriber organizational name for web server Certificates and individual Certificates that have an organization affiliation.
Organizational Unit (OU) =	**TRUST ITALIA SPA** end-user Subscriber Certificates may contain multiple OU attributes. Such attributes may contain one or more of the following: • Subscriber organizational unit (for individual Certificates that have organization affiliation) • Symantec Trust Network • VeriSign Trust Network • A statement referencing the applicable Relying Party Agreement governing terms of use of the Certificate • A copyright notice • "Authenticated by Trust Italia S.p.A." • "Persona Not Validated" for Level 1 Individual Certificates • Text to describe the type of Certificate.
State or Province (S) =	Indicates the Subscriber's State or Province (State is not a required field in certificates issued to individuals).
Locality (L) =	Indicates the Subscriber's Locality (Locality is not a required field in certificates issued to individuals).
Common Name (CN) =	This attribute includes: • The OCSP Responder Name (for OCSP Responder Certificates) • "Persona Not Validated" for Level 1 individual Certificates • Person's name (for individual Certificates or code-signing certificates issued to individuals).
E-Mail Address (E) =	E-mail address for Level 1 and Level 2 individual Certificates and generally for Subscriber Certificates

Table 5 – Distinguished Name Attributes in End User Subscriber Certificates

The Common Name (CN=) component of the Subject distinguished name of end-user Subscriber Certificates is authenticated in the case of Level 2 Certificates.

- The authenticated Common Name value included in the Subject distinguished names of organizational Certificates is a domain name or the legal name of the organization or unit within the organization.

- The Common Name value included in the Subject distinguished name of individual Certificates represents the individual's generally accepted personal name.

3.1.2 Need for Names to be Meaningful

Level 2 end-user Subscriber Certificates contain names with commonly understood semantics permitting the determination of the identity of the individual or organization that is the Subject of the Certificate.

TRUST ITALIA SPA CA certificates contain names with commonly understood semantics permitting the determination of the identity of the CA that is the Subject of the Certificate.

3.1.3 Anonymity or Pseudonymity of Subscribers

The identity of Level 1 individual Subscribers is not authenticated. Level 1 subscribers may use pseudonyms. Unless when required by law or requested by a State or Government authority to protect the identity of certain end user subscribers (e.g., minors, or sensitive government employee information), Level 2 Subscribers are not permitted to use pseudonyms (names other than a Subscriber's true personal or organizational name). Each request for anonymity in a certificate will be evaluated on its merits by the PMA and, if allowed the certificate will indicate that identity has been authenticated but is protected.

3.1.4 Rules for Interpreting Various Name Forms

Distinguished Names in Certificates are interpreted using X.500 standards and ASN.1 syntax.

3.1.5 Uniqueness of Names

TRUST ITALIA SPA ensures that Subject Distinguished Names of Subscriber are unique within the domain of a specific CA through automated components of the Subscriber enrollment process. It is possible for a Subscriber to have two or more certificates with the same Subject Distinguished Name.

3.1.6 Recognition, Authentication, and Role of Trademarks

Certificate Applicants are prohibited from using names in their Certificate Applications that infringe upon the Intellectual Property Rights of others. **TRUST ITALIA SPA**, however, does not verify whether a Certificate Applicant has Intellectual Property Rights in the name appearing in a Certificate Application or arbitrate, mediate, or otherwise resolve any dispute concerning the ownership of any domain name, trade name, trademark, or service mark. **TRUST ITALIA SPA** is entitled, without liability to any Certificate Applicant, to reject or suspend any Certificate Application because of such dispute.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

The certificate applicant must demonstrate that it rightfully holds the private key corresponding to the public key to be listed in the Certificate. The method to prove possession of a private key shall be PKCS #10, another cryptographically equivalent demonstration, or another **TRUST ITALIA SPA** -

approved and DigiCert-approved method. This requirement does not apply where a key pair is generated by a CA on behalf of a Subscriber, for example where generated keys are saved encrypted at the CA's systems for recovery purpose.

3.2.2 Authentication of Organization identity and Email Control

Whenever a certificate contains an organization name, the identity of the organization and other enrollment information provided by Certificate Applicants (except for Non-verified Subscriber Information) is confirmed in accordance with the procedures set forth in **TRUST ITALIA SPA**'s documented Validation Procedures.

At a minimum **TRUST ITALIA SPA** shall:

- determine that the organization exists by using at least one third party identity proofing service or database, or alternatively, organizational documentation issued by or filed with the applicable government agency or competent authority that confirms the existence of the organization,
- confirm by telephone, confirmatory postal mail, or comparable procedure to the Certificate Applicant certain information about the organization, that the organization has authorized the Certificate Application, and that the person submitting the Certificate Application on behalf of the Certificate Applicant is authorized to do so.

  When a certificate includes the name of an individual as an authorized representative of the Organization, the employment of that individual and his/her authority to act on behalf of the Organization shall also be confirmed.

Where a domain name or e-mail address is included in the certificate **TRUST ITALIA SPA** authenticates the Organization's right to use that domain name either as a fully qualified Domain name or an e-mail domain, as per Table 6 below.

Additional checks necessary to satisfy United States export regulations and licenses issued by the United States Department of Commerce Bureau of Industry and Science ("BIS") are performed by **TRUST ITALIA SPA** when required.

Additional procedures are performed for specific types of Certificates as described in Table 6 below.

Certificate Type	***Additional Procedures***
S/MIME Certificates issued as Level 1-2 certificates	Trust Italia verifies an individual's or organization's right to use or control an email address to be contained in a certificate, completing the following authentication: 1. Manual Authentication: The Applicant submits enrollment information and a Public Key/CSR. An RA reviews the enrollment information received from the Applicant in a customized interface. If approved, the system automatically sends a PIN to the enrolled email address for the Applicant to use to retrieve the Certificate at a specified URL. If the Applicant's Private Key matches, the Certificate is installed.

Table 6. Specific Authentication Procedures

3.2.3 Authentication of Individual Identity

Authentication of individual identity differs according to the Level of Certificate. The minimum authentication standard for each Level of certificates is explained in Table 7 below.

Certificate Level	Authentication of Identity
Level 1	No identity authentication. There is a limited confirmation of the Subscriber's e-mail address by requiring the Subscriber to be able to answer an e-mail to that address.
Level 2	Authenticate identity by matching the identity provided by the Subscriber to: o information residing in the database of a TRUST ITALIA SPA -approved identity proofing service, such as a major credit bureau or other reliable source of information providing, or o information contained in the business records or databases of business information (employee or customer directories) of an RA approving certificates to its own affiliated individuals

Table 7. Authentication of individual identity

3.2.4 Non-Verified Subscriber information

Non-verified subscriber information includes:

- Organization Unit (OU)
- Subscriber's name in Level 1 certificates
- Any other information designated as non-verified in the certificate.

3.2.5 Validation of Authority

Whenever an individual's name is associated with an Organization name in a certificate in such a way to indicate the individual's affiliation or authorization to act on behalf of the Organization **TRUST ITALIA SPA** or a RA:

- determines that the organization exists by using at least one third party identity proofing service or database, or alternatively, organizational documentation issued by or filed with the applicable government that confirms the existence of the organization, and
- Uses information contained in the business records or databases of business information (employee or customer directories) of an RA approving certificates to its own affiliated individuals or confirms by telephone, confirmatory postal mail, or comparable procedure to the organization, the employment with the Organization of the individual submitting the Certificate Application and, when appropriate, his/her authority to act on behalf of the Organization.

3.2.6 Criteria for Interoperation

TRUST ITALIA SPA may provide interoperation services that allow a non-Sub-domain CA to be able to interoperate with the Sub-domain by unilaterally certifying that CA. CAs enabled to interoperate in this way will comply with the DigiCert CP as supplemented by additional policies when required.

TRUST ITALIA SPA shall only allow interoperation with the Sub-domain of a non-Sub-domain CA in circumstances where the CA, at a minimum:

- Enters into a contractual agreement with **TRUST ITALIA SPA**
- Operates under a CPS that meets this CPS requirements for the Levels of certificates it will issue oPasses a compliance assessment before being allowed to interoperate
- Passes an annual compliance assessment for ongoing eligibility to interoperate.

7 **TRUST ITALIA SPA** may approve Administrator Certificates to be associated with a non-human recipient such as a device, or a server. Authentication of a Level 3 Administrator Certificate Applications for a non-human recipient shall include:
• Authentication of the existence and identity of the service named as the Administrator in the Certificate Application
• Authentication that the service has been securely implemented in a manner consistent

3.3 Identification and Authentication for Re-key Requests

Prior to the expiration of an existing Subscriber's Certificate, it is necessary for the Subscriber to obtain a new certificate to maintain continuity of Certificate usage. **TRUST ITALIA SPA** generally requires that the Subscriber generate a new key pair to replace the expiring key pair (technically defined as "rekey") However, in certain cases Subscribers may request a new certificate for an existing key pair (technically defined as "renewal").

Generally speaking, both "Rekey" and "Renewal" are commonly described as "Certificate Renewal", focusing on the fact that the old Certificate is being replaced with a new Certificate and not emphasizing whether or not a new key pair is generated. For all Level and Types of **TRUST ITALIA SPA** Certificates, this distinction is not important as a new key pair is always generated as part of **TRUST ITALIA SPA**'s end-user Subscriber Certificate replacement process.

3.3.1 Identification and Authentication for Routine Re-key

Re-key procedures ensure that the person or organization seeking to rekey an end-user Subscriber Certificate is in fact the Subscriber of the Certificate.

One acceptable procedure is through the use of a Challenge Phrase (or the equivalent thereof), or proof of possession of the private key. Subscribers choose and submit with their enrollment information a Challenge Phrase. Upon renewal of a Certificate, if a Subscriber correctly submits the Subscriber's Challenge Phrase (or the equivalent thereof) with the Subscriber's reenrollment information, and the enrollment information (including Corporate and Technical contact information) has not changed, a renewal Certificate is automatically issued. As an alternative to using a challenge phrase (or equivalent) **TRUST ITALIA SPA** may send an e-mail message to the e-mail address associated with the verified corporate contact for the certificate being renewed, requesting confirmation of the Certificate renewal order and authorization to issue the Certificate. Upon receipt of confirmation authorizing issuance of the Certificate, **TRUST ITALIA SPA** will issue the Certificate if the enrollment information (including Corporate and
Technical contact information[9]) has not changed.

After rekeying or renewal in this fashion, and on at least alternative instances of subsequent rekeying or renewal thereafter, **TRUST ITALIA SPA** or the RA reconfirms the identity of the Subscriber in accordance with the identification and authentication requirements of an original Certificate Application.

TRUST ITALIA SPA will not have to reconfirm by telephone, confirmatory postal mail, or comparable procedure to the Certificate Applicant certain information about the organization, that the organization has authorized the Certificate Application, and that the person submitting the Certificate Application on behalf of the Certificate Applicant is authorized to do so.

Rekey after 30-days from expiration of the Certificate are re-authenticated as an original Certificate Application and are not automatically issued.

3.3.2 Identification and Authentication for Re-key After Revocation

Re-key/renewal after revocation is not permitted.

• with it performing an Administrative function

• Confirmation of the identity and authorization of the person enrolling for the Administrator certificate for the service named as Administrator in the Certificate Application.

9 If contact information has changed via an approved formal contact change procedure the certificate shall still qualify for automated renewal.

10

3.4 Identification and Authentication for Revocation Request

Prior to the revocation of a Certificate, **TRUST ITALIA SPA** verifies that the revocation has been requested by the Certificate's Subscriber, the entity that approved the Certificate Application.

Acceptable procedures for authenticating the revocation requests of a Subscriber include:

- Having the Subscriber for certain certificate types submit the Subscriber's Challenge Phrase (or the equivalent thereof), and revoking the Certificate automatically if it matches the Challenge Phrase (or the equivalent thereof) on record. (Note that this option may not be available to all customers.)
- Receiving a message from the Subscriber that requests revocation and contains a digital signature verifiable with reference to the Certificate to be revoked,
- Communication with the Subscriber providing reasonable assurances in light of the Level of Certificate that the person or organization requesting revocation is, in fact the Subscriber. Such communication, depending on the circumstances, may include one or more of the following: telephone, facsimile, e-mail, postal mail, or courier service.

TRUST ITALIA SPA Administrators are entitled to request the revocation of end-user Subscriber Certificates within **TRUST ITALIA SPA**'s Sub domain. **TRUST ITALIA SPA** authenticates the identity of Administrators via access control using SSL and client authentication before permitting them to perform revocation functions, or another Sub-domain-approved procedure.

RAs using an Automated Administration Software Module may submit bulk revocation requests to **TRUST ITALIA SPA**. Such requests shall be authenticated via a digitally signed request signed with the private key in the RA's Automated Administration hardware token.

The requests to revoke a CA Certificate shall be authenticated by the **TRUST ITALIA SPA** to ensure that the revocation has in fact been requested by the CA.

4. Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

Below is a list of people who may submit certificate applications:

- Any individual who is the subject of the certificate,
- Any authorized representative of an Organization or entity,
- Any authorized representative of a CA,
- Any authorized representative of an RA.

4.1.2 Enrollment Process and Responsibilities

4.1.2.1 End-User Certificate Subscribers

All end-user Certificate Subscribers shall manifest assent to the relevant Subscriber Agreement that contains representations and warranties described in Section 9.6.3 and undergo an enrollment process consisting of:

- completing a Certificate Application and providing true and correct information,
- generating, or arranging to have generated, a key pair,
- delivering his, her, or its public key, directly or through an RA, to **TRUST ITALIA SPA**
- demonstrating possession and/or exclusive control of the private key corresponding to the public key delivered to **TRUST ITALIA SPA.**

4.1.2.2 CA and RA Certificates

Subscribers of CA and RA Certificates enter into a contract with **TRUST ITALIA SPA.** CA and RA Applicants shall provide their credentials to demonstrate their identity and provide contact information during the contracting process. During this contracting process or, at the latest, prior to the Key Generation Ceremony to create a CA or RA key pair, the applicant shall cooperate with **TRUST ITALIA SPA** to determine the appropriate distinguished name and the content of the Certificates to be issued by the applicant.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

TRUST ITALIA SPA or an RA shall perform identification and authentication of all required Subscriber information in terms of Section 3.2

4.2.2 Approval or Rejection of Certificate Applications

TRUST ITALIA SPA or an RA will approve an application for a certificate if the following criteria are met:

- Successful identification and authentication of all required Subscriber information in terms of Section 3.2
- Payment has been received

TRUST ITALIA SPA or an RA will reject a certificate application if:

- identification and authentication of all required Subscriber information in terms of Section 3.2 cannot be completed, or
- The Subscriber fails to furnish supporting documentation upon request, or
- The Subscriber fails to respond to notices within a specified time, or
- Payment has not been received, or
- The RA believes that issuing a certificate to the Subscriber may bring the Sub-domain into disrepute.

4.2.3 Time to Process Certificate Applications

TRUST ITALIA SPA begins processing certificate applications within a reasonable time of receipt. There is no time stipulation to complete the processing of an application unless otherwise indicated in the relevant Subscriber Agreement, CPS or other Agreement between Sub-domain participants. A certificate application remains active until rejected.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

A Certificate is created and issued following the approval of a Certificate Application by **TRUST ITALIA SPA** or following receipt of an RA's request to issue the Certificate. **TRUST ITALIA SPA** creates and issues to a Certificate Applicant a Certificate based on the information in a Certificate Application following approval of such Certificate Application.

4.3.2 Notifications to Subscriber by the CA of Issuance of Certificate

TRUST ITALIA SPA shall, either directly or through an RA, notify Subscribers that they have created such Certificates, and provide Subscribers with access to the Certificates by notifying them that their Certificates are available. Certificates shall be made available to end-user Subscribers, either by allowing them to download them from a web site or via a message sent to the Subscriber containing the Certificate.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

The following conduct constitutes certificate acceptance:

- Downloading a Certificate or installing a Certificate from a message attaching it constitutes the Subscriber's acceptance of the Certificate.
- Failure of the Subscriber to object to the certificate or its content constitutes certificate acceptance.

4.4.2 Publication of the Certificate by the CA

TRUST ITALIA SPA publishes the Certificates it issues by delivering them to the Subscriber.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

RAs may receive notification of the issuance of certificates they approve.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

Use of the private key corresponding to the public key in the certificate shall only be permitted once the Subscriber has agreed to the Subscriber agreement and accepted the certificate. The certificate shall be used lawfully in accordance with **TRUST ITALIA SPA**'s Subscriber Agreement the terms of the DigiCert CP and this CPS. Certificate use must be consistent with the KeyUsage field extensions included in the certificate (e.g., if Digital Signature is not enabled then the certificate must not be used for signing).

Subscribers shall protect their private keys from unauthorized use and shall discontinue use of the private key following expiration or revocation of the certificate. Parties other than the Subscriber shall not archive the Subscriber Private Key except as set forth in section 4.12.

4.5.2 Relying Party Public Key and Certificate Usage

Relying parties shall assent to the terms of the applicable relying party agreement as a condition of relying on the certificate.

Reliance on a certificate must be reasonable under the circumstances. If the circumstances indicate a need for additional assurances, the Relying Party must obtain such assurances for such reliance to be deemed reasonable.

Before any act of reliance, Relying Parties shall independently assess:

- the appropriateness of the use of a Certificate for any given purpose and determine that the Certificate will, in fact, be used for an appropriate purpose that is not prohibited or otherwise restricted by this CPS. **TRUST ITALIA SPA** is not responsible for assessing the appropriateness of the use of a Certificate.
- That the certificate is being used in accordance with the KeyUsage field extensions included in the certificate (e.g., if Digital Signature is not enabled then the certificate may not be relied upon for validating a Subscriber's signature).
- The status of the certificate and all the CAs in the chain that issued the certificate. If any of the Certificates in the Certificate Chain have been revoked, the Relying Party is solely responsible to investigate whether reliance on a digital signature performed by an end-user Subscriber Certificate prior to revocation of a Certificate in the Certificate chain is reasonable. Any such reliance is made solely at the risk of the Relying party.

Assuming that the use of the Certificate is appropriate, Relying Parties shall utilize the appropriate software and/or hardware to perform digital signature verification or other cryptographic operations they wish to perform, as a condition of relying on Certificates in connection with each such operation. Such operations include identifying a Certificate Chain and verifying the digital signatures on all Certificates in the Certificate Chain.

4.6 Certificate Renewal

Certificate renewal is the issuance of a new certificate to the subscriber without changing the public key or any other information in the certificate.

4.6.1 Circumstances for Certificate Renewal

Prior to the expiration of an existing Subscriber's Certificate, it is necessary for the Subscriber to renew a new certificate to maintain continuity of Certificate usage. A certificate may also be renewed after expiration.

4.6.2 Who May Request Renewal

Only the subscriber for an individual certificate or an authorized representative for an Organizational certificate may request certificate renewal.

4.6.3 Processing Certificate Renewal Requests

Renewal procedures ensure that the person or organization seeking to renew an end-user Subscriber Certificate is in fact the Subscriber (or authorized by the Subscriber) of the Certificate.

One acceptable procedure is through the use of a Challenge Phrase (or the equivalent thereof), or proof of possession of the private key. Subscribers choose and submit with their enrollment information a Challenge Phrase (or the equivalent thereof). Upon renewal of a Certificate, if a Subscriber correctly submits the Subscriber's Challenge Phrase (or the equivalent thereof) with the Subscriber's reenrollment information, and the enrollment information (including Corporate and Technical contact information[11]) has not changed, a renewal Certificate is automatically issued. As an alternative to using a challenge phrase (or equivalent) **TRUST ITALIA SPA** may send an e-mail message to the e-mail address associated with the verified corporate contact for the certificate being renewed, requesting confirmation of the Certificate renewal order and authorization to issue the Certificate. Upon receipt of confirmation authorizing issuance of the Certificate, **TRUST ITALIA SPA** will issue the Certificate if the enrollment information (including corporate and technical contact information[12]) has not changed.

After renewal in this fashion, and on at least alternative instances of subsequent renewal thereafter, **TRUST ITALIA SPA** or an RA shall reconfirm the identity of the Subscriber in accordance with the requirements specified in this CPS for the authentication of an original Certificate Application.

TRUST ITALIA SPA will not have to reconfirm by telephone, confirmatory postal mail, or comparable procedure to the Certificate Applicant certain information about the organization, that the

11 If contact information has changed via an approved formal contact change procedure the certificate shall still qualify for automated renewal.

12 If contact information has changed via an approved formal contact change procedure the certificate shall still qualify for automated renewal.

organization has authorized the Certificate Application, and that the person submitting the Certificate Application on behalf of the Certificate Applicant is authorized to do so.

Other than this procedure or another **TRUST ITALIA SPA** -approved procedure, the requirements for the authentication of an original Certificate Application shall be used for renewing an end-user Subscriber Certificate.

4.6.4 Notification of New Certificate Issuance to Subscriber

Notification of issuance of certificate renewal to the Subscriber is in accordance with Section 4.3.2

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Conduct constituting Acceptance of a renewed certificate is in accordance with Section 4.4.1

4.6.6 Publication of the Renewal Certificate by the CA

The renewed certificate is published in TRUST ITALIA SPA's publicly accessible repository.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

RAs may receive notification of the issuance of certificates they approve.

4.7 Certificate Re-Key

Certificate rekey is the application for the issuance of a new certificate that certifies the new public key. Certificate rekey is supported for all certificate Levels.

4.7.1 Circumstances for Certificate Re-Key

Prior to the expiration of an existing Subscriber's Certificate, it is necessary for the Subscriber to re-key the certificate to maintain continuity of Certificate usage. A certificate may also be re-keyed after expiration.

4.7.2 Who May Request Certification of a New Public Key

Only the subscriber for an individual certificate or an authorized representative for an Organizational certificate may request certificate renewal

4.7.3 Processing Certificate Re-Keying Requests

Re-key procedures ensure that the person or organization seeking to renew an end-user Subscriber Certificate is in fact the Subscriber (or authorized by the Subscriber) of the Certificate.

One acceptable procedure is through the use of a Challenge Phrase (or the equivalent thereof), or proof of possession of the private key. Subscribers choose and submit with their enrollment information a Challenge Phrase (or the equivalent thereof). Upon renewal of a Certificate, if a Subscriber correctly submits the Subscriber's Challenge Phrase (or the equivalent thereof) with the Subscriber's reenrollment information, and the enrollment information (including contact information[13]) has not changed, a renewal Certificate is automatically issued. Subject to the provisions of Section 3.3.1, after re-keying in this fashion, and on at least alternative instances of

13 If contact information has changed via an approved formal contact change procedure the certificate shall still qualify for automated renewal.

subsequent re-keying thereafter, TRUST ITALIA SPA or an RA shall reconfirm the identity of the Subscriber in accordance with the requirements specified in this CPS for the authentication of an original Certificate Application.

Other than this procedure or another DigiCert-approved procedure, the requirements for the authentication of an original Certificate Application shall be used for re-keying an end-user Subscriber Certificate.

4.7.4 Notification of New Certificate Issuance to Subscriber

Notification of issuance of a re-keyed certificate to the Subscriber is in accordance with Section 4.3.2.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

Conduct constituting Acceptance of a re-keyed certificate is in accordance with Section 4.4.1.

4.7.6 Publication of the Re-Keyed Certificate by the CA

The re-keyed certificate is published in TRUST ITALIA SPA's publicly accessible repository.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

RAs may receive notification of the issuance of certificates they approve.

4.8 Certificate Modification

4.8.1 Circumstances for Certificate Modification

Certificate modification refers to the application for the issuance of a new certificate due to changes in the information in an existing certificate (other than the subscriber's public key).

Certificate modification is considered a Certificate Application in terms of Section 4.1.

4.8.2 Who May Request Certificate Modification

See Section 4.1.1

4.8.3 Processing Certificate Modification Requests

TRUST ITALIA SPA or an RA shall perform identification and authentication of all required Subscriber information in terms of Section 3.2.

4.8.4 Notification of New Certificate Issuance to Subscriber

See Section 4.3.2.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

See Section 4.4.1.

4.8.6 Publication of the Modified Certificate by the CA

See Section 4.4.2.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

See Section 4.4.3.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

Only in the circumstances listed below, will an end-user Subscriber certificate be revoked by **TRUST ITALIA SPA** (or by the Subscriber) and published on a CRL. Upon request from a subscriber who can no longer use (or no longer wishes to use) a certificate for a reason other than one mentioned below, **TRUST ITALIA SPA** will flag the certificate as inactive in its database but will not publish the certificate on a CRL.

An end-user Subscriber Certificate is revoked if:

- **TRUST ITALIA SPA**, a Customer, or a Subscriber confirming that the Certificate no longer complies with the requirements of Sections 6.1.5 and 6.1.6 of the CA/B forum baseline requirements or any section of the Mozilla Root Store policy;
- **TRUST ITALIA SPA** obtains evidence that the Certificate was misused and/or used outside the intended purpose as indicated by the relevant agreement;
- **TRUST ITALIA SPA** confirms a material change in the information contained in the Certificate;
- **TRUST ITALIA SPA** confirms that the Certificate was not issued in accordance with the CA/B forum requirements or relevant browser policy;
- **TRUST ITALIA SPA** determines or confirms that any of the information appearing in the Certificate is inaccurate;
- **TRUST ITALIA SPA** received a lawful and binding order from a government or regulatory body to revoke the Certificate;
- The technical content or format of the Certificate presents an unacceptable risk to application software vendors, Relying Parties, or others;
- The Subscriber was added as a denied party or prohibited person to a blacklist or is operating from a destination prohibited under the laws of the United States;
- the binding between the subject and the subject's Public Key in the certificate is no longer valid or if an associated Private Key is compromised;
- **TRUST ITALIA SPA** obtains evidence that use of the email address in the certificate is no longer legally permitted; **TRUST ITALIA SPA** or a Customer has reason to believe that the Subscriber has materially breached a material obligation, representation, or warranty under the applicable Subscriber Agreement,
- The Subscriber Agreement with the Subscriber has been terminated,
- The affiliation between an Enterprise Customer with a Subscriber is terminated or has otherwise ended,
- In the case of Level 3 organizational Certificates, the Subscriber's organization name changes,
- The Subscriber has not submitted payment when due, or
- The continued use of that certificate is harmful to the Sub-domain.

TRUST ITALIA SPA will request to revoke a Subordinate CA Certificate within seven days to DigiCert after confirming one or more of the following occurred:

- The Subordinate CA requests revocation in writing;
- The Subordinate CA notifies **TRUST ITALIA SPA** that the original Certificate request was not authorized and does not retroactively grant authorization;
- **TRUST ITALIA SPA** obtains evidence that the Subordinate CA's Private Key corresponding to the Public Key in

the Certificate suffered a key compromise or no longer complies with the requirements of Sections 6.1.5 and 6.1.6 of the CA/B forum baseline requirements or any section of the Mozilla Root Store policy;

- **TRUST ITALIA SPA** obtains evidence that the CA Certificate was misused and/or used outside the intended purpose as indicated by the relevant agreement;
- **TRUST ITALIA SPA** confirms that the CA Certificate was not issued in accordance with or that Subordinate CA has not complied with this document or the applicable Certificate Policy or Certification Practice Statement;
- **TRUST ITALIA SPA** determines that any of the information appearing in the CA Certificate is inaccurate or misleading;
- **TRUST ITALIA SPA** or the Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the CA Certificate;
- **TRUST ITALIA SPA**'s or the Subordinate CA's right to issue Certificates under the Baseline Requirements expires or is revoked or terminated, unless **TRUST ITALIA SPA** has made arrangements to continue maintaining the CRL/OCSP Repository;
- Revocation is required by **TRUST ITALIA SPA**'s Certificate Policy and/or Certification Practice Statement; or
- The technical content or format of the CA Certificate presents an unacceptable risk to application software suppliers or Relying Parties.

When considering whether certificate usage is harmful to the Sub-domain, **TRUST ITALIA SPA** considers, among other things, the following:

- The nature and number of complaints received
- The identity of the complainant(s)
- Relevant legislation in force
- Responses to the alleged harmful use from the Subscriber

TRUST ITALIA SPA may also revoke an Administrator Certificate if the Administrator's authority to act as Administrator has been terminated or otherwise has ended.

TRUST ITALIA SPA Subscriber Agreements require end-user Subscribers to immediately notify TRUST ITALIA SPA of a known or suspected compromise of its private key.

4.9.2 Who Can Request Revocation

Individual Subscribers can request the revocation of their own individual Certificates through an authorized representative of **TRUST ITALIA SPA** or an RA. In the case of organizational Certificates, a duly authorized representative of the organization shall be entitled to request the revocation of Certificates issued to the organization. A duly authorized representative of **TRUST ITALIA SPA** or a RA shall be entitled to request the revocation of an RA Administrator's Certificate. The entity that approved a Subscriber's Certificate Application shall also be entitled to revoke or request the revocation of the Subscriber's Certificate.

Only **TRUST ITALIA SPA** is entitled to request or initiate the revocation of the Certificates issued to its own CAs. RAs are entitled, through their duly authorized representatives, to request the revocation of their own Certificates, and their Superior Entities shall be entitled to request or initiate the revocation of their Certificates.

4.9.3 Procedure for Revocation Request

4.9.3.1 Procedure for Requesting the Revocation of an End-User Subscriber Certificate

An end-user Subscriber requesting revocation is required to communicate the request to the **TRUST ITALIA SPA** or the Customer approving the Subscriber's Certificate Application, who in turn will initiate revocation of the certificate promptly. For Enterprise customers, the Subscriber is required to communicate the request to the Enterprise Administrator who will communicate the revocation request

to **TRUST ITALIA SPA** for automated processing. Communication of such revocation request shall be in accordance with CPS § 3.4. Non-Enterprise customers shall communicate a revocation request in accordance with CPS
§ 3.4.

Where an Enterprise Customer initiates revocation of an end-user Subscriber Certificate upon its own initiative, the Managed PKI Customer or ASB Customer instructs **TRUST ITALIA SPA** to revoke the Certificate.

4.9.3.2 Procedure for Requesting the Revocation of a CA or RA Certificate

A CA or RA requesting revocation of its CA or RA Certificate is required to communicate the request to **TRUST ITALIA SPA**. **TRUST ITALIA SPA** will then revoke the Certificate. **TRUST ITALIA SPA** may also initiate CA or RA Certificate revocation.

If **TRUST ITALIA SPA** determines that revocation is appropriate, **TRUST ITALIA SPA** personnel revoke the Certificate and update the CRL.

4.9.4 Revocation Request Grace Period

Revocation requests shall be submitted as promptly as possible within a commercially reasonable time.

4.9.5 Time within Which CA Must Process the Revocation Request

TRUST ITALIA SPA takes commercially reasonable steps to process revocation requests without delay.

4.9.6 Revocation Checking Requirements for Relying Parties

Relying Parties shall check the status of Certificates on which they wish to rely. One method by which Relying Parties may check Certificate status is by consulting the most recent CRL from the CA that issued the Certificate on which the Relying Party wishes to rely. Alternatively, Relying Parties may meet this requirement either by checking Certificate status using the applicable web-based repository or by using OCSP (if available). CAs shall provide Relying Parties with information on how to find the appropriate CRL, web-based repository, or OCSP responder (where available) to check for revocation status.

4.9.7 CRL Issuance Frequency

TRUST ITALIA SPA publish CRLs for end-user Subscriber Certificates at least every seven days.
DigiCert will issue CRLs for **TRUST ITALIA SPA** intermediate CAs following DigiCert's CPS requirements.

If a Certificate listed in a CRL expires, it may be removed from later-issued CRLs after the Certificate's expiration.

4.9.8 Maximum Latency for CRLs

CRLs are posted to the repository within a commercially reasonable time after generation. This is generally done automatically within minutes of generation.

4.9.9 On-Line Revocation/Status Checking Availability

Online revocation and other Certificate status information are available via a web-based repository and, where offered, OCSP. In addition to publishing CRLs, **TRUST ITALIA SPA** provides Certificate status information through query functions in the **TRUST ITALIA SPA** repository.

Certificate status information is available through web-based query functions accessible through the **TRUST ITALIA SPA** Repository at

- http://onsitecrl.trustitalia.it/TrustItaliaSpAConsumerServiceCenterClass1G2/LatestCRL.crl (for Level 1 Individual Certificates) and
- http://onsitecrl.trustitalia.it/TrustItaliaSpAConsumerServiceCenterClass2G2/LatestCRL.crl (for Level 2 Individual Certificates)

TRUST ITALIA SPA also provides OCSP Certificate status information. Enterprise Customers who contract for OCSP services may check Certificate status through the use of OCSP. The URL for the relevant OCSP Responder is communicated to the Enterprise Customer.

OCSP responses are provided within a commercially reasonable time and no later than ten seconds after the request is received, subject to transmission latencies over the Internet.

OCSP responses conform to RFC 5019 and/or RFC 6960. OCSP responses either:

1. Are signed by the CA that issued the Certificates whose revocation status is being checked, or
2. Are signed by an OCSP Responder whose Certificate is signed by the CA that issued the Certificate whose revocation status is being checked.

.

4.9.10 On-Line Revocation Checking Requirements

A relying party must check the status of a certificate on which he/she/it wishes to rely. If a Relying Party does not check the status of a Certificate on which the Relying Party wishes to rely by consulting the most recent relevant CRL, the Relying Party shall check Certificate status by consulting the applicable repository or by requesting Certificate status using the applicable OCSP responder (where OCSP services are available)

For the status of Subscriber Certificates:

- OCSP responses have a validity interval greater than or equal to eight hours;
- OCSP responses have a validity interval less than or equal to ten days;
- For OCSP responses with validity intervals less than sixteen hours, then TRUST ITALIA SPA. updates the information provided via an Online Certificate Status Protocol prior to one-half of the validity period before the nextUpdate; and
- For OCSP responses with validity intervals greater than or equal to sixteen hours, then TRUST ITALIA SPA updates the information provided via an Online Certificate Status Protocol at least eight hours prior to the nextUpdate, and no later than four days after the thisUpdate.

For Publicly Trusted Subordinate CA or Intermediate CA Certificates:
TRUST ITALIA SPA updates information provided via an Online Certificate Status Protocol:

- at least every twelve months; and
- within 24 hours after revoking a Subordinate CA Certificate.

4.9.11 Other Forms of Revocation Advertisements Available

No Stipulation.

4.9.12 Special Requirements regarding Key Compromise

TRUST ITALIA SPA uses commercially reasonable efforts to notify potential Relying Parties if it discovers, or have reason to believe, that there has been a Compromise of the private key of one of their own CAs or one of the CAs within their sub-domains.

4.9.13 Circumstances for Suspension

No stipulation.

4.9.14 Who Can Request Suspension

No stipulation.

4.9.15 Procedure for Suspension Request

No stipulation.

4.9.16 Limits on Suspension Period

No stipulation.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

The Status of public certificates is available via CRL at **TRUST ITALIA SPA**'s website, LDAP directory and via an OCSP responder (where available). The serial number of a revoked Certificate remains on the CRL until one additional CRL is published after the end of the Certificate's validity period. OCSP information for subscriber Certificates is updated at least every four days. OCSP information for **TRUST ITALIA SPA** Intermediate CAs subordinate CA Certificates is updated by DigiCert as described in section 4.10.1 of DigiCert' CPS

4.10.2 Service Availability

Certificate Status Services are normally available 24/7 without scheduled interruption.

4.10.3 Optional Features

OCSP is an optional status service feature that is not available for all products and must be specifically enabled for other products.

4.11 End of Subscription

A subscriber may end a subscription for a **TRUST ITALIA SPA** certificate by:

- Allowing his/her/its certificate to expire without renewing or re-keying that certificate
- Revoking of his/her/its certificate before certificate expiration without replacing the certificates.

4.12 Key Escrow and Recovery

With the exception of enterprises deploying Managed PKI Key Management Services no Sub-domain participant may escrow CA, RA or end-user Subscriber private keys.

Enterprise customers using the Key Escrow option within the DigiCert Managed PKI Service can escrow copies of the private keys of Subscribers whose Certificate Applications they approve. The enterprise customer may escrow keys either within the enterprise's premises or **TRUST ITALIA SPA's** secure data center. If operated out of the enterprise's premises, **TRUST ITALIA SPA** does not store copies of Subscriber private keys but plays an important role in the Subscriber key recovery process.

4.12.1 Key Escrow and Recovery Policy and Practices

Enterprise customers using the Key Escrow option within the DigiCert Managed PKI service (or an equivalent service approved by DigiCert) are permitted to escrow end-user Subscribers' private key. Escrowed private keys shall be stored in encrypted form using the Managed PKI Key Manager software. Except for enterprise customers using the Managed PKI Key Manager Service (or an equivalent service approved by DigiCert), the private keys of CAs or end-user Subscribers shall not be escrowed.

End-user Subscriber private keys shall only be recovered under the circumstances permitted within the Managed PKI Key Management Service Administrator's Guide, under which:

- Enterprise customers using Managed PKI Key Manager shall confirm the identity of any person purporting to be the Subscriber to ensure that a purported Subscriber request for the Subscriber's private key is, in fact, from the Subscriber and not an imposter,
- Enterprise customers shall recover a Subscriber's private key without the Subscriber's authority only for their legitimate and lawful purposes, such as to comply with judicial or administrative process or a search warrant, and not for any illegal, fraudulent, or other wrongful purpose, and
- Such Enterprise customers shall have personnel controls in place to prevent Key Management Service Administrators and other persons from obtaining unauthorized access to private keys.

It is recommended that Enterprise Customers using the Key Escrow option within the Symantec Managed PKI Service:

- Notify the subscribers that their private keys are escrowed
- Protect subscribers' escrowed keys from unauthorized disclosure,Protect all information, including the administrator's own key(s) that could be used to recover subscribers' escrowed keys.
    - Release subscribers' escrowed keys only for properly authenticated and authorized requests for recovery.
    - Revoke the Subscriber's Key pair prior to recovering the encryption key under certain circumstances such as to discontinue the use of a lost certificate.
    - Not be required to communicate any information concerning a key recovery to the subscriber except when the subscriber him/herself has requested recovery.
    - Not disclose or allow to be disclosed escrowed keys or escrowed key-related information to any third party unless required by the law, government rule, or regulation; by the enterprise's organization policy; or by order of a court of competent jurisdiction.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Private keys are stored in the Key Manager database in encrypted form. Each Subscriber's private key is individually encrypted with its own triple-DES symmetric key. A Key Escrow Record (KER) is generated, then the triple-DES key is combined with a random session key to form a session key mask. The resulting masked session key (MSK) is securely sent and stored in the Managed PKI database at **TRUST ITALIA SPA**. The KER (containing the end user's private key) and the random session key mask are stored in the Key Manager database and all residual key material is destroyed.

The Managed PKI database is operated out of **TRUST ITALIA SPA's** secure data center. The enterprise customer may choose to operate the Key Manager database either on the enterprise's premises or out of **TRUST ITALIA SPA's** secure data center.

Recovery of a private key and digital certificate requires the Managed PKI administrator to securely log on to the Managed PKI Control Center, select the appropriate key pair to recover and click a "recover" hyperlink. Only after an approved administrator clicks the "recover" link is the MSK for that key pair returned from the Managed PKI database. The Key Manager retrieves the session key from the KMD and

combines it with the MSK to regenerate the triple-DES key which was used to originally encrypt the private key, allowing recovery of the end user's private key. As a final step, an encrypted PKCS#12 file is returned to the administrator and ultimately distributed to the end user.

5. Facility, Management, and Operational Controls

5.1 Physical Controls

TRUST ITALIA SPA has implemented the **TRUST ITALIA SPA** Physical Security Policy, which supports the security requirements of this CPS. Compliance with these policies is included in **TRUST ITALIA SPA**'s independent audit requirements described in Section 8. The **TRUST ITALIA SPA** Physical Security Policy contains sensitive security information and is only available upon agreement with **TRUST ITALIA SPA**. An overview of the requirements are described below.

5.1.1 Site Location and Construction

TRUST ITALIA SPA CA and RA operations are conducted within a physically protected environment that deters, prevents, and detects unauthorized use of, access to, or disclosure of sensitive information and systems whether covert or overt.

TRUST ITALIA SPA also maintains disaster recovery facilities for its CA operations. **TRUST ITALIA SPA**'s disaster recovery facilities are protected by multiple tiers of physical security comparable to those of **TRUST ITALIA SPA**'s primary facility.

5.1.2 Physical Access

Systems providing online certificate issuance (e.g. Issuer CAs) are located in **TRUST ITALIA SPA** data centers. **TRUST ITALIA SPA** protects such online equipment (including certificate status servers and CMS equipment) from unauthorized access and implements physical controls to reduce the risk of equipment tampering

TRUST ITALIA SPA CA systems are protected by a minimum of four tiers of physical security, with access to the lower tier required before gaining access to the higher tier.

Progressively restrictive physical access privileges control access to each tier. Sensitive CA operational activity, any activity related to the lifecycle of the certification process such as authentication, verification, and issuance, occur within very restrictive physical tiers. Access to each tier requires the use of a proximity card employee badge. Physical access is automatically logged and video recorded. Additional tiers enforce individual access control through the use of two factor authentication including biometrics. Unescorted personnel, including untrusted employees or visitors, are not allowed into such secured areas.

The physical security system includes additional tiers for key management security which serves to protect both online and offline storage of CSUs and keying material. Areas used to create and store cryptographic material enforce dual control, each through the use of two factor authentication including biometrics. Online CSUs are protected through the use of locked cabinets. Offline CSUs are protected through the use of locked safes, cabinets and containers. Access to CSUs and keying material is restricted in accordance with **TRUST ITALIA SPA**'s segregation of duties requirements. The opening and closing of cabinets or containers in these tiers is logged for audit purposes.

5.1.3 Power and Air Conditioning

TRUST ITALIA SPA's secure facilities are equipped with primary and backup:

- power systems to ensure continuous, uninterrupted access to electric power and
- heating/ventilation/air conditioning systems to control temperature and relative

humidity.

5.1.4 Water Exposures

TRUST ITALIA SPA has taken reasonable precautions to minimize the impact of water exposure to **TRUST ITALIA SPA** systems.

5.1.5 Fire Prevention and Protection

TRUST ITALIA SPA has taken reasonable precautions to prevent and extinguish fires or other damaging exposure to flame or smoke. **TRUST ITALIA SPA**'s fire prevention and protection measures have been designed to comply with local fire safety regulations.

5.1.6 Media Storage

All media containing production software and data, audit, archive, or backup information is stored within **TRUST ITALIA SPA** facilities or in a secure off-site storage facility with appropriate physical and logical access controls designed to limit access to authorized personnel and protect such media from accidental damage (e.g., water, fire, and electromagnetic).

5.1.7 Waste Disposal

Sensitive documents and materials are shredded before disposal. Media used to collect or transmit sensitive information are rendered unreadable before disposal. Cryptographic devices are physically destroyed or zeroized in accordance the manufacturers' guidance prior to disposal. Other waste is disposed of in accordance with **TRUST ITALIA SPA**'s normal waste disposal requirements.

5.1.8 Off-Site Backup

TRUST ITALIA SPA performs routine backups of critical system data, audit log data, and other sensitive information. Offsite backup media are stored in a physically secure manner using a bonded third party storage facility and **TRUST ITALIA SPA**'s disaster recovery facility.

5.2 Procedural Controls

5.2.1 Trusted Roles

Trusted Persons include all employees, contractors, and consultants that have access to or control authentication or cryptographic operations that may materially affect:

- the validation of information in Certificate Applications;
- the acceptance, rejection, or other processing of Certificate Applications, revocation requests, renewal requests, or enrollment information;
- the issuance, or revocation of Certificates, including personnel having access to restricted portions of its repository;
- the handling of Subscriber information or requests.

Trusted Persons include, but are not limited to:

- customer service personnel
- cryptographic business operations personnel
- security personnel
- system administration personnel
- designated engineering personnel and
- executives that are designated to manage infrastructural trustworthiness.

TRUST ITALIA SPA considers the categories of personnel identified in this section as Trusted Persons

having a Trusted Position. Persons seeking to become Trusted Persons by obtaining a Trusted Position must successfully complete the screening requirements set out in this CPS.

5.2.2 Number of Persons Required per Task

TRUST ITALIA SPA has established, maintains, and enforces rigorous control procedures to ensure the segregation of duties based on job responsibility and to ensure that multiple Trusted Persons are required to perform sensitive tasks.

Policy and control procedures are in place to ensure segregation of duties based on job responsibilities. The most sensitive tasks, such as access to and management of CA cryptographic hardware (cryptographic signing unit or CSU) and associated key material, require multiple Trusted Persons.

These internal control procedures are designed to ensure that at a minimum, two trusted personnel are required to have either physical or logical access to the device. Access to CA cryptographic hardware is strictly enforced by multiple Trusted Persons throughout its lifecycle, from incoming receipt and inspection to final logical and/or physical destruction. Once a module is activated with operational keys, further access controls are invoked to maintain split control over both physical and logical access to the device. Persons with physical access to modules do not hold “Secret Shares” and vice versa.

Other manual operations, not issued by an automated validation and issuance system, require the participation of at least 2 Trusted Persons, or a combination of at least one trusted person and an automated validation and issuance process. Manual operations for Key Recovery may optionally require the validation of two (2) authorized Administrators.

5.2.3 Identification and Authentication for Each Role

For all personnel seeking to become Trusted Persons, verification of identity is performed through the personal (physical) presence of such personnel before Trusted Persons performing TRUST ITALIA SPA HR or security functions and a check of well-recognized forms of identification (e.g., passports and driver’s licenses). Identity is further confirmed through the background checking procedures in CPS § 5.3.1.

TRUST ITALIA SPA ensures that personnel have achieved Trusted Status and departmental approval has been given before such personnel are:

- issued access devices and granted access to the required facilities;
- issued electronic credentials to access and perform specific functions on STN CA, RA, or other IT systems.

5.2.4 Roles Requiring Separation of Duties

Roles requiring Separation of duties include (but are not limited to):

- the validation of information in Certificate Applications;
- the acceptance, rejection, or other processing of Certificate Applications, revocation requests, recovery requests or renewal requests, or enrollment information;
- the issuance, or revocation of Certificates, including personnel having access to restricted portions of the repository;
- the handling of Subscriber information or requests
- the generation, issuing or destruction of a CA certificate
- the loading of a CA to a Production environment

5.3 Personnel Controls

Personnel seeking to become Trusted Persons must present proof of the requisite background, qualifications, and experience needed to perform their prospective job responsibilities

competently and satisfactorily, as well as proof of any government clearances, if any, necessary to perform certification services under government contracts. Background checks are repeated at least every 5 years for personnel holding Trusted Positions.

5.3.1 Qualifications, Experience, and Clearance Requirements

TRUST ITALIA SPA requires that personnel seeking to become Trusted Persons present proof of the requisite background, qualifications, and experience needed to perform their prospective job responsibilities competently and satisfactorily, as well as proof of any government clearances, if any, necessary to perform certification services under government contracts.

5.3.2 Background Check Procedures

Prior to commencement of employment in a Trusted Role, **TRUST ITALIA SPA** conducts background checks which include the following:

- confirmation of previous employment
- check of professional reference
- confirmation of the highest or most relevant educational degree obtained
- search of criminal records (local, state or provincial, and national)
- check of credit/financial records, search of driver's license records, and
- search of Social Security Administration records.

To the extent that any of the requirements imposed by this section cannot be met due to a prohibition or limitation in local law or other circumstances, **TRUST ITALIA SPA** will utilize a substitute investigative technique permitted by law that provides substantially similar information, including but not limited to obtaining a background check performed by the applicable governmental agency.

The factors revealed in a background check that may be considered grounds for rejecting candidates for Trusted Positions or for taking action against an existing Trusted Person generally include (but are not limited to) the following:

- Misrepresentations made by the candidate or Trusted Person
- Highly unfavorable or unreliable professional references
- Certain criminal convictions, and
- Indications of a lack of financial responsibility.

Reports containing such information are evaluated by human resources and security personnel, who determine the appropriate course of action in light of the type, magnitude, and frequency of the behavior uncovered by the background check. Such actions may include measures up to and including the cancellation of offers of employment made to candidates for Trusted Positions or the termination of existing Trusted Persons.

The use of information revealed in a background check to take such actions is subject to the applicable federal, state, and local laws.

5.3.3 Training Requirements

TRUST ITALIA SPA provides its personnel with training upon hire as well as the requisite on-the-job training needed for them to perform their job responsibilities competently and satisfactorily. **TRUST ITALIA SPA** maintains records of such training. **TRUST ITALIA SPA** periodically reviews and enhances its training programs as necessary.

TRUST ITALIA SPA's training programs are tailored to the individual's responsibilities and include the following as relevant:

- Basic PKI concepts
- Job responsibilities
- TRUST ITALIA SPA security and operational policies and procedures
- Use and operation of deployed hardware and software
- Incident and Compromise reporting and handling, and
- Disaster recovery and business continuity procedures.

5.3.4 Retraining Frequency and Requirements

TRUST ITALIA SPA provides refresher training and updates to their personnel to the extent and frequency required to ensure that such personnel maintain the required level of proficiency to perform their job responsibilities competently and satisfactorily.

5.3.5 Job Rotation Frequency and Sequence

No Stipulation

5.3.6 Sanctions for Unauthorized Actions

Appropriate disciplinary actions are taken for unauthorized actions or other violations of **TRUST ITALIA SPA** policies and procedures. Disciplinary actions may include measures up to and including termination and are commensurate with the frequency and severity of the unauthorized actions.

5.3.7 Independent Contractor Requirements

In limited circumstances, independent contractors or consultants may be used to fill Trusted Positions. Any such contractor or consultant is held to the same functional and security criteria that apply to a **TRUST ITALIA SPA** employees in a comparable position.

Independent contractors and consultants who have not completed or passed the background check procedures specified in CPS § 5.3.2 are permitted access to **TRUST ITALIA SPA**'s secure facilities only to the extent they are escorted and directly supervised by Trusted Persons at all times.

5.3.8 Documentation Supplied to Personnel

TRUST ITALIA SPA provides its employees the requisite training and other documentation needed to perform their job responsibilities competently and satisfactorily.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

TRUST ITALIA SPA manually or automatically logs the following significant events:

- CA key life cycle management events, including:
  - Key generation, backup, storage, recovery, archival, and destruction
  - Cryptographic device life cycle management events.
- CA and Subscriber certificate life cycle management events, including:
  - Certificate Applications, renewal, rekey, and revocation
  - Successful or unsuccessful processing of requests
  - Generation and issuance of Certificates and CRLs.

- Security-related events including:
  - Successful and unsuccessful PKI system access attempts
  - PKI and security system actions performed by TRUST ITALIA SPA personnel
  - Security sensitive files or records read, written or deleted
  - Security profile changes
  - System crashes, hardware failures and other anomalies
  - Firewall and router activity
  - CA facility visitor entry/exit.

Log entries include the following elements:

- Date and time of the entry
- Serial or sequence number of entry, for automatic journal entries
- Identity of the entity making the journal entry
- Description/kind of entry.

TRUST ITALIA SPA RAs and Enterprise Administrators log Certificate Application information including:

- Kind of identification document(s) presented by the Certificate Applicant
- Record of unique identification data, numbers, or a combination thereof (e.g., Certificate Applicant's drivers license number) of identification documents, if applicable
- Storage location of copies of applications and identification documents
- Identity of entity accepting the application
- Method used to validate identification documents, if any
- Name of receiving CA or submitting RA, if applicable.

5.4.2 Frequency of Processing Log

The CA system is continuously monitored to provide real time alerts of significant security and operational events for review by designated system security personnel. In accordance with ISO/IEC 27001 requirements the log are elaborate by an automated process in order to guarantee that have not been tampered, and audited.Actions taken based on audit log reviews are also documented.

5.4.3 Retention Period for Audit Log

Audit logs shall be retained onsite for at least five weeks after processing and thereafter archived in accordance with Section 5.5.2.

5.4.4 Protection of Audit Log

Audit logs are protected with an electronic audit log system that includes mechanisms to protect the log files from unauthorized viewing, modification, deletion, or other tampering.

5.4.5 Audit Log Backup Procedures

Audit log are in HA/FT.

5.4.6 Audit Collection System (Internal vs. External)

Automated audit data is generated and recorded at the application, network and operating system level. Manually generated audit data is recorded by **TRUST ITALIA SPA** personnel.

5.4.7 Notification to Event-Causing Subject

Where an event is logged by the audit collection system, no notice is required to be given to the individual, organization, device, or application that caused the event.

5.4.8 Vulnerability Assessments

Events in the audit process are logged, in part, to monitor system vulnerabilities. The archiving model and the monitoring system will alert in case of suspect log. Periodically the monitoring system log are assessed to verify the presence of vulnerabilities[1]

5.5 Records Archival

5.5.1 Types of Records Archived

TRUST ITALIA SPA archives:

- All audit data collected in terms of Section 5.4 o Certificate application information
- Documentation supporting certificate applications
- Certificate lifecycle information e.g., revocation, rekey and renewal application information

5.5.2 Retention Period for Archive

Records shall be retained for at least the time periods set forth below following the date the Certificate expires or is revoked.

- Five (5) years for Level 1 Certificates,
- Ten (10) years and six (6) months for Level 2

5.5.3 Protection of Archive

TRUST ITALIA SPA protects the archive so that only authorized Trusted Persons are able to obtain access to the archive. The archive is protected against unauthorized viewing, modification, deletion, or other tampering by storage within a Trustworthy System. The media holding the archive data and the applications required to process the archive data shall be maintained to ensure that the archive data can be accessed for the time period set forth in this CPS.

5.5.4 Archive Backup Procedures

TRUST ITALIA SPA incrementally backs up electronic archives of its issued Certificate information on a daily basis and performs full backups on a weekly basis. Copies of paper-based records shall be maintained in an off-site secure facility.

5.5.5 Requirements for Time-Stamping of Records

Certificates, CRLs, and other revocation database entries shall contain time and date information. Such time information need not be cryptographic-based.

5.5.6 Archive Collection System (Internal or External)

TRUST ITALIA SPA archive collection systems are internal, except for enterprise RA Customers. **TRUST ITALIA SPA** assists its enterprise RAs in preserving an audit trail. Such an archive collection system therefore is external to that enterprise RA.

5.5.7 Procedures to Obtain and Verify Archive Information

Only authorized Trusted Personnel are able to obtain access to the archive. The integrity of the information is verified when it is restored.

[1] Details about monitoring and assessment result and periodicity are present in TRUST ITALIA SPA 27001 repository and documentation

5.6 Key Changeover

TRUST ITALIA SPA CA key pairs are retired from service at the end of their respective maximum lifetimes as defined in this CPS. **TRUST ITALIA SPA** CA Certificates may be renewed as long as the cumulative certified lifetime of the CA key pair does not exceed the maximum CA key pair lifetime. New CA key pairs will be generated as necessary, for example to replace CA key pairs that are being retired, to supplement existing, active key pairs and to support new services.

Prior to the expiration of the CA Certificate for a Superior CA, key changeover procedures are enacted to facilitate a smooth transition for entities within the Superior CA's hierarchy from the old Superior CA key pair to new CA key pair(s). **TRUST ITALIA SPA**'s CA key changeover process requires that:

- A Superior CA ceases to issue new Subordinate CA Certificates no later than 60 days before the point in time ("Stop Issuance Date") where the remaining lifetime of the Superior CA key pair equals the approved Certificate Validity Period for the specific type(s) of Certificates issued by Subordinate CAs in the Superior CA's hierarchy.
- Upon successful validation of Subordinate CA (or end-user Subscriber) Certificate requests received after the "Stop Issuance Date," Certificates will be signed with a new CA key pair.

The Superior CA continues to issue CRLs signed with the original Superior CA private key until the expiration date of the last Certificate issued using the original key pair has been reached

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

Backups of the following CA information shall be kept in off-site storage and made available in the event of a Compromise or disaster: Certificate Application data, audit data, and database records for all Certificates issued. Back-ups of CA private keys shall be generated and maintained in accordance with CP § 6.2.4. TRUST ITALIA SPA maintains backups of the foregoing CA information for their own CAs, as well as the CAs of Enterprise Customers within its Sub-domain.

5.7.2 Computing Resources, Software, and/or Data Are Corrupted

In the event of the corruption of computing resources, software, and/or data, such an occurrence is reported to **TRUST ITALIA SPA** Security and **TRUST ITALIA SPA**'s incident handling procedures are enacted. Such procedures require appropriate escalation, incident investigation, and incident response. If necessary, **TRUST ITALIA SPA**'s key compromise or disaster recovery procedures will be enacted.

5.7.3 Entity Private Key Compromise Procedures

Upon the suspected or known Compromise of a **TRUST ITALIA SPA** CA, STN infrastructure or Customer CA private key, **TRUST ITALIA SPA**'s Key Compromise Response procedures are enacted by the **TRUST ITALIA SPA** Security Incident Response Team (IRT) This team, which includes Security, Cryptographic Business Operations, Production Services personnel, and other TRUST ITALIA SPA management representatives, assesses the situation, develops an action plan, and implements the action plan with approval from **TRUST ITALIA SPA** executive management.

If CA Certificate revocation is required, the following procedures are performed:

- The Certificate's revoked status is communicated to Relying Parties through the TRUST ITALIA SPA Repository in accordance with CPS § 4.9.7,
- Commercially reasonable efforts will be made to provide additional notice of the revocation to all affected STN Participants, and
- The CA will generate a new key pair in accordance with CPS § 5.6, except where the CA is being terminated in accordance with CPS § 5.8.

5.7.4 Business Continuity Capabilities after a Disaster

Trust Italia SpA has created and maintains business continuity plans so that in the event of a business disruption, critical business functions may be resumed. Trust Italia SpA maintains a Disaster Recovery Facility (DRF) located at a Trust Italia SpA -owned facility geographically separate from the primary Production Facility. The DRF is a hardened facility designed to federal government and military specifications and is also specifically equipped to meet Trust Italia SpA's security standards.

In the event of a natural or man-made disaster requiring permanent cessation of operations from Trust Italia SpA's primary facility, the Corporate Trust Italia SpA Business Continuity Team and the Trust Italia SpA Authentication Operations Incident Management Team will coordinate with cross functional management teams to make the decision to formally declare a disaster situation and manage the incident. Once a disaster situation is declared, restoration of Trust Italia SpA's Production services functionality at the DRF will be initiated.

Trust Italia SpA has developed a Disaster Recovery Plan (DRP) for its managed PKI services. The DRP identifies conditions for activating the plan and what constitutes an acceptable system outage and recovery time. The DRP defines the procedures for the teams to reconstitute STN operations using backup data and backup copies of the Sub-domain keys. Additionally, Trust Italia SpA's DRP includes:

- Frequency for taking backup copies of essential business information and software
- Requirement to store critical cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location
- Separation distance of the Disaster recovery site to the CA's main site
- Procedures for securing the Disaster facility during the period of time following a disaster and prior to restoring a secure environment either at the original or a remote site

Trust Italia SpA's DRP identifies administrative requirements

- including: maintenance schedule for the plan;
- Awareness and education requirements;
- Responsibilities of the individuals; and
- Regular testing of contingency plans.

The target recovery time for restoring critical Production service functionality is no greater than 24 hours.

Trust Italia SpA conducts at least one disaster recovery test per calendar year to ensure functionality of services at the DRF. Formal Business Continuity Exercises are also conducted yearly in coordination with the Corporate Trust Italia SpA Business Continuity Team where procedures for additional types of scenarios (e.g. pandemic, earthquake, flood, power outage) are tested and evaluated.

Trust Italia SpA takes significant steps to develop, maintain, and test sound business recovery plans, and Trust Italia SpA's planning for a disaster or significant business disruption is consistent with many of the best practices established within the industry.

Trust Italia SpA maintains redundant hardware and backups of its CA and infrastructure system software at its disaster recovery facility. In addition, CA private keys are backed up and maintained for disaster recovery purposes in accordance with CPS § 6.2.4.

TRUST ITALIA SPA maintains offsite backups of important CA information for TRUST ITALIA SPA CAs as well as the CAs of Service Centers, and Enterprise Customers, within TRUST ITALIA's Sub-domain. Such information includes, but is not limited to: Certificate Application data, audit data (per Section 4.5), and database records for all Certificates issued.

5.8 CA or RA Termination

In the event that it is necessary for a **TRUST ITALIA SPA** CA, or Enterprise Customer CA to cease operation, **TRUST ITALIA SPA** makes a commercially reasonable effort to notify Subscribers, Relying Parties, and other affected entities of such termination in advance of the CA termination. Where CA termination is required, **TRUST ITALIA SPA** and, in the case of a Customer CA, the applicable Customer, will develop a termination plan to minimize disruption to Customers, Subscribers, and Relying Parties. Such termination plans may address the following, as applicable:

- Provision of notice to parties affected by the termination, such as Subscribers, Relying Parties, and Customers, informing them of the status of the CA,
- Handling the cost of such notice,
- The revocation of the Certificate issued to the CA by TRUST ITALIA SPA,
- The preservation of the CA's archives and records for the time periods required in this CPS,
- The continuation of Subscriber and customer support services,
- The continuation of revocation services, such as the issuance of CRLs or the maintenance of online status checking services,
- The revocation of unexpired unrevoked Certificates of end-user Subscribers and subordinate CAs, if necessary,
- Refunding (if necessary) Subscribers whose unexpired unrevoked Certificates are revoked under the termination plan or provision, or alternatively, the issuance of replacement Certificates by a successor CA,
- Disposition of the CA's private key and the hardware tokens containing such private key, and
- Provisions needed for the transition of the CA's services to a successor CA.

6. Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

CA key pair generation is performed by multiple pre-selected, trained and trusted individuals using Trustworthy Systems and processes that provide for the security and required cryptographic strength for the generated keys. For PCA and Issuing Root CAs, the cryptographic modules used for key generation meet the requirements of FIPS 140-2 level 3. For other CAs (including **TRUST ITALIA SPA** CAs and Managed PKI Customer CAs), the cryptographic modules used meet the requirements of at least FIPS 140-2 level 2.

All CA key pairs are generated in pre-planned Key Generation Ceremonies. The activities performed in each key generation ceremony are recorded, dated and signed by all individuals involved. The activities performed in each key generation ceremony are recorded, dated and signed by all individuals involved. These records are kept for audit and tracking purposes for a length of time deemed appropriate by **TRUST ITALIA SPA** Management.

Generation of RA key pairs is generally performed by the RA using a FIPS 140-1 level 1 certified cryptographic module provided with their browser software.

Enterprise Customers generate the key pair used by their Automated Administration servers. **TRUST ITALIA SPA** recommends that Automated Administration server key pair generation be performed using a FIPS 140-1 level 2 certified cryptographic module.

Generation of end-user Subscriber key pairs is generally performed by the Subscriber. For Level 1

Certificates, Level 2 Certificates, the Subscriber typically uses a FIPS 140-1 level 1 certified cryptographic module provided with their browser software for key generation.

6.1.2 Private Key Delivery to Subscriber

When end-user Subscriber key pairs are generated by the end-user Subscriber, private key delivery to a Subscriber is not applicable.

Where RA or end-user Subscriber key pairs are pre-generated by **TRUST ITALIA SPA** on hardware tokens or smart cards, such devices are distributed to the RA or end-user Subscriber using a commercial delivery service and tamper evident packaging. The data required to activate the device is communicated to the RA or end-user Subscriber using an out of band process.
Where end-user Subscriber key pairs are pre-generated by Enterprise Customers on hardware tokens or smart cards, such devices are distributed to the end-user Subscriber using a commercial delivery service and tamper evident packaging. The required activation data required to activate the device is communicated to the RA or end-user Subscriber using an out of band process. The distribution of such devices is logged by the Enterprise Customer.

For Enterprise Customers using Managed PKI Key Manager for key recovery services, the Customer may generate encryption key pairs (on behalf of Subscribers whose Certificate Applications they approve) and transmit such key pairs to Subscribers via a password protected PKCS # 12 file.

6.1.3 Public Key Delivery to Certificate Issuer

End-user Subscribers and RAs submit their public key to TRUST ITALIA SPA for certification electronically through the use of a PKCS#10 Certificate Signing Request (CSR) or other digitally signed package in a session secured by Secure Sockets Layer (SSL). Where CA, RA, or end-user Subscriber key pairs are generated by TRUST ITALIA SPA, this requirement is not applicable.

6.1.4 CA Public Key Delivery to Relying Parties

TRUST ITALIA SPA generally provides the full certificate chain (including the issuing CA and any CAs in the chain) to the end-user Subscriber upon Certificate issuance. **TRUST ITALIA SPA** CA Certificates may also be downloaded from the **TRUST ITALIA SPA** website on www.trustitalia.it

6.1.5 Key Sizes

Key pairs shall be of sufficient length to prevent others from determining the key pair's private key using cryptanalysis during the period of expected utilization of such key pairs. The **TRUST ITALIA SPA** CA certificates are generate using 2048-bit or greater RSA Key (with a modulus size in bits divisible by 8).

TRUST ITALIA SPA requires end-entity Certificates to contain a key size that is at least 2048 bits for RSA

For DigiCert root key pairs and strengths, refer to DigiCert CP and CPS section 6.1.5 and https://www.digicert.com/legal-repository/ for the root Certificates..

6.1.6 Public Key Parameters Generation and Quality Checking

Refer to section 6.1.6 of DigiCert CP.

6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field)

TRUST ITALIA SPA's Certificates include key usage extension fields that specify the intended use of the Certificate and technically limit the Certificate's functionality in X.509v3-compliant software.
The use of a specific key is determined by the key usage extension in the X.509 Certificate.

Subscriber Certificates assert key usages based on the intended application of the Key Pair and cannot include anyExtendedKeyUsage as specified by section 7.1.2 of the DigiCert CP and this CPS.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

TRUST ITALIA SPA has implemented a combination of physical, logical, and procedural controls to ensure the security of **TRUST ITALIA SPA** and Enterprise Customer CA private keys. Subscribers are required by contract to take necessary precautions to prevent the loss, disclosure, modification, or unauthorized use of private keys.

6.2.1 Cryptographic Module Standards and Controls

For PCA and Issuing Root CA key pair generation and CA private key storage, **TRUST ITALIA SPA** uses hardware cryptographic modules that are certified at or meet the requirements of FIPS 140-2 Level 3.

6.2.2 Private Key (m out of n) Multi-Person Control

TRUST ITALIA SPA has implemented technical and procedural mechanisms that require the participation of multiple trusted individuals to perform sensitive CA cryptographic operations. **TRUST ITALIA SPA** uses "Secret Sharing" to split the activation data needed to make use of a CA private key into separate parts called "Secret Shares" which are held by trained and trusted individuals called "Shareholders." A threshold number of Secret Shares (m) out of the total number of Secret Shares created and distributed for a particular hardware cryptographic module (n) is required to activate a CA private key stored on the module.

The threshold number of shares needed to sign a CA certificate is 3. It should be noted that the number of shares distributed for disaster recovery tokens may be less than the number distributed for operational tokens, while the threshold number of required shares remains the same. Secret Shares are protected in accordance with this CPS.

6.2.3 Private Key Escrow

CA private keys are not escrowed. Escrow of private keys for end user subscribers is explained in more detail in Section 4.12.

6.2.4 Private Key Backup

TRUST ITALIA SPA creates backup copies of CA private keys for routine recovery and disaster recovery purposes. Such keys are stored in encrypted form within hardware cryptographic modules and associated key storage devices. Cryptographic modules used for CA private key storage meet the requirements of this CPS. CA private keys are copied to backup hardware cryptographic modules in accordance with this CPS.

Modules containing onsite backup copies of CA private keys are subject to the requirements of CPS. Modules containing disaster recovery copies of CA private keys are subject to the requirements of this CPS.

TRUST ITALIA SPA does not store copies of RA private keys. For the backup of end-user Subscriber private keys, see Section 6.2.3 and Section 4.12. For ACS Application IDs, **TRUST ITALIA SPA** does not store copies of Subscriber private keys.

6.2.5 Private Key Archival

Upon expiration of a **TRUST ITALIA SPA** CA Certificate, the key pair associated with the certificate will be securely retained for a period of at least 5 years using hardware cryptographic modules that meet the requirements of this CPS. These CA key pairs shall not be used for any signing events after the expiration date of the corresponding CA Certificate, unless the CA Certificate has been renewed in terms of this CPS.

TRUST ITALIA SPA does not archive copies of RA and Subscriber private keys.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

TRUST ITALIA SPA generates CA key pairs on the hardware cryptographic modules in which the keys will be used. In addition, **TRUST ITALIA SPA** makes copies of such CA key pairs for routine recovery and disaster recovery purposes. Where CA key pairs are backed up to another hardware cryptographic module, such key pairs are transported between modules in encrypted form.

6.2.7 Private Key Storage on Cryptographic Module

CA or RA private keys held on hardware cryptographic modules shall be stored in encrypted form.

6.2.8 Method of Activating Private Key

All **TRUST ITALIA SPA** sub-domain Participants shall protect the activation data for their private keys against loss, theft, modification, unauthorized disclosure, or unauthorized use.

6.2.8.1 Level 1 Certificates

The Standard for Level 1 private key protection is for Subscribers to take commercially reasonable measures for the physical protection of the Subscriber's workstation to prevent use of the workstation and its associated private key without the Subscriber's authorization. In addition, **TRUST ITALIA SPA** recommends that Subscribers use a password in accordance with Section 6.4.1 or security of equivalent strength to authenticate the Subscriber before the activation of the private key, which includes, for instance, a password to operate the private key, a Windows logon or screen saver password, or a network logon password.

6.2.8.2 Level 2 Certificates

The Standard for Level 2 Private Key protection is for Subscribers to:

- Use a password in accordance with Section 6.4.1 or security of equivalent strength to authenticate the Subscriber before the activation of the private key, which includes, for instance, a password to operate the private key, a Windows logon or screen saver password; and
- Take commercially reasonable measures for the physical protection of the Subscriber's workstation to prevent use of the workstation and its associated private key without the Subscriber's authorization.

When deactivated, private keys shall be kept in encrypted form only.

6.2.8.3 Administrators' Private Keys (Level 3)

The Standard for Administrators' private key protection requires them to:

- Use a smart card, biometric access device, password in accordance with Section 6.4.1, or security of equivalent strength to authenticate the Administrator before the activation of the private key, which includes, for instance, a password to operate the private key, a Windows logon or screen saver password, or a network logon password; and
- Take commercially reasonable measures for the physical protection of the Administrator's workstation to prevent use of the workstation and its associated private key without the Administrator's authorization.

TRUST ITALIA SPA recommends that Administrators use a smart card, biometric access device, or security of equivalent strength along with the use of a password in accordance with Section 6.4.1 to authenticate the Administrator before the activation of the private key.

When deactivated, private keys shall be kept in encrypted form only.

6.2.8.4 Enterprise RAs using a Cryptographic Module (with Automated Administration or with Managed PKI Key Manager Service)

The Standard for private key protection for Administrators using such a cryptographic module requires them to:

- Use the cryptographic module along with a password in accordance with Section 6.4.1 to authenticate the Administrator before the activation of the private key; and
- Take commercially reasonable measures for the physical protection of the workstation housing the cryptographic module reader to prevent use of the workstation and the private key associated with the cryptographic module without the Administrator's authorization.

6.2.8.5 Private Keys Held by Processing Centers (Level 1-2)

An online CA's private key shall be activated by a threshold number of Shareholders, as defined in Section 6.2.2, supplying their activation data (stored on secure media). Once the private key is activated, the private key may be active for an indefinite period until it is deactivated when the CA goes offline. Similarly, a threshold number of Shareholders shall be required to supply their activation data in order to activate an offline CA's private key. Once the private key is activated, it shall be active only for one time.

6.2.9 Method of Deactivating Private Key

TRUST ITALIA SPA CA private keys are deactivated upon removal from the token reader. **TRUST ITALIA SPA** RA private keys (used for authentication to the RA application) are deactivated upon system log off. TRUST ITALIA SPA RAs are required to log off their workstations when leaving their work area.

Client Administrators, RA, and end-user Subscriber private keys may be deactivated after each operation, upon logging off their system, or upon removal of a smart card from the smart card reader depending upon the authentication mechanism employed by the user. In all cases, end-user Subscribers have an obligation to adequately protect their private key(s) in accordance with this CPS.

6.2.10 Method of Destroying Private Key

Where required, **TRUST ITALIA SPA** destroys CA private keys in a manner that reasonably ensures that there are no residuals remains of the key that could lead to the reconstruction of the key. **TRUST ITALIA SPA** utilizes the zeroization function of its hardware cryptographic modules and other appropriate means to ensure the complete destruction of CA private keys. When performed, CA key destruction activities are logged. The private key associated with an ACS Application ID is deleted immediately after it has been used for code signing.

6.2.11 Cryptographic Module Rating

See Section 6.2.1

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

TRUST ITALIA SPA CA, RA and end-user Subscriber Certificates are backed up and archived as part of **TRUST ITALIA SPA**'s routine backup procedures.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The Operational Period of a Certificate ends upon its expiration or revocation. The Operational Period for key pairs is the same as the Operational Period for the associated Certificates, except that they may continue to be used for decryption and signature verification. The maximum Operational Periods for **TRUST ITALIA SPA** Certificates for Certificates issued on or after the effective date of this CPS are set forth in Table 8 below. End user Subscriber Certificates that are renewals of existing subscriber certificates may have a longer validity period (up to 3 months).

In addition, **TRUST ITALIA SPA** CAs stop issuing new Certificates at an appropriate date prior to the expiration of the CA's Certificate such that no Certificate issued by a Subordinate CA expires after the expiration of any Superior CA Certificates.

Certificate Issued By:	***Validity Period***
PCA self-signed (2048 bit RSA)	Up to 25 years
PCA self-signed (256 bit ECC)	Up to 25 years
PCA self-signed (384 bit ECC)	Up to 25 years
PCA to Offline intermediate CA	Up to 15 years
PCA to online CA	Up to 15 years
Offline intermediate CA to online CA	Up to 15 years

[15] The Symantec Onsite Administrator CA-Level 3 has a validity beyond 10 years to support legacy systems and shall be revoked when appropriate

[16] If 6-year end-user subscriber certificates are issued, the online CA certificate's operational period will be 10 years with no option to renew. CA re-key will be required after 5 years.

Certificate Issued By:	*Validity Period*
Online CA to End-user Individual Subscriber	Normally up to 3 years, but under the conditions described below, up to 6 years[17] with no option to renew or re-key. After 6 years new enrollment is required.
Online CA to End-Entity Organizational Subscriber	Normally up to 3 years.

Table 8 – Certificate Operational Periods

Except as noted in this section, **TRUST ITALIA SPA** Sub-domain Participants shall cease all use of their key pairs after their usage periods have expired.

Certificates issued by CAs to end-user Subscribers may have Operational Periods longer than three years, up to six years, if the following requirements are met:

- Protection of the Subscriber key pairs in relation to its operational environment for Organizational Certificates, operation within the enhanced protection of a data center and for Individual Certificates, the Subscribers' key pairs reside on a hardware token, such as a smart card,
- Subscribers are required to undergo re-authentication at least every 3 years under Section 3.2.3,
- Subscribers shall prove possession of the private key corresponding to the public key within the Certificate at least every 25 months under Section 3.2.3,
- If a Subscriber is unable to complete re-authentication procedures successfully or is unable to prove possession of such private key when required by the foregoing, the CA shall revoke the Subscriber's Certificate.

The validity interval of an OCSP response is the difference in time between the thisUpdate and nextUpdate field, inclusive. For purposes of computing differences, a difference of 3,600 seconds shall be equal to one hour, and a difference of 86,400 seconds shall be equal to one day

[17] If 6-year end-user subscriber certificates are issued, the online CA certificate's operational period will be 10 years with no option to renew. CA re-key will be required after 5 years.

[19] At a minimum, the Distinguished Name of certificates issued with a validity of more than 3 years is re-verified after three years from date of certificate issuance. With the exception of the Symantec Automated Administration certificate, Organizational end-entity certificates used solely to support the operation of a portion of the STN may be issued with a validity period of 5 years and up to a maximum of 10 years after renewal.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

Activation data (Secret Shares) used to protect tokens containing **TRUST ITALIA SPA** CA private keys is generated in accordance with the requirements of CPS § 6.2.2 and the Key Ceremony Reference Guide. The creation and distribution of Secret Shares is logged.

RAs are required to select strong passwords to protect their private keys. TRUST ITALIA's password selection guidelines require that passwords:

- be generated by the user;
- have at least fifteen characters;
- have at least one alphabetic and one numeric
- character; have at least one lower-case letter;
- not contain many occurrences of the same character;
- not be the same as the operator's profile name;
- and not contain a long substring of the user's profile name.

TRUST ITALIA SPA strongly recommends that Enterprise Administrators, RAs, and end-user Subscribers choose passwords that meet the same requirements. **TRUST ITALIA SPA** also recommends the use of two factor authentication mechanisms (e.g., token and passphrase, biometric and token, or biometric and passphrase) for private key activation.

6.4.2 Activation Data Protection

TRUST ITALIA SPA Shareholders are required to safeguard their Secret Shares and sign an agreement acknowledging their Shareholder responsibilities.

TRUST ITALIA SPA RAs are required to store their Administrator/RA private keys in encrypted form using password protection and their browser's "high security" option.

TRUST ITALIA SPA strongly recommends that Client Administrators, RAs and end-user Subscribers store their private keys in encrypted form and protect their private keys through the use of a hardware token and/or strong passphrase. The use of two factor authentication mechanisms (e.g., token and passphrase, biometric and token, or biometric and passphrase) is encouraged.

6.4.3 Other Aspects of Activation Data

6.4.3.1 Activation Data Transmission

To the extent activation data for private keys are transmitted, Sub-domain Participants shall protect the transmission using methods that protect against the loss, theft, modification, unauthorized disclosure, or unauthorized use of such private keys. To the extent Windows or network logon user name/password combination is used as activation data for an end-user Subscriber, the passwords transferred across a network shall be protected against access by unauthorized users.

6.4.3.2 Activation Data Destruction

Activation data for CA private keys shall be decommissioned using methods that protect against the loss, theft, modification, unauthorized disclosure, or unauthorized use of the private keys protected by such activation data. After the record retention periods in Section 5.5.2 lapse, **TRUST ITALIA SPA** shall decommission activation data by overwriting and/or physical destruction.

6.5 Computer Security Controls

TRUST ITALIA SPA performs all CA and RA functions using Trustworthy Systems that meet the requirements of DigiCert's Certification Practice Statement.

6.5.1 Specific Computer Security Technical Requirements

TRUST ITALIA SPA ensures that the systems maintaining CA software and data files are Trustworthy Systems secure from unauthorized access. In addition, **TRUST ITALIA SPA** limits access to production servers to those individuals with a valid business reason for such access. General application users do not have accounts on production servers.

TRUST ITALIA SPA's production network is logically separated from other components. This separation prevents network access except through defined application processes. **TRUST ITALIA SPA** uses firewalls to protect the production network from internal and external intrusion and limit the nature and source of network activities that may access production systems.

TRUST ITALIA SPA requires the use of passwords that have a minimum character length and a combination of alphanumeric and special characters. **TRUST ITALIA SPA** requires that passwords be changed on a periodic basis.

Direct access to **TRUST ITALIA SPA** databases supporting **TRUST ITALIA SPA**'s CA Operations is limited to Trusted Persons in **TRUST ITALIA SPA**'s Production Operations group having a valid business reason for such access.

6.5.2 Computer Security Rating

No stipulation.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

Applications are developed and implemented by DigiCert in accordance with DigiCert systems development and change management standards. **TRUST ITALIA SPA** provides DigiCert software to its Enterprise Customers for performing RA and certain CA functions. Such software is developed in accordance with DigiCert system development standards. DigiCert developed software, when first loaded, provides a method to verify that the software on the system originated from DigiCert or **TRUST ITALIA SPA**, has not been modified prior to installation, and is the version intended for use.

6.6.2 Security Management Controls

DigiCert as mechanisms and/or policies in place to control and monitor the configuration of its CA systems. DigiCert creates a hash of all software packages and DigiCert software updates. This hash is used to verify the integrity of such software manually. Upon installation and periodically thereafter, DigiCert validates the integrity of its CA systems.

6.6.3 Life Cycle Security Controls

No stipulation

6.7 Network Security Controls

TRUST ITALIA SPA performs all its CA and RA functions using networks secured in accordance with **TRUST ITALIA SPA** internal security policies to prevent unauthorized access and other malicious activity. These documents are available upon request by qualified auditors in accordance with section 8.2 of this CPS or customer under appropriate legal agreements. **TRUST ITALIA SPA** protects its communications of sensitive information through the use of encryption and digital signatures.

6.8 Time-Stamping

Certificates, CRLs, and other revocation database entries shall contain time and date information. Such time information need not be cryptographic-based.

7. Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

TRUST ITALIA SPA uses the ITU X.509, version 3 standard to construct digital Certificates. **TRUST ITALIA SPA** generates non-sequential Certificate serial numbers (positive numbers greater than zero) that contain at least 64 bits of output from a CSPRNG.

7.1.1 Version Number(s)

TRUST ITALIA SPA Certificates are X.509 Version 3 Certificates although certain Root Certificates are permitted to be X.509 Version 1 Certificates to support legacy systems. CA certificates shall be X.509 Version 1 or Version 3 CA Certificates. End-user Subscriber Certificates shall be X.509 Version 3.

7.1.2 Certificate Extensions

TRUST ITALIA SPA populates X.509 Version 3 Certificates with the extensions required by Section 7.1.2.1-7.1.2.8. Private extensions are permissible, but the use of private extensions is not warranted under the DigiCert CP and the applicable CPS unless specifically included by reference. For, Subordinate CA, and Subscriber certificates used for publicly-trusted certificates, TRUST ITALIA SPA will abide by section 7.1.2 of the Baseline Requirements and configure the Certificate extensions to those requirements.

7.1.2.1 Key Usage

X.509 Version 3 Certificates are generally populated in accordance with RFC 5280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, April 2002. The criticality field of the KeyUsage extension is generally set to TRUE for CA certificates and may be set to either TRUE, or FALSE for end entity Subscriber certificates.

7.1.2.2 Certificate Policies Extension

CertificatePolicies extension of X.509 Version 3 Certificates are populated with the object identifier for the DigiCert CP in accordance with CP Section 7.1.6 and with policy qualifiers set forth in the DigiCert CP Section 7.1.8. The criticality field of this extension shall be set to FALSE.

7.1.2.3 Subject Alternative Names

The *subjectAltName* extension of X.509 Version 3 Certificates are populated in accordance with RFC5280 with the exception of those issued under Public Lite accounts which may optionally exclude the email address in *SubjectAltName*. The criticality field of this extension shall be set to
FALSE.

7.1.2.4 Basic Constraints

TRUST ITALIA SPA X.509 Version 3 CA Certificates *BasicConstraints* extension shall have the CA field set to TRUE.End-user Subscriber Certificates *BasicConstraints* extension shall have the CA field set to FALSE. The criticality field of this extension shall be set to TRUE for CA Certificates.

TRUST ITALIA SPA X.509 Version 3 CA Certificates shall have a "*pathLenConstraint*" field of the *BasicConstraints* extension set to the maximum number of CA certificates that may follow this Certificate in a certification path. CA Certificates issued to an online Enterprise Customer issuing end- user Subscriber Certificates shall have a "*pathLenConstraint*" field set to a value of "0" indicating that only an end-user

Subscriber Certificate may follow in the certification path.

7.1.2.5 Extended Key Usage

Certificates must contain the ExtendedKeyUsage extension, aligning to Application Software Supplier granted trust bits and private PKI use cases.
TRUST ITALIA SPA never includes in any publicly-trusted certificate:

- id-kp-serverAuth;
- id-kp-codeSigning
- id-kp-timeStamping

Publicy trusted Subscriber Certificates may not contain the anyEKU value and id-kp-clientAuth must be present. Id-kp-clientAut may be present.
Subordinate CA Certificates created after January 1, 2019 for publicly trusted certificates, with the exception of cross-certificates that share a private key with a corresponding root certificate:

- will contain an EKU extension;
- and cannot include the anyExtendedKeyUsage KeyPurposeId,

..

Technically Constrained Subordinate CA Certificates include an Extended Key Usage (EKU) extension specifying all extended key usages for which the Subordinate CA Certificate is authorized to issue certificates. The anyExtendedKeyUsage KeyPurposeId does not appear in the EKU extension of publicly trusted certificates. id-kp-clientAuth and. Id-kp-clientAut may be both present

7.1.2.6 CRL Distribution Points

Most **TRUST ITALIA SPA** X.509 Version 3 end user Subscriber Certificates and Intermediate CA Certificates include the *cRLDistributionPoints* extension containing the URL of the location where a Relying Party can obtain a CRL to check the CA Certificate's status. The criticality field of this extension is set to FALSE.

7.1.2.7 Authority Key Identifier

TRUST ITALIA SPA generally populates the Authority Key Identifier extension of X.509 Version 3 end user Subscriber Certificates and Intermediate CA Certificates. When the certificate issuer contains the Subject Key Identifier extension, the Subject Key Identifier is used as Authority Key Identifier extension. Otherwise, the Authority Key Identifier extension includes the issuing CA's subject distinguished name and serial number. The criticality field of this extension is set to FALSE.

7.1.2.8 Subject Key Identifier

Where **TRUST ITALIA SPA** populates X.509 Version 3 Certificates with a *subjectKeyIdentifier* extension, the *keyIdentifier* based on the public key of the Subject of the Certificate is generated in accordance with one of the methods described in RFC5280. Where this extension is used, the criticality field of this extension is set to FALSE.

7.1.2.9 Authority Information Access

In case a Root CA or a Subordinate CA support and serve OCSP, *authorityInformationAccess* extension must be present into Subscriber Certificate and must contain the HTTP URL of the Issuing CA's OCSP responder and should also contain the HTTP URL of the Issuing CA's Certificate.

In case a Root CA or a Subordinate CA does not support or serve OCSP, *authorityInformationAccess* extension may be present into Subscriber Certificate, and must contain HTTP URL of the Issuing CA's Certificate

For Subordinate CA certificates, the extension must be present and must not be marked critical. It should contain the HTTP URL of the Issuing CA's certificate and it may contain the HTTP URL of the Issuing CA's OCSP responder.

7.1.3 Algorithm Object Identifiers

TRUST ITALIA SPA Certificates are signed using one of following algorithms.

- ***sha-1WithRSAEncryption*** OBJECT IDENTIFIER ::={iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1(1) 5}
- ***sha256withRSAEncryption*** OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}

Publicly-trusted certificates, Trust Italia are not signed with *sha-1WithRSAEncryption* and uses the keys and hash algorithms specified in the CAB forum baseline requirements.

Certificate signatures produced using these algorithms shall comply with RFC 3279

7.1.4 Name Forms

TRUST ITALIA SPA populates Certificates with an Issuer Name and Subject Distinguished Name in accordance with Section 3.1.1. The Issuer Name shall be populated in each Certificate issued containing the Country, Organization Name and the Common Name of the Issuer CA. Issuer DNs meet the requirements in the CAB forum baseline requirements.

In addition, **TRUST ITALIA SPA** may include within end-user Subscriber Certificates an additional Organizational Unit field that contains a notice stating that the terms of use of the Certificate are set forth in a URL which is a pointer to the applicable Relying Party Agreement. Exceptions to the foregoing requirement are permitted only when space, formatting, or interoperability limitations within Certificates make such an Organizational Unit impossible to use in conjunction with the application for which the Certificates are intended, or if a pointer to the applicable Relying Party Agreement is included in the policy extension of the certificate.

7.1.5 Name Constraints

TRUST ITALIA SPA may include name constraints in the nameConstraints field when appropriate.

7.1.5.1 Name-Constrained emailProtection CAs

If the technically constrained Subordinate CA certificate includes the id-kp-emailProtection extended key usage, it also includes the Name Constraints X.509v3 extension with constraints on rfc822Name, with at least one name in permittedSubtrees, each such name having its ownership validated according to section 3.2.2.4 of the Baseline Requirements.

7.1.6 Certificate Policy Object Identifier

Where the Certificate Policies extension is used, Certificates contain the object identifier for the Certificate Policy corresponding to the appropriate Class or Level of Certificate as set forth in the DigiCert CP Section 1.2. For legacy Certificates issued prior to the publication of the DigiCert CP which include the Certificate Policies extension, Certificates refer to the deprecated STN CPS contained in the DigiCert Legal Repository in the archive section.

7.1.7 Usage of Policy Constraints Extension

No stipulation

7.1.8 Policy Qualifiers Syntax and Semantics

TRUST ITALIA SPA generally populates X.509 Version 3 Certificates with a policy qualifier within the Certificate Policies extension. Generally, such Certificates contain a CPS pointer qualifier that points to the applicable Relying Party Agreement or the **TRUST ITALIA SPA** CPS. In addition, some Certificates contain a User Notice Qualifier which points to the applicable Relying Party Agreement.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No stipulation

7.2 CRL Profile

As applicable to the Certificate type, corresponding CRLs conform to the current version of the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates.

For revoked issuing CAs, the CRLReason indicated cannot be unspecified (0) or certificateHold(6). If the reason for revocation is unspecified, **TRUST ITALIA SPA** will omit the reasonCode entry extension, when not technically not capable of issuance.

If a reasonCode CRL entry extension is present, the CRLReason must indicate the most appropriate reason for revocation of the certificate. **TRUST ITALIA SPA** specifies the following reason codes from RFC 5280, section 5.3.1 as appropriate for most instances when used in accordance with the practices in this section and this CPS:

- Unspecified (0)[2]
- KeyCompromise (1)
- CACompromise (2)
- AffiliationChanged (3)
- Superseded (4)[3]
- CessationOfOperation (5)[4]

Version 2 CRLs conform to RFC 5280 and contain the basic fields and contents specified in Table 13 below:

Field	Value or Value constraint
Version	See Section 7.2.1.
Signature Algorithm	sha-256WithRSAEncryption [1 2 840 113549 1 1 11]
Issuer	Entity who has signed and issued the CRL.
This Update	Issue date of the CRL. CRLs are effective upon issuance.
Next Update	Date by which the next CRL will be issued. CRL issuance frequency is in accordance with the requirements of Section 4.4.7.
Revoked Certificates	Listing of revoked certificates, including the Serial Number of the revoked Certificate and the Revocation Date.

Table 13 – CRL Profile Basic Fields

[2] Reason code (0)_unspecified is only used if it is omitted from the CRL and OCSP in accordance with the baseline requirements

[3] When a reason code is not specified, TrustItalia will log the revocation as (4) superseded or (5) Cessation of Operation.

[4] When a reason code is not specified, TrustItalia will log the revocation as (4) superseded or (5) Cessation of Operation.

7.2.1 Version Number(s)

TRUST ITALIA SPA supports both X.509 Version1 and Version 2 CRLs. Version 2 CRLs comply with the requirements of RFC 5280.

7.2.2 CRL and CRL Entry Extensions

CRLs have the following extensions:

Extension	Value
CRL Number	Never repeated monotonically increasing integer
Authority Key Identifier	Same as the Authority Key Identifier listed in the Certificate
Invalidity Date	Optional date in UTC format
Reason Code	Appropriate reason for revocation from list in section 7.2, unless permitted to be omitted.

7.3 OCSP Profile

If an OCSP response is for a Root CA or Subordinate CA Certificate, including Cross Certificates, and that certificate has been revoked, then the revocationReason field within the RevokedInfo of the CertStatus is present and asserted.

The CRLReason indicated contains a value permitted for CRLs, as specified in Section 7.2.2.

7.3.1 Version Number(s)

TRUST ITALIA SPA's OCSP responders conform to version 1 of RFC 6960.

7.3.2 OCSP Extensions

The singleExtension of an OCSP response cannot contain the reasonCode (OID 2.5.29.21) CRL entry extension.

8. Compliance Audit and Other Assessments

The practices in this CPS are designed to meet or exceed the requirements of generally accepted industry standards, including the latest versions of Mozilla Root Store policy and other programs listed in section 1.1 and 1.6.3.

An annual ETSI 319 411-1 at the most current version available at the point of the audit that is required by external requirements examination is performed for **TRUST ITALIA SPA**'s data center operations and key management operations supporting **TRUST ITALIA SPA**'s public and Managed PKI CA services including the DigiCert Root CAs, Level 2 Organizational and Individual CAs, and Level 1 Individual CAs specified in Section 1.3.1.

Customer-specific CAs not issuing public trusted certificates are not specifically audited as part of the audit of **TRUST ITALIA SPA**'s operations unless required by the Customer. **TRUST ITALIA SPA** shall be entitled to require that Enterprise Customers undergo a compliance audit under this CPS and audit programs for these types of Customers.

8.1 Frequency and Circumstances of Assessment

Compliance Audits are conducted at least annually at the sole expense of the audited entity. Audits are conducted over unbroken sequences of audit periods with each period no longer than one year duration.

8.2 Identity/Qualifications of Assessor

Auditors must meet the requirements of Section 8.2 of the CA/Browser Baseline Requirements.

8.3 Assessor's Relationship to Assessed Entity

TRUST ITALIA SPA's auditor does not have a financial interest, business relationship, or course of dealing that could foreseeably create a significant bias for or against **TRUST ITALIA SPA**.

8.4 Topics Covered by Assessment

The scope of TRUST ITALIA SPA's annual audit includes CA environmental controls, key management operations and Infrastructure/Administrative CA controls, certificate life cycle management and CA business practices disclosure.
The audit verifies that **TRUST ITALIA SPA** is compliant with this CPS.

8.5 Actions Taken as a Result of Deficiency

If an audit reports a material noncompliance with applicable law, this CPS, or any other contractual obligations related to **TRUST ITALIA SPA**'s services, then (1) the auditor will document the discrepancy, (2) the auditor will promptly notify **TRUST ITALIA SPA**, and (3) **TRUST ITALIA SPA** will develop a plan to cure the noncompliance. **TRUST ITALIA SPA** will submit the plan to any third party that **TRUST ITALIA SPA** is legally obligated to satisfy. **TRUST ITALIA SPA** is entitled to suspend and/or terminate of services through revocation or other actions as needed to address the non-compliant Issuer CA.

8.6 Communications of Results

The results of each audit are reported to any third party entities which are entitled by law, regulation, or agreement to receive a copy of the audit results.

TRUST ITALIA SPA makes its annual Audit Report publicly available no later than three (3) months after the end of the audit period. In the event of a delay greater than three months, **TRUST ITALIA SPA** shall provide an explanatory letter signed by the Qualified Auditor. A copy of **TRUST ITALIA SPA**'s ETSI 319 411-

1 at the most current version available at the point of the audit that is required by external requirements audit report can be found at https://www.trustitalia.it/documenti under section “Assessment”.

9. Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

TRUST ITALIA SPA, is entitled to charge end-user Subscribers for the issuance, management, and renewal of Certificates.

9.1.2 Certificate Access Fees

TRUST ITALIA SPA does not charge a fee as a condition of making a Certificate available in a repository or otherwise making Certificates available to Relying Parties.

9.1.3 Revocation or Status Information Access Fees

TRUST ITALIA SPA does not charge a fee as a condition of making the CRLs required by the DigiCert CP available in a repository or otherwise available to Relying Parties. **TRUST ITALIA SPA** is, however, entitled to charge a fee for providing customized CRLs, OCSP services, or other value-added revocation and status information services. **TRUST ITALIA SPA** does not permit access to revocation information, Certificate status information, or time stamping in their repositories by third parties that provide products or services that utilize such Certificate status information without **TRUST ITALIA SPA**'s prior express written consent.

9.1.4 Fees for Other Services

TRUST ITALIA SPA does not charge a fee for access to this CPS. Any use made for purposes other than simply viewing the document, such as reproduction, redistribution, modification, or creation of derivative works, shall be subject to a license agreement with the entity holding the copyright to the document.

9.1.5 Refund Policy

TRUST ITALIA SPA adheres to, and stands behind, rigorous practices and policies in undertaking certification operations and in issuing certificates. Nevertheless, if for any reason a subscriber is not completely satisfied with the certificate issued to him, her, or it, the subscriber may request that **TRUST ITALIA SPA** revoke the certificate within thirty (30) days of issuance and provide the subscriber with a refund. Following the initial thirty (30) day period, a subscriber may request that **TRUST ITALIA SPA** revoke the certificate and provide a refund if **TRUST ITALIA SPA** has breached a warranty or other material obligation under this CPS relating to the subscriber or the subscriber's certificate. All details about refund policies are described in Subscriber Agreement and General Term and Conditions available at **TRUST ITALIA SPA** website.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

Enterprise Customers are encouraged to maintain a commercially reasonable level of insurance coverage for errors and omissions, either through an errors and omissions insurance program with an insurance carrier or a self-insured retention. **TRUST ITALIA SPA** maintains such errors and omissions insurance coverage.

9.2.2 Other Assets

Enterprise Customers shall have sufficient financial resources to maintain their operations and perform their duties, and they must be reasonably able to bear the risk of liability to Subscribers and Relying

Parties. **TRUST ITALIA SPA**'s financial resources are set forth in disclosures.

9.2.3 Extended Warranty Coverage

No stipulation

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

The following records of Subscribers shall, subject to Section 9.3.2, be kept confidential and private ("Confidential/Private Information"):

- CA application records, whether approved or disapproved,
- Certificate Application records,
- Private keys held by enterprise Customers using Managed PKI Key Manager and information needed to recover such Private Keys,
- Transactional records (both full records and the audit trail of transactions),
- Audit trail records created or retained by TRUST ITALIA SPA or a
- Customer, Audit reports created by TRUST ITALIA SPA or a Customer (to the extent such reports are maintained), or their respective auditors (whether internal or public),
- Audit logs and archive records
- Contingency planning and disaster recovery plans, and
- Security measures controlling the operations of TRUST ITALIA SPA hardware and software and

the administration of Certificate services and designated enrollment services.

9.3.2 Information Not Within the Scope of Confidential Information

Certificates, Certificate revocation and other status information, **TRUST ITALIA SPA** repositories and information contained within them are not considered Confidential/Private Information.

Information not expressly deemed Confidential/Private Information under Section 9.3.1 shall be considered neither confidential nor private. This section is subject to applicable privacy laws.

9.3.3 Responsibility to Protect Confidential Information

TRUST ITALIA SPA secures private information from compromise and disclosure to third parties. Employees receive training on how to handle confidential information

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

TRUST ITALIA SPA has implemented a privacy policy, which is located at: www.trustitalia.it

9.4.2 Information Treated as Private

Any information about Subscribers that is not publicly available through the content of the issued certificate, certificate directory and online CRLs is treated as private.

9.4.3 Information Not Deemed Private

Subject to local laws, all information made public in a certificate and CRL is deemed not private.

9.4.4 Responsibility to Protect Private Information

TRUST ITALIA SPA employees and contractors are expected to handle personal information in strict confidence and meet the requirements of GDPR and of Italian Privacy law concerning the protection of personal data. All sensitive information is securely stored and protected against accidental disclosure..

9.4.5 Notice and Consent to Use Private Information

Unless where otherwise stated in this CPS, the applicable Privacy Policy or by agreement, private information will not be used without the consent of the party to whom that information applies. This section is subject to applicable privacy laws.
All Subscribers must consent to the global transfer and publication of any personal data contained in a Certificate.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

TRUST ITALIA SPA shall be entitled to disclose Confidential/Private Information if, in good faith, **TRUST ITALIA SPA** believes that:

- disclosure is necessary in response to subpoenas and search warrants.
- disclosure is necessary in response to judicial, administrative, or other legal process during the discovery process in a civil or administrative action, such as subpoenas, interrogatories, requests for admission, and requests for production of documents.

This section is subject to applicable privacy laws.

9.4.7 Other Information Disclosure Circumstances

No stipulation

9.5 Intellectual Property rights

The allocation of Intellectual Property Rights among **TRUST ITALIA SPA** Sub-domain Participants other than Subscribers and Relying Parties is governed by the applicable agreements among such **TRUST ITALIA SPA** Sub-domain Participants. The following subsections of Section 9.5 apply to the Intellectual Property Rights in relation to Subscribers and Relying Parties.

9.5.1 Property Rights in Certificates and Revocation Information

CAs retain all Intellectual Property Rights in and to the Certificates and revocation information that they issue. **TRUST ITALIA SPA** and Customers grant permission to reproduce and distribute Certificates on a nonexclusive royalty-free basis, provided that they are reproduced in full and that use of Certificates is subject to the Relying Party Agreement referenced in the Certificate. **TRUST ITALIA SPA** and Customers shall grant permission to use revocation information to perform Relying Party functions subject to the applicable CRL Usage Agreement, Relying Party Agreement, or any other applicable agreements.

9.5.2 Property Rights in the CPS

Sub-domain Participants acknowledge that **TRUST ITALIA SPA** retains all Intellectual Property Rights in and to this CPS.

9.5.3 Property Rights in Names

A Certificate Applicant retains all rights it has (if any) in any trademark, service mark, or trade name contained in any Certificate Application and distinguished name within any Certificate issued to such Certificate Applicant.

9.5.4 Property Rights in Keys and Key Material

Key pairs corresponding to Certificates of CAs and end-user Subscribers are the property of the CAs and end-user Subscribers that are the respective Subjects of these Certificates, subject to the rights of

enterprise Customers using Managed PKI Key Manager, regardless of the physical medium within which they are stored and protected, and such persons retain all Intellectual Property Rights in and to these key pairs. Without limiting the generality of the foregoing, DigiCert's Root public keys and the Root Certificates containing them, including all PCA public keys and self-signed Certificates, are the property of DigiCert. DigiCert licenses software and hardware manufacturers to reproduce such root Certificates to place copies in trustworthy hardware devices or software. Finally, Secret Shares of a CA's private key are the property of the CA, and the CA retains all Intellectual Property Right in and to such Secret Shares even though they cannot obtain physical possession of the those shares or the CA from DigiCert.

9.5.5 Violation of Property Rights

Issuer CAs shall not knowingly violate the intellectual property rights of any third party.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

TRUST ITALIA SPA warrants that:

- There are no material misrepresentations of fact in the Certificate known to or originating from the entities approving the Certificate Application or issuing the Certificate,
- There are no errors in the information in the Certificate that were introduced by the entities approving the Certificate Application or issuing the Certificate as a result of a failure to exercise reasonable care in managing the Certificate Application or creating the Certificate,
- Their Certificates meet all material requirements of this CPS, and
- Revocation services and use of a repository conform to the applicable CPS in all material aspects.

Subscriber Agreements may include additional representations and warranties.

9.6.2 RA Representations and Warranties

RAs warrant that:

- There are no material misrepresentations of fact in the Certificate known to or originating from the entities approving the Certificate Application or issuing the Certificate,
- There are no errors in the information in the Certificate that were introduced by the entities approving the Certificate Application as a result of a failure to exercise reasonable care in managing the Certificate Application,
- Their Certificates meet all material requirements of this CPS, and
- Revocation services (when applicable) and use of a repository conform to the applicable CPS in all material aspects.

Subscriber Agreements may include additional representations and warranties.

9.6.3 Subscriber Representations and Warranties

Subscribers warrant that:

- Each digital signature created using the private key corresponding to the public key listed in the Certificate is the digital signature of the Subscriber and the Certificate has been accepted and is operational (not expired or revoked) at the time the digital signature is created,
- Their private key is protected and that no unauthorized person has ever had access to the Subscriber's private key,
- All representations made by the Subscriber in the Certificate Application the Subscriber submitted are true,
- All information supplied by the Subscriber and contained in the Certificate is true,
- The Certificate is being used exclusively for authorized and legal purposes, consistent with this CPS, and

- The Subscriber is an end-user Subscriber and not a CA, and is not using the private key corresponding to any public key listed in the Certificate for purposes of digitally signing any Certificate (or any other format of certified public key) or CRL, as a CA or otherwise.

Subscriber Agreements may include additional representations and warranties.

9.6.4 Relying Party Representations and Warranties

Relying Party Agreements require Relying Parties to acknowledge that they have sufficient information to make an informed decision as to the extent to which they choose to rely on the information in a Certificate, that they are solely responsible for deciding whether or not to rely on such information, and that they shall bear the legal consequences of their failure to perform the Relying Party obligations in terms of this CPS.

Relying Party Agreements may include additional representations and warranties.

9.6.5 Representations and Warranties of Other Participants

No stipulation

9.7 Disclaimers of Warranties

TRUST ITALIA SPA does not guarantee the availability of any products or services and may modify or discontinue any product or service offering at any time. To the extent permitted by applicable law, Subscriber Agreements and Relying Party Agreements shall disclaim **TRUST ITALIA SPA**'s possible warranties, including any warranty of merchantability or fitness for a particular purpose.

9.8 Limitations of Liability

To the extent **TRUST ITALIA SPA** has issued and managed the Certificate(s) at issue in compliance with the DigiCert Certificate Policy and the **TRUST ITALIA SPA** Certification Practice Statement, **TRUST ITALIA SPA** shall have no liability to the Subscriber, any Relying Party, or any other third parties for any damages or losses suffered as a result of the use or reliance on such Certificate(s). To the extent permitted by applicable law, Subscriber Agreements and Relying Party Agreements shall limit **TRUST ITALIA SPA**'s liability. Limitations of liability shall include an exclusion of indirect, special, incidental, and consequential damages.

The liability (and/or limitation thereof) of Subscribers are detailed in Subscriber Agreement and General Term and Conditions available on **TRUST ITALIA SPA** website.

The liability (and/or limitation thereof) of enterprise RAs and the applicable CA shall be set out in the agreement(s) between them.

The liability (and/or limitation thereof) of Relying Parties shall be as set forth in the applicable Relying Party Agreements.

9.9 Indemnities

9.9.1 Indemnification by Subscribers

To the extent permitted by applicable law, Subscribers are required to indemnify **TRUST ITALIA SPA** for:

- Falsehood or misrepresentation of fact by the Subscriber on the Subscriber's Certificate Application,
- Failure by the Subscriber to disclose a material fact on the Certificate Application, if the misrepresentation or omission was made negligently or with intent to deceive any party,
- The Subscriber's failure to protect the Subscriber's private key, to use a Trustworthy System, or to otherwise take the precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorized use of the Subscriber's private key, or

- The Subscriber's use of a name (including without limitation within a common name, domain name, or e-mail address) that infringes upon the Intellectual Property Rights of a third party.

The applicable Subscriber Agreement and General Term and Conditions may include additional indemnity obligations.

9.9.2 Indemnification by Relying Parties

To the extent permitted by applicable law, Relying Party Agreements shall require Relying Parties to indemnify **TRUST ITALIA SPA** for:

- The Relying Party's failure to perform the obligations of a Relying Party,
- The Relying Party's reliance on a Certificate that is not reasonable under the circumstances, or
- The Relying Party's failure to check the status of such Certificate to determine if the Certificate is expired or revoked.

The applicable Relying Party Agreement may include additional indemnity obligations.

9.9.3 Indemnification of Application Software Suppliers

Notwithstanding any limitations on its liability to Subscribers and Relying Parties, the CA understands and acknowledges that the Application Software Suppliers who have a Root Certificate distribution agreement in place with the DigiCert Root CA do not assume any obligation or potential liability of the CA under these Requirements or that otherwise might exist because of the issuance or maintenance of Certificates or reliance thereon by Relying Parties or others.

Thus the CA shall defend, indemnify, and hold harmless each Application Software Supplier for any and all claims, damages, and losses suffered by such Application Software Supplier related to a Certificate issued by the CA, regardless of the cause of action or legal theory involved. This does not apply, however, to any claim, damages, or loss suffered by such Application Software Supplier related to a Certificate issued by the CA where such claim, damage, or loss was directly caused by such Application Software Supplier's software displaying as not trustworthy a Certificate that is still valid, or displaying as trustworthy: (1) a Certificate that has expired, or (2) a Certificate that has been revoked (but only in cases where the revocation status is currently available from the CA online, and the application software either failed to check such status or ignored an indication of revoked status).

9.10 Term and Termination

9.10.1 Term

The CPS becomes effective upon publication in the **TRUST ITALIA SPA** repository. Amendments to this CPS become effective upon publication in the **TRUST ITALIA SPA** repository.

9.10.2 Termination

This CPS as amended from time to time shall remain in force until it is replaced by a new version.

9.10.3 Effect of Termination and Survival

Upon termination of this CPS, **TRUST ITALIA SPA** sub-domain participants are nevertheless bound by its terms for all certificates issued for the remainder of the validity periods of such certificates.

9.11 Individual Notices and Communications with Participants

TRUST ITALIA SPA accepts notices related to this CPS at the locations specified in Section 2.2. Notices are

deemed effective after the sender receives a valid and digitally signed acknowledgment of receipt from **TRUST ITALIA SPA**. If an acknowledgement of receipt is not received within five days, the sender must resend the notice in paper form to the street address specified in Section 2.2 using either a courier service that confirms delivery or via certified or registered mail with postage prepaid and return receipt requested. **TRUST ITALIA SPA** may allow other forms of notice in its Subscriber Agreements.

TRUST ITALIA SPA will notify DigiCert if:
1. Ownership or control of the CA certificates changes;
2. An organization other than the CA obtains control of an unconstrained intermediate certificate (as defined in section 5.3.2 of the Mozilla Root Store policy) that directly or transitively chains to sub-domain's included certificate(s);
3. Ownership or control of **TRUST ITALIA SPA**'s operations changes; or
4. There is a material change in **TRUST ITALIA SPA**'s operations (e.g., when the cryptographic hardware related to a certificate in Mozilla's root store is consequently moved from one secure location to another).

TRUST ITALIA SPA will notify DigiCert if the following occurs:

1. Revoking of an Intermediate certificate chaining up to DigiCert CA Roots is due for security concern;
2. A change in root store is due for security concern;
3. **TRUST ITALIA SPA** CAs fails to comply with the requirements or a contractual agreement.

9.12 Amendments

9.12.1 Procedure for Amendment

This CPS is reviewed annually. Amendments are made by posting an updated version of the CPS to the online repository. Updates supersede any designated or conflicting provisions of the referenced version of the CPS.

9.12.2 Notification Mechanism and Period

TRUST ITALIA SPA posts CPS revisions to its website. **TRUST ITALIA SPA** does not guarantee or set a notice-and-comment period and may make changes to this CPS without notice and without changing the version number

9.12.3 Circumstances under Which OID Must be Changed

No stipulation.

9.13 Dispute Resolution Provisions

9.13.1 Disputes among DigiCert, Affiliates, and Customers

Disputes among **TRUST ITALIA SPA** sub-domain participants shall be resolved pursuant to provisions in the applicable agreements among the parties.

9.13.2 Disputes with End-User Subscribers or Relying Parties

To the extent permitted by applicable law, Subscriber Agreements and Relying Party Agreements shall contain a dispute resolution clause. Disputes shall be resolved pursuant to provisions in the applicable agreements among the parties.

9.14 Governing Law

Subject to any limits appearing in applicable law, the laws of **Italy** shall govern the enforceability, construction, interpretation, and validity of this CPS, irrespective of contract or other choice of law provisions and without the requirement to establish a commercial nexus in **Italy**. This choice of law is

made to ensure uniform procedures and interpretation for all **TRUST ITALIA SPA** sub-domain participants, no matter where they are located.

This governing law provision applies only to this CPS. Agreements incorporating the CPS by reference may have their own governing law provisions, provided that this Section 9.14 governs the enforceability, construction, interpretation, and validity of the terms of the CPS separate and apart from the remaining provisions of any such agreements, subject to any limitations appearing in applicable law.

9.15 Compliance with Applicable Law

This CPS is subject to applicable national, state, local and foreign laws, rules, regulations, ordinances, decrees, and orders including, but not limited to, restrictions on exporting or importing software, hardware, or technical information. **TRUST ITALIA SPA** licenses its CAs in each jurisdiction that it operates where licensing is required by the law of such jurisdiction for the issuance of Certificates.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

No stipulation

9.16.2 Assignment

No stipulation

9.16.3 Severability

In the event that a clause or provision of this CPS is held to be unenforceable by a court of law or other tribunal having authority, the remainder of the CPS shall remain valid.

9.16.4 Enforcement (Attorney's Fees and Waiver of Rights)

No stipulation

9.16.5 Force Majeure

To the extent permitted by applicable law, Subscriber Agreements and Relying Party Agreements shall include a force majeure clause protecting DigiCert and **TRUST ITALIA SPA**.

9.17 Other Provisions

No stipulation

Appendix A. Table of Acronyms and definitions

Table of Acronyms

Term	Definition
AICPA	American Institute of Certified Public Accountants.
ANSI	The American National Standards Institute.
ACS	Authenticated Content Signing.
BIS	The United States Bureau of Industry and Science of the United States Department of Commerce.
CA	Certification Authority.
ccTLD	Country Code Top-Level Domain
CICA	Canadian Instituted of Chartered Accountants
CP	Certificate Policy.
CPS	Certification Practice Statement.
CRL	Certificate Revocation List.
DBA	Doing Business As
DNS	Domain Name System
FIPS	United State Federal Information Processing Standards.
FQDN	Fully Qualified Domain Name
ICC	International Chamber of Commerce.
IM	Instant Messaging
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ISO	International Organization for Standardization
KRB	Key Recovery Block.
LSVA	Logical security vulnerability assessment.
NIST	(US Government) National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol.
OID	Object Identifier
PCA	Primary Certification Authority.
PIN	Personal identification number.
PKCS	Public-Key Cryptography Standard.
PKI	Public Key Infrastructure.
PMA	Policy Management Authority.
RA	Registration Authority.
RFC	Request for comment.
SAR	Security and Audit Requirements
S/MIME	Secure multipurpose Internet mail extensions.
SSL	Secure Sockets Layer.
STN	Symantec Trust Network.
TLD	Top-Level Domain
TLS	Transport Layer Security
VOID	Voice Over Internet Protocol

Definitions

Term	Definition
Administrator	A Trusted Person within the organization of a Processing Center, Service Center, Managed PKI Customer, or Gateway Customer that performs validation and other CA or RA functions.
Administrator Certificate	A Certificate issued to an Administrator that may only be used to perform CA or RA functions.
Affiliate	A leading trusted third party, for example in the technology, telecommunications, or financial services industry, that has entered into an agreement with DigiCert to be a STN distribution and services channel within a specific territory. In the CAB Forum context, the term "*Affiliate*" refers to: A corporation, partnership, joint venture or other entity controlling, controlled by, or under common control with another entity, or an

Term	Definition
	agency, department, political subdivision, or any entity operating under the direct control of a Government Entity.
Affiliate Practices Legal Requirements Guidebook	A Symantec document setting forth requirements for Affiliate CPSs, agreements, validation procedures, and privacy policies, as well as other requirements that Affiliates must meet.
Affiliated Individual	A natural person that is related to a Managed PKI Customer, Managed PKI Lite Customer, or Gateway Customer entity (i) as an officer, director, employee, partner, contractor, intern, or other person within the entity, (ii) as a member of a DigiCert registered community of interest, or (iii) as a person maintaining a relationship with the entity where the entity has business or other records providing appropriate assurances of the identity of such person.
Applicant	The natural person or Legal Entity that applies for (or seeks renewal of) a Certificate. Once the Certificate issues, the Applicant is referred to as the Subscriber. For Certificates issued to devices, the Applicant is the entity that controls or operates the device named in the Certificate, even if the device is sending the actual certificate request.
Applicant Representative	A natural person or human sponsor who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant: (i) who signs and submits, or approves a certificate request on behalf of the Applicant, and/or (ii) who signs and submits a Subscriber Agreement on behalf of the Applicant, and/or (iii) who acknowledges and agrees to the Certificate Terms of Use on behalf of the Applicant when the Applicant is an Affiliate of the CA.
Application Software Supplier	A supplier of Internet browser software or other relying-party application software that displays or uses Certificates and incorporates Root Certificates.
Attestation Letter	A letter attesting that Subject Information is correct written by an accountant, lawyer, government official, or other reliable third party customarily relied upon for such information.
Audit Report	A report from a Qualified Auditor stating the Qualified Auditor's opinion on whether an entity's processes and controls comply with the mandatory provisions of these Requirements.
Applicant	The natural person or Legal Entity that applies for (or seeks renewal of) a Certificate. Once the Certificate issues, the Applicant is referred to as the Subscriber. For Certificates issued to devices, the Applicant is the entity that controls or operates the device named in the Certificate, even if the device is sending the actual certificate request.
Automated Administration	A procedure whereby Certificate Applications are approved automatically if enrollment information matches information contained in a database.
Automated Administration Software Module	Software provided by Symantec that performs Automated Administration.
Certificate	A message that, at least, states a name or identifies the CA, identifies the Subscriber, contains the Subscriber's public key, identifies the Certificate's Operational Period, contains a Certificate serial number, and is digitally signed by the CA.
Certificate Applicant	An individual or organization that requests the issuance of a Certificate by a CA.
Certificate Application	A request from a Certificate Applicant (or authorized agent of the Certificate Applicant) to a CA for the issuance of a Certificate.
Certificate Chain	An ordered list of Certificates containing an end-user Subscriber Certificate and CA Certificates, which terminates in a root Certificate.
Certificate Data	Certificate requests and data related thereto (whether obtained from the Applicant or otherwise) in the CA's possession or control or to which the CA has access.
Certificate Management Control Objectives	Criteria that an entity must meet in order to satisfy a Compliance Audit.
Certificate Management Process	Processes, practices, and procedures associated with the use of keys, software, and hardware, by which the CA verifies Certificate Data, issues Certificates, maintains a Repository, and revokes Certificates.
Certificate Policies (CP)	The "DigiCert Certificate Policy for Symantec Trust Network" and is the principal statement of policy governing the STN
Certificate Problem Report	Complaint of suspected Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to Certificates
Certificate Revocation List (CRL)	A periodically (or exigently) issued list, digitally signed by a CA, of identified Certificates that have been revoked prior to their expiration dates in accordance with CP § 3.4. The list generally indicates the CRL issuer's name, the date of issue, the date of the next scheduled CRL issue, the revoked Certificates' serial numbers, and the specific times and reasons for revocation.
Certificate Signing Request	A message conveying a request to have a Certificate issued.
Certification Authority (CA)	An entity authorized to issue, manage, revoke, and renew Certificates in the STN.
Certification Practice Statement (CPS)	A statement of the practices that DigiCert or an Affiliate employs in approving or rejecting Certificate Applications and issuing, managing, and revoking Certificates, and requires its Managed PKI Customers and Gateway Customers to employ.
Challenge Phrase	A secret phrase chosen by a Certificate Applicant during enrollment for a Certificate. When issued a Certificate, the Certificate Applicant becomes a Subscriber and a CA or RA can use the

Term	Definition
	Challenge Phrase to authenticate the Subscriber when the Subscriber seeks to revoke or renew the Subscriber's Certificate.
Client Service Center	A Service Center that is an Affiliate providing client Certificates either in the Consumer or Enterprise line of business.
Compliance Audit	A periodic audit that a Processing Center, Service Center, Managed PKI Customer, or Gateway Customer undergoes to determine its conformance with STN Standards that apply to it.
Compromise	A violation (or suspected violation) of a security policy, in which an unauthorized disclosure of, or loss of control over, sensitive information may have occurred. With respect to private keys, a Compromise is a loss, theft, disclosure, modification, unauthorized use, or other compromise of the security of such private key.
Confidential/Private Information	Information required to be kept confidential and private pursuant to CP § 2.8.1.
Cross Certificate	A certificate that is used to establish a trust relationship between two Root CAs.
CRL Usage Agreement	An agreement setting forth the terms and conditions under which a CRL or the information in it can be used.
Delegated Third Party	A natural person or Legal Entity that is not the CA but is authorized by the CA to assist in the Certificate Management Process by performing or fulfilling one or more of the CA requirements found herein.
Customer	An organization that is either a Managed PKI Customer, Gateway Customer, or ASB Customer.
Domain Authorization	Correspondence or other documentation provided by a Domain Name Registrant attesting to the authority of an Applicant to request a Certificate for a specific Domain Namespace.
Domain Name	The label assigned to a node in the Domain Name System.
Domain Namespace	The set of all possible Domain Names that are subordinate to a single node in the Domain Name System.
Domain Name Registrant	Sometimes referred to as the "owner" of a Domain Name, but more properly the person(s) or entity(ies) registered with a Domain Name Registrar as having the right to control how a Domain Name is used, such as the natural person or Legal Entity that is listed as the "Registrant" by WHOIS or the Domain Name Registrar.
Domain Name Registrar	A person or entity that registers Domain Names under the auspices of or by agreement with: (i) the Internet Corporation for Assigned Names and Numbers (ICANN), (ii) a national Domain Name authority/registry, or (iii) a Network Information Center (including their affiliates, contractors, delegates, successors, or assigns).
Enterprise, as in Enterprise Service Center	A line of business that an Affiliate enters to provide Managed PKI services to Managed PKI Customers.
Exigent Audit/Investigation	An audit or investigation by DigiCert where DigiCert has reason to believe that an entity's failure to meet STN Standards, an incident or Compromise relating to the entity, or an actual or potential threat to the security of the STN posed by the entity has occurred.
Expiry Date	The "Not After" date in a Certificate that defines the end of a Certificate's validity period.
Fully-Qualified Domain Name	A Domain Name that includes the labels of all superior nodes in the Internet Domain Name System.
Government Entity	A government-operated legal entity, agency, department, ministry, branch, or similar element of the government of a country, or political subdivision within such country (such as a state, province, city, county, etc.).
Intellectual Property Rights	Rights under one or more of the following: any copyright, patent, trade secret, trademark, and any other intellectual property rights.
Intermediate Certification Authority (Intermediate CA)	A Certification Authority whose Certificate is located within a Certificate Chain between the Certificate of the root CA and the Certificate of the Certification Authority that issued the end-user Subscriber's Certificate.
Internal Server Name	A Server Name (which may or may not include an Unregistered Domain Name) that is not resolvable using the public DNS.
International Organization	An International Organization is an organization founded by a constituent document, e.g., charter, treaty, convention, or similar document, signed by, or on behalf of, a minimum of two or more Sovereign State governments.
Issuing CA	In relation to a particular Certificate, the CA that issued the Certificate. This could be either a Root CA or a Subordinate CA.
Key Compromise	A Private Key is said to be compromised if its value has been disclosed to an unauthorized person, an unauthorized person has had access to it, or there exists a practical technique by which an unauthorized person may discover its value.
Key Generation Ceremony	A procedure whereby a CA's or RA's key pair is generated, its private key is transferred into a cryptographic module, its private key is backed up, and/or its public key is certified.
Key Generation Script	A documented plan of procedures for the generation of a CA Key Pair.

Term	Definition
Key Manager Administrator	An Administrator that performs key generation and recovery functions for a Managed PKI Customer using Managed PKI Key Manager.
Key Pair	The Private Key and its associated Public Key.
Key Recovery Block (KRB)	A data structure containing a Subscriber's private key that is encrypted using an encryption key. KRBs are generated using Managed PKI Key Manager software.
Key Recovery Service	A DigiCert service that provides encryption keys needed to recover a Key Recovery Block as part of a Managed PKI Customer's use of Managed PKI Key Manager to recover a Subscriber's private key.
Level	A specified level of assurances as defined within the CP. See CP § 1.1.1.
Legal Entity	An association, corporation, partnership, proprietorship, trust, government entity or other entity with legal standing in a country's legal system.
Managed PKI	DigiCert's fully integrated managed PKI service that allows enterprise Customers of DigiCert and its Affiliates to distribute Certificates to individuals, such as employees, partners, suppliers, and customers, as well as devices, such as servers, routers, and firewalls. Managed PKI permits enterprises to secure messaging, intranet, extranet, virtual private network, and e-commerce applications.
Managed PKI Administrator	An Administrator that performs validation or other RA functions for an Managed PKI Customer.
Managed PKI Control Center	A web-based interface that permits Managed PKI Administrators to perform Manual Authentication of Certificate Applications
Managed PKI Key Manager	A key recovery solution for those Managed PKI Customers choosing to implement key recovery under a special Managed PKI Agreement.
Managed PKI Key Management Service Administrator's Guide	A document setting forth the operational requirements and practices for Managed PKI Customers using Managed PKI Key Manager.
Manual Authentication	A procedure whereby Certificate Applications are reviewed and approved manually one-by-one by an Administrator using a web-based interface.
NetSure Protection Plan	An extended warranty program, which is described in CPS § 9.2.3.
Non-verified Subscriber Information	Information submitted by a Certificate Applicant to a CA or RA, and included within a Certificate, that has not been confirmed by the CA or RA and for which the applicable CA and RA provide no assurances other than that the information was submitted by the Certificate Applicant.
Non-repudiation	An attribute of a communication that provides protection against a party to a communication falsely denying its origin, denying that it was submitted, or denying its delivery. Denial of origin includes the denial that a communication originated from the same source as a sequence of one or more prior messages, even if the identity associated with the sender is unknown. Note: only an adjudication by a court, arbitration panel, or other tribunal can ultimately prevent repudiation. For example, a digital signature verified with reference to a STN Certificate may provide proof in support of a determination of Non-repudiation by a tribunal, but does not by itself constitute Non-repudiation.
Object Identifier	A unique alphanumeric or numeric identifier registered under the International Organization for Standardization's applicable standard for a specific object or object Level.
OCSP (Online Certificate Status Protocol)	An online Certificate-checking protocol for providing Relying Parties with real-time Certificate status information.
OCSP Responder	An online server operated under the authority of the CA and connected to its Repository for processing Certificate status requests. See also, Online Certificate Status Protocol.
Offline CA	STN PCAs, Issuing Root CAs and other designated intermediate CAs that are maintained offline for security reasons in order to protect them from possible attacks by intruders by way of the network. These CAs do not directly sign end user Subscriber Certificates.
Online CA	CAs that sign end user Subscriber Certificates are maintained online so as to provide continuous signing services.
Online Certificate Status Protocol (OCSP)	A protocol for providing Relying Parties with real-time Certificate status information.
Operational Period	The period starting with the date and time a Certificate is issued (or on a later date and time certain if stated in the Certificate) and ending with the date and time on which the Certificate expires or is earlier revoked.
PKCS #10	Public-Key Cryptography Standard #10, developed by RSA Security Inc., which defines a structure for a Certificate Signing Request.
PKCS #12	Public-Key Cryptography Standard #12, developed by RSA Security Inc., which defines a secure means for the transfer of private keys.
Policy Management Authority (PMA)	The organization within Symantec responsible for promulgating this policy throughout the STN.
Primary Certification Authority (PCA)	A CA that acts as a root CA for a specific Level of Certificates, and issues Certificates to CAs subordinate to it.
Private Key	The key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create

Term	Definition
	Digital Signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.
Processing Center	An organization (DigiCert or certain Affiliates) that creates a secure facility housing, among other things, the cryptographic modules used for the issuance of Certificates. In the Consumer and Web Site lines of business, Processing Centers act as CAs within the STN and perform all Certificate lifecycle services of issuing, managing, revoking, and renewing Certificates. In the Enterprise line of business, Processing Centers provide lifecycle services on behalf of their Managed PKI Customers or the Managed PKI Customers of the Service Centers subordinate to them.
Public Key	The key of a Key Pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify Digital Signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.
Public Key Infrastructure (PKI)	The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a Certificate-based public key cryptographic system. The STN PKI consists of systems that collaborate to provide and implement the STN.
Publicly-Trusted Certificate	A Certificate that is trusted by virtue of the fact that its corresponding Root Certificate is distributed as a trust anchor in widely-available application software.
Qualified Auditor	A natural person or Legal Entity that meets the requirements of Section 17.6 (Auditor Qualifications).
Registered Domain Name	A Domain Name that has been registered with a Domain Name Registrar.
Registration Authority (RA)	An entity approved by a CA to assist Certificate Applicants in applying for Certificates, and to approve or reject Certificate Applications, revoke Certificates, or renew Certificates.
Reliable Method of Communication	A method of communication, such as a postal/courier delivery address, telephone number, or email address, that was verified using a source other than the Applicant Representative.
Relying Party	An individual or organization that acts in reliance on a certificate and/or a digital signature.
Relying Party Agreement	An agreement used by a CA setting forth the terms and conditions under which an individual or organization acts as a Relying Party.
Repository	An online database containing publicly-disclosed PKI governance documents (such as Certificate Policies and Certification Practice Statements) and Certificate status information, either in the form of a CRL or an OCSP response.
Reseller	An entity marketing services on behalf of DigiCert or an Affiliate to specific markets.
Reserved IP Address	An IPv4 or IPv6 address that the IANA has marked as reserved: http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xml
Retail Certificate	A Certificate issued by DigiCert or an Affiliate, acting as CA, to individuals or organizations applying one by one to DigiCert or an Affiliate on its web site.
Root CA	The top level Certification Authority whose Root Certificate is distributed by Application Software Suppliers and that issues Subordinate CA Certificates.
Root Certificate	The self-signed Certificate issued by the Root CA to identify itself and to facilitate verification of Certificates issued to its Subordinate CAs.
RSA	A public key cryptographic system invented by Rivest, Shamir, and Adelman.
Secret Share	A portion of a CA private key or a portion of the activation data needed to operate a CA private key under a Secret Sharing arrangement.
Secret Sharing	The practice of splitting a CA private key or the activation data to operate a CA private key in order to enforce multi-person control over CA private key operations under CP § 6.2.2.
Secure Sockets Layer (SSL)	The industry-standard method for protecting Web communications developed by Netscape Communications Corporation. The SSL security protocol provides data encryption, server authentication, message integrity, and optional client authentication for a Transmission Control Protocol/Internet Protocol connection.
Security and Audit Requirements (SAR) Guide	A Symantec document that sets forth the security and audit requirements and practices for Processing Centers and Service Centers.
Security and Practices Review	A review of an Affiliate performed by DigiCert before an Affiliate is permitted to become operational.
Service Center	An Affiliate that does not house Certificate signing units for the issuance of Certificates for the purpose of issuing Certificates of a specific Level or type, but rather relies on a Processing Center to perform issuance, management, revocation, and renewal of such Certificates.
Sub-domain	The portion of the STN under control of an entity and all entities subordinate to it within the STN hierarchy.

Term	Definition
Subject	The natural person, device, system, unit, or Legal Entity identified in a Certificate as the Subject and holder of a private key corresponding to a public key. The Subject is either the Subscriber or a device under the control and operation of the Subscriber. The term "Subject" can, in the case of an organizational Certificate, refer to the equipment or device that holds a private key. A Subject is assigned an unambiguous name, which is bound to the public key contained in the Subject's Certificate.
Subject Identity Information	Information that identifies the Certificate Subject. Subject Identity Information does not include a domain name listed in the *subjectAltName* extension or the Subject *commonName* field.
Subordinate CA	A Certification Authority whose Certificate is signed by the Root CA, or another Subordinate CA.
Subscriber	In the case of an individual Certificate, a person who is the Subject of, and has been issued, a Certificate. In the case of an organizational Certificate, an organization that owns the equipment or device that is the Subject of, and that has been issued, a Certificate. A Subscriber is capable of using, and is authorized to use, the private key that corresponds to the public key listed in the Certificate.
Subscriber Agreement	An agreement used by a CA or RA setting forth the terms and conditions under which an individual or organization acts as a Subscriber.
Superior Entity	An entity above a certain entity within a Sub-domain hierarchy (the Level 1, 2, or 3 hierarchy).
Supplemental Risk Management Review	A review of an entity by DigiCert following incomplete or exceptional findings in a Compliance Audit of the entity or as part of the overall risk management process in the ordinary course of business.
Reseller	An entity marketing services on behalf of DigiCert or an Affiliate to specific markets.
Terms of Use	Provisions regarding the safekeeping and acceptable uses of a Certificate issued in accordance with these Requirements when the Applicant/Subscriber is an Affiliate of the CA.
Trusted Person	An employee, contractor, or consultant of an entity within the Sub-domain responsible for managing infrastructural trustworthiness of the entity, its products, its services, its facilities, and/or its practices as further defined in CP § 5.2.1.
Trusted Position	The positions within a Sub-domain entity that must be held by a Trusted Person.
Trustworthy System	Computer hardware, software, and procedures that are reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy. A trustworthy system is not necessarily a "trusted system" as recognized in classified government nomenclature.
Symantec Trust Network (STN)	The Certificate-based Public Key Infrastructure governed by the Symantec Trust Network Certificate Policies, which enables the worldwide deployment and use of Certificates by Symantec and its Affiliates, and their respective Customers, Subscribers, and Relying Parties.
Sub-domain Participant	An individual or organization that is one or more of the following within the Sub-domain of TRUST ITALIA SPA: , a Customer, , a Reseller, a Subscriber, or a Relying Party.
Unregistered Domain Name	A Domain Name that is not a Registered Domain Name.
Valid Certificate	A Certificate that passes the validation procedure specified in RFC 5280.
Validation Specialists	Someone who performs the information verification duties specified by these Requirements.
Validity Period	The period of time measured from the date when the Certificate is issued until the Expiry Date.