KPN B.V.

Certification Practice Statement

Symantec Trust Network

Version 4.0

Effective Date: October 30th, 2019

KPN B.V.
Fauststraat 1
P.O. Box 9105
7300 HN Apeldoorn
The Netherlands
Phone: +31 (0)88 661 05 00
https://certificaat.kpn.com

KPN Certification Practice Statement

Revision date: October 30, 2019

Important – Acquisition Notice
On Oct 31, 2017, DigiCert Inc completed the acquisition of Symantecs Website Security and related PKI solutions. As a result DigiCert is now the registered owner of the STN Certificate Policy document and the PKI Services described within that document.
However a hybrid of references to both “DigiCert” and “Symantec” 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 Symantec as a corporate entity should be strictly considered to be legacy language that solely reflects the history of ownership.

Trademark and Tradename Notices

KPN B.V. is registered under number 27124701 at the Chamber of Commerce (“*Kamer van Koophandel*”) in Rotterdam, The Netherlands. KPN B.V. (KPN) is a subsidiary of Koninklijke KPN N.V.

The MegaSign brand was formerly used for the technical back-end operations and the publication of CRLs. “OnSite” is the former name of “Managed PKI”.

Symantec, the Symantec Logo, and the Checkmark Logo 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 and licensed by Symantec Corporation. 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 Symantec Corporation.

Notwithstanding the above, permission is granted to reproduce and distribute this KPN Certification Practice Statement 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 Symantec Corporation.

Requests for any other permission to reproduce this KPN Certification Practice Statement (as well as requests for copies from KPN) must be addressed to KPN Security Services Attn: Policy Management Authority (PMA). Tel: +31 (0) 88 661 0500 E-mail: pkisupport@kpn.com.

Acknowledgement

KPN and Symantec acknowledge the assistance of many reviewers of the document specializing in diverse areas of business, law, policy, and technology.

Table of Contents

1 INTRODUCTION 9

1.1 Overview 9
1.1.1 Target Group and Guidelines 9
1.1.2 CPS Purpose 9
1.1.3 CP/CPS Relationship 10
1.1.4 Status 11
1.2 Document Name and Identification 11
1.3 PKI Participants 11
1.3.1 Certification Authorities 11
1.3.2 Registration Authorities 11
1.3.3 Subscribers 11
1.3.4 Relying Parties 12
1.3.5 Other Participants 12
1.4 Certificate Usage 12
1.4.1 Appropriate Certificate Usages 12
1.4.1.1 Certificates Issued to Individuals 12
1.4.1.2 Assurance levels 13
1.4.2 Prohibited Certificate Uses 13
1.5 CPS Administration 13
1.5.1 Organization Administering the Document 13
1.5.2 Contact Person 13
1.5.3 Person Determining CP Suitability for the Policy 14
1.5.4 CPS Approval Procedure 14
1.6 Definitions and Acronyms 14

2 Publication and Repository Responsibilities 15

2.1 Repository 15
2.2 Publication of Certificate Information 15
2.3 Certificate Publication 16
2.4 Time or Frequency of Publication 16
2.5 Access Controls on Repositories 16

3 Identification and Authentication 17

3.1 Naming 17
3.1.1 Types of Names 17
3.1.2 Need for Names to be Meaningful 18
3.1.3 Anonymity or Pseudonymity of Subscribers 18
3.1.4 Rules for Interpreting Various Name Forms 18
3.1.5 Uniqueness of Names 19
3.1.6 Resolving Name Claim Disputes 19
3.1.7 Recognition, Authentication, and Role of Trademarks 19
3.2 Initial Identity Validation 19
3.2.1 Method to Prove Possession of Private Key 19
3.2.2 Authentication of Organizational Identity 19
3.2.3 Authentication of Individual Identity 20
3.2.4 Non-Verified Subscriber Information 20
3.2.5 Validation of Authority 20
3.2.6 Criteria for Interoperation 20
3.3 Identification and Authentication for Re-key Requests 21
3.3.1 Identification and Authentication for Routine Re-key 21

3.3.2 Identification and Authentication for Re-key After Revocation 22
3.4 Identification and Authentication for Revocation Request 22

4 Certificate Life-Cycle Operational Requirements 24

4.1 Certificate Application 24
4.1.1 Who Can Submit a Certificate Application 24
4.1.2 Responsibilities and Obligations 24
4.1.2.1 Responsibilities and Obligations of the CSP 24
4.1.2.2 Responsibilities and Obligations of the Client 24
4.1.2.3 Responsibilities and Obligations of the End-user Subscriber 24
4.1.2.4 Responsibilities and Obligations of the Relying Party 24
4.1.3 Enrollment Process and Responsibilities 24
4.2 Certificate Application Processing 25
4.2.1 Performing Identification and Authentication Functions 25
4.2.2 Approval or Rejection of Certificate Applications 25
4.2.3 Time to Process Certificate Applications 25
4.3 Certificate Issuance 25
4.4 Certificate Acceptance 26
4.4.1 Conduct Constituting Certificate Acceptance 26
4.4.2 Publication of the Certificate by the CA 26
4.4.3 Notification of Certificate Issuance by the CA to Other Entities 26
4.4.4 Notifications to Subscriber by the CA of Issuance of Certificate 26
4.5 Key Pair and Certificate Usage 26
4.5.1 Subscriber Private Key and Certificate Usage 26
4.5.2 Relying Party Public Key and Certificate Usage 26
4.6 Certificate Renewal 27
4.6.1 Circumstances for Certificate Renewal 27
4.6.2 Who May Request Renewal 27
4.6.3 Processing Certificate Renewal Requests 27
4.6.4 Notification of New Certificate Issuance to Subscriber 28
4.6.5 Conduct Constituting Acceptance of a Renewal Certificate 28
4.6.6 Publication of the Renewal Certificate by the CA 28
4.6.7 Notification of Certificate Issuance by the CA to Other Entities 28
4.7 Certificate Re-Key 29
4.7.1 Circumstances for Certificate Re-Key 29
4.7.2 Who May Request Certification of a New Public Key 29
4.7.3 Processing Certificate Re-Keying Requests 29
4.7.4 Notification of New Certificate Issuance to Subscriber 29
4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate 29
4.7.6 Publication of the Re-Keyed Certificate by the CA 29
4.7.7 Notification of Certificate Issuance by the CA to Other Entities 30
4.8 Certificate Modification 30
4.8.1 Circumstances for Certificate Modification 30
4.8.2 Who May Request Certificate Modification 30
4.8.3 Processing Certificate Modification Requests 30
4.8.4 Notification of New Certificate Issuance to Subscriber 30
4.8.5 Conduct Constituting Acceptance of Modified Certificate 30
4.8.6 Publication of the Modified Certificate by the CA 30
4.8.7 Notification of Certificate Issuance by the CA to Other Entities 30
4.9 Certificate Revocation and Suspension 30
4.9.1 Circumstances for Revocation 30
4.9.2 Who Can Request Revocation? 31
4.9.3 Procedure for Revocation Request 32
4.9.3.1 Procedure for Requesting the Revocation of an end-user Subscriber Certificate 32
4.9.3.2 Procedure for Requesting the Revocation of a CA or RA Certificate 32

4.9.4 Revocation Request Grace Period 32
4.9.5 Time within Which CA Must Process the Revocation Request 32
4.9.6 Revocation Checking Requirements for Relying Parties 32
4.9.7 CRL Issuance Frequency 32
4.9.8 Maximum Latency for CRLs 33
4.9.9 On-Line Revocation/Status Checking Availability 33
4.9.10 Other Forms of Revocation Advertisements Available 33
4.9.11 Special Requirements regarding Key Compromise 33
4.9.12 Certificate Suspension 33
4.10 Certificate Status Service 34
4.11 End of Subscription 34
4.12 Key Escrow and Recovery 34
4.12.1 Key Escrow and Recovery Policy and Practices 34
4.12.2 Session Key Encapsulation and Recovery Policy and Practices 35
4.12.3 Private Key Escrow for Qualified Certificates 35

5 Facility, Management, and Operational Controls 36

5.1 Physical Controls 36
5.1.1 Site Location and Construction 36
5.1.2 Physical Access 36
5.1.3 Power and Air Conditioning 36
5.1.4 Water Exposures 37
5.1.5 Fire Prevention and Protection 37
5.1.6 Media Storage 37
5.1.7 Waste Disposal 37
5.1.8 Off-site Backup 37
5.2 Procedural Controls 37
5.2.1 Confidential jobs 38
5.2.2 Number of Persons Required per Task 38
5.2.3 Management and Security 38
5.2.4 Separation of Duties 38
5.3 Personnel Controls 39
5.3.1 Trusted Employee Policy 39
5.3.2 Expertise, Experience and Qualifications 39
5.3.3 Independent Contractor Requirements 39
5.3.4 Documentation Supplied to Personnel 40
5.4 Audit Logging Procedures 40
5.4.1 Types of Events Recorded 40
5.4.2 Frequency of Processing Log 40
5.4.3 Retention Period for Audit-Log 41
5.4.4 Protection of Audit-Log 41
5.4.5 Audit Log Backup Procedures 41
5.4.6 Audit Collection System (Internal vs. External) 41
5.4.7 Notification to Event-Causing Subject 41
5.4.8 Vulnerability Assessments 41
5.5 Records Archival 41
5.5.1 Types of Records Archived 41
5.5.2 Retention Period for Archive 41
5.5.3 Protection of Archive 42
5.5.4 Archive Backup Procedures 42
5.5.5 Requirements for Time-Stamping of Records 42
5.5.6 Archive Collection System (Internal or External) 42
5.5.7 Procedures to Obtain and Verify Archive Information 42
5.6 Key Changeover 42

5.7 Compromise and Disaster Recovery 43
5.7.1 Incident and Compromise Handling Procedures 43
5.7.2 Entity Private Key Compromise Procedures 43
5.7.3 Disaster Recovery 43
5.7.4 Key Compromise 44
5.7.5 Secure Facility After a Natural or Other Type of Disaster 44
5.8 CA or RA Termination 44
5.8.1 Termination of a KPN customer CA 44
5.8.2 Termination of a KPN CA 45

6 Technical Security Controls 46

6.1 Key Pair Generation and Installation 46
6.1.1 Key Pair Generation 46
6.1.2 Private Key Delivery to Subscriber 46
6.1.3 Public Key Delivery to Certificate Issuer 46
6.1.4 CA Public Key Delivery to Relying Parties 47
6.1.5 Key Sizes 47
6.1.6 Public Key Parameters Generation and Quality Checking 47
6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field) 47
6.2 Private Key Protection and Cryptographic Module engineering Controls 47
6.2.1 Cryptographic Module Standards and Controls 47
6.2.2 Private Key (m out of n) Multi-Person Control 48
6.2.3 Private Key Escrow 48
6.2.4 Private Key Backup 48
6.2.5 Private Key Archival 48
6.2.6 Private Key Transfer Into or From a Cryptographic Module 49
6.2.7 Private Key Storage on Cryptographic Module 49
6.2.8 Method of Activating Private Key 49
6.2.8.1 Class 2 Certificates 49
6.2.8.2 Enterprise RAs using a Cryptographic Module (with Automated Administration or with Managed PKI Key Manager Service) 49
6.2.8.3 Private Keys Held by Processing Centers 49
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 50
6.4 Activation Data 51
6.4.1 Activation Data Generation and Installation 51
6.4.2 Activation Data Protection 52
6.5 Computer Security Controls 52
6.5.1 Specific Computer Security Technical Requirements 52
6.5.2 Computer Security Rating 52
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 53
6.7 Network Security Controls 53
6.8 Time-stamping 54

7 Certificate, CRL and OCSP Profiles 55

7.1 Certificate Profile 55
7.1.1 Version Number(s) 55

7.1.2 Certificate Extensions *55*
7.1.2.1 Key Usage 55
7.1.2.2 Certificate Policies Extension 56
7.1.2.3 Subject Alternative Names 56
7.1.2.4 Basic Constraints 56
7.1.2.5 Extended Key Usage 56
7.1.2.6 CRL Distribution Points 57
7.1.2.7 Authority Key Identifier 57
7.1.2.8 Subject Key Identifier 57
7.1.3 Algorithm Object Identifiers *58*
7.1.4 Name Forms *58*
7.1.5 Name Constraints *58*
7.1.6 Certificate Policy Object Identifier *58*
7.1.7 Usage of Policy Constraints Extension *58*
7.1.8 Policy Qualifiers Syntax and Semantics *58*
7.1.9 Processing Semantics for the Critical Certificate Policies Extension *58*
7.2 CRL Profile 58
7.2.1 Version Number(s) *59*
7.2.2 CRL and CRL Entry Extensions *59*
7.3 OCSP Profile 59
7.3.1 Version Number(s) *59*
7.3.2 OCSP Extensions *59*

8 Compliance Audits and other Assessments 60

8.1 Frequency and Circumstances of Assessment 60
8.2 Identity/Qualifications of Assessor 60
8.3 Assessor's Relationship to Assessed Entity 60
8.4 Topics Covered by Assessment 60
8.5 Actions Taken as a Result of Deficiency 61
Communications of Results 61
8.6 61

9 Other Business and Legal Matters 62

9.1 Fees 62
9.1.1 Certificate Issuance or Renewal Fees *62*
9.1.2 Certificate Access Fees *62*
9.1.3 Revocation or Status Information Access Fees *62*
9.1.4 Fees for Other Services *62*
9.2 Financial Responsibility 62
9.2.1 Insurance Coverage *62*
9.2.2 Other Assets *62*
9.3 Confidentiality of Business Information 63
9.3.1 Scope of Confidential Information *63*
9.3.2 Information Not Within the Scope of Confidential Information *63*
9.3.3 Responsibility to Protect Confidential Information *63*
9.4 Privacy of Personal Information 63
9.4.1 Privacy Policy *63*
9.4.2 Information Treated as Private *64*
9.4.3 Information Not Deemed Private *64*
9.4.4 Responsibility to Protect Private Information *64*
9.4.5 Notice and Consent to Use Private Information *64*
9.4.6 Sharing Information Due to Legal Subpoena *64*
9.4.7 Sharing Information in Relation to Private Law Argumentation *64*
9.4.8 Sharing Information After a Request by the Owner *64*
9.4.9 Making Certificate Revocation Information Public *65*

9.4.10 Other Information Disclosure Circumstances *65*
9.5 Intellectual Property Rights 65
9.5.1 Property Rights in Certificates and Revocation Information *65*
9.5.2 Property Rights in the CPS *65*
9.5.3 Property Rights in Names *65*
9.5.4 Property Rights in Keys and Key Material *65*
9.6 Representations and Warranties 66
9.6.1 CA Representations and Warranties *66*
9.6.2 RA Representations and Warranties *66*
9.6.3 Subscriber Representations and Warranties *66*
9.6.4 Relying Party Representations and Warranties *66*
9.6.5 Representations and Warranties of Other Participants *66*
9.7 Disclaimers of Warranties 66
9.8 Limitations of Liability 66
9.9 Indemnities 66
9.9.1 Indemnification by Subscribers *66*
9.9.2 Indemnification by Relying Parties *66*
9.10 Term and Termination 67
9.10.1 Term *67*
9.10.2 Termination *67*
9.10.3 Effect of Termination and Survival *67*
9.11 Individual Notices and Communications with Participants 67
9.12 Amendments 67
9.12.1 Procedure for Amendment *67*
9.12.2 Notification Mechanism and Period *68*
9.12.2.1 Comment Period 68
9.12.2.2 Mechanism to Handle Comments 68
9.12.3 Circumstances under Which OID Must be Changed *68*
9.13 Dispute Resolution Provisions 68
9.13.1 Disputes among KPN and Customers *68*
9.13.2 Disputes with End-User Subscribers or Relying Parties *68*
9.13.3 Governing Law *69*
9.14 Compliance with Applicable Law 69
9.15 Miscellaneous Provisions 69
9.15.1 Entire Agreement *69*
9.15.2 Assignment *69*
9.15.3 Severability *69*
9.15.4 Enforcement (Attorney's Fees and Waiver of Rights) *69*
9.15.5 Force Majeure *69*
9.16 Other Provisions 69

Annex 1 CA model 70

Annex 2 Acronyms 71

Annex 3 Definitions 72

1 INTRODUCTION

This document is the KPN Certification Practice Statement (“CPS”). It describes the practices that KPN Certification Authorities (“KPN 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 Trust Network Certificate Policies (“CP”) and European Directive Policies (“EDP”).

The CP and EDP are the principal statements of policies governing the Symatec Trust Network (“SSTNSTN”). The CP and EDP establish the business, legal, and technical requirements for approving, issuing, managing, using, revoking, and renewing, digital Certificates within the STNSTN and providing associated trust services. These requirements, called the “STNSTN Standards”, protect the security and integrity of the STN, apply to all STN Participants, and thereby provide assurances of uniform trust throughout the STN. More information concerning the STN and STN Standards is available in the CP.

Symantec and each Affiliate have authority over a portion of the STN. The portion of the STN controlled by Symantec or an Affiliate is called its Subdomain of the STN. An Affiliate’s Subdomain includes entities subordinate to it such as its Customers, Subscribers, and Relying Parties (collectively called the Affiliate’s Subdomain Participants). KPN, Symantec and each of the Affiliates have a CPS that governs its Subdomain within the STN.

The structure of this CPS generally corresponds to the ‘Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework’ known as the RFC 3647 Standard of the Internet Engineering Task Force (see http://www.ietf.org for more information.)

KPN operates as Certification Service Provider (“CSP”) within the STN, for both KPN Customers and former KPN Customers. The name KPN is used throughout this document and refers to KPN as CSP in general. Where KPN CAs, KPN CRL or OCSP and KPN Certificates are explicitly mentioned, the former KPN CAs, CRLs, OCSP and Certificates are also referred to. It does not refer to other services offered by KPN. KPN B.V. is explicitly mentioned whenever it is referred to.

1.1 Overview

1.1.1 Target Group and Guidelines

This CPS’s primary target group consists of:

- Subscribers,
- Subjects (if applicable),
- Relying Parties.

1.1.2 CPS Purpose

KPN currently offers only Class 2 Certificates, see Appendix 1. This CPS describes how KPN meets the relevant CP and EDP requirements within its Subdomain. Thus, the CPS, as a single document, covers practices and procedures concerning the issuance and management of the mentioned Certificate Classes. Private CAs and hierarchies managed by KPN are outside the scope of this CPS.

This CPS describes, among other things:

- Obligations of Certification Authorities, Registration Authorities, Subscribers, and Relying Parties within KPN’s Subdomain of the STN,

- Legal matters that are covered in Subscriber Agreements and Relying Party Agreements within KPN's Subdomain,
- Audit and related security and practices reviews that KPN and KPN Subdomain Participants undertake,
- Methods used within KPN's Subdomain to confirm the identity of Certificate Applicants for each Class of Certificate,
- Operational procedures for Certificate lifecycle services undertaken in KPN's Subdomain: Certificate Applications, issuance, acceptance, revocation, and renewal,
- Operational security procedures for audit logging, records retention, and disaster recovery used within KPN's Subdomain,
- Physical, personnel, key management, and logical security practices of KPN Subdomain Participants,
- Certificate and Certificate Revocation List content within KPN's Subdomain, and
- Administration of the CPS, including methods of amending it.

The CPS is only one of a set of documents relevant to KPN's Subdomain of the STN. These other documents include:

- Ancillary security and operational documents that supplement the CP and this CPS by providing more detailed requirements, such as:
  - The KPN and Symantec Security Policies, which sets forth security principles governing the STN infrastructure,
  - The Symantec Security and Audit Requirements Guide, which describes detailed requirements for KPN concerning personnel, physical, telecommunications, logical, and cryptographic key management security,
  - The Symantec Enterprise Security Guide, which describes detailed requirements for Managed PKI Customers concerning personnel, physical, telecommunications, logical, and cryptographic key management security, and
  - Symantec Key Ceremony Reference Guide, which presents detailed key management operational requirements.
- Ancillary agreements imposed by KPN, such as the KPN Master Services Agreement and the KPN Relying Party and Subscriber agreements. These agreements would bind Customers, Subscribers, and Relying Parties of KPN. Among other things, the agreements flow down STN Standards to these STN Participants and, in some cases, state specific practices for how they must meet STN Standards.

In many instances, the CPS refers to these ancillary documents for specific, detailed practices implementing STN Standards where including the specifics in the CPS could compromise the security of KPN's Subdomain of the STN.

1.1.3 CP/CPS Relationship

While the CP and EDP set forth requirements that STN Participants must meet, this CPS describes how KPN meets these requirements within KPN's Subdomain of the STN. More specifically, this CPS describes the practices that KPN employs for:

- securely managing the core infrastructure that supports the STN, and
  issuing, managing, revoking, and renewing STN Certificates within KPN's Subdomain of the STN, in accordance with the requirements of the CP/EDP and the STN Standards.[1]

[1] Although DigiCert CAs certify the STN CAs of Affiliates, the practices relating to an Affiliate are covered in the Affiliate's CPS

1.1.4 Status

This CPS goes into effect the day it is published (see date on title page) and remains valid as long as the KPN service continues or until the CPS is replaced by a newer version (in which case the version number is to be increased by 1 in the case of major changes or by 0.1 in the case of minor changes of an editorial nature).

1.2 Document Name and Identification

The formal name of this document is: 'KPN Certification Practice Statement' but it may also be referred to as 'KPN CPS' or simply 'CPS' in the course of this document. Wherever this acronym is used, this document is referred to.

1.3 PKI Participants

The STN community of users consists of Certification Authorities, Registration Authorities, Subscribers and Relying Parties.

1.3.1 Certification Authorities

The term Certification Authority (CA) is an umbrella term that refers to all entities authorized to issue public key certificates within the STN. The CA term encompasses a subcategory of issuers called Primary Certification Authorities (PCA). PCAs act as roots of four domains, one for each class of Certificate. Each PCA is a Symantec entity. Subordinate to the PCAs are Certification Authorities that issue Certificates to end-user Subscribers or other CAs.

KPN enterprise customers may operate their own CAs as subordinate CAs to a KPN CA. Such a customer enters into a contractual relationship with KPN to abide by all the requirements of the STN CP and the KPN CPS. These subordinate CAs may, however implement 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 and initiates or passes along revocation requests for certificates for end-user certificates on behalf of a CA. KPN may act as an RA for certificates it issues. Third parties, who enter into a contractual relationship with KPN, may operate their own RA and authorize the issuance of certificates by a KPN CA. Third party RAs must abide by all the requirements of the STN CP, the KPN CPS and the terms of their enterprise services agreement with KPN. RAs may, however implement more restrictive practices based on their internal requirements.[2]

1.3.3 Subscribers

Subscribers under the STN include all end users (including entities) of certificates issued by a STN CA. 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

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

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 Symantec 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 it may also include the Subject. The context of its use in this CPS will invoke the correct understanding.

CAs are technically also subscribers of certificates within the STN, 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.

1.3.4 Relying Parties

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

1.3.5 Other Participants

No stipulation.

1.4 Certificate Usage

Certificates issued by KPN are issued in accordance with the requirements of the STN CP.

1.4.1 Appropriate Certificate Usages

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, by the STN CP, by any CPS under which the certificate has been issued and any agreements with Subscribers.

Certificate Class	***Assurance Level***		***Usage***		
	Medium assurance	High assurance	Signing	Encryption	Client Authentication
Class 2	X		X	X	X

Table 1. Individual Certificate Usage

1.4.1.2

1.4.1.2 Assurance levels

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.

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. KPN 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. 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.

KPN periodically re-keys 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 re-keyed. KPN 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.

1.5 CPS Administration

1.5.1 Organization Administering the Document

The organization administering this CPS is the KPN Policy Management Authority (“PMA”). Inquiries to KPN PMA should be addressed as follows:

KPN B.V.
Attn: KPN Security Services, Policy Management Authority
Fauststraat 1
P.O. Box 9105
7300 HN Apeldoorn
The Netherlands
Phone: +31 (0)88 661 05 00
E-mail: pkisupport@kpn.com

1.5.2 Contact Person

Address inquiries about the CPS to the address identified in CPS § 1.5.1

For commercial questions on certificates and related services write to pkisales@kpn.com. More information on Certification Services offered by KPN can be found in the Electronic Repository at https://certificaat.kpn.com/repository.

Other documents pertaining to services related to KPN Certificates can be found in the Electronic Repository.

1.5.3 Person Determining CP Suitability for the Policy

The organization identified in CPS § 1.5.1 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 and applicable under the CP, EDP 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 KPN Repository located at: https://certificaat.kpn.com/repository/. Updates supersede any designated or conflicting provisions of the referenced version of the CPS.

1.6 Definitions and Acronyms

See Appendix 2 and 3 for tables of acronyms and definitions.

2 Publication and Repository Responsibilities

2.1 Repository

KPN is responsible for the repository functions for its own CAs and the CAs of its customers. KPN publishes Certificates it issues in the KPN repository in accordance with CPS § 2.2.

Upon revocation of an end-user Subscriber's Certificate, KPN publishes notice of such revocation in the repository. KPN issues CRLs for its own CAs and customers within its Subdomain, pursuant to the provisions of this CPS. In addition, for customers who have contracted for Online Certificate Status Protocol ("OCSP") services, KPN provides OCSP services pursuant to the provisions of this CPS.

2.2 Publication of Certificate Information

DigiCert maintains and is responsible for a web-based repository function for STN Public Primary Certification Authorities (PCAs) and STN Infrastructure/Administrative CAs supporting the STN. See www.digicert.com/legal-repository. Among other documents, DigiCert publishes the STN CP and EDP in this repository.

KPN maintains and is responsible for the repository function within KPN's Subdomain of the STN.

KPN therefore maintains a web-based repository. See https://certificaat.kpn.com/repository/

KPN will at all times publish a current version of:

- This CPS
- STN CP and EDP
- Subscriber Agreements
- Relying Party Agreements
- Recent copies of its ETSI EN 319 411-2-certificates and WebTrust reports.

The Repository permits Relying Parties to make online inquiries regarding revocation and other Certificate status information. KPN 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.

KPN publishes the Certificates it issues on behalf of its own CAs and the CAs of customers in it's Subdomain. Upon revocation of an end-user Subscriber's Certificate, KPN shall publish notice of such revocation in the Repository. In addition, KPN 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 Subdomain.

DigiCert publishes the Certificates issued on behalf of KPN. Upon revocation of an end-user Subscriber's Certificate, Symantec shall publish notice of such revocation in the Repository. In addition, DigiCert issues Certificate Revocation Lists (CRLs) and, if available, provides OCSP services (Online Certificate Status Protocol).

Certificates are published in accordance with Table 3 below.

Certificate Type	*Publication Requirements*
STN PCA and STN 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.
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 KPN CA supporting Managed PKI Lite Certificates and CA Certificates of Managed PKI Customers	Available through query of the KPN LDAP directory server at directory.managedpki.com, only for customers enable this repository service.
OCSP Responder Certificates	Available through query of the KPN OCSP service at ocsp.managedpki.com, only for OCSP enabled managedPKI accounts
End-User Subscriber Certificates	Available to Relying Parties through query functions in the KPN repository at: https://certificaat.kpn.com/repository/ Former KPN issued Certificates are available to Relying Parties through query functions in the STN repository at: http://www.symantec.com/about/profile/policies/repository.jsp
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 serial number.

Table 3 – Certificate Publication Requirements

2.3 Certificate Publication

Issued Certificates are published in the Directory Service.

2.4 Time or Frequency of Publication

Changes in CSP-information, except for what follows in this paragraph, are published as soon as they occur or as soon as possible after the change occurs, in accordance with the applicable stipulations (e.g. see § 9.12 Amendments).
Certificates are published as soon as they are produced. The CRL is refreshed once every twelve hours.

2.5 Access Controls on Repositories

Information published in the repository portion of the KPN web site is publicly accessible information. Read only access to such information is unrestricted. KPN requires persons to agree to a Relying Party Agreement as a condition for accessing Certificates, Certificate status information, or CRLs.

KPN has implemented personal, organizational, physical and logical security measures, and furthermore uses Trustworthy Systems to prevent unauthorized persons from adding, deleting, or modifying repository entries.

3 Identification and Authentication

This section describes the process used to identify and authenticate certificate applicants during the initial registration procedure. It also describes KPN's naming criteria.

3.1 Naming

Unless indicated otherwise in the CP, and this CPS or the content of the digital certificate, names appearing in Certificates issued under STN are authenticated.

3.1.1 Types of Names

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

Attribute	***Value***
Country (C) =	"NL" or not used.
Organization (O) =	KPN B.V., KPN Corporate Market B.V., Getronics, Getronics PinkRoccade, PinkRoccade, Roccade, KPN Telecom B.V. or Koninklijke KPN N.V.
Organizational Unit (OU) =	CA Certificates may contain multiple OU attributes. Such attributes may contain one or more of the following: • CA Name • DigiCert Trust Network or Symantec Trust Network • A statement referencing the applicable Relying Party Agreement governing terms of use of the Certificate and • A copyright notice.
State or Province (S) =	Not used.
Locality (L) =	Not used.
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, issued under either a CA governed by KPN's STN Subdomain or a STN CA, 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) =	NL or US or not used.
Organization (O) =	The Organization attribute is used as follows: • KPN B.V., KPN Corporate Market B.V., Getronics, Getronics PinkRoccade, PinkRoccade, Roccade, KPN Telecom B.V. or Koninklijke KPN N.V. for Getronics and KPN OCSP Responder and individual Certificates. • Subscriber organizational name for web server Certificates and Qualified Certificates.
Organizational Unit (OU) =	End-user Subscriber Certificates may contain multiple OU attributes. Such attributes may contain one or more of the following: • Subscriber organizational unit (for organizational Certificates)

Attribute	Value
	• DigiCert Trust Network (or Symantec Trust Network) • A statement referencing the applicable Relying Party Agreement governing terms of use of the Certificate • A copyright notice • "Authenticated by KPN" and "Member, DigiCert Trust Network" (or "Symantec Trust Network") in Certificates whose applications were authenticated by KPN • Text to describe the type of Certificate.
State or Province (S) =	Indicates the Subscriber's State or Province or not used.
Locality (L) =	Indicates the Subscriber's Locality or not used.
Common Name (CN) =	This attribute includes: • The OCSP Responder Name (for OCSP Responder Certificates) • Domain name (for web server Certificates) • Name (for individual Certificates).
E-Mail Address (E) =	E-mail address (for individual 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 Class 2 Certificates.

The authenticated common name value included in the Subject distinguished names of organizational Certificates is 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

Class 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.

KPN 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

For Class 2 end-user Subscriber Certificates, end-user Subscriber pseudonyms (names other than a Subscriber's true personal or organizational name) are not permitted. KPN shall ensure that the requirements of the national data protection legislation are adhered to during the pseudonym registration process.

3.1.4 Rules for Interpreting Various Name Forms

No stipulation.

3.1.5 Uniqueness of Names

KPN ensures that Subject Distinguished Names 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 Resolving Name Claim Disputes

In cases where parties do not agree on the usage of names, KPN will decide which name to use after taking into account the interests of the parties, in far as this is not covered by imperative Dutch law or other relevant laws.

3.1.7 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. KPN, 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. KPN is entitled, without liability to any Certificate Applicant, to reject or suspend any Certificate Application because of such disputes.

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 of proving possession of a private key shall be PKCS #10, an other cryptographically equivalent demonstration, or an other KPN approved method. This requirement does not apply where a key pair is generated by a CA on behalf of a Subscriber, e.g. pregenerated keys placed on SSCD's.

3.2.2 Authentication of Organizational Identity

Whenever a certificate contains an organization's name, the identity of the organization and other enrollment information provided by Certificate Applicants is confirmed in accordance with the procedures set forth in KPN's documented Validation Procedures.

At a minimum KPN 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, KPN authenticates the Organization's right to use that domain name either as a fully qualified Domain name or an e-mail domain.

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 KPN when required.

3.2.3 Authentication of Individual Identity

Authentication of individual identity differs according to the Class of Certificate. The minimum authentication standard for each class of STN certificate KPN supplies, is explained in the following paragraphs.
The subscriber/applicant proves his/her identity. KPN authenticates identity by matching the identity provided by the subscriber to:

- Information residing in the database of a DigiCert / KPN approved identity proofing service, such as a major credit bureau of other reliable source of information provision, or
- Information contained in the business information (employee or customer directories) of an RA approving certificates to its own affiliated individuals.

3.2.4 Non-Verified Subscriber Information

Non-verified subscriber information includes:

- Organization Unit (OU)
- 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 as to indicate the individual's affiliation or authorization to act on behalf of the Organization KPN 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

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

DigiCert shall only allow interoperation with the STN of a non-STN CA in circumstances where the CA, at a minimum:

- Enters into a contractual agreement with DigiCert
- Operates under a CPS that meets STN requirements for the classes of certificates it will issue
- Passes a compliance assessment before being allowed to interoperate
- Passes an annual compliance assessment for ongoing eligibility to interoperate.

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. KPN generally requires that the Subscriber generate a new key pair to replace the expiring key pair (technically defined as a "re-key") However, in certain cases (i.e., for web server certificates) Subscribers may request a new certificate for an existing key pair (technically defined as a "renewal").

Generally speaking, both "Re-key" 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 Classes and Types of KPN Certificates this distinction is not important as a new key pair is always generated as part of KPN'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 re-key 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 a Challenge Phrase with their enrollment information. Upon renewal of a Certificate, if a Subscriber correctly submits the Subscriber's Challenge Phrase (or the equivalent thereof) with the Subscriber's re-enrollment 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) KPN 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, KPN will issue the Certificate if the enrollment information (including Corporate and Technical contact information[3]) has not changed.

After re-keying or renewal in this fashion, and on at least alternative instances of subsequent re-keying or renewal thereafter, KPN or the RA reconfirms the identity of the Subscriber in accordance with the identification and authentication requirements of an original Certificate Application.[4]

In particular, for subsequent re-key requests for retail Class 3 Organizational SSL Certificates, KPN reauthenticates the Organization name and domain name included in the certificate. In circumstances where:

- The challenge phrase is correctly used for the subsequent renewal certificate, or a confirmatory response is obtained to an e-mail to the corporate contact and:
- The certificate Distinguished Name has not been changed, and
- The Corporate and Technical Contact information remains unchanged from that which was previously verified,

KPN 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

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

[4] The authentication of a request to re-key/renew a Class 3 Organizational ASB Certificate, however, requires the use of a Challenge Phrase as well as the same identification and authentication as for the original Certificate Application.

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

Re-key requests received more than 30 days after expiration of the Certificate are reauthenticated as an original Certificate Application and are not automatically issued.

The KPN CA-Certificate is not routinely renewed. The validity of the CA-Certificate is extended around five years before its expiration (if so desired) or it is renewed if there has been a change in information it contains. It is also renewed if the key-pair validity is in danger of expiring. Renewal of the CA-Certificate is carried out in accordance with a strict procedure.

3.3.2 Identification and Authentication for Re-key After Revocation

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

- the Certificate was issued to a person other than the one named as the Subject of the Certificate, or
- the Certificate was issued without the authorization of the person or entity named as the Subject of such Certificate, or
- 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
- For any other reason deemed necessary by KPN 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 is in fact the Subscriber of the Certificate. Renewed organizational Certificates shall contain the same Subject distinguished name as the Subject distinguished name of the organizational Certificate being renewed.

During renewal of an individual Certificate following revocation KPN must ensure that the person seeking renewal is, in fact, the Subscriber. One acceptable procedure is the use of a Challenge Phrase (or the equivalent thereof). Other than this procedure or another Symantec approved procedure, the requirements for the identification and authentication of an original Certificate Application shall be used for renewing a Certificate following revocation.

3.4 Identification and Authentication for Revocation Request

Prior to the revocation of a Certificate, KPN 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.
- 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 Class 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.

KPN Administrators are entitled to request the revocation of end-user Subscriber Certificates within KPN's Subdomain. KPN authenticates the identity of Administrators via access control using SSL and

client authentication before permitting them to perform revocation functions, or other STN approved procedures.

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

Requests to revoke a CA Certificate shall be authenticated by KPN 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

Only an authorized representative of an Organization or entity, including an authorized representative of a CA or a RA, may submit certificate applications.

4.1.2 Responsibilities and Obligations

The obligations and responsibilities of parties involved - KPN, Subscriber and Relying Party - have been described in the Subscriber and Relying Party Agreement.

4.1.2.1 Responsibilities and Obligations of the CSP

KPN is ultimately responsible for the complete certification service and guarantees its Subscribers and Relying Parties that it will adhere to the applicable General and Specific Conditions, the CPS and all applicable CPs.

4.1.2.2 Responsibilities and Obligations of the Client

The Subscriber is responsible for correctly supplying all necessary information for the production and issuance of certificates and for the correct usage of those certificates. The Subscriber guarantees to KPN and Relying Parties that it will adhere to the applicable General and Specific Conditions, the CPS and all applicable CPs.

4.1.2.3 Responsibilities and Obligations of the End-user Subscriber

The Subject, as the one who holds the Certificate that has been requested on behalf of the Subscriber, is also responsible for correctly supplying all necessary information for the production and issuance of certificates and for the correct usage of those certificates. The Subject guarantees KPN, the Subscriber and the Relying Parties that he/she will adhere to the applicable General and Specific Conditions, the CPS and all applicable CPs.

4.1.2.4 Responsibilities and Obligations of the Relying Party

The Relying Party is responsible for correctly trusting a Certificate and guarantees KPN, the Subject and the Subscriber that it will adhere to the applicable General and Specific Conditions, the CPS and all applicable CPs.

4.1.3 Enrollment Process and Responsibilities

All end-user Certificate Subscribers shall manifest assent to the relevant Subscriber Agreement that contains representations and warranties described in § 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 KPN,

- demonstrating possession of the private key corresponding to the public key delivered to KPN.

KPN has identified two steps in the processing of an application it receives. The first step in processing an application consists of registering the application, determining the completeness and accuracy of the application and supporting documents, and reaching a decision on the application. The second step entails the execution of the decision, the production and issuance of the certificate, and the informing of those involved.
Subscribers of CA and RA Certificates enter into a contract with KPN. 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 KPN 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

For all Certificates KPN or an RA shall perform identification and authentication of all required Subscriber information in terms of § 3.2.

4.2.2 Approval or Rejection of Certificate Applications

KPN, 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 § 3.2,
- Payment information has been received.

KPN, or an RA, will reject a certificate application if:
- Identification and authentication of all required Subscriber information in terms of § 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 information has not been received, or
- The RA believes that issuing a certificate to the Subscriber may bring the STN into disrepute.

4.2.3 Time to Process Certificate Applications

KPN takes 2 to 5 business days to process certificate applications for STN end-entity certificates. Qualified Certificates take a maximum of 10 business days.

4.3 Certificate Issuance

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

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

KPN publishes the Certificates it issues in a publicly accessible repository.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

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

4.4.4 Notifications to Subscriber by the CA of Issuance of Certificate

KPN shall, either directly or through an RA, notify Subscribers that it has 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, or information on how to obtain the certificate.

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 KPN's Subscriber Agreement, the terms of the STN 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.

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. KPN 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. Certificate renewal is supported for Class 3 certificates where the key pair is generated on a web server as most web server key generation tools permit the creation of a new Certificate Request for an existing key pair.

4.6.1 Circumstances for Certificate Renewal

Prior to the expiration of an existing valid 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 for Class 2 certificates 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[5]) has not changed, a renewal Certificate is automatically issued. As an alternative to using a Challenge Phrase (or equivalent) KPN 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.

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

Upon receipt of confirmation authorizing issuance of the Certificate, KPN will issue the Certificate if the enrollment information (including Corporate and Technical contact information[6]) has not changed.

After renewal in this fashion, and on at least alternative instances of subsequent renewal thereafter, KPN 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.

In particular, for subsequent renewal requests for retail Class 3 Organizational SSL Certificates, KPN reauthenticates the Organization name and domain name included in the certificate. In circumstances where:

- The Challenge Phrase is correctly used for the subsequent renewal certificate, or a confirmatory response is obtained to an e-mail to the corporate contact, and:
- The certificate Distinguished Name has not been changed, and
- The Corporate and Technical Contact information remains unchanged from that which was previously verified,

KPN 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.

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

KPN does not offer routine renewals of Qualified Certificates. A request for renewal will be processed as a request for a new Certificate. The Subject Serial Number of the Certificate will be transferred to the renewed Certificate.

4.6.4 Notification of New Certificate Issuance to Subscriber

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

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

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

4.6.6 Publication of the Renewal Certificate by the CA

The renewed certificate is published in KPN'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.

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

4.7 Certificate Re-Key

Certificate re-key is the application for the issuance of a new certificate that certifies the new public key. Certificate re-key is supported for all certificate Classes, except Qualified Certificates.

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[7]) has not changed, a renewal Certificate is automatically issued. Subject to the provisions of § 3.3.1, after re-keying in this fashion, and on at least alternative instances of subsequent re-keying thereafter, KPN 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 KPN 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 § 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 § 4.4.1

4.7.6 Publication of the Re-Keyed Certificate by the CA

The re-keyed certificate is published in KPN's publicly accessible repository.

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

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).

KPN does not offer the possibility of modifying the content of Certificates. If the information contained in the Certificate is no longer accurate, the Subscriber must immediately revoke the Certificate. After revoking the Certificate, the Subscriber may apply for a new Certificate, if desired.

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

4.8.2 Who May Request Certificate Modification

See § 4.1.1

4.8.3 Processing Certificate Modification Requests

KPN or an RA shall perform identification and authentication of all required Subscriber information in terms of § 3.2

4.8.4 Notification of New Certificate Issuance to Subscriber

See § 4.3.2

4.8.5 Conduct Constituting Acceptance of Modified Certificate

See § 4.4.1

4.8.6 Publication of the Modified Certificate by the CA

See § 4.4.2

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

See § 4.4.3

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

In the following cases, the Subscriber and/or the Subject is required to immediately submit a request for revocation of the Certificate by KPN :

- KPN, a Customer, or a Subscriber has reason to believe or strongly suspects that there has been a Compromise of a Subscriber's private key,

- KPN 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 a customer and a Subscriber is terminated or has otherwise ended,
- KPN or a Customer has reason to believe that the Certificate was issued in a manner not materially in accordance with the procedures required by the applicable CPS, the Certificate was issued to a person other than the one named as the Subject of the Certificate, or the Certificate was issued without the authorization of the person named as the Subject of such Certificate,
- KPN or a Customer has reason to believe that a material fact in the Certificate Application is false,
- KPN or a Customer determines that a material prerequisite to Certificate Issuance was neither satisfied nor waived,
- The information within the Certificate, other than Non-verified Subscriber Information, is incorrect or has changed, or
- The continued use of the certificate is harmful to the STN.
- When considering whether certificate usage is harmful to the STN, KPN 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

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

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

KPN can unilaterally revoke certificates if the Subscriber or end-user Subscriber do not fulfill their responsibilities as stipulated in the Subscriber Agreement and/or the Relying Party Agreement. KPN always records its motivations for unilateral revocation of a certificate and communicates them to the affected parties.

KPN ensures that the date and time of revocation of Certificates can be exactly determined. In case of doubt, the point in time give by KPN will be considered the time of revocation.

4.9.2 Who Can Request Revocation?

Subscribers and Subjects can request the revocation of their own individual Certificates. 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 KPN 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 KPN 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 KPN 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 KPN for processing. Communication of such revocation request shall be in accordance with CPS § 3.4.

Where a customer initiates revocation of an end-user Subscriber Certificate upon its own initiative, the Managed PKI Customer instructs KPN 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 KPN. KPN will then revoke the Certificate. KPN 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. As mentioned earlier: if immediate revocation is necessary due to an emergency situation, it should be requested electronically, using the online / real time revocation service.

4.9.5 Time within Which CA Must Process the Revocation Request

Revocation requests handled via the KPN website will be revoked online / in real time, and it is guaranteed that they will be revoked within twenty-four hours of receiving the request at the latest. Revocation requests received in writing by mail will be processed one business day after they are received. There is a guarantee that they will be processed within twenty-four hours. KPN takes commercially reasonable steps to process these revocation requests without delay.

4.9.6 Revocation Checking Requirements for Relying Parties

Relying Parties are required to check the current status (revoked / not revoked) of a Certificate by consulting the certificate status information. Certificate status information can be obtained by consulting the CRL, OCSP or Directory Service. Furthermore, Relying Parties are expected to check the reliability of such information.

Revoked Certificates remain on the CRL as long as their original expiry date has not been reached yet. After the expiry date, Relying Parties can only verify the status of the Certificate by consulting KPN's Directory Service or by making use of OCSP.

KPN 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. Generally, this information is available from the Certificate itself.

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 yearly, but 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.

4.9.8 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. However, it is always done within the legally allowed time (if applicable).

4.9.9 On-Line Revocation/Status Checking Availability

In addition to the publication of CRLs, KPN also offers certificate status information through the so-called OCSP. The setup of the OCSP is in accordance with IETC RFC 6960.

OCSP validation is an online validation method in which KPN sends the Relying Party an electronically signed message (OCSP response) in answer to a specific request for status information (OCSP request) sent by the Relying Party to the KPN's OCSP service (OCSP responder). The OCSP response contains the requested status information of the Certificate concerned.

The OCSP responder can be reached through its URL as contained in the Certificate concerned.

The status of a certificate can take on one of three values: good, revoked or unknown. If, for whatever reason, no OCSP response is received, no conclusions regarding the status of the certificate can be drawn. The OCSP responder URL that can be used to validate the revocation status of a Certificate can be found in the AuthorityInfoAccess.uniformResourceIndicator attribute of the certificate.

An OCSP response always gets sent and signed by the OCSP responder. The Relying Party is required to verify the OCSP response signature by comparing it to the system certificate sent along in the OCSP response. This system certificate and the Certificate whose status is being checked are both issued by the same CA.

The information given by an OCSP responder may be more up to date than the information in the CRL. This is only the case if a revocation has taken place and the regular update of the CRL has not taken place yet.

4.9.10 Other Forms of Revocation Advertisements Available

In addition to making use of the CRL and OCSP, the revocation status of a certificate can also be determined by consulting the Directory Service.

4.9.11 Special Requirements regarding Key Compromise

KPN uses commercially reasonable efforts to notify potential Relying Parties if it discovers, or has 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 subdomains.

4.9.12 Certificate Suspension

Suspension of certificates is not supported by KPN.

4.10 Certificate Status Service

The Status of certificates is available via CRL at KPN's website, Directory Service and via an OCSP responder (where available). Certificate Status Services are available 7 days a week, 24 hours a day.

Even in the case of system malfunctions, system service activities or other factors beyond the control of KPN. KPN has designed a backup site and backup scenario that is regularly tested in conjunction with redundant data processing and storage.

4.11 End of Subscription

A subscriber may end a subscription for a KPN 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 certificate.

4.12 Key Escrow and Recovery

With the exception of enterprises deploying a KPN key recovery service to Managed PKI, no STN participant may escrow CA, RA or end-user Subscriber private keys.

Customers using a KPN key recovery service can escrow copies of the private keys of Subscribers whose Certificate Applications they approve. KPN 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 a KPN key recovery service are permitted to escrow end-user Subscribers' private keys. 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 KPN), 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 KPN key recovery service, 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 Administrators and other persons of a KPN key recovery service from obtaining unauthorized access to private keys.

It is recommended that customers using Key Manager 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.
- 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 on the enterprise's premises 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 mask generated in hardware and destroyed. Only the resulting masked session key (MSK) is securely sent and stored at KPN. The KER (containing the end user's private key) and the random session key mask are stored in the Key Manager database on the enterprise premises.

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 operated out of KPN's secure data center. The Key Manager combines the MSK with the random session key mask and regenerates 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.

4.12.3 Private Key Escrow for Qualified Certificates

CA private keys and end-user Subscriber signature private keys shall not be escrowed. Therefore, notwithstanding the provision of CPS § 4.12.1, Managed PKI Customers shall not use the Managed PKI Key Manager service to escrow end-user Subscribers single private key (in single key pair systems).

Managed PKI Customers wishing to use the Managed PKI Key Manager service shall use dual key pair systems and escrow only the decryption private keys of end-user Subscribers.

5 Facility, Management, and Operational Controls

The section of KPN that is responsible for providing certification services is ISO9001: 2000, ISO27001:2005 and ETSI or WebTrust certified. Both the Quality Management System and the Information Security Management System make use of the PDCA-cycle to ensure continual system improvement.

The infrastructure (Enterprise Service Center) used to facility the Managed PKI Client Certificates of former KPN Customers, is hosted by DigiCert. Therefor the Facility, Management, and Operational Controls are described in the DigiCert CPS, chapter 5.

5.1 Physical Controls

KPN has described and implemented a Physical Security Policy. This policy meets the STN's Security and Audit Requirements. This Physical Security Policy contains sensitive security information and is not available for the public. An overview of the measures taken is described below.

5.1.1 Site Location and Construction

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

5.1.2 Physical Access

KPN 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/or 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 HSMs 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 HSMs are protected through the use of locked cabinets. Offline HSMs are protected through the use of locked safes, cabinets and containers.

Access to HSMs and keying material is restricted in accordance with STN'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

KPN'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

KPN has taken reasonable precautions to minimize the impact of water exposure to KPN systems, including but not limited to, the choice for a geographical location which is, for it's primary location, above sea level. It's secondary location being beneath sea level is a more than accepted risk in the Netherlands.

5.1.5 Fire Prevention and Protection

KPN has taken reasonable precautions to prevent and extinguish fires or other damaging exposure to flame or smoke. KPN'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 are stored within KPN facilities 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

KPN has a contract with a professional waste disposal company for the safe disposal of waste, used paper and such. KPN personnel is required to dispose of used paper in the closed paper disposal containers located throughout the building.

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 KPN's normal waste disposal requirements.

5.1.8 Off-site Backup

KPN 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 KPN's disaster recovery facility.

5.2 Procedural Controls

Security tasks and responsibilities, including confidential tasks, are documented in job descriptions. These are based on the segregation of duties and the sensitivity of the job is also indicated. Whenever necessary, a differentiation between general jobs and specific CSP jobs is made in the additional detailed role descriptions.

Procedures have been developed and are implemented for all confidential and administrative tasks that influence the delivery of Certification Services.

The authorizations of CSP personnel are based on a need-to-know principle.

5.2.1 Confidential jobs

KPN has implemented a Trusted Employee Policy. Among others, this policy describes which categories of personnel have a “Trusted” status. It mainly concerns personnel that are involved in the management of certificates and key material, personnel that are involved in system development, management, and maintenance and personnel within security management, quality management and auditing. See also § 5.3.2 Trusted Employee Policy.

KPN 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 the Trusted Employee Policy.

5.2.2 Number of Persons Required per Task

Several personnel are required for the execution of certain, previously defined, activities in the areas of key and certificate management, system development, maintenance and management. The necessity to have several people working on a certain activity is enforced through technical measures, authorizations combined with identification/authentication, and additional procedures.

5.2.3 Management and Security

KPN applies ITIL management processes to ensure procedural security. ITIL is a methodology for the standardization of IT management processes that is focused on bringing the quality of these processes to a certain level and maintaining that quality.

KPN has separate systems for development, testing, acceptance and production. These systems are managed using the aforementioned ITIL procedures. The procedure for change management is used to monitor the transfer of programs from one environment to another. This procedure includes things like the monitoring and registration of versions, modifications and emergency repairs of all operational software.

The integrity of all systems and information used for Certificates is protected from viruses, harmful software and other possible disruptions of service through a tailored combination of physical, logical and organizational measures. These measures are preventative, inhibitive and curative in nature. For example, measures taken include: logging, firewalls, intrusion detection and redundancy of systems.

KPN has provided for timely, coordinated action to be taken to react quickly to incidents and to limit the influence of intrusion on the security system. All incidents are reported as soon as possible after their occurrence.

5.2.4 Separation of Duties

KPN maintains a separation between executive, decision making and monitoring duties. Furthermore separation is maintained between system management and operation of the systems used for Certificates, as well as between security officers, system auditors, system managers and system operators.

5.3 Personnel Controls

5.3.1 Trusted Employee Policy

KPN has drafted and implemented a Trusted Employee Policy for its Certification Service. The Policy describes at great length how to deal with things like pre-employment screening (mandatory for employees involved in certification services), the delivery of a Certificate of Behavior ("*Verklaring omtrent het Gedrag*") required by the Law on Justice Information ("*Wet Justitiële Informatie*"), and the implementation of security investigations for services like the General Intelligence and Security Service ("*Algemene Inlichtingen- en Veiligheidsdienst*") or the Military Intelligence and Security Service ("*Militaire Inlichtingen- en Veiligheidsdienst*") in order to obtain a Declaration of No Objection ("*Verklaring van Geen Bezwaar*"). The policy also describes the options open to management if a (future) employee refuses to cooperate or if the result of the investigation is negative.

Other stipulations from the Trusted Employee Policy are:

- A trusted duty or role may only be carried out by an employee after the relevant security screening has been completed without objections having come forward, and he or she has been formally appointed as Trusted Employee by the management.
- Assessing the security risks during a person's employment is the responsibility of the employee's supervisor, as part of the PPM-cycle.

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 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.

5.3.2 Expertise, Experience and Qualifications

KPN employs personnel with sufficient expertise, experience and qualifications for the delivery of Certificates.

KPN has determined what knowledge and experience is needed for proper execution of each task. Because of the rapid developments in the specialism, this knowledge is actively maintained. KPN also registers the knowledge and experience of each of its employees. As part of the annual Planning and Control cycle, a training plan is developed and after it is approved, the necessary budget for execution of the plan is made available. The implementation of the plan is closely monitored and the courses followed are registered. Professional training is stimulated wherever possible and where necessary it is made mandatory. Employees are also trained on the job. The training offered employees covers a wide range of knowledge so that, on the one hand, they can be widely deployed, while on the other hand, it is possible to offer them variation in the tasks they need to perform.

A Personnel Performance Management (PPM) cycle is used to monitor employees' progress. The PPM cycle includes the setting of goals, job evaluation and assessments,.

5.3.3 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 KPN 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 KPN's secure facilities only to the extent they are escorted and directly supervised by Trusted Persons at all times.

5.3.4 Documentation Supplied to Personnel

As part of its QMS and ISMS, KPN provides its employees all the documentation needed to perform their job responsibilities competently and satisfactorily.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

KPN keeps registrations of the following events for audit purposes:
- account creation;
- installation of new software or software updates
- date and time of backups and other information describing backups;
- date and time of all hardware changes;
- date and time of audit log dumps;
- shut down and (re)start of systems;

KPN 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, re-key, 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 KPN 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
• Kind of entry.

5.4.2 Frequency of Processing Log

Audit logs are examined on a regular daily basis for significant security and operational events. In addition, KPN reviews its audit logs for suspicious or unusual activity in response to alerts generated based on irregularities and incidents within KPN, CA and RA systems.

Audit log processing consists of a review of the audit logs and documentation for all significant events in an audit log summary. Audit log reviews include a verification that the log has not been tampered with, a brief inspection of all log entries, and a more thorough investigation of any alerts or irregularities in the logs. Actions taken based on audit log reviews are also documented.

5.4.3 Retention Period for Audit-Log

Audit logs shall be retained on site for at least two (2) months after processing and thereafter archived in accordance with § 5.5.2.

5.4.4 Protection of Audit-Log

Electronic and manual audit log files are protected from unauthorized viewing, modification, deletion, or other tampering through the use of physical and logical access controls.

5.4.5 Audit Log Backup Procedures

Incremental backups of audit logs are created daily and full backups are performed weekly.

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 KPN 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. Logical security vulnerability assessments ("LSVAs") are performed, reviewed, and revised following an examination of these monitored events. LSVAs are based on real-time automated logging data and are performed on a daily, monthly, and annual basis. An annual LSVA will be an input into an entity's annual Compliance Audit.

5.5 Records Archival

5.5.1 Types of Records Archived

KPN archives:

- All audit data collected in terms of § 5.4,
- Certificate application information,
- Documentation supporting certificate applications,
- Certificate lifecycle information e.g., revocation, re-key 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.
• Ten (10) years and six (6) months for Class 2 and Class 3 Certificates
• Seven (7) years after the expiry date or date of revocation for Qualified Certificates

5.5.3 Protection of Archive

KPN implements the archiving of information itself. It ensures the integrity and availability of the archived information for the duration of the storage period through a fitting combination of security measures. All equipment and programs necessary for accessing the information are stored for the same length of time. KPN ensures all information is stored and archived carefully and securely.

5.5.4 Archive Backup Procedures

KPN incrementally backs up electronic archives of its issued Certificate information on a daily basis and performs full backups on a weekly basis.

5.5.5 Requirements for Time-Stamping of Records

The exact time and date of relevant events in the life cycle of certificates and keys are recorded. The same is true for important events in the life cycle of the systems used for or supporting the certification service.

5.5.6 Archive Collection System (Internal or External)

KPN archive collection systems are internal, except for enterprise RA Customers. KPN 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.

5.6 Key Changeover

Old keys are stored on the token if the new keys are also placed on it. Old tokens are destroyed (by zeroizing) when their life cycle and the appropriate archive period have ended.

Keys belonging to end-user Subscribers will not be reused after their validity has expired or after the revocation of the Certificates that go with them.

KPN CA key pairs are retired from service at the end of their respective maximum lifetimes as defined in this CPS. KPN 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). KPN'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") that 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

KPN has implemented a robust combination of physical, logical, and procedural controls to minimize the risk and potential impact of a key Compromise or disaster. In addition, KPN has implemented disaster recovery procedures described in CPS § 5.7.3 and Key Compromise response procedures described in CPS § 5.7.2. KPN's Compromise and disaster recovery procedures have been developed to minimize the potential impact of such an occurrence and restore KPN s operations within a commercially reasonable period of time.

In case of any of the algorithms, or associated parameters, used by KPN should become insufficient for it's remaining intended usage KPN shall:

- Inform all subscribers and relying parties;
- Revoke any affected certificate.

5.7.1 Incident and Compromise Handling Procedures

In the event of the corruption of computing resources, software, and/or data, such an occurrence is reported to KPN Security and KPN's incident handling procedures are enacted.

Such procedures require appropriate escalation, incident investigation, and incident response. If necessary, KPN's key compromise or disaster recovery procedures will be enacted.

5.7.2 Entity Private Key Compromise Procedures

Upon the suspected or known Compromise of a KPN CA, KPN infrastructure or Customer CA private key, KPN's Key Compromise Response procedures are enacted by the Compromise Incident Response Team/Crisis Team (CIRT). This team, which includes Security, Key Management, Production Services personnel, and KPN management representatives, assesses the situation, develops an action plan, and implements the action plan with approval from KPN 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 KPN repository,
- 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, except where the CA is being terminated.

5.7.3 Disaster Recovery

KPN has implemented mission critical components of its CA infrastructure in redundant configurations. This applies both to hardware and software components. In addition, CA private keys are backed up and maintained for disaster recovery purposes. KPN has implemented detailed change and incident management procedures to allow for controlled and accountable recovery from system and application disasters.

KPN has fitted a complete backup facility for its CRL and online revocation service. The programs and data at the backup facility are identical to those in the production environment and it is possible to

immediately switch to the backup facility when necessary (e.g. in case of a disaster). This kind of switch to the backup facility is regularly tested and the procedure is maintained. The backup facility is located at a different KPN location that has a similar level of security.

KPN maintains offsite backups of important CA information for KPN issued CAs within the KPN Subdomain. Such information includes, but is not limited to: application logs, Certificate Application data, audit data and database records for all Certificates issued.

5.7.4 Key Compromise

Upon the suspected or known Compromise of a KPN CA, KPN infrastructure or Customer CA private key, KPN's Key Compromise Response procedures are enacted by the Compromise Incident Response Team/Crisis Team (CIRT). This team, which includes Security, Key Management, Production Services personnel, and KPN management representatives, assesses the situation, develops an action plan, and implements the action plan with approval from KPN executive management.

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

- The Certificate's revoked status in communicated to Relying Parties through the KPN 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.

5.7.5 Secure Facility After a Natural or Other Type of Disaster

A backup scenario has been effected for the parts of the CA system not mentioned in § 5.7.3. The scenario provides for a backup within 24 hours and is maintained and tested annually.

KPN will restore all its services within one week.

5.8 CA or RA Termination

5.8.1 Termination of a KPN customer CA

In the event that it is necessary for a KPN customer CA to cease operation, the applicable Customer will develop a termination plan to minimize disruption to Subscribers and Relying parties. Such a termination plan may address the following, as applicable:

- Provision of notice to parties affected by the termination, such as subscribers and relying parties, informing them of the status of the CA,
- Handling the cost of such notice,
- The revocation of the Certificate issued to the CA by KPN,
- The preservation of the CAs archives and records for the required time periods by KPN,
- The continuation of Subscriber and customer support services by KPN,
- The continuation of revocation services, such as the issuance of CRLs or the maintenance of online status checking services by KPN,
- The revocation of unexpired unrevoked certificates of end-user Subscribers and subordinate CAs, if necessary, by KPN,
- Disposition of the CAs private key and the hardware tokens containing this private key by KPN, and

- Provisions needed for the transition of the CAs services to a successor CA, if necessary.

5.8.2 Termination of a KPN CA

In the event that it is necessary for KPN to cease operation, KPN has developed a CA Termination Plan, laid down in the CA Termination Handbook. As part of the Termination Plan, KPN and Symantec have put into place contractual agreements that include, but are not limited to, the following

- Provision of notice to parties affected by the termination, such as subscribers and relying parties, informing them of the status of the CA,
- Handling the cost of such notice,
- The revocation of the Certificate issued to the CA by KPN,
- The preservation of the CAs archives and records for the required time periods,
- The continuation of Subscriber and customer support services by Symantec,
- The continuation of revocation services, such as the issuance of CRLs or the maintenance of online status checking services by Symantec,
- The revocation of unexpired unrevoked certificates of end-user Subscribers and subordinate CAs, if necessary,
- The payment of compensation (if necessary) to 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 CAs private key and the hardware tokens containing this private key, and
- Provisions needed for the transition of the CAs 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, Issuing Root CAs and all online KPN and Managed PKI Customer CAs the cryptographic modules used for key generation meet the requirements of FIPS 140-1 level 3. For some offline CAs, the cryptographic modules used meet the requirements of at least FIPS 140-1 level 2.

All CA key pairs are generated in pre-planned Key Generation Ceremonies in accordance with the requirements of the Key Ceremony Reference Guide, the CA Key Management Tool User's Guide, and the STN Security and Audit Requirements Guide. 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 KPN 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.

Customers generate the key pair used by their Automated Administration servers. KPN recommends that Automated Administration server key pair generation be performed using a FIPS 140-1 level 2 or higher certified cryptographic module.

Generation of end-user Subscriber key pairs is generally performed by the Subscriber. For Class 2 Certificates, the Subscriber typically uses a FIPS 140-1 level 1 certified cryptographic module provided with their browser software for key generation, or a SSCD. For server Certificates, the Subscriber typically uses the key generation utility provided with the web server software.

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 KPN on hardware tokens or SSCD's, 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. The distribution of such devices is logged by KPN.

For 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 KPN 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 KPN, this requirement is not applicable.

6.1.4 CA Public Key Delivery to Relying Parties

KPN makes the CA Certificates for its PCAs and root CAs available to Subscribers and Relying Parties through their inclusion in web browser software. As new PCA and root CA Certificates are generated, DigiCert or KPN provides such new Certificates to the browser manufacturers for inclusion in new browser releases and updates.

KPN generally provides the full certificate chain (including the issuing CA and any CAs in the chain) to the end-user Subscriber upon Certificate issuance. KPN CA Certificates may also be downloaded from the LDAP Directory at directory.managedpki.com.

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.
DigiCert recommends the use of a minimum key size equivalent in strength to 2048 bit RSA for RAs and end entity certificates key pairs.
The KPN Standard for minimum key sizes is the use of key pairs equivalent in strength to 2048 bit RSA for PCAs and CAs.

All Classes of STN and KPN PCAs and CAs, and RAs and end entity certificates use SHA-2 for digital signature hash algorithm and support the use of SHA-256 and SHA-384 hash algorithms in end-entity Subscriber Certificates.

6.1.6 Public Key Parameters Generation and Quality Checking

Not applicable.

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

The Certificates, including corresponding key pairs, may only be used for the purposes described in this CPS and are published in the (Extended) Key usage extension of the Certificate.

Refer to § 7.1.2.1.

6.2 Private Key Protection and Cryptographic Module engineering Controls

KPN has implemented a combination of physical, organizational, logical, and procedural controls to ensure the security of KPN and 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, Symantec and KPN use hardware cryptographic modules that are certified at or meet the requirements of FIPS 140-1 Level 3.

For some offline CAs, KPN uses hardware cryptographic modules that are certified to at least FIPS 140-1 Level 2.

The Hardware Security Modules (HSMs) are delivered by the vendor in tamper-evident bags, a type of packaging that shows whether it has been tampered with. Each shipment is checked against its out-of-band list immediately upon arrival.

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

KPN has implemented technical and procedural mechanisms that require the participation of multiple trusted individuals to perform sensitive CA cryptographic operations. KPN 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 § 4.12.

6.2.4 Private Key Backup

KPN 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 this CPS.

KPN does not store copies of RA private keys. For the backup of end-user Subscriber private keys, see § 6.2.3 and § 4.12.

6.2.5 Private Key Archival

When KPN CA key pairs reach the end of their validity period, such CA key pairs will be archived for a period of at least 5 years. Archived CA key pairs will be securely stored using hardware cryptographic modules that meet the requirements of this CPS. Procedural controls prevent archived CA key pairs from being returned to production use. Upon the end of the archive period, archived CA private keys will be securely destroyed in accordance with this CPS.

Upon expiration of a KPN 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 their expiration date, unless the CA Certificate has been renewed in terms of this CPS.

KPN does not archive copies of RA and Subscriber private keys.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

KPN generates CA key pairs on the hardware cryptographic modules in which the keys will be used. In addition, KPN 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 are stored in encrypted form.

6.2.8 Method of Activating Private Key

All KPN Subdomain Participants protect the activation data for their private keys against loss, theft, modification, unauthorized disclosure, or unauthorized use.

6.2.8.1 Class 2 Certificates

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

- Use a password in accordance with § 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, a network logon 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.

6.2.8.2 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 § 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.

6.2.8.3 Private Keys Held by Processing Centers

An online CA's private key shall be activated by a threshold number of Shareholders, as defined in § 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

KPN CA private keys are deactivated upon removal from the token reader. KPN RA private keys (used for authentication to the RA application) are deactivated upon system log off. KPN 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 SSCD from the SSCD 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, Symantec and KPN destroy CA private keys in a manner that reasonably ensures that there are no residual remains of the key that could lead to the reconstruction of the key. Symantec and KPN utilize 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.

6.2.11 Cryptographic Module Rating

See § 6.2.1

6.3 Other Aspects of Key Pair Management

All aspects of key pair management are carried out by KPN by following careful procedures that match the intended goal.

6.3.1 Public Key Archival

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

6.3.2 Certificate Operational Periods and Key Pair Usage

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 KPN Certificates for Certificates issued on or after the effective date of this CPS are set forth in Table 7 below.

In addition, 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 (1024 bits)	Up to 30 years
PCA self-signed (2048 bits)	Up to 50 years
PCA to Offline intermediate CA	Generally 10 years but up to 15 years after renewal
PCA to online CA	Generally 5 years but up to 10 years after renewal
Offline intermediate CA to online CA	Generally 5 years but up to 10 years after renewal[17]

Certificate Issued By:	*Validity Period*
Online CA to end-user Subscriber	Normally up to 2 years, but up to 5 years under the conditions described below[18]
Online CA to End-Entity Organizational Subscriber	Normally up to 3 years[19]

Table 7 – Certificate Operational Periods

[17] If 5-year end-user subscriber certificates are issued, the online CA certificate's operational period will be 10 years with no option to renew. Re-key will be required after 5 years.
[18] If 5-year end-user subscriber certificates are issued, the online CA certificate's operational period will be 10 years with no option to renew. Re-key will be required after 5 years.
[19] 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 year and up to a maximum of 10 years after renewal.

Except as noted in this section, KPN Subdomain 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 two years, up to five years, if the following requirements are met:

- The Certificates are individual Certificates,
- Subscribers' key pairs reside on a hardware token, such as a SSCD.

KPN also uses a Secure Server CA as a legacy self-signed issuing root CA which is part of the Symantec Trust Network and has an operational period of up to 15 years. end-user Subscriber Certificates issued by this CA meet the requirements for CA to end-user Subscriber Certificates specified in Table 7 above.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

Activation data (Secret Shares) used to protect tokens containing KPN 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.

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

- be generated by the user;
- have at least eight 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.

KPN strongly recommends that Enterprise Administrators, RAs, and end-user Subscribers choose passwords that meet the same requirements. KPN 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.

The SSCD or SUD that the Key pair and its associated Qualified Certificate are stored in, is supplied with the activation data. This PIN and PUK code are generated by a trusted system, consist of five characters and are printed out on a PIN-mail. After the PIN-mail is accepted, the system destroys the PIN and PUK code. In the period of time between generation and destroying of the codes, they are stored by the trusted system in encrypted form.

6.4.2 Activation Data Protection

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

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

KPN 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.

6.5 Computer Security Controls

KPN performs all CA and RA functions using Trustworthy Systems. Customers must use Trustworthy Systems.

6.5.1 Specific Computer Security Technical Requirements

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

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

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

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

6.5.2 Computer Security Rating

A version of Symantec's core Processing Center software has satisfied the EAL 4 assurance requirements of ISO/IEC 15408-3:1999, *Information technology - Security techniques -- Evaluation criteria for IT security -- Part 3: Security assurance requirements*, based on an independent laboratory's Common Criteria evaluation of the software against the Symantec Processing Center Security Target. Symantec will, from time to time, evaluate new releases of the Processing Center software under the Common Criteria.

The version of Processing Center used by KPN is positively audited against CWA 14167-1 *Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures – Part 1: System Security Requirements* by an independent auditor.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

Applications are developed and implemented by Symantec in accordance with Symantec systems development and Symantec/ KPN change management standards. KPN also provides software to its customers for performing RA and certain CA functions. Such software is developed in accordance with Symantec system development standards.

Symantec developed software, when first loaded, provides a method to verify that the software on the system originated from Symantec, has not been modified prior to installation, and is the version intended for use.

For the issuance of Qualified Certificates on SSCDs, a Card Management System is used that is built and maintained by KPN around a modular product from a specialized provider. This CMS is positively evaluated against the CWA 14167-1 requirements.

A segregation of functions has been made between the development organisation, the users organisation and the management organisation in the management of the CMS. This segregation of functions has been extended to the segregation of the production, test and development environments. The existing change management procedure is used to carefully make the move from the development environment to the testing environment and on to the production environment. This change management procedure includes tracking and registering versions, modifications and emergency repairs to all operational software.

By means of capacity management, KPN registers the use of it's computer resources and makes forecasts of it's use in the future, KPN anticipates on future needs of these resources.

KPN maintains an inventory of information assets and ensures that these assets receive an appropriate level of protection.

6.6.2 Security Management Controls

KPN has mechanisms and/or policies in place to control and monitor the configuration of its CA systems. Symantec 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, KPN validates the integrity of its CA systems.

6.6.3 Life Cycle Security Controls

No stipulation.

6.7 Network Security Controls

KPN performs all its CA and RA functions using networks secured in accordance with the Security and Audit Requirements Guide to prevent unauthorized access and other malicious activity. KPN

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 is not cryptographic-based.

Time and date information is based on one or more trusted time sources.

7 Certificate, CRL and OCSP Profiles

7.1 Certificate Profile

KPN Certificates conform to:
(a) ITU-T Recommendation X.509 (1997): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, June 1997, and
(b) RFC 8399: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, May 2018 ("RFC 8399").

At a minimum, X.509 Certificates shall contain the basic fields and indicated prescribed values or value constraints in Table 8 below:

Field	***Value or Value constraint***
Serial Number	Unique value per Issuer DN
Signature Algorithm	Name of the algorithm used to sign the certificate (See CPS § 7.1.3)
Issuer DN	See CPS § 7.1.4
Valid From	Universal Coordinate Time base. Synchronized to Master Clock of GPS and DCF. Encoded in accordance with RFC 8399.
Valid To	Universal Coordinate Time base. Synchronized to Master Clock of GPS and DCF. Encoded in accordance with RFC 8399.
Subject DN	See CPS § 7.1.4
Subject Public Key	Encoded in accordance with RFC 8399
Signature	Generated and encoded in accordance with RFC 8399

Table 8 – Certificate Profile Basic Fields

7.1.1 Version Number(s)

All certificates are X.509 Version 3 Certificates

7.1.2 Certificate Extensions

KPN populates X.509 Version 3 STN Certificates with the extensions required by §7.1.2.1 - 7.1.2.8. Private extensions are permissible, but the use of private extensions is not warranted under the STN CP and this CPS unless specifically included by reference.

7.1.2.1 Key Usage

X.509 Version 3 Certificates are generally populated in accordance with RFC 8399.

The KeyUsage extension in X.509 Version 3 Certificates is generally configured so as to set and clear bits and the criticality field in accordance with Table 9 below. 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.

Field		CAs	Class 2 End-User Subscri-bers	Automated Administra-tion tokens	Dual Key Pair Signature (Managed PKI Key Manager)	Dual Key Pair Encipherment (Managed PKI Key Manager)
Criticality		True	False	False	False	False
0	digitalSignature	Clear	Set	Set	Set	Clear
1	nonRepudiation	Clear	Clear	Clear	Clear	Clear
2	keyEncipherment	Clear	Set	Set	Clear	Set
3	dataEncipherment	Clear	Clear	Clear	Clear	Clear
4	keyAgreement	Clear	Clear	Clear	Clear	Clear
5	keyCertSign	Set	Clear	Clear	Clear	Clear
6	CRLSign	Set	Clear	Clear	Clear	Clear
7	encipherOnly	Clear	Clear	Clear	Clear	Clear
8	decipherOnly	Clear	Clear	Clear	Clear	Clear

Table 9 – Settings for KeyUsage Extension

7.1.2.2 Certificate Policies Extension

CertificatePolicies extension of X.509 Version 3 Certificates are populated with the object identifier for the STN CP in accordance with CP § 7.1.6 and with policy qualifiers set forth in CP § 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 RFC 8399. The criticality field of this extension shall be set to FALSE.

7.1.2.4 Basic Constraints

KPN X.509 Version 3 CA Certificates BasicConstraints extension shall have the CA field set to TRUE. end-user Subscriber Certificates BasicConstraints extension, shall be populated with a value of an empty sequence. The criticality field of this extension shall be set to TRUE for CA Certificates, but otherwise set to FALSE.

KPN 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 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

KPN makes use of the ExtendedKeyUsage extension for the specific types of KPN X.509 Version 3 Certificates listed in Table 10 below. For other types of Certificates, KPN does not usually use the Extended Key Usage extension.

Certificate Category Type	Certificate Type
OCSP Responder	Class 2 Public Primary OCSP Responders Secure Server OCSP Responder

Certificate Category Type	*Certificate Type*
Individual Certificates	Class 2 Individual Certificates

Table 10 – Certificates using the Extended Key Usage Extension

For these Certificates, KPN populates the ExtendedKeyUsage extension in accordance with Table 11 below.

		OCSP Respon-ders	Class 2 Individual Certificates
Criticality		FALSE	FALSE
0	ServerAuth	Clear	Clear
1	ClientAuth	Set	Set
2	CodeSigning	Clear	Clear
3	E-mailProtection	Set	Set
4	IpsecEndSystem	Clear	Clear
5	IpsecTunnel	Clear	Clear
6	IpsecUser	Clear	Clear
7	TimeStamping	Clear	Clear
8	OCSP Signing	Set	Clear
-	Microsoft Server Gated Crypto (SGC) OID: 1.3.6.1.4.1.311.10.3.3	Clear	Clear
-	Netscape SGC - OID: 2.16.840.1.113730.4.1	Clear	Clear
-	TBD – OID: 2.16.840.1.113733.1.8.1	Clear	Clear

Table 11 – Settings for ExtendedKeyUsage Extension

7.1.2.6 CRL Distribution Points

Generally 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

KPN 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 Authority Key Identifier is composed of the 256-bit SHA-2 hash of the public key of the CA issuing the Certificate. 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 KPN populates X.509 Version 3 STN 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 RFC 8399. Where this extension is used, the criticality field of this extension is set to FALSE.

7.1.3 Algorithm Object Identifiers

KPN STN Certificates are signed using the algorithm SHA256withRSAEncryption (OID: 1.2.840.113549.1.1.11).

Certificate signatures produced using this algorithm shall comply with RFC 3279.

7.1.4 Name Forms

KPN populates STN Certificates with an Issuer and Subject Distinguished Name in accordance with § 3.1.1.

In addition, KPN includes within end-user Subscriber Certificates either an additional Organizational Unit field or a Certificate Policy Extension 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 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.

7.1.5 Name Constraints

Name contraints are in accordance with the Mozilla Root Store Policy.

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 §1.2. For legacy Certificates issued prior to the publication of the STN CP which include the Certificate Policies extension, Certificates refer to the KPN CPS.

7.1.7 Usage of Policy Constraints Extension

No stipulation.

7.1.8 Policy Qualifiers Syntax and Semantics

KPN 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 KPN 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

CRLs contain the basic fields and contents specified in Table 12 below:

Field	Value or Value constraint
Version	See CPS §7.2.1.
Signature Algorithm	**SHA256withRSAEncryption**. (OID: 1.2.840.113549.1.1.11)
Issuer	Entity who has signed and issued the CRL. The CRL Issuer Name is in accordance with the Issuer Distinguished Name requirements specified in CPS § 7.1.4.
Effective Date	Issue date of the CRL. CRL are effective upon issuance.
Next Update	Date by which the next CRL will be issued. The Next Update date for KPN CRLs is set as follows: 3 months from the Effective Date for STN PCAs and 10 days from the Effective Date for other KPN CAs. CRL issuance frequency is in accordance with the requirements of CPS § 4.9.7.
Revoked Certificates	Listing of revoked Certificates, including the Serial Number of the revoked Certificate and the Revocation Date.

Table 12 – CRL Profile Basic Fields

7.2.1 Version Number(s)

KPN supports both X.509 Version 1 and Version 2 CRLs. Version 2 CRLs comply with the requirements of RFC 8399.

7.2.2 CRL and CRL Entry Extensions

No stipulation.

7.3 OCSP Profile

OCSP (Online Certificate Status Protocol) is a way to obtain timely information about the revocation status of a particular certificate. KPN uses OCSP to validateClass 2 Enterprise certificates. OCSP responders conform to RFC 6960.

7.3.1 Version Number(s)

Version 1 of the OCSP specification as defined by RFC 6960 is supported.

7.3.2 OCSP Extensions

KPN does not use a nonce to establish the current freshness of each OCSP response and clients should not expect a nonce in the response to a request that contains a nonce. Instead, clients should use the local clock to check for response freshness.

8 Compliance Audits and other Assessments

An annual WebTrust for Certification Authorities examination is performed for the STN Intermediate CAs as specified in CPS § 1.3.1.

Customer-specific CAs are also audited against WebTrust for their RA operations.

In addition to compliance audits, DigiCert and/or KPN shall be entitled to perform other reviews and investigations to ensure the trustworthiness of KPN's Subdomain of the STN, which include, but are not limited to:

- KPN shall be entitled, within its sole and exclusive discretion, to perform at any time an "Exigent Audit/Investigation" on a Customer in the event KPN has reason to believe that the audited entity has failed to meet STN Standards, has experienced an incident or compromise, or has acted or failed to act, such that the audited entity's failure, the incident or compromise, or the act or failure to act poses an actual or potential threat to the security or integrity of the STN.
- KPN shall be entitled to perform "Supplemental Risk Management Reviews" on a Customer following incomplete or exceptional findings in a Compliance Audit or as part of the overall risk management process in the ordinary course of business.

KPN shall be entitled to delegate the performance of these audits, reviews, and investigations to a third party audit firm. Entities that are subject to an audit, review, or investigation shall provide reasonable cooperation with DigiCert and the personnel performing the audit, review, or investigation.

8.1 Frequency and Circumstances of Assessment

Compliance Audits are conducted at least annually at the sole expense of the audited entity.

8.2 Identity/Qualifications of Assessor

KPN's CA compliance audits are performed by a public accounting firm that is listed on webtrust.org.

8.3 Assessor's Relationship to Assessed Entity

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

8.4 Topics Covered by Assessment

The scope of KPN's annual audit includes CA environmental controls, key management operations and Infrastructure/Administrative CA controls, certificate life cycle management and CA business practices disclosure.

8.5 Actions Taken as a Result of Deficiency

With respect to compliance audits of KPN'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 KPN management with input from the auditor. KPN management is responsible for developing and implementing a corrective action plan. If KPN 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, KPN Management will evaluate the significance of such issues and determine the appropriate course of action.

8.6 Communications of Results

Results of the compliance audit of KPN's operations may be released at the discretion of KPN management.

9 Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

KPN and Customers are entitled to charge end-user Subscribers for the issuance, management, and renewal of Certificates.

9.1.2 Certificate Access Fees

KPN and Customers do 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

KPN does not charge a fee as a condition of making the CRLs required by the STN CP available in a repository or otherwise available to Relying Parties. KPN is, however, entitled to charge a fee for providing customized CRLs, OCSP services, or other value-added revocation and status information services. KPN 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 KPN's prior express written consent.

9.1.4 Fees for Other Services

KPN 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.

9.2 Financial Responsibility

KPN has taken adequate arrangements, in the form of insurances, among others, to cover the financial risks related to providing certification services. Furthermore, KPN possesses the financial stability and resources needed for the healthy operation of its enterprise.

9.2.1 Insurance Coverage

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. KPN maintains such errors and omissions insurance coverage.

9.2.2 Other Assets

KPN has enough financial stability and resources required to operate as a Certification Service Provider.
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.

9.3 Confidentiality of Business Information

KPN B.V.'s annual financial report is integrated into Koninklijke KPN N.V. annual financial report. Koninklijke KPN N.V. is listed on the stock market and is thus not allowed to provide financial information other than through regular financial reports and official channels.

9.3.1 Scope of Confidential Information

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

- CA application records, whether approved or disapproved,
- Certificate Application records,
- Private keys held by Customers using Managed PKI Key Manager and information needed to recover such Private Keys,
- PIN codes, PUK codes and Challenge Phrases,
- Transaction records (both full records and the audit trail of transactions),
- Audit trail records created or retained by KPN or a Customer,
- Audit reports created by KPN or a Customer (to the extent such reports are maintained), or their respective auditors (whether internal or public),
- Quality Management and Information Security Management System, such as
    - Contingency planning and disaster recovery plans, and
    - Security measures controlling the operations of Symantec 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, KPN repositories and information contained within them are not considered Confidential/Private Information. Information not expressly deemed Confidential/Private Information under § 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

KPN has policy in place for all information related to security issues (see § 9.3.1, among others). One thing the policy states is that this information is confidential and is only made available on a need-to-know basis. This means that the information can only be accessed by third parties within the KPN building after a strict pledge of secrecy has been given and after showing a clear need (e.g. performing an audit) to access the information.

9.4 Privacy of Personal Information

KPN meets the requirements of the General Data Protection Regulation (GDPR). KPN is registered with the Dutch Data Protection Authority as a company responsible for processing personal information for the purpose of providing certification services.

9.4.1 Privacy Policy

KPN has implemented a privacy policy, which is located at: https://certificaat.kpn.com/repository/. This policy is in compliance with the applicable General Data Protection Regulation (GDPR).

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

The data published concerning certificates is publicly accessible. The information given regarding published and revoked certificates is limited to what is mentioned in Chapter 7 *"Certificate, CRL and OCSP Profiles"* of this CPS. Information on the revocation of certificates is available through the CRL. The information given in the CRL is limited to the certificate number, the time of revocation and the status (valid/revoked) of the certificate.

9.4.4 Responsibility to Protect Private Information

KPN, as other STN participants, receiving private information shall secure it from compromise and disclosure to third parties and shall comply with all local privacy laws in their jurisdiction.

9.4.5 Notice and Consent to Use Private Information

Unless 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.

The Subscriber and Subject agree to the publication of certificate data by signing the Subscriber Agreement and the applicable conditions. KPN considers the completion of the application procedure by a end-user Subscriber to be the permission to publish the information in the Certificate.

9.4.6 Sharing Information Due to Legal Subpoena

KPN does not provide confidential information to criminal investigators unless Dutch laws and regulations require KPN to do so, in which case the information will only be shared after a legal subpoena has been given.

9.4.7 Sharing Information in Relation to Private Law Argumentation

KPN stores the Certificate and the information given during Certificate application for a period of time - the length of which will be communicated to the client and/or the end-user Subscriber - and for the purpose of providing proof of certification in a judicial process, should this prove necessary. Confidential information will only be given to parties other than the client and the end-user Subscriber for the purpose of argumentation in a court case after the client or end-user Subscriber has given prior written consent.

9.4.8 Sharing Information After a Request by the Owner

If a client and/or end-user Subscriber requests KPN to share the personal information it has stored on them, KPN will do so. If a client requests the personal information of a end-user Subscriber that has received a Certificate based on the client's Certificate application, KPN will share the information with them. KPN has the right to charge a reasonable fee for every provision of such information.

9.4.9 Making Certificate Revocation Information Public

Information on the revocation of Certificates is available in the CRL. The information listed in the CRL is limited to the Certificate number and the time of revocation. Should KPN unilaterally revoke a Certificate, it will be published in the CRL.

9.4.10 Other Information Disclosure Circumstances

No Stipulation.

9.5 Intellectual Property Rights

The allocation of Intellectual Property Rights among KPN Subdomain Participants other than Subscribers and Relying Parties is governed by the applicable agreements among such KPN Subdomain Participants. The following subsections of § 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. KPN 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. KPN 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

KPN Subdomain Participants acknowledge that KPN 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, STN’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 KPN.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

See the General and/or Specific Conditions for this.

9.6.2 RA Representations and Warranties

See the General and/or Specific Conditions for this.

9.6.3 Subscriber Representations and Warranties

See the General and/or Specific Conditions for this.

9.6.4 Relying Party Representations and Warranties

See the General and/or Specific Conditions for this.

9.6.5 Representations and Warranties of Other Participants

No stipulation

9.7 Disclaimers of Warranties

See the General and/or Specific Conditions for this.

9.8 Limitations of Liability

See the General and/or Specific Conditions for this.

9.9 Indemnities

9.9.1 Indemnification by Subscribers

See the General and/or Specific Conditions for this.

9.9.2 Indemnification by Relying Parties

See the General and/or Specific Conditions for this.

9.10 Term and Termination

9.10.1 Term

The CPS becomes effective upon publication in the KPN repository. Amendments to this CPS become effective upon publication in the KPN 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, KPN Subdomain 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, KPN Subdomain participants shall use commercially reasonable methods to communicate with each other, taking into account the criticality and subject matter of the communication.

KPN s uses several methods to communicate with those concerned. One way is when the Validation department employees that process Certificate applications talk to clients in person or by telephone. This department can be reached by telephone at +31[0]55 577 8395

The aforementioned documents and much other information is available in the Electronic Repository. It is also always possible to ask questions or discuss other matters by sending an e-mail to pkivalidation@kpn.com.

9.12 Amendments

9.12.1 Procedure for Amendment

KPN has the right to modify or make additions to this CPS. The functioning of the valid CPS is evaluated at least once a year by the KPN PMA. Clients and Relying Parties may submit remarks on CPS content to the KPN PMA (pkisupport@kpn.com). Should changes to the CPS be necessary based on these remarks, the PMA will make the necessary changes in accordance with the change management process that has been set up for this purpose.

Modifications to the CPS are determined by the KPN PMA. Editorial changes or correction of apparent writing or spelling errors can go into effect without prior notification and can be recognized through a change in the version number by 0.1 (e.g. 1.1 becomes 1.2). In the case of major modifications, a new version of the CPS is produced and the version number is increased by 1 (e.g. 1.0 becomes 2.0)

Amended versions or updates shall be linked to the Practices Updates and Notices section of the KPN Repository located at: https://certificaat.kpn.com/repository.

9.12.2 Notification Mechanism and Period

KPN and the PMA reserve the right to amend the CPS without notification for amendments that are not material, including, without limitation: corrections of typographical errors, changes to URLs, and changes to contact information. The PMA's decision to designate amendments as material or non-material shall be within the PMA's sole discretion.

In case of material amendments, proposed amendments to the CPS shall appear in the Practices Updates and Notices section of the KPN Repository, which is located at: https://certificaat.kpn.com/repository/, fifteen (15) days before the intended publish date (see § 9.12.2.1). The PMA solicits proposed amendments to the CPS from other KPN Subdomain participants. If the PMA considers such an amendment desirable and proposes to implement the amendment, the PMA shall provide notice of such amendment in accordance with this section.

Notwithstanding anything in the CPS to the contrary, if the PMA believes that material amendments to the CPS are necessary immediately to stop or prevent a breach of the security of the STN or any portion of it, KPN and the PMA shall be entitled to make such amendments by publication in the KPN Repository. Such amendments will be effective immediately upon publication.

9.12.2.1 Comment Period

Except as otherwise stated, the comment period for any material amendments to the CPS shall be fifteen (15) days, starting on the date on which the amendments are posted on the KPN Repository. Any KPN Subdomain participant shall be entitled to file comments with the PMA up until the end of the comment period.

9.12.2.2 Mechanism to Handle Comments

The PMA shall consider any comments on the proposed amendments. The PMA shall either (a) allow the proposed amendments to become effective without amendment, (b) amend the proposed amendments and republish them as a new amendment when required, or (c) withdraw the proposed amendments. The PMA is entitled to withdraw proposed amendments by providing notice in the Practices Updates and Notices section of the KPN Repository. Unless proposed amendments are amended or withdrawn, they shall become effective upon the expiration of the comment period.

9.12.3 Circumstances under Which OID Must be Changed

No stipulation.

9.13 Dispute Resolution Provisions

KPN has a complaints procedure in place. Complaints can be directed to the director of KPN.

9.13.1 Disputes among KPN and Customers

Disputes among KPN Subdomain 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

Disputes between KPN and one of its end-user Subscribers or Relying Parties shall be resolved pursuant to provisions in the Subscriber Agreement and the Relying Party Agreement.

9.13.3 Governing Law

Subject to any limits appearing in applicable law, the Dutch Law governs 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 The Netherlands. This choice of law is made to ensure uniform procedures and interpretation for all KPN Subdomain 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 § 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.

This CPS is subject to Dutch Law.

9.14 Compliance with Applicable Law

In general KPN and its STN-participants within the KPN -Subdomain comply with Dutch Law.

9.15 Miscellaneous Provisions

9.15.1 Entire Agreement

Not applicable.

9.15.2 Assignment

Not applicable.

9.15.3 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.

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

Not applicable.

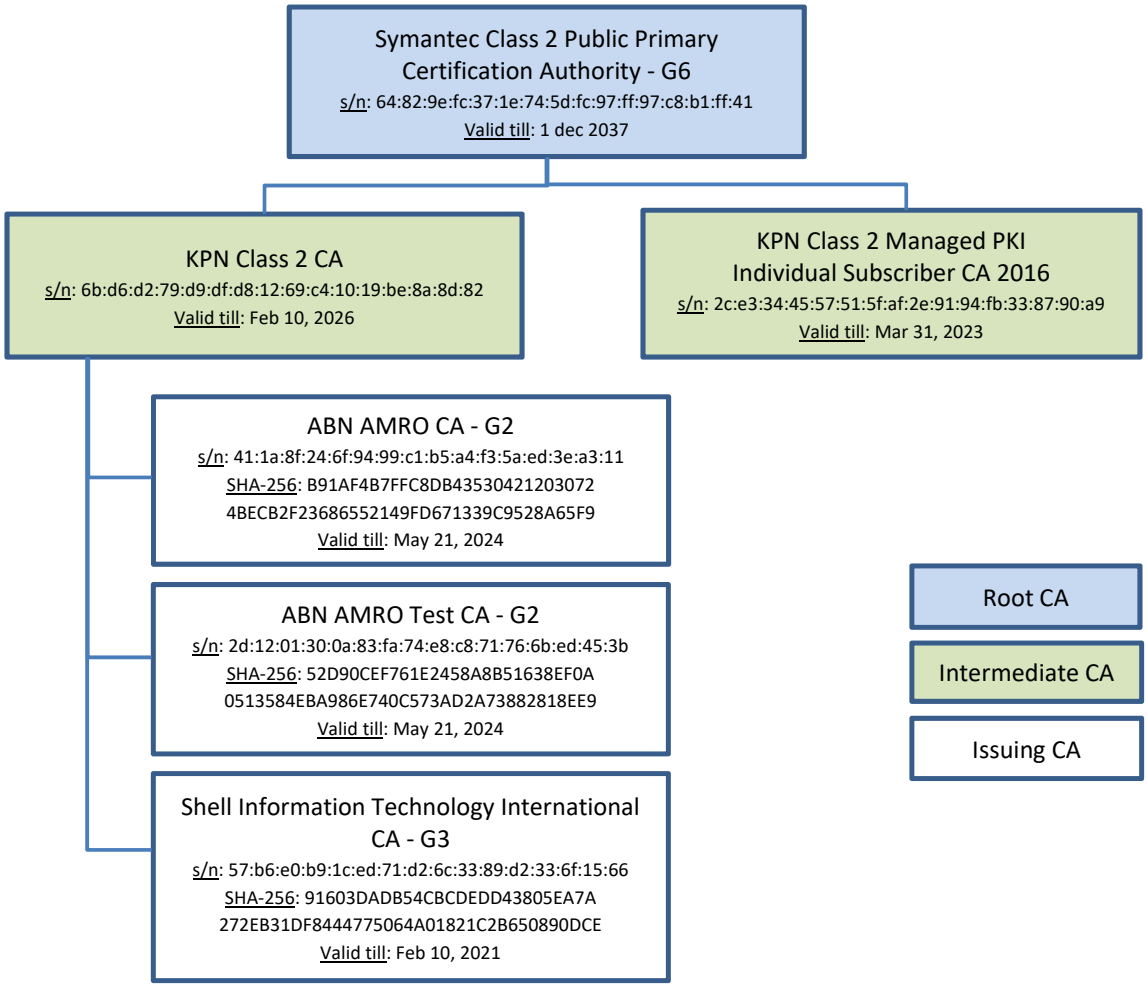
9.15.5 Force Majeure

To the extent permitted by applicable law, Subscriber Agreements and Relying Party Agreements shall include a force majeure clause protecting KPN.

9.16 Other Provisions

Not applicable.

Annex 1 CA model



Annex 2 Acronyms

Acronym	Definition
CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificates Revocation List
CSP	Certification Service Provider
EESSI	European Electronic Signature Standardization Initiative
ETSI	European Telecommunication Standardization Institute
FIPS	Federal Information Processing Standards
GDPR	General Data Protection Regulation
HSM	Hardware Security Module
LRA	Local Registration Authority
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OPTA	Independent Post and Telecommunication Authority
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PMA	Policy Management Authority
PUK	Personal Unlock Code (“*Persoonlijk Unlock Kengetal”*)
RA	Registration Authority
SSCD	Secure Signature Creation Device
SUD	Secure User Device
WJI	Law on Judicial Information (“*Wet Justitiële Informatie*”)
WID	Law on Identification Obligation(“*Wet op de Identificatieplicht*”)

Annex 3 Definitions

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 VeriSign to be a VTN distribution and services channel within a specific territory.
Affiliate Audit Program Guide	A VeriSign document containing requirements for the Compliance Audits of Affiliates, including Certificate Management Control Objectives against which Affiliates will be audited.
Affiliate Practices Legal Requirements Guidebook	A VeriSign document setting forth requirements for Affiliate CPSs, agreements, validation procedures, and privacy policies, as well as other requirements that Affiliates must meet.

Term	Definition
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 VeriSign 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 Private Organization or Government Entity that applies for (or seeks renewal of) an EV Certificate naming it as the Subject.
Applicant Representative	An individual person employed by the Applicant for an EV certificate: (i) who signs and submits, or approves an EV Certificate Request on behalf of an Applicant, and/or (ii) who signs and submits a Subscriber Agreement on behalf of an Applicant.
Application Software Vendor	A developer of Internet browser software or other software that displays or uses certificates and distributes root certificates, such as KDE, Microsoft Corporation, Mozilla Corporation, Opera Software ASA, and Red Hat, Inc.
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 VeriSign 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 Approver	[defined in Section 10]
Certificate Chain	An ordered list of Certificates containing an end-user Subscriber Certificate and CA Certificates, which terminates in a root Certificate.
Certificate Management Control Objectives	Criteria that an entity must meet in order to satisfy a Compliance Audit.
Certificate Policies (CP)	This document, which is entitled "VeriSign Trust Network Certificate Policies" and is the principal statement of policy governing the VTN.
Certificate Requester: [defined in Section 10]	
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 VTN.
Certification Practice Statement (CPS)	A statement of the practices that VeriSign 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 Challenge Phrase to authenticate the Subscriber when the Subscriber seeks to revoke or renew the Subscriber's Certificate.
Class	A specified level of assurances as defined within the CP. See CP § 1.1.1.
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 VTN 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.
Contract Signer: [defined in Section 10]	

Term	Definition
CRL Usage Agreement	An agreement setting forth the terms and conditions under which a CRL or the information in it can be used.
Customer	An organization that is either a Managed PKI Customer, Gateway Customer, or ASB Customer.
Demand Deposit Account	A deposit account held at a bank or other financial institution, the funds deposited in which are payable on demand. The primary purpose of demand accounts is to facilitate cashless payments by means of check, bank draft, direct debit, electronic funds transfer, etc. Usage varies among countries, but a demand deposit account is commonly known as: a checking account, a share draft account, a current account, or a checking account.
Enterprise, as in Enterprise Service Center	A line of business that an Affiliate enters to provide Managed PKI services to Managed PKI Customers.
Enterprise EV Certificate:	An EV Certificate that an Managed PKI for SSL Customer authorizes VeriSign to issue at third and higher domain levels that contain the domain that have been verified by VeriSign.
Enterprise RA	A Managed PKI for SSL customer that can request multiple valid EV Certificates for Domains and Organizations verified by VeriSign for domains at third and higher domain levels that contain a domain that was verified by VeriSign in the original EV Certificate, in accordance with the requirements of these Guidelines.
Enterprise Roaming Server	A server residing at the site of a Managed PKI Customer used in conjunction with the VeriSign Roaming Service to hold Roaming Subscribers' encrypted private keys and portions of symmetric keys used to encrypt and decrypt Roaming Subscribers' private keys.
EV Certificate:	A digital certificate that contains information specified in the EV Guidelines and that has been validated in accordance with the Guidelines.
EV OID	An identifying number, called an "object identifier," that is included in the certificatePolicies field of an EV certificate that: (i) indicates which CA policy statement relates to that certificate, and which, (ii) by pre-agreement with one or more Application Software Vendor, marks the certificate as being an EV Certificate.
Exigent Audit/Investigation	An audit or investigation by VeriSign where VeriSign has reason to believe that an entity's failure to meet VTN Standards, an incident or Compromise relating to the entity, or an actual or potential threat to the security of the VTN posed by the entity has occurred.
Extended Validation	Validation Procedures defined by the Guidelines for Extended Validation Certificates published by a forum consisting of major certification authorities and browser vendors.
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.
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 Manager Administrator	An Administrator that performs key generation and recovery functions for a Managed PKI Customer using Managed PKI Key Manager.
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 VeriSign 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.
Managed PKI	VeriSign's fully integrated managed PKI service that allows enterprise Customers of VeriSign 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-

Term	Definition
	one by an Administrator using a web-based interface.
NetSure Protection Plan	An extended warranty program, which is described in CP § 1.1.2.2.3.
Nonverified 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 VTN Certificate may provide proof in support of a determination of Non-repudiation by a tribunal, but does not by itself constitute Non-repudiation.
Offline CA	VeriSign 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 VeriSign responsible for promulgating this policy throughout the VTN.
Primary Certification Authority (PCA)	A CA that acts as a root CA for a specific Class of Certificates, and issues Certificates to CAs subordinate to it.
Processing Center	An organization (VeriSign 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 VTN 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 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 VTN PKI consists of systems that collaborate to provide and implement the VTN.
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.
Regulated Financial Institution	A financial institution that is regulated, supervised, and examined by governmental, national, state or provincial, or local authorities having regulatory authority over such financial institution based on the governmental, national, state or provincial, or local laws under which such financial institution was organized and/or licensed.
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.
Retail Certificate	A Certificate issued by VeriSign or an Affiliate, acting as CA, to individuals or organizations applying one by one to VeriSign or an Affiliate on its web site.
Roaming Subscriber	A Subscriber using the VeriSign Roaming Service whose private key is encrypted and decrypted with a symmetric key that is split between the VeriSign Roaming Server and an Enterprise Roaming Server.
RSA	A public key cryptographic system invented by Rivest, Shamir, and Adelman.
RSA Secure Server Certification Authority (RSA Secure Server CA)	The Certification Authority that issues Secure Server IDs.

Term	Definition
RSA Secure Server Hierarchy	The PKI hierarchy comprised of the RSA Secure Server Certification Authority.
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 Server ID	A Class 3 organizational Certificate used to support SSL sessions between web browsers and web servers.
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 Guide	A VeriSign 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 VeriSign 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 Class or type, but rather relies on a Processing Center to perform issuance, management, revocation, and renewal of such Certificates.
Subdomain	The portion of the VTN under control of an entity and all entities subordinate to it within the VTN hierarchy.
Subject	The holder of a private key corresponding to a public key. 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.
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 VTN hierarchy (the Class 1, 2, or 3 hierarchy).
Supplemental Risk Management Review	A review of an entity by VeriSign 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 VeriSign or an Affiliate to specific markets.
Trusted Person	An employee, contractor, or consultant of an entity within the VTN 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 VTN 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.
VeriSign	Means, with respect to each pertinent portion of this CPS, VeriSign, Inc. and/or any wholly owned VeriSign subsidiary responsible for the specific operations at issue.
VeriSign Digital Notarization Service	A service offered to Managed PKI Customers that provides a digitally signed assertion (a Digital Receipt) that a particular document or set of data existed at a particular point in time.
VeriSign Repository	VeriSign's database of Certificates and other relevant VeriSign Trust Network information accessible on-line.
VeriSign Roaming Server	A server residing at VeriSign's Processing Center used in conjunction with the VeriSign Roaming Service to hold portions of symmetric keys used to encrypt and decrypt Roaming Subscribers' private keys.
VeriSign Roaming Service	The service offered by VeriSign that enables a Subscriber to download his or her private key and perform private key operations on different client terminals.
VeriSign Trust Network (VTN)	The Certificate-based Public Key Infrastructure governed by the VeriSign Trust Network Certificate Policies, which enables the worldwide deployment and use of Certificates by VeriSign and its Affiliates, and their respective Customers, Subscribers, and Relying Parties.
VTN Participant	An individual or organization that is one or more of the following within the VTN: VeriSign,

Term	Definition
	an Affiliate, a Customer, a Universal Service Center, a Reseller, a Subscriber, or a Relying Party.
VTN Standards	The business, legal, and technical requirements for issuing, managing, revoking, renewing, and using Certificates within the VTN.