DigiCert

Certification Practices Statement for Symantec Trust Network (STN)

Version 3.1 3
June 25, 2019

DigiCert, Inc.
2801 N. Thanksgiving Way
Suite 500
Lehi, UT 84043
USA
Tel: 1-801-877-2100
Fax: 1-801-705-0481
www.digicert.com

© 2017-2019 DigiCert, Inc. All rights reserved.
Printed in the United States of America.

Published date: June 25, 2019

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.

Trademark Notices

Symantec, the Symantec logo, and related marks are the registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. The VeriSign logo, VeriSign Trust and other related marks are the trademarks or registered marks of VeriSign, Inc. or its affiliates or subsidiaries in the U.S. and other countries. Other names may be trademarks of their respective owners.

Without limiting the rights reserved above, and except as licensed below, no part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), without prior written permission of DigiCert, Inc.

Notwithstanding the above, permission is granted to reproduce and distribute this DigiCert Certification Practices Statement for Symantec Trust Network (STN) on a nonexclusive, royalty-free basis, provided that (i) the foregoing copyright notice and the beginning paragraphs are prominently displayed at the beginning of each copy, and (ii) this document is accurately reproduced in full, complete with attribution of the document to DigiCert, Inc.

Requests for any other permission to reproduce this DigiCert Certification Practices Statement for Symantec Trust Network (STN) (as well as requests for copies from DigiCert) must be addressed to DigiCert, Inc., 2801 N. Thanksgiving Way, Suite 500, Lehi, UT 84043 USA Tel 1-801-877-2100 Fax 1-801-705-0481 Email: legal@digicert.com.

Table of Contents

1. INTRODUCTION .....

6.2.6 Private Key Transfer Into or From a Cryptographic Module 47
6.2.7 Private Key Storage on Cryptographic Module 47
6.2.8 Method of Activating Private Key 48
6.2.9 Method of Deactivating Private Key 50
6.2.10 Method of Destroying Private Key 50
6.2.11 Cryptographic Module Rating 50
6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT 50
6.3.1 Public Key Archival 50
6.3.2 Certificate Operational Periods and Key Pair Usage Periods 50
6.4 ACTIVATION DATA 52
6.4.1 Activation Data Generation and Installation 52
6.4.2 Activation Data Protection 52
6.4.3 Other Aspects of Activation Data 52
6.5 COMPUTER SECURITY CONTROLS 53
6.5.1 Specific Computer Security Technical Requirements 53
6.5.2 Computer Security Rating 53
6.6 LIFE CYCLE TECHNICAL CONTROLS 53
6.6.1 System Development Controls 53
6.6.2 Security Management Controls 53
6.6.3 Life Cycle Security Controls 54
6.7 NETWORK SECURITY CONTROLS 54
6.8 TIME-STAMPING 54

7. CERTIFICATE, CRL, AND OCSP PROFILES 54

7.1 CERTIFICATE PROFILE 54
7.1.1 Version Number(s) 55
7.1.2 Certificate Extensions 55
7.1.3 Algorithm Object Identifiers 57
7.1.4 Name Forms 57
7.1.5 Name Constraints 58
7.1.6 Certificate Policy Object Identifier 58
7.1.7 Usage of Policy Constraints Extension 58
7.7 Extension 3.1
Consttttai and Tc 0.5 (e)]TJ0 Tc 0 Tw ( )Tj-0.027 T1 0.027 Tw 2.S76 0 Tde (s)TjEMC /Referenc754MCID

9.13.2 Disputes with End-User Subscribers or Relying Parties 70
9.14 GOVERNING LAW 70
9.15 COMPLIANCE WITH APPLICABLE LAW 70
9.16 MISCELLANEOUS PROVISIONS 71
9.16.1 Entire Agreement 71
9.16.2 Assignment 71
9.16.3 Severability 71
9.16.4 Enforcement (Attorney's Fees and Waiver of Rights) 71
9.16.5 Force Majeure 71
9.17 OTHER PROVISIONS 71

APPENDIX A: TABLE OF ACRONYMS AND DEFINITIONS 72

TABLE OF ACRONYMS 72
DEFINITIONS ..... 73 -4Tw ( )

Change History Table

Version	Changes made
3.1	Made the list of requirements for key recovery a VeriSign recommendation. Completed additional document-wide revisions.
3.2	Added TLS as an appropriate use for organization certificates. Specified that it is the Corporate Contact and

Version	Changes made
3.8.16	Added language to specifically include STN CAs managed by Symantec Japan Inc. in the definition of 'Symantec's Sub-

1.2 Document Name and Identification

This document is the DigiCert Certification Practices Statement for Symantec Trust Network

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 Class 1 and 3.

DigiCert Basic DV Certificates are issued to domains to provide encryption. DigiCert validates that the person enrolling for the certificate has control of the domain by a Domain Authorization or by having the Applicant demonstrate practical control over the FQDN. No organization authentication is performed on the owner of the domain.

High assurance certificates are individual and organizational certificates Class 3 Certificates that provide a high level of assurance of the identity of the Subscriber in comparison with Class 1 and 2.

High assurance with extended validation certificates are Class 3 certificates issued by DigiCert in conformance with the Guidelines for Extended Validation Certificates.

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 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, Class 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.

The STN and its Participants do not issue any certificate that can be used for man-in-the-middle (MITM) or traffic management of domain names or IP addresses that the certificate holder does not legitimately own or control. Such certificate usage is expressly prohibited.

DigiCert periodically rekeys Intermediate CAs. Third party applications or platforms that have an Intermediate CA embedded as a root certificate may not operate as designed after the Intermediate CA has been rekeyed. DigiCert 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. DigiCert recommends the use of PCA Roots as root certificates.

1.5 Policy Administration

1.5.1 Organization Administering the Document

This CPS and the documents referenced herein are maintained by the DigiCert Policy Authority (DCPA), which can be contacted at:

DigiCert Policy Authority
Suite 500
2801 N. Thanksgiving Way

1.6 Definitions and Acronyms

See Appendix A for a table of acronyms and definitions.

1.6.1 References

See section 1.6.3 of the DigiCert CP for relevant references.

2. Publication and Repository Responsibilities

2.1 Repositories

DigiCert is responsible for the repository functions for its own CAs and the CAs of its Enterprise Customers (Managed PKI customers).

Upon revocation of an end-user Subscriber's Certificate, DigiCert publishes notice of such revocation in the repository. DigiCert 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, DigiCert provides OCSP services pursuant to the provisions of this CPS.

2.2 Publication of Certificate Information

DigiCert 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.

DigiCert issues Certificate Revocation Lists (CRLs) and, if available, provides OCSP services (Online Certificate Status Protocol) for its own CAs and the CAs of Service Centers within its Sub-domain.

DigiCert will at all times publish a current version of:

- The DigiCert STN CP
- This DigiCert STN CPS,
- Subscriber Agreements,
- Relying Party Agreements

DigiCert is responsible for the repository function for:

- DigiCert's Public Primary Certification Authorities (PCAs) and DigiCert Infrastructure/Administrative CAs supporting the STN, and
- DigiCert's CAs and Enterprise Customers' CAs that issue Certificates within DigiCert's Sub-domain of the STN.

DigiCert publishes the STN CP, this CPS, Subscriber Agreements, and Relying Party Agreements in the repository section of DigiCert's web site.

2.3 Time or Frequency of Publication

Updates to this CPS are published in accordance with Section 9.12. Updates to Subscriber Agreements and Relying Party Agreements are published as necessary. CA information is

The Common Name (CN=) component of the Subject distinguished name of end-user Subscriber Certificates is authenticated in the case of Class 2-3 Certificates. The Common Name is either omitted or may contain “Persona Not Validated” for Class 1 Certificates.

- The authenticated Common Name value included in the Subject DN of Organizational Certificates is a domain name) or the legal name of the organization or unit within the organization.
- The authenticated Common Name value included in the Subject DN of a Class 3 Organizational ASB Certificate, however, is the generally accepted personal name of the organizational representative authorized to use the organization’s private key, and the organization (O=) component is the legal name of the organization.
- The Common Name value included in the Subject DN of individual Certificates represents the individual’s generally accepted personal name.
- For all web server certificates, the subjectAltName extension is populated with the authenticated value in the Common Name field of the subject DN (domain name or public iPAddress). The subjectAltName extension may contain additional domain names or public iPAddresses which will be authenticated in the same way as the Common Name value. For internationalized domain names, the Common Name will be represented as a Unicode encoded U-label value designed for human comprehension and that Common Name will be represented in the Subject Alternative Name extension as a puny-coded A-label value designed for automated comprehension. These different encodings of the same name are treated as equal values for the purposes of Common Name to Subject Alternative Name duplication requirements.

EV SSL certificate content and profile requirements are discussed in Appendix B2 to this CPS.

3.1.3 Anonymity or Pseudonymity of Subscribers

The identity of Class 1 individual Subscribers is not authenticated. Class 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), Class 2 and 3 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 DCPA and, if allowed the certificate will indicate that identity has been authenticated but is protected.

3.1.4 Rules for Interpreting Various Name Forms

No stipulation

3.1.5 Uniqueness of Names

DigiCert ensures that Subject Distinguished Name (DN) of the Subscriber is 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 DN.

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. For EV SSL Certificates, DigiCert implements a process that prevents EV Certificates from including a name, DBA, tradename, trademark, address, location, or other text that refers to a specific natural person or Legal Entity unless DigiCert has verified this information in accordance with the EV Guidelines and section 3.2 of the DigiCert CP and CPS. For all other Certificate types, DigiCert 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. DigiCert 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

For FBCA certificates, where the party named in a certificate generates its own keys, 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 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 pre-generated keys are placed on smart cards.

3.2.2 Authentication of Organization Identity and Domain 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 section 3.2.2 of the DigiCert Certificate Policy and in the DigiCert Certification Practices Statement, version 4.14, or higher, available at https://www.digicert.com/CPS.

At a minimum DigiCert shall:

- Any other information designated as non-verified in the certificate.

3.2.5 Validation of Authority

DigiCert will take reasonable steps to establish that a Certificate request made on behalf of an Organization is legitimate and properly authorized. Affirmation of authority is typically derived from the Applicant's actions in confirming the right to use or control the requested domain names using procedures listed in Section 3.2.2 of the DigiCert CPS. To prove that a Certificate is duly authorized by the Organization in other situations, DigiCert will typically request the name of a contact person who is employed by or is an officer of the Organization.

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 the DigiCert 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 appl43.1 (i)-40.3 (ng)5.T iel iltel tse ( )]TJ 5.882 -1data6 (')-40.3 'ere.1 (5 ( )-58.8 (na02 Tw - (c)-56.4 (al)18.5

information) has not changed and the previous validations were performed within the allowable data reuse limits specified in the CA/Browser Forum Baseline Requirements and EV Guidelines, a renewal Certificate is automatically issued.

3.3.2 Identification and Authentication for Re -key After Revocation

Re-key/renewal after revocation is not permitted if the revocation occurred because:

- x the Certificate (other than a Class 1 Certificate) was issued to a person other than the one named as the Subject of the Certificate, or
- x the Certificate (other than a Class 1 Certificate) was issued without the authorization of the person or entity named as the Subject of such Certificate, or
- x the entity approving the Subscriber's Certificate Application discovers or has reason to believe that a material fact in the Certificate Application is false. or
- x For any other reason deemed necessary by DigiCert to protect the STN

Subject to the foregoing paragraph, renewal of an Organizational or CA Certificate following revocation of the Certificate is permissible as long as renewal procedures ensure that the Organization or CA seeking renewal lreaso(od <0078>T0)]TJ 0.102 Tw 0 -1.176 TD [(app-46.9 (ev)6 (ec)-56.4 15.7 (i)-4

The requests to revoke a CA Certificate shall be authenticated by DigiCert 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?

4.2.2

4.3.2 Notifications to Subscriber by the CA of Issuance of Certificate

DigiCert 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.

4.3.3 CAB Forum Requirements (ev1.4.2) (EV 7.5.6.4 (cont.)) 58 0 R 70 0 54.1 (E)-70.47111.8 (ls)0.57 Tc 0.337 Trtif5.1158.9

EV SSL Certificates, EV Code Signing, and domain-validated and organization-validated SSL Certificates conform to the 7 (ov)61.3(f)-43.1 (i)-40.3 (c)-56.4 (at)15.7 (e6PrhR)-43.1 (i)-40.3 (c)-56.4 (at)15.7 (es)2.4 (,)-4

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.

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

No stipulation.

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 Classes.

P

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 Processi 1.

3. The Subscriber or the cross-certified CA breached a material obligation under the CP, this CPS, or the relevant agreement;
4. DigiCert confirms any circumstance indicating that use of a FQDN or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name registrant and the Applicant has terminated, or the Domain Name registrant has failed to renew the Domain Name);
5. DigiCert confirms that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate FQDN;
6. DigiCert confirms a material change in the information contained in the Certificate;
7. DigiCert confirms that the Certificate was not issued in accordance with the CA/B forum requirements or the DigiCert CP or this CPS;
8. DigiCert determines or confirms that any of the information appearing in the Certificate is inaccurate;
9. DigiCert's right to issue Certificates under the CA/B forum requirements expires or is revoked or terminated, unless DigiCert has made arrangements to continue maintaining the CRL/OhentAe;

4.9.3.3 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 DigiCert. DigiCert will then revoke the Certificate. DigiCert may also initiate CA or RA Certificate revocation.

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

DigiCert takes commercially reasonable steps to process revocation requests without delay. DigiCert will revoke a CA Certificate within one hour after receiving clear instructions from the DCPA.

Within 24 hours after receiving a Certificate problem report, DigiCert investigates the facts and circumstances related to a Certificate problem report and will provide a preliminary report on its findings to both the Subscriber and the entity who filed the Certificate problem report.

After reviewing the facts and circumstances, DigiCert works with the Subscriber and any entity reporting the Certificate problem report or other revocation-related notice to establish whether or not the certificate will be revoked, and if so, a date which DigiCert will revoke the certificate. The period from receipt of the Certificate problem report or revocation-related notice to published revocation must not exceed the time frame set forth in Section 4.9.1. The date selected by DigiCert will consider the following criteria:

1. The nature of the alleged problem (scope, context, severity, magnitude, risk of harm);
2. The consequences of revocation (direct and collateral impacts to Subscribers and Relying Parties);
3. The number of Certificate problem reports received about a particular Certificate or Subscriber;
4. The entity making the complaint (for example, a complaint from a law enforcement official that a Web site is engaged in illegal activities should carry more weight than a complaint from a consumer alleging that she didn't receive the goods she ordered); and
5. Relevant legislation.

Under normal operating circumstances, DigiCert will revoke Certificates as quickly as practical after validating the revocation request following the guidelines of this section and Section 4.9.1, generally within the following time frames:

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). DigiCert 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.

Due to the numerous and varying locations for CRL repositories, relying parties are advised to access CRLs using the URL(s) embedded in a certificate's CRL Distribution Points extension. The proper OCSP responder for a given certificate is placed in its Authority Information Access extension.

4.9.7 CRL Issuance Frequency

CRLs for end-user Subscriber Certificates are issued at least once per day. CRLs for CA Certificates shall be issued at least annually, but also whenever a CA Certificate is revoked. [14]

CRLs for Authenticated Content Signing (ACS) Root CAs are published annually and also whenever a CA Certificate is revoked.

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

4.9.7.1 CABF Requirements for CRL Issuance

CRL issuance for EV SSL Certificates, EV Code Signing, and domain-validated and organization-validated SSL Certificates conform to the respective CA / Browser Forum requirements as set forth in the DigiCert CP and CPS.

4.9.7.2 Microsoft Requirements for CRL Issuance

Frequency of CRL issuance for code signing and timestamp certificates is documented in this CPS and complies with section 13,2,2 of the Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates published at https://aka.ms/csbr.

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, DigiCert provides Certificate status information through query functions in the DigiCert Repository.

[14] CRLs for the "Symantec Class 3 Organizational VIP Device CA" are only issued whenever a certificate issued by that CA is revoked.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

The Status of public certificates is available via CRL at DigiCert's website and via an OCSP responder (where available).

4.10.2 Service Availability

Certificate Status Services are available 24 U7.

Certificate status services for EV SSL Certificates, EV Code Signing, and Organization-validated and Domain-validated SSL Certificates, conform to the respective CA / Browser Forum requirements as set forth in the DigiCert CP and CPS.

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 DigiCert 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 STN participant may escrow CA, RA or end-user Subscriber private keys.

Enterprise customers using the Key Escrow option within the Symantec 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 DigiCert's secure data center. If operated out of the enterprise's premises, DigiCert does not store copies of Subscriber private keys but nevertheless 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 Symantec 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,

x

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

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 DigiCert 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 DigiCert 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 DigiCert'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

DigiCert 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

DigiCert manually or automatically logs the following significant events:

- CA key life cycle management events, including:
  - Key generation, backup, storage, recovery, archival, and destruction
  - Changes to CA details or keys
  - Cryptographic device life cycle management events.
- CA and Subscriber certificate life cycle management events, including:
  - Certificate Applications, issuance, renewal, rekey, and revocation
  - Successful or unsuccessful processing of requests
  - Changes to certificate creation policies
  - Generation and issuance of Certificates and CRLs.
- Trusted Employee Events, including:
  - Logon and logoff attempts
  - Attempts to create, remove, set passwords or change the system privileges of any privileged users
  - Personnel changes.
- Security-related events including:
  - Successful and unsuccessful PKI system access attempts
  - Start-up and shutdown of systems and applications
  - Possession of activation data for CA private key operations
  - System configuration changes and maintenance
  - PKI and security system actions performed by DigiCert personnel
  - Security sensitive files or records read, written, deleted or destroyed
  - Security profile changes
  -

5.6 Key Changeover

STN CA key pairs are retired from service at the end of their respective maximum lifetimes as defined in this CPS. STN 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). DigiCert'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. DigiCert 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 DigiCert Security and DigiCert's incident handling procedures are enacted. Such procedures require appropriate escalation, incident investigation, and incident response. If necessary, DigiCert's key compromise or disasteror nfo28aiomprTJ -13.765 DIn the56.4 (TJ -10.2 30 322.8 /l)18.5 (C)-1

- 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.

5.9 Data Security

For the issuance of EV SSL Certificates, EV Code Signing, and Organization-validated and Domain-validated SSL Certificates, DigiCert conforms to the respective CA / Browser Forum requirements for Data Security as set forth in the DigiCert CP and CPS.

6. ren020 7 1eai(Tc 0 18 k-3.9 (P)]TJ -0.020 7 1g ra9 -079 0 Tc 77 <</MCID 0.30 .

Public Key Algorithm	Signature Algorithm	Class	Generation
2048 bit RSA	SHA1	Class 1, 2, 3 PCAs	G3 PCAs
		Class 3 PCA	G5 PCA
	SHA256	Class 1, 2 and Class 3 Universal Root PCA	G6 PCAs
384 bit ECC	SHA384	Class 1, 2, 3* PCAs	G4 PCAs
4096 bit RSA	SHA384	Class 3 PCA	G6 PCA
2048_256 bit DSA	SHA256	Class 1, 2, 3 PCAs	G7 PCAs
* There are two Class 3 G4 Roots (one branded VeriSign (legacy) and one branded Symantec).			

Table 8: DigiCert Root CAs and Key Sizes

All Classes of STN PCAs and CAs, and RAs and end entity certificates use SHA-2 for digital signature hash algorithm and certain versions of DigiCert Processing Center support the use of SHA-256 and SHA-384 hash algorithms in end-entity Subscriber Certificates. SHA-1 may be used to support legacy applications and use cases other than SSL and EV Code Signing provided that such usage does not violate procedures and policies set forth by the CA/Browser Forum and related Application Software Suppliers.

6.1.5.1 CABF Requirements for Key Sizes

EV SSL Certificates, EV Code Signing, and domain-validated and organization-validated SSL Certificates conform to the respective CA /Browser Forum requirements as set forth in the DigiCert CP and CPS[15].

DigiCert Root CA Certificates meet the following requirements for algorithm type and key size:

	Validity period beginning on or before 31 Dec 2010	Validity period beginning after 31 Dec 2010
Digest algorithm	MD5 Not Recommended, SHA-1, SHA-256, SHA-384 or SHA-512	SHA-1*, SHA-

ECC curve	NIST P-256, P-384 or P-521	NIST P-256, P-384 or P-521

Table 10 – Algorithms and key sizes for Subordinate CA Certificates

DigiCert CAs shall only issue Subscriber certificates with keys containing the following algorithm types and key sizes.

	Validity period ending on or before 31 Dec 2013	Validity period

6.2.8 Method of Activating Private Key

accordance with Section 10.3.2(2) in the Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates

Symantec Secure App Service (SAS) ensures that a Subscriber's private key is generated, stored, and used in a secure environment that has controls to prevent theft or misuse. SAS enforces multi-factor authentication to access and authorize Code Signing and obtain a representation from the Subscriber that they will securely store the tokens required for multi-factor access. SAS systems used to host a Signing Service are not used for web browsing, run a regularly updated antivirus solution to scan the service for possible virus infection, and comply with the CA/Browser Forum Network Security Guidelines as a "Delegated Third Party".

6.2.8.4 Administrators' wPrivate Keys ( )(rt)62.7 (y)-9t- TT8.3 (v)40.2 (ng S)-7 (e* 0 Td ( )Tj -0.0 Tw 3.882 0 Td [(f)-43.1

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 Offline intermediate CA to online CA	Up to 15 years[17]

6.5 Computer Security Controls

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

6.5.1 Specific Computer Security Technical Requirements

DigiCert ensures that the systems maintaining CA software and data files are Trustworthy Systems secure from unauthorized access. In addition, DigiCert 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.

DigiCert's production network is logically separated from other components. This separation prevents network access except through defined application processes. DigiCert 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.

DigiCert requires the use of passwords that have a minimum character length and a combination of alphanumeric and special characters.

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

6.5.1.1 CABF Requirements for System Security

EV SSL Certificates, EV Code Signing, and domain validated and organization validated SSL Certificates conform to the respective CA /Browser Forum requirements as set forth in the DigiCert CP and CPS.

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. DigiCert also provides 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, has not been modified prior to installation, and is the version intended for use.

6.6.2 Security Management Controls

DigiCert has 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 daily thereafter, DigiCert validates the integrity of its CA systems.

6.6.3 Life Cycle Security Controls

No stipulation

6.7 Network Security Controls

DigiCert 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 timSn Lsmofm04

7.1.1 Version Number(s)

DigiCert 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

DigiCert populates X.509 Version 3 STN 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 this CP and the applicable CPS unless specifically included by reference.

EV SSL certificate extension requirements are described in Appendix B2 to this CPS.

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, May 2008. The criticality field of the KeyUsage extension is generally set to TRUE for CA certificates and for end entity Subscriber certificates.

Note: The non-Repudiation bit[22] is not required to be set in these Certificates because the PKI industry has not yet reached a consensus as to what the non-Repudiation bit means. Until such a consensus emerges, the non-Repudiation bit might not be meaningful for potential Relying Parties. Moreover, the most commonly used applications do not always respect the non-Repudiation bit. Therefore, setting the bit might not help Relying Parties make a trust decision. Consequently, this CPS does not require that the non-Repudiation bit be set. It may be set in the case of dual key pair signature Certificates issued through Managed PKI Key Manager, or as otherwise requested. Any dispute relating to non-repudiation arising from the use of a digital certificate is a matter solely between the Subscriber and the Relying Party(s). DigiCert shall incur no liability in relation thereto.

7.1.2.2 Certificate Policies Extension

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

7.1.2.2.1 CABF Requirement for Certificate Policies Extension

EV SSL Certificates, EV Code Signing, and domain-validated and organization-validated SSL Certificates conform to the respective CA / Browser Forum requirements as set forth in the DigiCert CP and CPS.

7.1.2.3 Subject Alternative Names

The *subjectAltName* extension of X.509 Version 3 Certificates are populated in accordance with RFC 5280 with the exception of those issued under Public Lite accounts which may optionally

[22] The non-Repudiation bit may also be refer-Repudi

exclude the email address in *SubjectAltName*. The criticality field of this extension shall be set to FALSE.

For all web server certificates, the SubjectAltName extension is populated with the authenticated value in the Common Name field of the subject DN (domain name or public iPAddress). The SubjectAltName extension may contain additional authenticated domain names or public iPAddresses. For internationalized domain names, the Common Name will be represented as a Unicode encoded U-label value designed for human comprehension and that Common Name will be represented in the Subject Alternative Name extension as a puny-coded A-label value designed for automated comprehension. These different encodings of the same name are treated as equal when performing name matching according to RFC 5280.

set to FALSE. URLs comply with Mozilla requirements to exclude the LDAP protocol, and may appear multiple times within a *cRLDistributionPoints* extension.

7.1.2.7 Authority Key Iden]TJw 10.2 -0 0 10.2 298.8 37.8 Tm (57)Tj ET Q q 291.6 34.8 28.2 13.199 re W n 34.8 28.2 1b-

7.1.5 Name Constraints

No stipulation

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 of Certificate as set forth in the STN CP Section 1.2. For legacy Certificates issued prior to the publication of the STN CP which include the Certificate Policies extension, Certificates refer to the STN CPS.

7.1.6.1 CABF Requirements for Certificate Policy Object Identifier

EV SSL Certificates, EV Code Signing, and domain-validated and organization-validated SSL Certificates conform to the respective CA / Browser Forum requirements as set forth in the DigiCert CP and CPS.

7.1.7 Usage of Policy Constraints Extension

No stipulation

7.1.8 Policy Qualifiers Syntax and Semantics

DigiCert generally populates X.509 Version 3 STN 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 STN 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.

Version 2 CRLs conform to RFC 5280 and contain the basic fields and contents specified in Table 14 below:

Field	Value or Value constraint
Version	See Section 7.2.1.
Signature Algorithm	

8.3 Assessor's Relationship to Assessed Entity

Compliance audits of DigiCert's operations are performed by a public accounting firm that is independent of DigiCert.

8.4 Topics Covered by Assessment

The scope of DigiCert's annual WebTrust for Certification Authorities (or equivalent) audit includes CA environmental controls, key management operations and Infrastructure/Administrative CA controls, certificate life cycle management and CA business practices disclosure.

Audits of RAs (Class 1- 2)

Enterprise customers approving Class 1 and 2 certificates may undergo an annual compliance audit. Upon request from DigiCert and/or a Superior Entity (if the Superior Entity is not DigiCert), Enterprise customers may undergo an audit noting any exceptions or irregularities to STN policies and the steps taken to remedy the irregularities.

Audit of an RA (Class 3)

Enterprise Customers authorizing the issuance of Class 3 certificates undergo an annual compliance audit of their obligations under the STN.[24] Upon request from DigiCert and/or a Superior Entity (if the Superior Entity is not DigiCert) Enterprise Customers undergo an audit noting any exceptions or irregularities to STN policies and the steps taken to remedy the irregularities.

Audit of DigiCert or an Affiliate (Class 1-3)

DigiCert and each Affiliate is audited pursuant to the guidelines provided in the American Institute of Certificate Public Accounts' Statement on Service Organizations Control (SOC) Reports on the risks associated with Service Organizations. Their Compliance Audits are the WebTrust for Certification Authorities audit or an equivalent audit standard approved by DigiCert which includes: A Report of Policies and Procedures in Operation and Test of Operational Effectiveness.

8.5 Actions Taken as a Result of Deficiency

With respect to compliance audits of DigiCert's operations, significant exceptions or deficiencies identified during the Compliance Audit will result in a determination of actions to be taken. This determination is made by DigiCert management with input from the auditor. DigiCert management is responsible for developing and implementing a corrective action plan. If DigiCert determines that such exceptions or deficiencies pose an immediate threat to the security or integrity of the STN, a corrective action plan will be developed within 30 days and implemented within a commercially reasonable period of time. For less serious exceptions or deficiencies, DigiCert Management will evaluate the significance of such issues and determine the appropriate course of action.

[24] DigiCert performs identification and authentication of Class 3 SSL certificates authorized for issuance byes 3 CID 2B17M8i.6 (i)-26.8 (s)-56.4MCID 2

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. DigiCert 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.

9.2.3 Extended Warranty Coverage

The NetSure Protection Plan is an extended warranty program that provides SSL and code signing certificate subscribers with protection against loss or damage that is due to a defect in DigiCert's issuance of the certificate or other malfeasance caused by DigiCert's negligence or breach of its contractual obligations, provided that the subscriber of the certificate has fulfilled its

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

Digicert has implemented a Privacy Policy, which is located at: digicert.com/legal-repository, in compliance with CP § 9.4.1.

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 is deemed not private.

9.4.4 Responsibility to Protect Private Information

Certificates is subject to the Relying Party Agreement referenced in the Certificate. DigiCert 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

STN Participants acknowledge that DigiCert 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-

9.8

9.9.2 Indemnification by Relying Parties

To the extent permitted by applicable law, Relying Party Agreements shall require Relying Parties to indemnify DigiCert 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 DigiCert Repository. Amendments to this CPS become effective upon publication in the DigiCert 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, DigiCert 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

Unless otherwise specified by agreement between the parties, DigiCert Sub-domain participants shall use commercially reasonable methods to communicate with each other, taking into account the criticality and subject matter of the communication.

9.12

9.12.3 Circumstances under Which OID Must be Changed

If the DCPA determines that a change is necessary in the object identifier corresponding to a Certificate policy, the amendment shall contain new object identifiers for the Certificate policies corresponding to each Class of Certificate. Otherwise, amendments shall not require a change in Certificate policy object identifier.

9.13 Dispute Resolution Provisions

9.13.1 Disputes among DigiCert, Affiliates, and Customers

Disputes among DigiCert Sun17A7 (1,u10.9 (i)-43 Tw 5.2 Tc 03>BDC Tj 9.55do( )-59 (nt)15.7 (ai)pa)-10.9 (er)-7 policpa-

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

Not applicable

9.16.2 Assignment

Not applicable

9.16.3 ablher0 T6ablr0 T6ablhe CTd ((9blP)-7 >S)-715 > (2Tj Eha6 (e)]TJ /P <</).8 -0.102.8 1278.8 709.8 [

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.
CSPRNG	Cryptographically Secure Pseudo-Random Number Generator
DBA	Doing Business As
DCPA	DigiCert Policy Authority
DNS	Domain Name System
EV	Extended Validation
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

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 “

Term	Definition
	Requester and to authorize other employees or third parties to act as a Certificate Requester, and (ii) to approve EV Certificate Requests submitted by other Certificate Requesters.
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 Requester	A Certificate Requester is a natural person who is employed and authorized by the Applicant, or an authorized agent who has express authority to represent the Applicant or a third party (such as an ISP or hosting company) that completes and submits an EV Certificate Request on behalf of the Applicant.
Certificate Revocation List (CRL)	A periodically (or exigently) issued list, digitally signed by a CA, of identified Certificates that have

Term	Definition
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 Contact	The Domain Name Registrant, technical contact, or administrative "corporate" contact (or the equivalent under a ccTLD) as listed in the WHOIS record of the Base Domain Name or in a DNS SOA record.
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. an-76.556. (t)7.39 Tc 76 egned t.5 (t)-4g (an-76.51.201 10.8 re W n B3m)-31.1 A/126.8.7 w2.4 (t) (an-
Domain Name Registrant	

Term	Definition
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.

[redacted]

Term	Definition
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 Adleman.
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 § (rg0.8 (v-43.3 (§ (rg0.8 (v-4[00

Term	Definition
Validity Period	The period of time measured from the date when the Certificate is issued until the Expiry Date.
Wildcard Certificate	A Certificate containing an asterisk (*) in the left-most position of any of the Subject Fully-Qualified Domain Names contained in the Certificate.

Appendix B1: Minimum Cryptographic Algorithm and Key Sizes for EV Certificates

1. Root CA Certificates

Digest algorithm	SHA-1*, SHA-256, SHA-384 or SHA-512
RSA	2048 bit
ECC	

Appendix B2: EV Certificates Required Certificate Extensions

1. Root CA Certificate

Root certificates generated after October 2006 MUST be X.509 v3.

(a) basicConstraints

If the certificate is v3 and is created after October 2006, this extension MUST appear as a basinraints

All other fields and extensions MUST be set in accordance to RFC 5280.

3. Subscriber Certificate

(a) certificatePolicies

MUST be present and SHOULD NOT be marked critical.

certificatePolicies:policyIdentifier (Required)

- EV policy OID

certificatePolicies:policyQualifiers:policyQualifierId (Required)

- id-qt 2 [RFC 5280]

certificatePolicies:policy (Required): (Q)45.1 (ual)18.5 (i)-40.3 (f)-49dt(es)2.4 ( )58.9 (s)2.4 (:)-4qualifes

o

Appendix B3: Foreign Organization Name Guidelines

NOTE: This appendix is only relevant to EV applications from countries that do not have Latin character organization name registrations. More specific information for particular countries may be added to this appendix in the future.

Where an EV Applicant's organization name is not registered with a QGIS in Latin characters and the applicant's foreign character organization name and registration have been verified with a QGIS in accordance with these Guidelines, DigiCert MAY include a Latin character organization name in the EV certificate. In such a case, DigiCert will follow the procedures laid down in this appendix.

Romanized Names
In order to include a transliteration/Romanization of the registered name, the Romanization will be verified by DigiCert using a system officially recognized by the Government in the Applicant's jurisdiction of incorporation.

If DigiCert cannot rely on a transliteration/Romanization of the registered name using a system officially recognized by the Government in the Applicant's jurisdiction of incorporation, then it MUST rely on one of the options below, in order of preference:

- A system recognized by the International Standards Organization (ISO),
- A system recognized by the United Nations or
- A Lawyers Opinion confirming the Romanization of the registered name.

English Name
In order to include a Latin character name that is not a Romanization of the registered name in the EV certificate, DigiCert will verify that the Latin character name is:

- Included in the Articles of Incorporation (or equivalent document) filed as part of the organization registration, or
- Recognized by a QGTIS in the Applicant's Jurisdiction of Incorporation as the applicant's recognized name for tax filings, or
- Confirmed with a QIIS to be the name associated with the registered organization, or
- Confirmed by a lawyer's opinion letter to be the trading name associated with the registered organization.

Country Specific Procedures

F-1. Japan
In addition to the procedures set out above:

- The Hepburn method of Romanization is acceptable for Japanese Romanizations.
- DigiCert MAY verify the Romanized transliteration of Applicant's formal legal name with either a QIIS or a lawyer's opinion letter.
- DigiCert MAY use the Financial Services Agency to verify an English Name. When used, DigiCert will verify that the English name is recorded in the audited Financial Statements filed with the Financial Services Agency.
- When relying ited yFinanci yeled e l e d