Date of publication
1 June 2004

Author
Businessline Enterprise Networks

Telephone
+31 70 3437920

Version
2.0

Certification Practice Statement

KPN Telecom B.V.

Public

KPN Telecom B.V.
Businessline Enterprise Networks
Koningin Wilhelminalaan 7-9
3527 LA Utrecht, the Netherlands
Phone: +31 (0)70 – 343 79 20
Fax: +31 (0)70 – 335 16 93
https://certificaat.kpn.com

Date of Publication
1 June 2004

Version
2.0

KPN Telecom B.V. Certification Practice Statement

Revision date: April - May 2004

Trademark Notices

Acknowledgement

KPN Telecom B.V. and VeriSign acknowledges the assistance of many reviewers of the document specializing in diverse areas of business, law, policy, and technology.

Date of Publication
1 June 2004

Version
2.0

Table of contents

Date of publication
1 June 2004

Version
2.0

1 Introduction

This document is the KPN Telecom B.V. Certification Practice Statement ("CPS") and is based upon the VeriSign Certification Practice Statement (see https://www.verisign.com/cps).[1] It states the practices that KPN Telecom B.V. ("KPN") certification authorities ("CAs") employ in providing certification services that include, but are not limited to, issuing, managing, revoking, and renewing certificates in accordance with the specific requirements of the VeriSign Trust Network Certificate Policies ("CP"). VeriSign, Inc. ("VeriSign") is the leading provider of trusted infrastructure services to web sites, enterprises, electronic commerce service providers, and individuals. VeriSign's domain name, digital certificate, and payment services provide the critical web identity, authentication, and transaction infrastructure that online businesses require to conduct secure e-commerce and communications.

The capitalized terms in this CPS are defined terms with specific meanings. Please see Section 9 for a list of definitions.

The CP describes the VeriSign Trust Network[SM] ("VTN"), which is a global public key infrastructure ("PKI") that provides digital certificates ("Certificates") for both wired and wireless applications. The VTN accommodates a large, public, and widely distributed community of users with diverse needs for communications and information security. VeriSign is one of the service providers within the VTN, together with KPN and a global network of affiliates ("Affiliates") throughout the world.

The CP is the principal statement of policy governing the VTN. It establishes the business, legal, and technical requirements for approving, issuing, managing, using, revoking, and renewing, digital Certificates within the VTN and providing associated trust services. These requirements, called the "VTN Standards", protect the security and integrity of the VTN, apply to all VTN Participants, and thereby provide assurances of uniform trust throughout the VTN. More information concerning the VTN and VTN Standards is available in the CP.[2]

VeriSign and each Affiliate has authority over a portion of the VTN. The portion of the VTN controlled by VeriSign or an Affiliate is called its "Subdomain" of the VTN. An Affiliate's Subdomain consists of the portion of the VTN under its control. An Affiliate's Subdomain includes entities subordinate to it such as its Customers, Subscribers, and Relying Parties.

KPN, VeriSign and each of the Affiliates have a CPS that governs its Subdomain within the VTN. While the CP sets forth requirements that VTN Participants must meet, this CPS describes how KPN meets these requirements within KPN's Subdomain of the VTN, which is primarily located in the Netherlands. More specifically, this CPS describes the practices that KPN employs for:

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

[1] Internal cross references to CPS sections (i.e., in the form of "CPS §") are references to sections of this document. Other references to the term "CPS" refer to a certification practice statement, which may include this document or the CPSs of others, such as VTN Affiliates. See CPS § 9 (Definitions).
[2] The CP is published in electronic form within the VeriSign Repository at https://www.verisign.com/CP. VeriSign also makes the CP available in Adobe Acrobat pdf or Word format upon request sent to CP-requests@verisign.com. The CP is available in paper form from the VeriSign Trust Network Policy Management Authority ("PMA") upon requests sent to: VeriSign, Inc., 487 East Middlefield Road, Mountain View, CA 94043 USA, Attn: Practices Development – CP.

within KPN's Subdomain of the VTN, in accordance with the requirements of the CP and its VTN Standards.[3]

1.1 Overview

This CPS is specifically applicable to:

- VeriSign's Public Primary Certification Authorities (PCAs), KPN Infrastructure CAs, and KPN Administrative CAs supporting the VeriSign Trust Network
- KPN's Public CAs and the CAs of Managed PKI[4] Customers, which issue Certificates within the VTN.

More generally, the CPS also governs the use of VTN services within KPN's Subdomain of the VTN by all individuals and entities within KPN's Subdomain (collectively, KPN Subdomain Participants"). Private CAs and hierarchies managed by KPN are outside the scope of this CPS.

The VTN includes three classes of Certificates, Classes 1, 2 and 3, and the CP describes how these three Classes correspond to three classes of applications with common security requirements. The CP is a single document that defines three certificate policies, one for each of the Classes, and sets VTN Standards for each Class.

KPN currently offers two of the three Classes of Certificates, Class 2 and 3, within its Subdomain of the VTN. This CPS describes how KPN meets the CP requirements for each Class within its Subdomain. Thus, the CPS, as a single document, covers practices and procedures concerning the issuance and management of Certificate Classes.

a) Role of the KPN CPS and Other Practices Documents

The CP describes at a general level the overall business, legal, and technical infrastructure of the VTN. This CPS then applies VTN Standards from the CP to KPN Subdomain Participants, and explains specific practices of KPN in response to the CP. More specifically, the CPS describes, among other things:

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

[3] Although VeriSign CAs certify the CAs of Affiliates, the practices relating to an Affiliate are covered in the Affiliate's CPS.
[4]The Managed PKI Service was formerly known as OnSite. All references to OnSite in this CPS have been changed to Managed PKI. Server OnSite has been changed to Managed PKI for SSL and Global Server OnSite has been changed to Managed PKI for SSL Premium Edition. Customers may still see references to OnSite in other Managed PKI documentation or URLs. The OnSite Service itself has not changed other then the name.

- 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.

KPN may publish Certificate policies supplemental to this CPS in order to comply with the specific policy requirements of Government, or other industry standards requirements. These supplemental certificate policies shall be made available to subscribers for the certificates issued under the supplemental policies and their relying parties.

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

- Ancillary security and operational documents that supplement the CP and CPS by providing more detailed requirements, such as:
  - The KPN and VeriSign Security Policies, which sets forth security principles governing the VTN infrastructure,
  - The VeriSign Security and Audit Requirements Guide, which describes detailed requirements for KPN concerning personnel, physical, telecommunications, logical, and cryptographic key management security,
  - The VeriSign 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 from VTN Standards to these VTN Participants and, in some cases, state specific practices for how they must meet VTN Standards.

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

Table 1 is a matrix showing various VTN and KPN practices documents, whether they are publicly available, and their locations. The list in Table 1 is not intended to be exhaustive. Note that documents not expressly made public are confidential to preserve the security of the VTN.

Documents	*Status*	*Where Available to the Public*
VeriSign Trust Network Certificate Policies	Public	VeriSign Repository at https://www.verisign.com/CP
VTN Ancillary Security and Operational Documents		
KPN and VeriSign Information Security Policies	Confidential	N/A
KPN Physical Security Policy	Confidential	N/A
VeriSign Security and Audit Requirements Guide	Confidential	N/A
VeriSign Key Ceremony Reference Guide	Confidential	N/A

Documents	*Status*	*Where Available to the Public*
Managed PKI Administrator's Handbook	Public	https://certificaat.kpn.com/documents
Managed PKI Key Management Service Administrator's Guide	Public	https://certificaat.kpn.com/documents
KPN Specific Documents		
KPN Certification Practice Statement	Public	KPN Repository at https://certificaat.kpn.com/repository
KPN Subscriber Agreements and Relying Party Agreements	Public	KPN Repository at https://certificaat.kpn.com/repository
KPN (Global) Server ID Agreements	Public	KPN Repository at https://certificaat.kpn.com/repository
KPN Privacy Statement	Public	KPN Repository at https://certificaat.kpn.com/repository
KPN Master Services Agreement	Confidential	N/A

Table 1 – Availability of Practices Documents

b) Background Concerning Digital Certificates and the VTN Hierarchy

This CPS assumes that the reader is generally familiar with Digital Signatures, PKIs, and the VTN. If not, KPN advises that the reader obtain some training in the use of public key cryptography and public key infrastructure as implemented in the VTN. General educational and training information is accessible from KPN at https://certificaat.kpn.com. Also, a brief summary of the roles of the different VTN Participants is set forth in the CP.

c) Compliance with Applicable Standards

The practices specified in this CPS have been designed to meet or exceed the requirements of generally accepted and developing industry standards including the AICPA/CICA WebTrust Program for Certification Authorities, ICTSB/EESSI (a cooperation between ETSI, CEN/ISSS and CENELEC to specify requirements for compliance with the European Directive nr. 1999/93/EG for Electronic Signatures), the ANS X9.79:2001 PKI Practices and Policy Framework, and other industry standards related to the operation of CAs.

The structure of this CPS generally corresponds to the *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*, known as RFC 2527 of the Internet Engineering Task Force, an Internet standards body. The RFC 2527 framework has become a standard in the PKI industry. This CPS conforms to the RFC 2527 framework in order to make policy mapping and comparisons, assessment, and interoperation easier for persons using or considering using KPN's Public Managed PKI Services.

KPN has conformed the CPS to the RFC 2527 structure where possible, although slight variances in title and detail are necessary because of the complexity of KPN business models. While KPN intends to continue the policy of adhering to RFC 2527 in the future, KPN reserves the right to vary from the RFC 2527 structure as needed, for example to enhance the quality of the CPS or its suitability to KPN Subdomain Participants. Moreover, the CPS structure may not correspond to future versions of RFC 2527.

1.1.1 Policy Overview

KPN currently offers two distinct classes of certification services, Classes 2 and 3, for both the wired and wireless Internet and other networks, corresponding to the Classes of Certificates whose policies are described in the CP. Each level, or class, of Certificate provides specific functionality and security features and corresponds to a specific level of trust. KPN Subdomain Participants choose which Classes of Certificates they need.

One of the functions of the CP is to describe the policies of Certificate Classes in detail.[5] Nonetheless, this section summarizes the Certificate Classes offered by KPN within its Subdomain.

Class 1 Certificates, which currently are not offered by KPN, offer the lowest level of assurances within KPN's Subdomain. They are individual Certificates, whose validation procedures are based on assurances that the Subscriber's distinguished name is unique and unambiguous within the CA's Subdomain and that a certain e-mail address is associated with a public key. They are appropriate for digital signatures, encryption, and access control for non-commercial or low-value transactions where proof of identity is unnecessary.

Class 2 Certificates offer a medium level of assurances in comparison with the other two Classes. Again, they are individual Certificates. In addition to the Class 1 validation procedures, Class 2 validation procedures add procedures based on a comparison of information submitted by the Certificate Applicant against information in business records or databases or the database of a KPN-approved identity proofing service. They can be used for digital signatures, encryption, and access control, including as proof of identity in medium-value transactions.

Class 3 Certificates provide the highest level of assurances within KPN's Subdomain. Class 3 Certificates are issued to individuals, organizations, and Administrators for CAs and RAs. Class 3 individual Certificates may be used for digital signatures, encryption, and access control, including as proof of identity, in high-value transactions. Class 3 individual Certificates provide assurances of the identity of the Subscriber based on the personal (physical) presence of the Subscriber before a person that confirms the identity of the Subscriber using, at a minimum, a well-recognized form of government-issued identification and one other identification credential. Other Class 3 organizational Certificates are issued to devices to provide authentication; message, software, and content integrity; and confidentiality encryption. Class 3 organizational Certificates provide assurances of the identity of the Subscriber based on a confirmation that the Subscriber organization does in fact exist, that the organization has authorized the Certificate Application, and that the person submitting the Certificate Application on behalf of the Subscriber was authorized to do so. Class 3 organizational Certificates for servers (Secure Server IDs and Global Server IDs) also provide assurances that the Subscriber is entitled to use the domain name listed in the Certificate Application.

Class 3 Organizational ASB Certificates (*see* CP § 1.1.2.2.1), which currently are not offered by KPN, are issued to an organization for use by a duly authorized representative, who uses the Certificate on behalf of the organization. Class 3 Organizational ASB Certificates provide an assurance that the person controlling the organization's private key is authorized to act on behalf

[5] *See* CP § 1.1.1.

of the organization in transactions entered into using the private key corresponding to the public key in the Certificate.

Table 2 below summarizes the Certificate Classes in compliance with the CP. It sets forth the properties of each Certificate class, based on whether they are issued to individuals or organizations, and whether they are offered on a Retail or Managed PKI basis, Authentication Service Bureau program, or issued to Administrators.

The specifications for Classes of Certificates in the CP, as summarized in this CPS, set forth the minimum level of assurances provided for each Class. For example, any Class 1 Certificate may be used for digital signatures, encryption, and access control where proof of identity is not necessary, that is, for applications requiring a low level of assurances. Nonetheless, by contract or within specific environments (such as an intra-company environment), KPN Subdomain Participants are permitted to use validation procedures stronger than the ones set forth within the CP, or use Certificates for higher security applications than the ones described in CPS §§ 1.1.1, 1.3.4.1. Any such usage, however, shall be limited to such entities and subject to CPS §§ 2.2.1.2, 2.2.2.2, and these entities shall be solely responsible for any harm or liability caused by such usage.

Class	*Issued to*	*Services Under Which Certificates are Available*[6]	*Confirmation of Certificate Applicants' Identity (CPS §§ 3.1.8.1, 3.1.9*	*Applications implemented or contemplated by Users (CPS § 1.3.4.1)*
Class 1[7]	Individuals	Retail	Name and e-mail address search to ensure that the distinguished name is unique and unambiguous within the CA's Subdomain.	Modestly enhancing the security of e-mail through confidentiality encryption, digital signatures, and web-based access control, where proof of identity is unnecessary. Applications requiring a low level of assurances in comparison with the other Classes, such as non-commercial web browsing and e-mail.

[6] Retail Certificates are Certificates issued by KPN, acting as CA, to individuals or organizations applying one by one to KPN on its web site. Managed PKI Certificates are based on a Certificate Application approved by a Managed PKI Customer that enters into a Managed PKI Agreement with KPN for the issuance of a certain quantity of Certificates (*see* CP § 1.1.2.1.1). In addition to Retail and Managed PKI Certificates, VTN Certificates are issued , for Administrators of CAs and RAs, and through the Authentication Service Bureau. For more information about Authentication Service Bureau, see CP § 1.1.2.2.1. Administrator Certificates are issued to CA or RA Administrators to allow them to perform administrative functions on behalf of the CA or RA.

[7] KPN currently is not offering Class 1 Individual Certificates.

Class	*Issued to*	*Services Under Which Certificates are Available*[6]	*Confirmation of Certificate Applicants' Identity (CPS §§ 3.1.8.1, 3.1.9*	*Applications implemented or contemplated by Users (CPS § 1.3.4.1)*
Class 2	Individuals	Retail and Authentication Service Bureau[8]	Same as Class 1 Retail, plus automated or Administrator-initiated enrollment information check with one or more third-party databases or comparable sources.	Enhancing the security of e-mail through confidentiality encryption, digital signatures for authentication, and web based access control. Applications requiring a medium level of assurances in comparison with the other Classes, such as some individual and intra- and inter-company e-mail, on-line subscriptions, account applications, and password replacement, including as proof of identity for medium-value transactions.
		Managed PKI	Same as Class 1 retail plus checking internal documentation or databases to confirm identity of the Certificate Applicant (e.g., human resources documentation) and that the Certificate Applicant is affiliated with the Managed PKI Customer.	
Class 3	Individuals	Retail[9]	Same as Class 1 Retail, plus personal presence and check of two or more ID credentials.	Enhancing the security of e-mail through confidentiality encryption, digital signatures for authentication, and web based access control. Applications requiring a high level of assurances in comparison with the other Classes, such as some online banking, corporate database access, and exchanging confidential information, including as proof of identity for high-value transactions.

[8] KPN currently is not offering Class 2 Individual Retail and Authentication Service Bureau Certificates.
[9] KPN currently is not offering Class 3 Individual Retail Certificates.

Class	*Issued to*	*Services Under Which Certificates are Available*[6]	*Confirmation of Certificate Applicants' Identity (CPS §§ 3.1.8.1, 3.1.9*	*Applications implemented or contemplated by Users (CPS § 1.3.4.1)*
		Administrators	Specialized confirmation procedures depending upon the type of Administrator. The identity of the Administrator and the organization utilizing the Administrator are confirmed. *See also* CPS § 5.2.3.	Administrator functions.
	Organizations	Retail	Check of third-party database or other documentation showing proof of right to use the organizational name. Validation check by telephone (or comparable procedure) to confirm information in, and authorization of, the Certificate Application. In the case of web server Certificates, confirmation that the Certificate Applicant has the right to use the domain name to be placed in the Certificate.	Server authentication (some examples being web, ftp, or directory authentication), secure SSL/TLS sessions, confidentiality encryption, and (when communicating with other servers) client authentication (Secure Server ID, Global Server ID, OFX); and authentication and integrity of software and other content (VeriSign Code and Content Signing Digital IDs).
		Authentication Service Bureau[10]	Check of third-party database or other documentation showing the existence of the organization. Validation check by telephone (or comparable procedure) to organization to confirm employment and authority of organizational representative, and to the representative to confirm his or her Certificate Application. Letter confirming the Certificate Application is sent to the representative.	Enhancing the security of e-mail sent on behalf of an organization through confidentiality encryption, digital signatures for authentication, and web based access control. Applications requiring a high level of assurances in comparison with the other Classes, such as gaining access to a B2B extranet or conducting high-value transactions on a B2B exchange.

[10] KPN currently is not offering Class 3 Authentication Service Bureau Certificates.

Class	*Issued to*	*Services Under Which Certificates are Available*[6]	*Confirmation of Certificate Applicants' Identity (CPS §§ 3.1.8.1, 3.1.9*	*Applications implemented or contemplated by Users (CPS § 1.3.4.1)*
		Managed PKI	Validation of Managed PKI for SSL Customer or Managed PKI for SSL Premium Edition Customer as in Class 3 organizational Retail, plus validation of Managed PKI Administrator.	Server authentication, confidentiality encryption, and (when communicating with other properly enabled servers) client authentication (Secure Server ID and Global Server ID).

Table 2 - Certificate Properties Affecting Trust

1.1.2 KPN's Offering of VTN Services

The VTN offers a series of services to assist in the deployment, management, and uses of Certificates, as described fully in CP § 1.1.2. This section discusses which VTN services KPN offers in accordance with CP § 1.1.2. For more information about any of these programs, consult KPN's web site at https://certificaat.kpn.com. All of such services are subject of the specific agreements with KPN. Table 3 summarizes KPN's offering of VTN services.

VTN Service	*Explanation in CP*	*KPN's Offering*
Certificate Distribution Services		
VeriSign Managed PKI®	CP § 1.1.2.1.1	KPN Managed PKI Service
		KPN Managed PKI Lite Service
		KPN Managed PKI for SSL Service
		KPN Managed PKI for SSL Premium Edition Service
VeriSign Web Host Program	CP § 1.1.2.1.4	KPN Web Host services[11] (ISP Program)
Value-Added Services		
VeriSign Authentication Services	CP § 1.1.2.2.1	KPN Outsourced authentication services (currently not offered)
		Authentication Service Bureau (currently not offered)
VeriSign Digital Notarization Service	CP § 1.1.2.2.2	KPN Digital Notarization services (currently not offered)
Special Services		
VeriSign Managed PKI Key Manager Services	CP § 1.1.2.3.2	KPN Managed PKI Key Manager Service
VeriSign Roaming Service	CP § 1.1.2.3.3	KPN Roaming Service

Table 3 – KPN's Offering of VTN Services

[11] KPN currently is not offering the Web Host Program

1.1.2.1 Certificate Distribution Services

1.1.2.1.1 KPN Managed PKI Services

KPN Managed PKI Service is a fully integrated managed PKI service that allows enterprise Customers of KPN to provide Certificates to individuals, such as employees, partners, suppliers, and customers, as well as devices, such as servers, routers, and firewalls. KPN Managed PKI Services is more fully described in CP § 1.1.2.1.1. Managed PKI is an outsourcing service. Customers of KPN Managed PKI Service ("Managed PKI Customers") fall into three categories.

First, some Managed PKI Customers ("Managed PKI Customers") provide client Certificates by becoming a Certification Authority within KPN's Subdomain of the VTN. Managed PKI Customers perform the RA "front-end" functions of approving or denying Certificate Applications, and initiating the revocation or renewal of Certificates using Managed PKI functionality. RA functions are a subset of CA functions.

At the same time, the Managed PKI Customer can leverage the secure PKI backbone of the VeriSign Trust Network by outsourcing all "back-end" Certificate issuing, management, revocation, and renewal functions to KPN.

The second category of Managed PKI Customers ("Managed PKI Lite Customers") uses Managed PKI Lite, which provides security for smaller enterprises and organizations than typical Managed PKI Customers. Managed PKI Lite Customers become Registration Authorities associated with a VeriSign CA, which is shared among KPN's Managed PKI Lite Customers of the specific class of Certificates. Managed PKI Lite Customers, like Managed PKI Customers, approve or deny Certificate Applications using Managed PKI functionality, and request the revocation or renewal of Certificates. As with Managed PKI Customers, KPN performs all the back-end Certificate issuance, management, revocation, and renewal functions, as with Managed PKI Customers.

The final categories of Managed PKI Customers approve Certificate Applications for server Certificates known as Secure Server IDs ("Managed PKI for SSL Customers") and for server Certificates known as Global Server IDs ("Managed PKI for SSL Premium Edition Customers"). Managed PKI for SSL Customers and Managed PKI for SSL Premium Edition Customers become Registration Authorities associated with a KPN CA, which is shared among all VTN (including KPN's) Managed PKI for SSL Customers or Managed PKI for SSL Premium Edition Customers. Managed PKI for SSL Customers and Managed PKI for SSL Premium Edition Customers, as with other Managed PKI Customers, approve or deny Certificate Applications using Managed PKI functionality, and request the revocation or renewal of Certificates. Moreover, as with other Managed PKI Certificates, KPN performs all the back-end Certificate issuance, management, revocation, and renewal functions.

KPN's Managed PKI Customers and Managed PKI Lite Customers are not permitted to approve the Certificate Applications of anyone other than one of their own Affiliated Individuals, except as noted below. Managed PKI Customers may not approve Certificate Applications for VTN Certificates issued to the general public. The Authentication Service Bureau[12], however, provides

[12] KPN currently is not offering the Authentication Service Bureau service.

one solution for organizations seeking to obtain Certificates for unaffiliated individuals and organizational representatives. *See* CPS § 1.1.2.2.1.

A Managed PKI for SSL Customer or Managed PKI for SSL Premium Edition Customer may only approve Certificate Applications for servers within their own organizations. Managed PKI for SSL Customers and Managed PKI for SSL Premium Edition Customers are not permitted to approve the Class 3 Certificate Applications of any servers outside their respective organizations, and may not issue Certificates to the general public.

1.1.2.1.2 VeriSign Affiliate Program

KPN is a Service Center as described in CP §1.1.2.1.2 which means KPN can approve or reject Certificate Applications in the case of Retail Certificates or, in the case of Managed PKI Certificates, arrange with a Processing Center to provide Managed PKI Customers with back-end Certificate lifecycle services. Service Center Affiliates providing client Certificates ("Client Service Centers") become CAs within the VTN but outsource back-end functions to VeriSign or another Processing Center. When providing server Certificates, however, Service Centers become RAs within the VTN for a VeriSign CA issuing either Secure Server IDs or Global Server IDs. These Service Centers ("Service Centers") perform validation functions to approve or reject Certificate applications for Secure Server IDs or Global Server IDs.

Service Centers can also provide VeriSign Managed PKI Services to their Managed PKI Customers. These Managed PKI Customers enter into a Managed PKI arrangement with the Service Center, which under its contract with VeriSign or another Processing Center, arranges to have the Processing Center provide back-end Certificate lifecycle services to these Managed PKI Customers.

1.1.2.1.3 Not Provided

1.1.2.1.4 The Web Host Program

KPN currently is not offering the Web Host Program.

1.1.2.2 Value-Added Certification Services

1.1.2.2.1 Authentication Services

KPN currently is not offering this service.

1.1.2.2.2 KPN Digital Notarization Service

KPN currently is not offering this service.

1.1.2.2.3 Not provided

1.1.2.3 Special Services

1.1.2.3.1 Not provided

1.1.2.3.2 KPN Managed PKI Key Manager Service

Key Management Service is an optional software system installed on an enterprise premises forming part of the KPN Managed PKI Service. Key Management Service operates in conjunction with the KPN Managed PKI Service. This combination allows an enterprise manager to control the backup and recovery of user private keys and digital certificates.

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 also generated in hardware and destroyed. Only the resulting masked session key (MSK) is securely sent and stored at VeriSign. 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, the MSK for that key pair is returned from the Managed PKI database operated out of VeriSign's Processing 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.

An enterprise using KMS shall, at a minimum:

- 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.

1.1.2.3.3 KPN Roaming Service

The KPN Roaming Service, as presented to KPN's Managed PKI Customers, enables a Subscriber to digitally sign critical transactions, such as stock trades, and obtain access to confidential information, without being bound to a single client terminal on which his or her private key resides. KPN's roaming technology permits Subscribers using the service ("Roaming Subscribers") to securely download their private keys and conduct private key operations on different client terminals. The Roaming Subscriber can use his or her private key from any client terminal.

The KPN Roaming Service encrypts Roaming Subscribers' private keys with symmetric

keys that are split and stored on one server or two servers in two physical locations to protect against attacks on a single credential server. The private key itself is stored in encrypted form on the Enterprise Roaming Server. The Roaming Subscriber authenticates himself or herself to the server(s) using a password, and assuming the password is successfully provided, the encrypted private key and the components of the symmetric key needed to decrypt the Subscriber's private key are downloaded to the client terminal. At the client terminal, the symmetric key is reconstituted, the Subscriber's private key is decrypted, and the private key is then available for use during a single session. Following the session, the private key on the client terminal is deleted such that it is unrecoverable.

1.2 Identification

This document is the KPN Certification Practice Statement. VTN Certificates contain object identifier values corresponding to the applicable VTN Class of Certificate. Therefore, KPN has not assigned this CPS an object identifier value. Certificate Policy Object Identifiers are used in accordance with CPS § 7.1.6.

1.3 Community and Applicability

The community governed by this CPS is KPN's Subdomain within the VeriSign Trust Network. The VTN is a PKI that accommodates a worldwide, large, public, and widely distributed community of wired and wireless users with diverse needs for communications and information security. KPN's Subdomain of the VTN is the portion of the VTN governed by this CPS, and the CPS is the document that governs KPN's Subdomain of the VTN. Most of the KPN Subdomain Participants are located in the Netherlands.

1.3.1 Certification Authorities

The term Certification Authority is an umbrella term that refers to all entities issuing Certificates within the VTN. The term "CA" encompasses a subcategory of issuers called Primary Certification Authorities ("PCA"). PCAs act as roots of three domains, one for each class of Certificate. Each PCA is a VeriSign entity. There are currently three generations of VeriSign PCAs (G1, G2 and G3) for each class of Certificate. Subordinate to the PCAs are Certification Authorities that issue Certificates to end-user Subscribers or other CAs. CAs within KPN's Subdomain fall into three categories: (1) KPN itself, (2) Managed PKI Customers, and (3) ASB Customers[13]. VeriSign is a Processing Center that hosts all VTN PCAs, KPN is a Service Center for which VeriSign is hosting all of the KPN CAs, and certain other CAs in the Processing Center of VeriSign.

KPN CAs perform all CA functions (including RA functions), except for the CAs that issue Certificates following approval of Certificate Applications by Managed PKI Lite Customers, Managed PKI for SSL Customers, and Managed PKI for SSL Premium Edition Customers. Managed PKI Customers become CAs within the VTN. Managed PKI Customers outsource back-end functions to a Processing Center, while retaining RA functions for themselves. ASB Customers contract with KPN to become a CA, which issues Certificates naming the ASB Customer as the CA. ASB Customers, however, outsource to KPN all front-end and back-end functions, except for the obligation to initiate revocation of Certificates issued by the ASB Customer's CA in accordance with CPS § 4.4.1.1.

[13] KPN currently is not offering ASB Services.

As discussed in CP § 1.3.1, the RSA Secure Server Certification Authority, which VeriSign acquired from RSA Security Inc., issues Secure Server IDs, which are deemed to be Class 3 Organizational Certificates. VeriSign has approved and designated the RSA Secure Server Certification Authority as a Class 3 CA within KPN's Subdomain of the VTN. The Certificates it issues, Secure Server IDs, are considered to provide assurances of trustworthiness comparable to other Class 3 organizational Certificates.

1.3.2 Registration Authorities

RAs assist a CA by performing front-end functions of confirming identity, approving or denying Certificate Applications, requesting revocation of Certificates, and approving or denying renewal requests. Within KPN's Subdomain of the VTN, RAs fall into four categories: (1) Managed PKI Customers, (2) Managed PKI Lite Customers, (3) Managed PKI for SSL Customers and Managed PKI for SSL Premium Edition Customers, and (4) KPN, in its role as ASB Provider[14]. Other types of RAs are permitted with KPN's advance written consent and if these RAs meet the obligations placed on Managed PKI Customers, subject to any modifications necessary to account for any differences between Managed PKI technology and the technology used by these RAs and the terms of an appropriate agreement.

Managed PKI Lite Customers become RAs assisting a VeriSign CA to issue client Certificates to end-user Subscribers. Similarly, Managed PKI for SSL Customers and Managed PKI for SSL Premium Edition Customers become RAs using Managed PKI that assist the RSA Secure Server CA, the VeriSign International Server CA – Class 3, or similar KPN CA to issue Secure Server IDs or Global Server IDs. KPN, as ASB Provider, offers Authentication Service Bureau services to its ASB Customers. KPN, as ASB Provider, performs both RA front-end functions and back-end functions for ASB Customer CAs.

1.3.3 End Entities

Table 4 shows the types of Subscribers for each Class and type of Certificate offered within KPN's Subdomain of the VTN.

[14] KPN currently is not providing ASB Services.

Class	*Issued to*	*Services Under Which Certificates are Available*	*Types of Subscribers*
Class 1	Individuals	Retail[15]	Any individual, including members of the general public.
Class 2	Individuals	Retail and Authentication Service Bureau[16]	Any individual, including members of the general public.
		Managed PKI	Individuals who are, in relation to the Managed PKI Customer, an Affiliated Individual, except under the Two-Tier Authentication Service. Managed PKI Customers obtaining services under the Two-Tier Authentication Service delegate RA functions to another organization with which it has a relationship, and individuals obtaining Managed PKI Certificates must be affiliated with the organization that has been delegated these RA functions as an Affiliated Individual.
Class 3	Individuals	Retail[17]	Any individual, including members of the general public.
		Administrators	Individuals serving in the role of Administrator (Trusted Persons who perform Certificate or certification service management functions on behalf of KPN, Managed PKI Customers, or trusted fourthparties).
	Organizations	Retail	Organizations that control a device include, but are not limited to: ♦ Web servers or web traffic management devices (Secure Server IDs and Global Server IDs) ♦ OFX servers ♦ Devices digitally signing code or other content.
		Authentication Service Bureau[18]	Organizations, whose private keys are controlled by authorized representatives of the organizations, where authentication procedures have confirmed that such representatives have the authority to act on behalf of their respective organizations.
		Managed PKI	Organizations that control multiple web servers, for which Managed PKI Administrator of such organization approve the issuance of Secure Server IDs and/or Global Server IDs.

Table 4 – Types of Subscribers Within KPN's Subdomain of the VTN

CAs are themselves, as a technical matter, Subscribers of Certificates, either as a PCA issuing a self-signed Certificate to itself, or as a CA issued a Certificate by a superior CA. References to "Subscribers" in this CPS, however, apply only to end-user Subscribers.

[15] KPN currently is not offering Individual Class 1 Retail Services.
[16] KPN currently is not offering Individual Class 2 Retail and Authentication Service Bureau Services.
[17] KPN currently is not offering Individual Class 3 Retail Services.
[18] KPN currently is not offering Organizational Class 3 Authentication Service Bureau Services.

1.3.4 Applicability

This CPS applies to all KPN Subdomain Participants, including KPN, Customers, Resellers, Subscribers, and Relying Parties. This CPS applies to KPN's Subdomain of the VTN and KPN's core infrastructure supporting the VTN. This CPS describes the practices governing the use of Certificates within KPN's Subdomain in each of Classes 1-3, as described in the CP. Each Class of Certificate is generally appropriate for use with the applications set forth in CP § 1.3.4.1 and CPS § 1.1.1 (Table 2). Nonetheless, by contract or within specific environments (such as an intra-company environment), VTN Participants are permitted to use Certificates for higher security applications than the ones described in CPS §§ 1.1.1, 1.3.4.1. Any such usage, however, shall be limited to such entities and subject to CPS §§ 2.2.1.2, 2.2.2, and these entities shall be solely responsible for any harm or liability caused by such usage.

1.3.4.1 Suitable Applications

For suitable applications, *see* CP § 1.3.4.1 and CPS § 1.1.1 (Table 2). These listings, however, are not intended to be exhaustive. Individual Certificates and some organizational Certificates permit Relying Parties to verify digital signatures. KPN Subdomain Participants acknowledge and agree, to the extent permitted by applicable law, that where a transaction is required to be in writing, a message or other record bearing a digital signature verifiable with reference to a VTN Certificate is valid, effective, and enforceable to an extent no less than had the same message or record been written and signed on paper. Subject to applicable law, a digital signature or transaction entered into with reference to a VTN Certificate shall be effective regardless of the geographic location where the VTN Certificate is issued or the digital signature created or used, and regardless of the geographic location of the place of business of the CA or Subscriber.

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

1.3.4.2 Restricted Applications

In general, VTN Certificates are general-purpose Certificates. VTN Certificates may be used globally and to interoperate with diverse Relying Parties worldwide. Usage of VTN Certificates is not generally restricted to a specific business environment, such as a pilot, financial services system, vertical market environment, or virtual marketplace. Nonetheless, such use is permitted and Customers using Certificates within their own environment may place further restrictions on Certificate use within these environments. KPN and other KPN Subdomain Participants, however, are not responsible for monitoring or enforcing any such restrictions in these environments.

Nonetheless, certain VTN Certificates are limited in function. For example, CA Certificates may not be used for any functions except CA functions. Moreover, client Certificates are intended for client applications and shall not be used as server or organizational Certificates. In addition, Class 3 organizational Certificates issued to devices are limited in function to web servers or web traffic management devices (in the case of Secure Server IDs and Global Server IDs)and to secure SSL/TLS

sessions and object signing (in the case of object signing Certificates). Further, Administrator Certificates shall only be used to perform Administrator functions.

Also, with respect to X.509 Version 3 VTN Certificates, the key usage extension is intended to limit the technical purposes for which a private key corresponding to the public key in a Certificate may be used within the VTN. *See* CP § 6.1.9. In addition, end-user Subscriber Certificates shall not be used as CA Certificates. This restriction is confirmed by the absence of a Basic Constraints extension. *See* CP § 7.1.2.4. The effectiveness of extension-based limitations, however, is subject to the operation of software manufactured or controlled by entities other than KPN.
More generally, Certificates shall be used only to the extent use is consistent with applicable law, and in particular shall be used only to the extent permitted by applicable export or import laws.

1.3.4.3 Prohibited Applications

VTN Certificates are not designed, intended, or authorized for use or resale as control equipment in hazardous circumstances or for uses requiring fail-safe performance such as the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control systems, or weapons control systems, where failure could lead directly to death, personal injury, or severe environmental damage. Also, subject to CPS § 1.3.4, Class 1 Certificates shall not be used as proof of identity or as support of nonrepudiation of identity or authority.

1.4 Contact Details

1.4.1 Specification Administration Organization

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

KPN
Businessline Enterprise Networks
Koningin Wilhelminalaan 7-9
P.O. Box 8204
3503 RE UTRECHT, the Netherlands
Attn: KPN Policy Management Authority
mailto:pma.en@kpn.com

1.4.2 Person Determining CPS Suitability for the Policy

The organization identified in CPS § 1.4.1 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 under the CP and this CPS.

2 General Provisions

2.1 Obligations

2.1.1 CA Obligations

CAs perform the specific obligations appearing throughout this CPS. The provisions of the CPS specify obligations of each category of CAs: KPN in its role as Service Center, Managed PKI Customers, and ASB Customers.

In addition, KPN uses commercially reasonable efforts to ensure that Subscriber Agreements and Relying Party Agreements bind Subscribers and Relying Parties within KPN's Subdomain. Examples of such efforts include, but are not limited to, requiring assent to a Subscriber Agreement as a condition of enrollment or requiring assent to a Relying Party Agreement as a condition of receiving Certificate status information. Similarly, Resellers (where required by contract) must use Subscriber Agreements and Relying Party Agreements in accordance with the requirements imposed by KPN. The Subscriber Agreements and Relying Party Agreements must include the provisions required by CPS §§ 2.2-2.4.

Managed PKI Customers are permitted to use Subscriber Agreements specific to them, although not required to do so. Managed PKI Customers using their own Subscriber Agreements must include the provisions required by CPS §§ 2.2-2.4. If a Managed PKI Customer, or Reseller, does not use its own Subscriber Agreement, the Subscriber Agreement of KPN shall apply. If a Reseller has no Relying Party Agreement, the Relying Party Agreement of KPN shall apply.

2.1.2 RA Obligations

RAs assist a Processing Center or Service Center CA by performing validation functions, approving or rejecting Certificate Applications, requesting revocation of Certificates, and approving renewal requests. The provisions of the CPS specify obligations of each category of RAs: Managed PKI Lite Customers, Managed PKI for SSL Customers, Managed PKI for SSL Premium Edition Customers, and KPN in its role as ASB Provider[19].

Also, KPN, as ASB Provider[20], ensures that Subscriber Agreements and Relying Party Agreements bind Subscribers and Relying Parties within its Subdomains in accordance with CPS § 2.1.1. Other RAs have no such obligation.

2.1.3 Subscriber Obligations

Subscriber obligations in the CP apply to Subscribers within KPN's Subdomain, through this CPS, by way of Subscriber Agreements approved by VeriSign. Certain Subscriber Agreements in force within KPN's Subdomain appear at: https://certificaat.kpn.com/repository.

Within KPN's Subdomain, Subscriber Agreements require that Certificate Applicants provide complete and accurate information on their Certificate Applications and manifest assent to the applicable Subscriber Agreement as a condition of obtaining a Certificate.

[19] KPN currently is not offering ASB Services.
[20] KPN currently is not offering ASB Services.

Subscriber Agreements apply the specific obligations appearing in the CP and CPS to Subscribers in KPN's Subdomain. Subscriber Agreements require Subscribers to use their Certificates in accordance with CPS § 1.3.4. They also require Subscribers to protect their private keys in accordance with CPS §§ 6.1-6.2, 6.4. Under these Subscriber Agreements, if a Subscriber discovers or has reason to believe there has been a Compromise of the Subscriber's Private Key or the activation data protecting such Private Key, or the information within the Certificate is incorrect or has changed, that the Subscriber must promptly:

- Notify the entity that approved the Subscriber's Certificate Application, either a CA or an RA, in accordance with CPS § 4.4.1.1 and request revocation of the Certificate in accordance with CPS §§ 3.4, 4.4.3.1, and
- Notify any person that may reasonably be expected by the Subscriber to rely on or to provide services in support of the Subscriber's Certificate or a digital signature verifiable with reference to the Subscriber's Certificate.

Subscriber Agreements require Subscribers to cease use of their private keys at the end of their key usage periods under CPS § 6.3.2.

Subscriber Agreements state that Subscribers shall not monitor, interfere with, or reverse engineer the technical implementation of the VTN, except upon prior written approval from VeriSign, and shall not otherwise intentionally compromise the security of the VTN.

2.1.4 Relying Party Obligations

Relying Party obligations in the CP apply to Relying Parties within KPN's Subdomain, through this CPS, by way of KPN's Relying Party Agreements. Relying Party Agreements in force within KPN's Subdomain appear at https:// certificaat.kpn.com/repository.

Relying Party Agreements within KPN's Subdomain state that before any act of reliance, Relying Parties must 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. They state that KPN, CAs, and RAs are not responsible for assessing the appropriateness of the use of a Certificate. Relying Party Agreements specifically state that Relying Parties must not use Certificates beyond the limitations in CPS § 1.3.4.2 and for purposes prohibited in CPS § 1.3.4.3.

Relying Party Agreements further state that Relying Parties must 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. Under these Agreements, Relying Parties must not rely on a Certificate unless these verification procedures are successful.

Relying Party Agreements also require Relying Parties to check the status of a Certificate on which they wish to rely, as well as all the Certificates in its Certificate Chain in accordance with CPS §§ 4.4.10, 4.4.12. If any of the Certificates in the Certificate Chain have been revoked, according to Relying Party Agreements, the Relying Party must not rely on the end-user Subscriber Certificate or other revoked Certificate in the Certificate Chain.

Finally, Relying Party Agreements state that assent to their terms is a condition of using or otherwise relying on Certificates. Relying Parties that are also Subscribers agree to be bound by Relying Party terms under this section, disclaimers of warranty, and limitations of liability when they agree to a Subscriber Agreement.

Relying Party Agreements state that if all of the checks described above are successful, the Relying Party is entitled to rely on the Certificate, provided that reliance upon the Certificate is 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.

Relying Party Agreements state that Relying Parties must not monitor, interfere with, or reverse engineer the technical implementation of the VTN, except upon prior written approval from VeriSign, and shall not otherwise intentionally compromise the security of the VTN.

2.1.5 Repository Obligations

KPN is responsible for the repository functions for its own CAs and the CAs of its Managed PKI Customers, and ASB Customers. KPN publish Certificates they issue in the repository set forth in Table 5 in accordance with CPS § 2.6.

CA	*Entity Issuing the Certificate on Behalf of the CA*	*Applicable Repository*
All KPN CA's	VeriSign	VeriSign Repository
Managed PKI Customer or KPN ASB Customer	VeriSign	VeriSign Repository

Table 5 – Applicable Repositories By Type of CA

Upon revocation of an end-user Subscriber's Certificate, KPN publishes notice of such revocation in the repository required by Table 5. KPN issues CRLs for its own CAs and the CAs of Managed PKI Customers, and ASB Customers within its Subdomain, pursuant to CPS §§ 2.6, 4.4.9, 4.4.11. In addition, for Managed PKI Customers who have contracted for Online Certificate Status Protocol ("OCSP") services, KPN provides OCSP services pursuant to CPS §§ 2.6, 4.4.9, 4.4.11.

2.2 Liability

2.2.1 Certification Authority Liability

The warranties, disclaimers of warranty, and limitations of liability among KPN, Resellers, and their respective Customers within KPN's Subdomain are set forth and governed by the agreements among them. This CPS § 2.2.1 relates only to the warranties that certain CAs (KPN, and Managed PKI Customers) must make to end-user Subscribers receiving Certificates from them and to Relying Parties, the disclaimers of warranties they shall make to such Subscribers and Relying Parties, and the limitations of liability they shall place on such Subscribers and Relying Parties. Since ASB Customers outsource all front-end and back-end functions to the ASB Provider, the warranty requirements of this section do not apply to ASB Customers.

KPN uses, and (where required) Resellers shall use, Subscriber Agreements and Relying Party Agreements in accordance with CPS § 2.1.1. Managed PKI Customers have the option of using a Subscriber Agreement. These Subscriber Agreements shall meet the requirements imposed by KPN (in the case of Resellers). Requirements that Subscriber Agreements contain warranties, disclaimers, and limitations of liability below apply to those Managed PKI Customers, and Resellers that use Subscriber Agreements. KPN adheres to such requirements in its Subscriber Agreements. KPN's practices concerning warranties, disclaimers, and limitations in Relying Party Agreements apply to KPN. Note that terms applicable to Relying Parties shall also be included in Subscriber Agreements, in addition to Relying Party Agreements, because Subscribers often act as Relying Parties as well.

2.2.1.1 Certification Authority Warranties to Subscribers and Relying Parties

KPN's Subscriber Agreements include, and other Subscriber Agreements shall include, a warranty to Subscribers that:

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

KPN's Relying Party Agreements contain a warranty to Relying Parties who reasonably rely on a Certificate that:

- All information in or incorporated by reference in such Certificate, except Nonverified Subscriber Information, is accurate,
- In the case of Certificates appearing in the KPN repository, that the Certificate has been issued to the individual or organization named in the Certificate as the Subscriber, and that the Subscriber has accepted the Certificate in accordance with CPS § 4.3, and
- The entities approving the Certificate Application and issuing the Certificate have substantially complied with this CPS when issuing the Certificate.

2.2.1.2 Certification Authority Disclaimers of Warranties

To the extent permitted by applicable law, KPN's Subscriber Agreements and Relying Party Agreements disclaim, and other Subscriber Agreements shall disclaim, KPN's possible warranties, including any warranty of merchantability or fitness for a particular purpose.

2.2.1.3 Certification Authority Limitations of Liability

To the extent permitted by applicable law, KPN's Subscriber Agreements and Relying Party Agreements limit, and other Subscriber Agreements shall limit, KPN's liability. Limitations of liability include an exclusion of indirect, special, incidental, and consequential damages. They also include the following liability caps limiting KPN's damages concerning a specific Certificate:

Class	*Liability Caps*
Class 2	Five Thousand Euro (€ 5.000,00)
Class 3	One Hundred Thousand Euro (€ 100.000,00)

Table 6 – Liability Caps

2.2.1.4 Force Majeure

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

2.2.2 Registration Authority Liability

The warranties, disclaimers of warranty, and limitations of liability between an RA and the CA it is assisting to issue Certificates, or the applicable Reseller, are set forth and governed by the agreements between them. KPN, in its role as ASB[21] Provider RA, uses Subscriber Agreements and Relying Party Agreements in accordance with CPS §§ 2.1.1-2.1.2, which have their own warranties, disclaimers, and limitations.

Managed PKI Lite Customers, Managed PKI for SSL Customers, and Managed PKI for SSL Premium Edition Customers do not use Subscriber Agreements or Relying Party Agreements. Thus, the practices disclosed in this section do not apply to them. Rather, the Subscriber Agreement of KPN shall apply.

KPN, on behalf of its ASB Customer CAs, includes within Subscriber Agreements and Relying Party Agreements the warranties, disclaimers of warranty, limitations of liability, and force majeure clauses set forth in CPS §§ 2.2.1.1-2.2.1.4.

2.2.3 Subscriber Liability

2.2.3.1 Subscriber Warranties

KPN's Subscriber Agreements require Subscribers to warrant that:

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

[21] KPN currently is not offering ASB services.

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

Other Subscriber Agreements shall also contain these requirements.

Where a Subscriber's Certificate Application was approved by a Managed PKI Customer using the Managed PKI Key Manager offering, however, the Subscriber warrants only that no unauthorized person has ever had access to the copy of the Subscriber's private key on the Subscriber's hardware/software platform. These Subscribers make no warranty concerning the copies of their private keys in the possession of the Managed PKI Customers using Managed PKI Key Manager.

2.2.3.2 Private Key Compromise

The CP sets forth VTN Standards for the protection of the private keys of Subscribers, which are included by virtue of CPS § 6.2.7.1 in Subscriber Agreements. Subscriber Agreements state that Subscribers failing to meet these VTN Standards are solely responsible for any loss or damage resulting from such failure

2.2.4 Relying Party Liability

Subscriber Agreements and Relying Party Agreements require Relying Parties to acknowledge that they have sufficient information to make an informed decision as to the extent to which they choose to rely on the information in a Certificate, that they are solely responsible for deciding whether or not to rely on such information, and that they shall bear the legal consequences of their failure to perform the Relying Party obligations in CPS § 2.1.4.

2.3 Financial Responsibility

2.3.1 Indemnification by Subscribers and Relying Parties

2.3.1.1 Indemnification by Subscribers

To the extent permitted by applicable law, KPN's Subscriber Agreement require, and other Subscriber Agreements shall require, Subscribers to indemnify KPN and any non-KPN CAs or RAs for:

- Falsehood or misrepresentation of fact by the Subscriber on the Subscriber's Certificate Application,
- Failure by the Subscriber to disclose a material fact on the Certificate Application, if the misrepresentation or omission was made negligently or with intent to deceive any party,
- The Subscriber's failure to protect the Subscriber's private key, to use a Trustworthy System, or to otherwise take the precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorized use of the Subscriber's private key, or
- The Subscriber's use of a name (including without limitation within a common name, domain name, or e-mail address) that infringes upon the Intellectual Property Rights of a third party.

2.3.1.2 Indemnification by Relying Parties

To the extent permitted by applicable law, KPN's Subscriber Agreements and Relying Party Agreements require, and other Subscriber Agreements shall require, Relying Parties to indemnify KPN and any non-KPN CAs or RAs for:

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

2.3.2 Fiduciary Relationships

To the extent permitted by applicable law, KPN's Subscriber Agreements and Relying Party Agreements disclaim, and other Subscriber Agreements shall disclaim, any fiduciary relationship between KPN or a non-KPN CA or RA on one hand and a Subscriber or Relying Party on the other hand.

2.3.3 Administrative Processes

Managed PKI 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. Managed PKI Customers shall also 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. This insurance requirement does not apply to governmental entities. KPN maintains such errors and omissions insurance coverage.

2.4 Interpretation and Enforcement

2.4.1 Governing Law

Subject to any limits appearing in applicable law, the laws of the Netherlands shall govern the enforceability, construction, interpretation, and validity of this CPS, irrespective of contract or other choice of law provisions and without the requirement to establish a commercial nexus in 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 CPS § 2.4.1 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 applicable national, state, local and foreign laws, rules, regulations, ordinances, decrees, and orders including, but not limited to, restrictions on exporting or importing software, hardware, or technical information.

2.4.2 Severability, Survival, Merger, Notice

To the extent permitted by applicable law, KPN's Subscriber Agreements and Relying Party Agreements contain, and other Subscriber Agreements shall contain, severability, survival, merger, and notice clauses. A severability clause in an agreement prevents any determination of the invalidity or unenforceability of a clause in the agreement from impairing the remainder of the agreement. A survival clause specifies the provisions of an agreement that continue in effect despite the termination or expiration of the agreement. A merger clause states that all understandings concerning the subject matter of an agreement are incorporated in the agreement. A notice clause in an agreement sets forth how the parties are to provide notices to each other.

2.4.3 Dispute Resolution Procedures

2.4.3.1 Disputes Among KPN and Customers

Disputes between KPN and one of its Customers shall be resolved pursuant to provisions in the applicable agreement between the parties.

2.4.3.2 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.

2.5 Fees

2.5.1 Certificate Issuance or Renewal Fees

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

2.5.2 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.

2.5.3 Revocation or Status Information Access Fees

KPN does not charge a fee as a condition of making the CRLs required by CPS § 4.4.9 available in a repository or otherwise available to Relying Parties. KPN does, however, 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 its repository by third parties that provide products or services that utilize such Certificate status information without KPN's prior express written consent.

2.5.4 Fees for Other Services Such as Policy Information

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

2.5.5 Refund Policy

Within KPN's Subdomain, the following refund policy is in effect for non Managed PKI Customers:

> KPN adheres to, and stands behind, rigorous practices and policies in undertaking certification operations and in issuing certificates. Nevertheless, if for any reason a subscriber is not completely satisfied with the certificate issued to him, her, or it, the subscriber may request that KPN revoke the certificate within thirty (30) days of issuance and provide the subscriber with a refund. Following the initial thirty (30) day period, a subscriber may request that KPN revoke the certificate and provide a refund if KPN has breached a warranty or other material obligation under this CPS relating to the subscriber or the subscriber's certificate. After KPN revokes the subscriber's certificate, KPN will promptly credit the subscriber's credit card account (if the certificate was paid for via credit card) or otherwise reimburse the subscriber via check, for the full amount of the applicable fees paid for the certificate. To request a refund, please send an e-mail at mailto:refund@certificaat.kpn.com. This refund policy is not an exclusive remedy and does not limit other remedies that may be available to subscribers.

2.6 Publication and Repository

2.6.1 Publication of CA Information

VeriSign is responsible for the repository function for VeriSign's Public Primary Certification Authorities (PCAs) and VeriSign Infrastructure/Administrative CAs supporting the VTN.

KPN is responsible for the repository function for KPN's Infrastructure, Administrative CA's and KPN's CAs, Managed PKI Customers' CAs, and ASB Customers' CAs which issue Certificates within KPN's Subdomain of the VTN.

KPN publishes certain CA information in the repository section of KPN's web site at https://certificaat.kpn.com/repository as described below.

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

KPN publishes Certificates in accordance with Table 7 below.

Certificate Type	*Publication Requirements*
VeriSign PCA and VeriSign 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.
KPN 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 Type	*Publication Requirements*
Certificate of the KPN CA supporting Managed PKI Lite Certificates and CA Certificates of Managed PKI Customers	Available through query of the VeriSign LDAP directory server at directory.verisign.com.
OCSP Responder Certificates	Available through query of the VeriSign LDAP directory server at directory.verisign.com.
End-User Subscriber Certificates	Available to relying parties through query functions in the KPN repository at: https://digitalid.kpn.com/repository. Also available through query of the VeriSign LDAP directory server at directory.verisign.com.
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 7 – Certificate Publication Requirements

KPN publishes Certificate status information in accordance with CPS § 4.4.11.

2.6.2 Frequency of Publication

Updates to this CPS are published in accordance with CPS § 8. Updates to Subscriber Agreements and Relying Party Agreements are published as necessary. Certificates are published upon issuance. Certificate status information is published in accordance with CPS §§ 4.4.9 and 4.4.11.

2.6.3 Access Controls

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 or CRL Usage Agreement as a condition to accessing Certificates, Certificate status information, or CRLs. KPN has implemented logical and physical security measures to prevent unauthorized persons from adding, deleting, or modifying repository entries.

2.6.4 Repositories

See CPS § 2.1.5.

2.7 Compliance Audit

An annual WebTrust for Certification Authorities examination is performed for KPN's Service Center operations supporting VeriSign's public and Managed PKI CA services including the VTN Root CAs, Class 3 Organizational CAs, Class 2 Organizational and Individual CAs, and Class 1 Individual CAs specified in CPS § 1.3.1. Customer-specific CAs are not specifically audited as part of the audit of KPN's operations unless required by the Customer. KPN shall be entitled to require that Managed PKI Customers undergo a compliance audit under this CPS § 2.7 and audit programs for these types of Customers.

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

- KPN or its authorized representative shall be entitled, within its sole and exclusive discretion, to perform at any time an "Exigent Audit/Investigation" on itself or a Customer in the event KPN or its authorized representative has reason to believe that the audited entity has failed to meet VTN 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 VTN.
- KPN or its authorized representative shall be entitled to perform "Supplemental Risk Management Reviews" on itself or 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 or its authorized representative 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 KPN and the personnel performing the audit, review, or investigation.

2.7.1 Frequency of Entity Compliance Audit

Compliance audits are performed on an annual basis at the sole expense of the audited entity.

2.7.2 Identity/Qualifications of Auditor

The audits for KPN's Service Center operations are performed by a public accounting firm that:

- Demonstrates proficiency in public key infrastructure technology, information security tools and techniques, security auditing, and the third-party attestation function, and
- Is registrated by the Nederlandse Orde van Register EDP-Auditors (NOREA) or similar entity, which requires the possession of certain skill sets, quality assurance measures such as peer review, competency testing, standards with respect to proper assignment of staff to engagements, and requirements for continuing professional education.

2.7.3 Auditor's Relationship to Audited Party

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

2.7.4 Topics Covered by Audit

The scope of KPN's annual WebTrust for Certification Authorities (or equivalent) includes all CA environmental controls, key management operations and Infrastructure/Administrative CA controls that are performed by KPN as a VTN Service Center. Specifically KPN's business practices disclosure, KPN's environmental controls and the certificate life cycle management as far as parts of the certificate life cycle management is performed by KPN.

2.7.5 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 VTN, 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.

2.7.6 Communications of Results

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

2.8 Confidentiality and Privacy

KPN has implemented a privacy policy, which is located at https://certificaat.kpn.com/repository, in compliance with the requirements of the Directive on the Protection of Individuals with Regard to the Processing of Personal Data on the Free Movement of such Data, CP § 2.8 and applicable Dutch privacy law (Wet Bescherming Persoonsgegevens).

2.8.1 Types of Information to be Kept Confidential and Private

The following records of Subscribers are, subject to CPS § 2.8.2, kept confidential and private ("Confidential/Private Information"):

- CA application records, whether approved or disapproved,
- Certificate Application records (subject to CPS § 2.8.2),
- Private keys held by Managed PKI Customers using Managed PKI Key Manager and information needed to recover such private keys,
- Transactional records (both full records and the audit trail of transactions),
- VTN audit trail records created or retained by VeriSign, an Affiliate, or a Customer,
- KPN audit reports created by KPN or their respective auditors (whether internal or public).
- Contingency planning and disaster recovery plans, and
- Security measures controlling the operations of KPN hardware and software and the administration of Certificate services and designated enrollment services.

2.8.2 Types of Information Not Considered Confidential or Private

KPN Subdomain Participants acknowledge that Certificates, Certificate revocation and other status information, KPN's repository, and information contained within them are not considered Confidential/Private Information. Information not expressly deemed Confidential/Private Information under CPS § 2.8.1 shall be considered neither confidential nor private. This section is subject to applicable privacy laws.

2.8.3 Disclosure of Certificate Revocation/Suspension Information

See CPS § 2.8.2.

2.8.4 Release to Law Enforcement Officials

KPN Subdomain Participants acknowledge that KPN shall be entitled to disclose Confidential/Private Information if, in good faith, KPN believes disclosure is necessary in response to subpoenas and search warrants. This section is subject to applicable privacy laws.

2.8.5 Release as Part of Civil Discovery

KPN Subdomain Participants acknowledge that KPN shall be entitled to disclose Confidential/Private Information if, in good faith, KPN believes disclosure is necessary in response to judicial, administrative, or other legal process during the discovery process in a civil or administrative action, such as subpoenas, interrogatories, requests for admission, and requests for production of documents. This section is subject to applicable privacy laws.

2.8.6 Disclosure Upon Owner's Request

KPN's privacy policy contains provisions relating to the disclosure of Confidential/Private Information to the person disclosing it to KPN. This section is subject to applicable privacy laws.

2.8.7 Other Information Release Circumstances

No stipulation.

2.9 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 CPS § 2.9 apply to the Intellectual Property Rights in relation to Subscribers and Relying Parties.

2.9.1 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.

2.9.2 Property Rights in the CPS

KPN Subdomain Participants acknowledge that KPN retains all Intellectual Property Rights in and to this CPS.

2.9.3 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.

2.9.4 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 Managed PKI 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. Notwithstanding the foregoing, VeriSign's root public keys and the root Certificates containing them, including all PCA public keys and self-signed Certificates, are the property of VeriSign. VeriSign licenses software and hardware manufacturers to reproduce such root Certificates to place copies in trustworthy hardware devices or software. Finally, without limiting the generality of the foregoing, a CA's private key is the property of the CA, and the CA retains all Intellectual Property Right in and to its private key.

3 Identification and Authentication

3.1 Initial Registration

3.1.1 Types of Names

KPN CA Certificates contain X.501 Distinguished Names in the Issuer and Subject fields. KPN CA Distinguished Names consist of the components specified in Table 8 below.

Attribute	*Value*
Country (C) =	"NL" or not used.
Organization (O) =	"KPN" or "KPN Telecom B.V." except for the Secure Server CA, which indicates "RSA Data Security, Inc.," but is now a VeriSign CA.
Organizational Unit (OU) =	KPN CA Certificates may contain multiple OU attributes. Such attributes may contain one or more of the following: ♦ CA Name ♦ VeriSign Trust Network ♦ A statement referencing the applicable Relying Party Agreement governing terms of use of the Certificate and ♦ A copyright notice. ♦ Text to describe the type of Certificate
State or Province (S) =	Not used.
Locality (L) =	Not used except for the VeriSign Commercial Software Publishers CA, which uses "Internet."
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 8 – Distinguished Name Attributes in CA Certificates

End-user Subscriber Certificates contain an X.501 distinguished name in the Subject name field and consist of the components specified in Table 9 below.

Attribute	*Value*
Country (C) =	"NL" or not used.
Organization (O) =	The Organization attribute is used as follows: ♦ "KPN" or "KPN Telecom B.V." for KPN OCSP Responder and optionally for individual Certificates that do not have an organization affiliation. ♦ Subscriber organizational name for web server Certificates and individual Certificates that have an organization affiliation. .
Organizational Unit (OU) =	KPN end-user Subscriber Certificates may contain multiple OU attributes. Such attributes may contain one or more of the following: ♦ Subscriber organizational unit (for organizational

Attribute	*Value*
	Certificates and individual Certificates that have an organization affiliation) ♦ VeriSign Trust Network ♦ A statement referencing the applicable Relying Party Agreement governing terms of use of the Certificate ♦ A copyright notice ♦ "Authenticated by KPN Telecom B.V." and "Member, VeriSign Trust Network" in Certificates whose applications were authenticated by KPN ♦ "Persona Not Validated" for Class 1 Individual Certificates ♦ 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) ♦ Organization name (for code/object signing Certificates) ♦ Name (for individual Certificates).
E-Mail Address (E) =	E-mail address for Class 1 individual Certificates and generally for MPKI Subscriber Certificates.

Table 9 – 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 2-3 Certificates.

- The authenticated common name value included in the Subject distinguished names of organizational Certificates is a domain name (in the case of Secure Server IDs and Global Server IDs) or the legal name of the organization or unit within the organization.
- The authenticated common name value included in the Subject distinguished name of a Class 3 Organizational ASB Certificate, however, is the generally accepted personal name of the organizational representative authorized to use the organization's private key, and the organization (O=) component is the legal name of the organization.
- The common name value included in the Subject distinguished name of individual Certificates represents the individual's generally accepted personal name.

3.1.2 Need for Names to be Meaningful

Class 2 and 3 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. For such Certificates, pseudonyms of end-user Subscribers (names other than a Subscriber's true personal or organizational name) are not permitted.

The use of pseudonyms is permitted only for Class 1 end-user Subscriber Certificates.

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 Rules for Interpreting Various Name Forms

No stipulation.

3.1.4 Uniqueness of Names

KPN ensures that Subject Distinguished Names of Subscribers 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

3.1.5 Name Claim Dispute Resolution Procedure

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 dispute.

3.1.6 Recognition, Authentication, and Role of Trademarks

See CPS § 3.1.5.

3.1.7 Method to Prove Possession of Private Key

KPN verifies the Certificate Applicant's possession of a private key through the use of a digitally signed certificate request pursuant to PKCS #10, another cryptographically-equivalent demonstration, or another KPN-approved method.

Where a key pair is generated by KPN on behalf of a Subscriber (e.g., where pre-generated keys are placed on smart cards), this requirement is not applicable.

3.1.8 Authentication of Organization Identity

KPN confirms the identity of Class 3 organizational end-user Subscribers and other enrollment information provided by Certificate Applicants (except for Nonverified Subscriber Information) in accordance with the procedures set forth in the subsections that follow. In addition to the procedures below, the Certificate Applicant must demonstrate that it rightfully holds the private key corresponding to the public key to be listed in the Certificate in accordance with CPS § 3.1.7.

3.1.8.1 Authentication of the Identity of Organizational End-User Subscribers

3.1.8.1.1 Authentication for Retail Organizational Certificates

KPN confirms the identity of a Certificate Applicant for a Retail organizational Certificate by:

- Verifying that the organization exists through the use of 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

- Confirming with an appropriate Organizational contact by telephone, postal mail, or a comparable procedure 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 Organization is authorized to do so.

Additional procedures are performed for specific types of Certificates as described in Table 10 below.

Certificate Type	*Additional Procedures*
All Server Certificates	KPN verifies that the Certificate Applicant is the record owner of the domain name of the server that is the Subject of the Certificate or is otherwise authorized to use the domain.
Global Server Ids	KPN performs the 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") (formerly known as the Bureau of Export Administration ("BXA")).

Table 10 – Specific Authentication Procedures

3.1.8.1.2 Authentication for Managed PKI for SSL or Managed PKI for SSL Premium Edition

With respect to Managed PKI for SSL Customers and Managed PKI for SSL Premium Edition Customers, the identity confirmation process begins with KPN's confirmation of the identity of the Managed PKI for SSL Customer or Managed PKI for SSL Premium Edition Customer itself in accordance with CPS § 3.1.8.2. Following such confirmation, the Managed PKI for SSL Customer or Managed PKI for SSL Premium Edition Customer is responsible for approving the issuance of Certificates to servers within its own organization by:

- Ensuring that the server designated as the Subject of a Secure Server ID or Global Server ID actually exists, and
- Ensuring the organization has authorized the issuance of a Secure Server ID or Global Server ID to the server.

3.1.8.1.3 Authentication for Class 3 Organizational ASB Certificates[22]

KPN's services as an ASB Provider include the following steps to confirm the identity of a Certificate Applicant for a Class 3 Organizational ASB Certificate:

- A determination 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,
- A confirmation by telephone, confirmatory postal mail, and/or comparable procedure to the Certificate Applicant to confirm certain information about the organization, confirm that the organization has authorized the Certificate Application, confirm the employment of the representative submitting the Certificate Application on behalf of the Certificate

[22] KPN currently is not offering ASB services

Applicant, and confirm the authority of the representative to act on behalf of the Certificate Applicant, and

- A confirmation by telephone, confirmatory postal mail, and/or comparable procedure to the Certificate Applicant's representative to confirm that the person named as representative has submitted the Certificate Application.

KPN may subcontract such services provided that the subcontractor meets these requirements, security requirements, and all other requirements imposed on KPN when performing these services under the CPS.

3.1.8.2 Authentication of the Identity of CAs and RAs

For KPN CA Certificate Applications, certificate requests are created, processed and approved by authorized KPN personnel using a controlled process that requires the participation of multiple trusted KPN employees.

Managed PKI Customers and ASB Customers enter into an agreement with KPN before becoming CAs or RAs. KPN authenticates the identity of the prospective Managed PKI Customer or ASB Customer, before final approval of its status as CA or RA by performing the checks required for the confirmation of the identity of organizational end-user Subscribers specified in CPS § 3.1.8.1, except that instead of a Certificate Application, the validation is of an application to become a Managed PKI Customer or ASB Customer. In addition, in the case of Managed PKI Customers, KPN confirms that the person identified as Managed PKI Administrator is authorized to act in the capacity. Optionally, KPN may require the personal appearance of an authorized representative of the organization before authorized KPN personnel.

In some cases, KPN may delegate responsibility for authentication of a prospective Managed PKI Customer or ASB Customer to a Reseller. Resellers' procedures for the authentication of the organizational identity of the prospective customer must be submitted to KPN for approval, and such approval is a condition of a Reseller beginning its operations as a provider of Managed PKI or Authentication Service Bureau services, as the case may be. Such procedures must meet the requirements specified in the previous paragraph.

3.1.9 Authentication of Individual Identity

For all Classes of individual Certificates, KPN (on behalf of its own CA or the CAs of its ASB Customers), or a Managed PKI Customer confirms that:

- The Certificate Applicant is the person identified in the Certificate Application (except for Certificate Applicants for Class 1 Certificates),
- The Certificate Applicant rightfully holds the private key corresponding to the public key to be listed in the Certificate in accordance with CPS § 3.1.7, and
- The information to be included in the Certificate is accurate, except for Nonverified Subscriber Information.

In addition, KPN performs the more detailed procedures described below for each Class of Certificate.

3.1.9.1 Class 1 Individual Certificates[23]

Authentication of individuals for Class 1 Certificates consists of a check to ensure that the Subject distinguished name is a unique and unambiguous Subject name within the KPN Class 1 CA Subdomain. Class 1 authentication does not provide assurances of identity (i.e., that a Subscriber is who he or she claims to be). The common name of the Subscriber is Nonverified Subscriber Information. Class 1 authentication also includes a limited confirmation of the Certificate Applicant's e-mail address.

3.1.9.2 Class 2 Individual Certificates

Authentication of Class 2 Certificates takes place in one of two ways. For Class 2 Managed PKI Certificates, Managed PKI Customers and Managed PKI Lite Customers use business records or databases of business information to approve or deny Certificate Applications in accordance with CPS § 3.1.9.2.1. For Retail Class 2 Certificates and Class 2 Individual ASB Certificates[24], KPN confirms the identity of Certificate Applicants using information residing in the database of a KPN-approved identity proofing service in accordance with CPS § 3.1.9.2.2.

3.1.9.2.1 Class 2 Managed PKI Certificates

For Class 2 Managed PKI Certificates, the Managed PKI Customer approves Certificate Applications using manual or automated authentication procedures or passcodes as discussed below. Managed PKI Customers and Managed PKI Lite Customers confirm the identity of individuals by comparing enrollment information against their own business records or databases of business information. For example, they may check enrollment information against employee or independent contractor records in a human resources department database. The Managed PKI Customer or Managed PKI Lite Customer may approve the Certificate Application manually using the Managed PKI Control Center if the enrollment information matches the records or database used for authentication. This process is known as "Manual Authentication."

Managed PKI's Automated Administration Software Module and other similar KPN software give Managed PKI Customers the option of automatic approval and revocation of users or devices directly from pre-existing administrative systems or databases, rather than requiring Manual Authentication for each Certificate Application. Managed PKI Customers using the Managed PKI Automated Administration Software Module authenticate the identity of potential Certificate Applications before placing their information in a database. When a Certificate Applicant submits a Certificate Application, then, the Automated Administration Software Module compares information in the Certificate Application with the database and, if the information matches, automatically approves the Certificate Application for immediate issuance by KPN. This process is called "Automated Administration."

KPN Managed PKI "Passcode" authentication ("Passcode Authentication") involves the automatic approval or rejection of Certificate Applications by comparing a Certificate Applicant's enrollment data with pre-configured authentication data that is provided by a Managed PKI Customer's Managed PKI Administrator. With Passcode Authentication, the Managed PKI Customer uses an offline process to distribute "passcodes" to prospective Certificate Applicants that have satisfied

[23] KPN currently is not offering Class 1 Certificates.
[24] KPN currently is not offering Class 2 Retail or Individual Authentication Service Bureau Certificates.

the appropriate level of authentication. The Certificate Applicant then provides this passcode when submitting a Certificate Application, along with other authentication information. The passcode and additional authentication information are compared to the passcode database previously configured by the Managed PKI Administrator, and if all the fields match, a Certificate is issued.

Managed PKI Customers not using Automated Administration or Passcode Authentication must use Manual Authentication.

3.1.9.2.2 Class 2 Retail Certificates[25]

KPN validates Certificate Applications for Class 2 Retail Certificates and Class 2 Individual ASB Certificates by determining if identifying information in the Certificate Application matches information residing in the database of a KPN-approved identity proofing service, such as a major credit bureau or other reliable source of information providing services. If the information in the Certificate Application matches the information in the database, KPN may approve the Certificate Application.

3.1.9.3 Class 3 Individual Certificates

3.1.9.3.1 Class 3 Individual Certificates[26]

The authentication of Class 3 individual Certificate Applications is based on the personal (physical) presence of the Certificate Applicant before an authorized KPN representative, Managed PKI Customer, notary public, or other official with comparable authority within the Certificate Applicant's jurisdiction. The agent, notary, or other official checks the identity of the Certificate Applicant against a well-recognized form of government-issued identification, such as a passport or driver's license and one other identification credential.

3.1.9.3.2 Class 3 Administrator Certificates

Various Administrator Certificates are used to control access to KPN CA systems and for authorizing certain actions within the VTN. The specific types of Class 3 Administrator Certificates are listed in CPS §1.3.1.

KPN authenticates Class 3 Administrator Certificate Applications for Managed PKI Customer and trusted third party employees as follows:

- KPN authenticates the existence and identity of the entity employing or retaining the Administrator pursuant to CPS § 3.1.8.2
- KPN confirms the employment and authorization of the person named as Administrator in the Certificate Application to act as Administrator.

KPN also approves Certificate Applications for its own Administrators. Administrators are "Trusted Persons" within their respective organization (see CPS § 5.2.1). In this case, authentication of their Certificate Applications is based on confirmation of their identity in connection with their

[25] KPN currently is not offering Class 2 Retail Certificates
[26] KPN currently is not offering Class 3 Individual Certificates

employment or retention as an independent contractor (see CPS § 5.2.3), background checking procedures (see CPS § 5.3.2), and authorization to act as Administrator.

KPN may also approve Certificate Applications for its own Administrator Certificates to be associated with a non-human recipient such as a device, or a service. KPN authenticates Class 3 Administrator Certificate Applications for a non-human recipient as follows:

- KPN authenticates the existence and identity of the service named as the Administrator in the Certificate Application
- KPN authenticates that the service has been securely implemented in a manner consistent with it performing an Administrative function
- KPN confirms the employment and authorization of the person enrolling for the Administrator certificate for the service named as Administrator in the Certificate Application.

3.2 Routine Rekey and Renewal

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 "rekey"). However, in certain cases (i.e., for web server certificates) KPN permits Subscribers to request a new certificate for an existing key pair (technically defined as "renewal"). Table 11 below describes KPN's requirements for routine rekey (issuance of a new certificate for a new key pair that replaces an existing key pair) and renewal (issuance of a new certificate for an existing key pair).

Generally speaking, both "Rekey" and "Renewal" are commonly described as "Certificate Renewal," focusing on the fact that the old Certificate is being replaced with a new Certificate and not emphasizing whether or not a new key pair is generated. For all Classes and Types of KPN Certificates, except for Class 3 Server 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.

However, for Class 3 Server Certificates, because the Subscriber key pair is generated on the web server and most web server key generation tools permit the creation of a new Certificate Request for an existing key pair, there is a distinction between "rekey" and "renewal." In addition, new CA Certificates may be issued for existing KPN CA key pairs subject to the constraints specified in Table 11 below.

Certificate Class and Type	*Routine Rekey and Renewal Requirements*
Class 1, Class 2, Class 3 Code and Object Signing, and Class 3 Administrator Certificates	For these types of Certificates, Subscriber key pairs are generally browser generated as part of the online enrollment process and the Subscriber does not have the option to submit an existing key pair for "renewal." Accordingly, for these types of Certificates, rekey is supported and Certificate renewal is not. In so far as a Customer is able to submit an existing key pair for "renewal" KPN may renew that Certificate. However, KPN

Certificate Class and Type	*Routine Rekey and Renewal Requirements*
	recommends that customers generate a new key pair as that is most secure.
Class 3 Server Certificates	For Secure Server IDs or Global Server IDs, Subscriber key pairs are generated outside of the online enrollment process (i.e., generated on a web server). Most server key generation tools, permit the Subscriber to create a new Certificate Signing Request (CSR) for a previously-used key pair. Accordingly, for Secure Server IDs and Global Server IDs, both rekey and Certificate renewal are supported.
CA Certificates	Renewal of CA Certificates is permitted as long as the cumulative certified lifetime of the CA key pair does not exceed the applicable maximum CA key pair lifetime specified in CPS § 6.3.2. KPN CAs may also be rekeyed in accordance with CPS § 4.7. Accordingly, for KPN CA Certificates both rekey and certificate renewal are supported.

Table 11 – Routine Rekey and Renewal Requirements

3.2.1 Routine Rekey and Renewal for End-User Subscriber Certificates

Subscriber Certificates, which have not been revoked, may be replaced (i.e., rekeyed or renewed) in accordance with the Table 12 below.

Timing	*Requirement*
Within 30 days before and 30 days after Certificate expiration	For all KPN Certificates (except for Class 3 Organizational ASB certificates), KPN or the Managed PKI Customer authenticates Subscribers seeking Certificate replacement through the use of a Challenge Phrase (or the equivalent thereof), or proof of possession of the private key. As part of the initial registration process, Subscribers choose and submit a Challenge Phrase with their enrollment information. Upon rekey or renewal of a Certificate within the specified timeframe, if a Subscriber correctly submits the Subscriber's Challenge Phrase (or the equivalent thereof) with the Subscriber's reenrollment information, or proves possession of the private key, and the enrollment information (including contact information) has not changed, a new Certificate is automatically issued[27]. After rekeying or renewal in this fashion, and on at least alternative instances of subsequent rekeying or renewal thereafter, the CA or RA shall reconfirm the identity of the Subscriber in accordance with the requirements specified in CPS § 3.1.8.1 for the authentication of an original Certificate Application. The authentication of a request to replace a Class 3 Organizational ASB

[27] Where the subscriber is unable to use a challenge phrase the subscriber's reenrollment information will be reauthenticated.

Timing	*Requirement*
	Certificate requires the use of a Challenge Phrase as well as the authentication procedures for an original Certificate Application under CPS § 3.1.8.1.3.
Beyond 30 days after Certificate expiration	In this scenario, the requirements specified in CPS § 3.1.8.1 and 3.1.9 for the authentication of an original Certificate Application are used for replacing an end-user Subscriber Certificate. The authentication of a request to replace a Class 3 Organizational ASB Certificate requires the use of a Challenge Phrase as well as the authentication procedures for an original Certificate Application under CPS § 3.1.8.1.3.

Table 12 – Routine Rekey and Renewal Requirements for End-User Subscriber Certificates

3.2.2 Routine Rekey and Renewal for CA Certificates

KPN CAs may be rekeyed periodically in accordance with CPS § 4.7.

KPN CA Certificates may be renewed within the parameters specified in CPS § 6.3.2. For example, if an initial PCA certificate was issued with a lifetime of 10 years, renewed certificates may be issued to extend the validity period of the CA's key pair for an additional 20 years, reaching the maximum permitted validity period of 30 years. CA Certificate Renewal is not permitted after Certificate Expiration.
For VeriSign self-signed PCA Certificates, other KPN root CAs, and KPN CA Certificates, renewal requests are created and approved by authorized VeriSign personnel through a controlled process that requires the participation of multiple trusted individuals.

For non-KPN CA Certificates which chain to the VeriSign PCAs, KPN performs appropriate procedures to verify that the Managed PKI Customer, or ASB Customer is in fact the Subscriber of the CA Certificate. Authentication procedures are the same as original enrollment pursuant to CPS § 3.1.8.3.

3.3 Rekey After Revocation

Rekey after revocation is not be permitted if:

- Revocation occurred because the Certificate (other than a Class 1 Certificate) was issued to a person other than the one named as the Subject of the Certificate,
- The Certificate (other than a Class 1 Certificate) was issued without the authorization of the person 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.

Subject to the foregoing paragraph, Subscriber Certificates, which have been revoked, may be replaced (i.e., rekeyed) in accordance with Table 13 below.

Timing	*Requirement*
Prior to Certificate expiration	For replacement of an organizational or individual Certificate following revocation of the Certificate, KPN verifies that the person seeking certificate replacement is, in fact, the Subscriber (for individuals) or an authorized organizational representative (for organizations) through the use of a Challenge Phrase (or the equivalent thereof), as described in CPS § 3.2.1. Other than this procedure, the requirements for the validation of an original Certificate Application in CPS §§ 3.1.8.1, 3.1.9 are used for replacing a Certificate following revocation. Such Certificates contain the same Subject distinguished name as the Subject distinguished name of the Certificate being replaced. The authentication of a request to replace a Class 3 Organizational ASB Certificate requires the use of a Challenge Phrase as well as the authentication procedures for an original Certificate Application under CPS § 3.1.8.1.3.
After Certificate expiration	In this scenario, the requirements specified in CPS §§ 3.1.8.1, § 3.1.9 for the authentication of an original Certificate Application shall be used for replacing an end-user Subscriber Certificate. The authentication of a request to replace a Class 3 Organizational ASB Certificate requires the use of a Challenge Phrase as well as the authentication procedures for an original Certificate Application under CPS § 3.1.8.1.3.

Table 13 – Requirements for Certificate Replacement After Revocation

3.4 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, or the applicable ASB Customer (in the case of Certificates issued by an ASB Customer CA). Acceptable procedures for authenticating Subscriber revocation requests include:

- Having the Subscriber submit the Subscriber's Challenge Phrase (or the equivalent thereof) and revoking the Certificate automatically if it matches the Challenge Phrase on record,
- Receiving a message purporting to be from the Subscriber that requests revocation and contains a digital signature verifiable with reference to the Certificate to be revoked, and
- 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. Depending on the circumstances, such communication 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. In the case of ASB Customers' CA Administrators providing revocation instructions, however, the ASB Providers shall authenticate the identity of such CA Administrators by telephone.

Managed PKI Customers using the Automated Administration Software Module may submit bulk revocation requests to KPN. Such requests are authenticated via a request digitally signed with the private key in the Managed PKI Customer's Automated Administration hardware token.

The requests of Managed PKI Customers to revoke a CA Certificate are authenticated by KPN to ensure that the revocation has in fact been requested by the CA.

4 Operational Requirements

4.1 Certificate Application

4.1.1 Certificate Applications for End-User Subscriber Certificates

For KPN Certificates, all end-user Certificate Applicants shall manifest assent to the relevant Subscriber Agreement and undergo an enrollment process consisting of:

- Completing a Certificate Application and providing the required information,
- Generating, or arranging to have generated, a key pair in accordance with CPS § 6.1,
- Delivering his, her, or its public key, directly or through a Managed PKI Customer, to KPN, in accordance with CPS § 6.1.3,
- Demonstrating to KPN pursuant to CPS § 3.1.7 that the Certificate Applicant has possession of the private key corresponding to the public key delivered to KPN, and

Web Hosts may submit Certificate Applications on behalf of their customers pursuant to the Web Host Program (see CPS § 1.1.2.6).

Certificate Applications are submitted either to KPN, or Managed PKI Customer for processing, either approval or denial. The entity processing the Certificate Application and the entity issuing the Certificate pursuant to CPS § 4.2 may be two different entities as shown in the following table.

Certificate Class/Category	*Entity Processing Certificate Applications*	*Entity Issuing Certificate*
Class 1 individual Retail Certificate	KPN	VeriSign
Class 1 individual Managed PKI Certificate	Class 1 Managed PKI Customer	VeriSign
Class 2 individual Retail Certificate	KPN	VeriSign
Class 2 individual ASB Certificate	KPN, as ASB Provider	VeriSign
Class 2 individual Managed PKI Certificate	Class 2 Managed PKI Customer or Managed PKI Lite Customer	VeriSign
Class 3 individual Retail Certificate	KPN	VeriSign
Class 3 Administrator Certificate	KPN	VeriSign
Class 3 organizational Retail Certificates	KPN	VeriSign
Class 3 organizational Managed PKI Certificates (Managed PKI for SSL or Managed PKI for SSL Premium Edition)	Managed PKI for SSL Customer or Managed PKI for SSL Premium Edition Customer	VeriSign
Class 3 organizational ASB Certificate	KPN, as ASB Provider	VeriSign
CA, Infrastructure and KPN Employee Certificates	KPN	VeriSign

Table 14 – Entities Receiving Certificate Applications

4.1.2 Certificate Applications for CA, RA, Infrastructure and Employee Certificates

4.1.2.1 CA Certificates

The VeriSign PCAs issue certificates only to CAs subordinate to them, including VeriSign, Affiliate, and Managed PKI Customer. For KPN CAs, which are subscribers of CA Certificates, certificate requests are created and approved by authorized KPN personnel through a controlled process that requires the participation of multiple trusted individuals.

Managed PKI Customers, which are subscribers of CA Certificates, are not required to complete formal Certificate Applications. Instead, they enter into a contract with KPN. CA Certificate Applicants are required to provide their credentials as required by CPS § 3.1.8.2 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 Managed PKI Customer's, or ASB Customer's CA key pair, the applicant shall cooperate with KPN to determine the appropriate distinguished name and the content of the Certificates to be issued to the applicant. For these CAs, certificate requests are created and approved by authorized KPN personnel through a controlled process that requires the participation of multiple trusted individuals.

4.1.2.2 RA Certificates

KPN operates several Administrative CAs, which issue certificates to RAs and RA systems including:

- KPN personnel (KPN RA Administrators) who process Certificate Applications on behalf of KPN CAs,
- Managed PKI Customer personnel (Managed PKI Administrators) who process Certificate Applications on behalf of the Managed PKI Customer within their organization and servers within their Subdomain, and
- Automated Administration servers, which process Certificate Applications for Managed PKI Customers where an Automated Administration authentication process has been established.

For all of these RAs, as subscribers to the relevant Administrative CA, the requirements for Class 3 Administrator Certificates specified in CPS § 4.1.1 apply.

4.1.2.3 Infrastructure Certificates

KPN also operates several Infrastructure CAs which issue Certificates to KPN infrastructure components (e.g., OCSP Responders providing Certificate status information and Roaming Servers, which support the KPN Roaming Service).

4.1.2.4 Not provided

4.2 Certificate Issuance

4.2.1 Issuance of End-User Subscriber Certificates

After a Certificate Applicant submits a Certificate Application, KPN, a Managed PKI Administrator (see CPS § 4.1.1) attempts to confirm the information in the Certificate Application (other than Non-Verified Subscriber Information) pursuant to CPS §§ 3.1.8.1, 3.1.9. Upon successful performance of all required authentication procedures pursuant to CPS § 3.1, KPN, a Managed PKI Administrator approves the Certificate Application. If authentication is unsuccessful, KPN, a Managed PKI Administrator denies the Certificate Application.
A Certificate is created and issued following the approval of a Certificate Application or following receipt of a RA's request to issue the Certificate. KPN creates and issues to a Certificate Applicant a Certificate based on the information in a Certificate Application following approval of such Certificate Application. When a Managed PKI Customer approves a Certificate Application and communicates the approval to KPN, KPN creates a Certificate and issues it to the Certificate Applicant. The procedures of this section are also used for the issuance of Certificates in connection with the submission of a request to replace (i.e., renew or rekey) a Certificate.

4.2.2 Issuance of CA, RA and Infrastructure Certificates

KPN authenticates the identity of entities wishing to become Customers in accordance with CPS § 3.1.8.2 and, upon approval, issues the Certificates needed to perform their CA or RA functions. Before KPN enters into a contract with Customer applicant under CPS § 4.1.2, the identity of the potential Customer is confirmed based on the credentials presented. The execution of such a contract indicates the complete and final approval of the application by KPN. The decision to approve or reject Customer application is solely at the discretion of KPN. Following such approval, KPN issues the Certificate to the Customer CA or RA in accordance with CPS § 6.1.

For KPN infrastructure components (e.g., OCSP Responders), Certificate requests are created and approved by authorized KPN personnel through a controlled process that requires the participation of multiple Trusted Persons.

4.3 Certificate Acceptance

Upon Certificate generation, KPN notifies Subscribers that their Certificates are available and notifies them of the means for obtaining such Certificates. For Managed PKI Customers, Subscribers are notified through the Managed PKI Administrator.

Upon issuance, Certificates are 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. For example, KPN may send the Subscriber a PIN, which the Subscriber enters into an enrollment web page to obtain the Certificate. The Certificate may also be sent to the Subscriber in an e-mail message. Downloading a Certificate, or installing a Certificate from a message attaching it constitutes the Subscriber's acceptance of the Certificate.

4.4 Certificate Suspension and Revocation

4.4.1 Circumstances for Revocation

4.4.1.1 Circumstances for Revoking End-User Subscriber Certificates

An end-user Subscriber Certificate is revoked if:

- 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 Managed PKI Customer, or an ASB Customer issuing Class 3 Organizational ASB Certificates, and a Subscriber is terminated or has otherwise ended,
- The affiliation between an organization that is a Subscriber of a Class 3 Organizational ASB Certificate and the organizational representative controlling the Subscriber's private key 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 (other than a Class 1 Certificate) was issued to a person other than the one named as the Subject of the Certificate, or the Certificate (other than a Class 1 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,
- In the case of Class 3 organizational Certificates, the Subscriber's organization name changes,
- The information within the Certificate, other than Nonverified Subscriber Information, is incorrect or has changed,

The Subscriber requests revocation of the Certificate in accordance with CPS § 3.4,
The continued use of that Certificate is harmful to the VTN.

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 in accordance with the procedures in CPS § 4.4.3.1.

4.4.1.2 Circumstances for Revoking CA, RA, or Infrastructure Certificates

KPN will revoke CA, RA, or infrastructure Certificates if:

- KPN discovers or has reason to believe that there has been a compromise of the CA, RA, or infrastructure private key,
- The agreement between the CA or RA with KPN has been terminated,

- KPN discovers or has reason to believe that the Certificate was issued in a manner not materially in accordance with the procedures required by this CPS, the Certificate was issued to an entity other than the one named as the Subject of the Certificate, or the Certificate was issued without the authorization of the entity named as the Subject of such Certificate,
- KPN determines that a material prerequisite to Certificate issuance was neither satisfied nor waived,
- The CA or RA requests revocation of the Certificate,
- The continued use of that Certificate is harmful to the VTN.

KPN requires that Managed PKI Customers, and ASB Customers notify KPN when revocation is required in accordance with the procedures in CPS § 4.4.3.1.

4.4.2 Who Can Request Revocation

4.4.2.1 Who Can Request Revocation of an End-User Subscriber Certificate

The following entities may request revocation of an end-user Subscriber Certificate:

- KPN or the Customer that approved the Subscriber's Certificate Application may request the revocation of any end-user Subscriber or Administrator Certificates in accordance with CPS § 4.4.1.1.
- Individual Subscribers may request revocation of their own individual Certificates.
- In the case of organizational Certificates, only a duly authorized representative of the organization is entitled to request the revocation of Certificates issued to the organization.
- An ASB Customer is entitled to initiate the revocation of Certificates issued by its CA.
- A duly authorized representative of KPN or a Managed PKI Customer whose Administrator received an Administrator Certificate is entitled to request the revocation of an Administrator's Certificate.

4.4.2.2 Who Can Request Revocation of a CA, RA, or Infrastructure Certificate

The following entities may request revocation of a CA, RA, or infrastructure Certificate:

- Only KPN is entitled to request or initiate the revocation of the Certificates issued to its own CAs, RAs, or infrastructure components.
- VeriSign and where subordinate to KPN, KPN may initiate the revocation of any Processing Center, Service Center, Managed PKI Customer, or ASB Customer CA, RA, or infrastructure Certificate in accordance with CPS § 4.4.1.2.
- Processing Centers, Service Centers, Managed PKI Customers, and ASB Customers are entitled, through their duly authorized representatives, to request the revocation of their own CA, RA, and infrastructure Certificates.

4.4.3 Procedure for Revocation Request

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

An end-user Subscriber requesting revocation is required to communicate the request to the KPN or the Customer approving the Subscriber's Certificate Application, who in turn will initiate

revocation of the certificate promptly. For Managed PKI customers, the Subscriber is required to communicate the request to the Managed PKI 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 Managed PKI Customer or ASB Customer initiates revocation of an end-user Subscriber Certificate upon its own initiative, the Managed PKI Customer or ASB Customer instructs KPN to revoke the Certificate.

4.4.3.2 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.

4.4.4 Revocation Request Grace Period

Revocation requests must be submitted as promptly as possible within a commercially reasonable period of time.

4.4.5 Circumstances for Suspension

KPN does not offer suspension services for CA or end-user Subscriber Certificates.

4.4.6 Who Can Request Suspension

Not applicable.

4.4.7 Procedure for Suspension Request

Not applicable.

4.4.8 Limits on Suspension Period

Not applicable.

4.4.9 CRL Issuance Frequency

KPN publishes CRLs showing the revocation of KPN Certificates and offers status checking services. CRLs for CAs that issue end-user Subscriber Certificates are published daily. CRLs for CAs that only issue CA Certificates are published quarterly and also whenever a CA Certificate is revoked. Expired Certificates may be removed from the CRL after the Certificate's expiration.

4.4.10 Certificate Revocation List Checking Requirements

Relying Parties must check the status of Certificates on which they wish to rely. One method by which Relying Parties may check Certificate status is by consulting the most recent CRL published by the CA that issued the Certificate on which the Relying Party wishes to rely.

- For VeriSign PCAs and Class 1-3 Certification Authorities, CRLs are posted in the VeriSign repository at http://crl.verisign.com.
- For Managed PKI Lite Customer CAs, CRLs are posted at https://onsite.verisign.com/<customernaming>/latest.crl

- For Managed PKI Customer CAs, CRLs are posted in customer-specific repositories, the location of which is communicated to the Managed PKI customer.

A "CRL reference Table" is also posted in the Repository to enable Relying Parties to determine the location of the CRL for the relevant CA.

4.4.11 On-Line Revocation/Status Checking Availability

In addition to publishing CRLs, KPN provides Certificate status information for Server Certificates through query functions in the KPN website at https://certificaat.kpn.com/index_ssi.html.

KPN also provides OCSP Certificate status information. Managed PKI Customers who contract for OCSP services may check Certificate status through the use of OCSP. The URL for the relevant OCSP Responder is communicated to the Managed PKI Customer.

4.4.12 On-Line Revocation Checking Requirements

If a Relying Party does not check the status of a Certificate on which the Relying Party wishes to rely by consulting the most recent relevant CRL, the Relying Party must check Certificate status using one of the applicable methods specified in CPS § 4.4.11.

4.4.13 Other Forms of Revocation Advertisements Available

No stipulation.

4.4.14 Checking Requirements for Other Forms of Revocation Advertisements

No stipulation.

4.4.15 Special Requirements Regarding Key Compromise

In addition to the procedures described in CPS §§ 4.4.9 – 4.4.14, KPN uses commercially reasonable efforts to notify potential Relying Parties if KPN discovers, or has reason to believe, that there has been a Compromise of the private key of a KPN CA.

4.5 Security Audit Procedures

4.5.1 Types of Events Recorded

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, rekey, and revocation
  - Successful or unsuccessful processing of requests
  - Generation and issuance of Certificates and CRLs.
- Security-related events including:
  - Successful and unsuccessful PKI system access attempts
  - PKI and security system actions performed by 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.

KPN RAs and Managed PKI Administrators log Certificate Application information including:

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

4.5.2 Frequency of Processing Log

Audit logs are examined on at least a weekly 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, an inspection of all log entries, and an investigation of any alerts or irregularities in the logs. Actions taken based on audit log reviews are also be documented.

4.5.3 Retention Period for Audit Log

Audit logs are retained onsite at least two (2) months after processing and thereafter archived in accordance with CPS § 4.6.2.

4.5.4 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.

4.5.5 Audit Log Backup Procedures

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

4.5.6 Audit Collection System

Automated audit data is generated and recorded at the application, network and operating system level. Manually generated audit data is recorded by KPN personnel.

4.5.7 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.

4.5.8 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 in accordance with the requirements of the Security and Audit Requirements Guide. An annual LSVA serves as an input into the annual Compliance Audit.

4.6 Records Archival

4.6.1 Types of Events Recorded

In addition to the audit logs specified in CPS § 4.5, KPN maintains records that include documentation of:

- KPN's compliance with the CPS and other obligations under its agreements with their Subscribers, and
- actions and information that are material to each Certificate Application and to the creation, issuance, use, revocation, expiration, and rekey or renewal of all Certificates it issues from the KPN Service Center.

KPN's records of Certificate life cycle events include:

- the identity of the Subscriber named in each Certificate (except for Class 1 Certificates, for which only a record of the Subscriber's unambiguous name is maintained),
- the identity of persons requesting Certificate revocation (except for Class 1 Certificates, for which only a record of the Subscriber's unambiguous name is maintained),
- other facts represented in the Certificate,
- time stamps, and
- certain foreseeable material facts related to issuing Certificates including, but not limited to, information relevant to successful completion of a Compliance Audit under CPS § 2.7.

Records may be maintained electronically or in hard copy, provided that such records are accurately and completely indexed, stored, preserved, and reproduced.

4.6.2 Retention Period for Archive

Records associated with a Certificate are retained for at least the time periods set forth below following the date the Certificate expires or is revoked:

- Five (5) years for Class 1 Certificates,
- Ten (10) years for Class 2 Certificates, and
- Thirty (30) years for Class 3 Certificates.

If necessary, KPN may implement longer retention periods in order to comply with applicable laws.

4.6.3 Protection of Archive

KPN protects its archived records compiled under CPS § 4.6.1 so that only authorized Trusted Persons are permitted to access archived data. Electronically archived data is protected against unauthorized viewing, modification, deletion, or other tampering through the implementation of appropriate physical and logical access controls. The media holding the archive data and the applications required to process the archive data are maintained to ensure that the archived data can be accessed for the time period set forth in CPS § 4.6.2.

4.6.4 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. Copies of paper-based records compiled under CPS § 4.6.1 are maintained in an off-site disaster recovery facility in accordance with CPS § 4.8.

4.6.5 Requirements for Time-Stamping of Records

Certificates, CRLs, and other revocation database entries contain time and date information. It should be noted that, in contrast with the KPN's Digital Notarization Service[28], such time information is not cryptographic-based (*see* CPS § 1.1.2.2.2).

4.6.6 Procedures to Obtain and Verify Archive Information

See CPS § 4.6.3.

4.7 Key Changeover

KPN CA key pairs are retired from service at the end of their respective maximum lifetimes as defined in CPS § 6.3.2. 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 in accordance with CPS § 6.1.

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") where the remaining lifetime of the Superior CA key pair equals the approved Certificate Validity Period for the specific type(s) of Certificates issued by Subordinate CAs in the Superior CA's hierarchy.
- Upon successful validation of Subordinate CA (or end-user Subscriber) Certificate requests received after the "Stop Issuance Date," Certificates will be signed with a new CA key pair.
- The Superior CA continues to issue CRLs signed with the original Superior CA private key until the expiration date of the last Certificate issued using the original key pair has been reached.

[28] KPN currently is not offering a Digital Notarization Service.

4.8 Disaster Recovery and Key Compromise

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 § 4.8.2 and Key Compromise response procedures described in CPS § 4.8.3. 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.

4.8.1 Corruption of Computing Resources, Software, and/or Data

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.

4.8.2 Disaster Recovery

4.8.2.1 VeriSign

For services where the entity issuing Certificates is VeriSign (see CPS §1.1.2.1.2), VeriSign has implemented a disaster recovery site more than 1000 miles from VeriSign's principal secure facilities. VeriSign has developed, implemented and tested a disaster recovery plan to mitigate the effects of any kind of natural or man-made disaster. This plan is regularly tested, verified, and updated to be operational in the event of a disaster.

Detailed disaster recovery plans are in place to address the restoration of information systems services and key business functions. VeriSign's disaster recovery site has implemented the physical security protections and operational controls required by the Security and Audit Requirements Guide to provide for a secure and sound backup operational setup.

In the event of a natural or man-made disaster requiring temporary or permanent cessation of operations from VeriSign's primary facility, VeriSign's disaster recovery process is initiated by the VeriSign Emergency Response Team (VERT).

VeriSign has the capability to restore or recover operations within twenty four (24) hours following a disaster with, at a minimum, support for the following functions:

- Certificate issuance,
- Certificate revocation,
- publication of revocation information, and
- provision of key recovery information for Managed PKI Customers using Managed PKI Key Manager.

VeriSign's disaster recovery database is synchronized regularly with the production database within the time limits set forth in the Security and Audit Requirements Guide. VeriSign's disaster recovery equipment is protected by physical security protections comparable to the physical security tiers specified in the VeriSign Certificate Practices Statement § 5.1.1.

VeriSign's disaster recovery plan has been designed to provide full recovery within one week following disaster occurring at VeriSign's primary site. VeriSign tests its equipment at its primary site to support CA/RA functions following all but a major disaster that would render the entire facility inoperable. Results of such tests are reviewed and kept for audit and planning purposes. Where possible, operations are resumed at VeriSign's primary site as soon as possible following a major disaster.

VeriSign maintains redundant hardware and backups of its CA and infrastructure system software at its disaster recovery facility. In addition, CA private keys are backed up and maintained for disaster recovery purposes in accordance with the VeriSign Certificate Practices Statement § 6.2.4.

VeriSign maintains offsite backups of important CA information for VeriSign CAs as well as the CAs of Service Centers, Managed PKI Customers, and ASB Customers within VeriSign's Subdomain. Such information includes, but is not limited to: Certificate Application data, audit data (per CPS § 4.5), and database records for all Certificates issued.

4.8.2.2 KPN

For services which KPN provides as a Service Center and where KPN is the entity issuing Certificates, (see CPS §1.1.2.1.2) KPN has implemented a disaster recovery site. KPN has developed, implemented and tested a disaster recovery plan to mitigate the effects of any kind of natural or man-made disaster. This plan is regularly tested, verified, and updated to be operational in the event of a disaster.

Detailed disaster recovery plans are in place to address the restoration of information systems services. KPN's disaster recovery site has implemented the physical security protections and operational controls required by the VeriSign Security and Audit Requirements Guide to provide for a secure and sound backup operational setup.

In the event of a natural or man-made disaster requiring temporary or permanent cessation of operations from KPN's primary facility, KPN's disaster recovery process is initiated by the KPN Security Incident Response Team (SIRT).

KPN has the capability to restore or recover operations within twenty four (24) hours following a disaster with, at a minimum, support for the following functions:

- Certificate Issuance;
- Certificate Revocation;
- Publication of Revocation Information;
- Provision of key recovery information for Managed PKI Customers using Managed PKI Key Manager.

KPN's disaster recovery equipment is protected by physical security protections comparable to the physical security tiers specified in CPS § 5.1.1.

KPN's disaster recovery plan has been designed to provide full recovery within one week following disaster occurring at KPN's primary site. KPN tests its equipment to support CA/RA

functions following all but a major disaster that would render the entire facility inoperable. Results of such tests are reviewed and kept for audit and planning purposes. Where possible, operations are resumed at KPN's primary site as soon as possible following a major disaster.

KPN maintains redundant hardware and backups and infrastructure system software at its disaster recovery facility. In addition, CA private keys are backed up and maintained for disaster recovery purposes by the VeriSign Processing Center..

KPN maintains offsite backups of important MPKI CA information for KPN CAs as well as the CAs of Service Centers, Managed PKI Customers, and ASB Customers within KPN's Subdomain. Such information includes, but is not limited to: application logs, Certificate Application data, audit data (per CPS § 4.5), and database records for all Certificates issued.

4.8.3 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 KPN Security Incident Response Team (SIRT). This team, which includes KPN Security, Production Services personnel, and other 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 in accordance with CPS § 4.4.9,
- Commercially reasonable efforts will be made to provide additional notice of the revocation to all affected VTN Participants, and
- The CA will generate a new key pair in accordance with CPS § 4.7, except where the CA is being terminated in accordance with CPS § 4.9.

4.9 CA Termination

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

- Provision of notice to parties affected by the termination, such as Subscribers, Relying Parties, and Customers, informing them of the status of the CA,
- Handling the cost of such notice,
- The revocation of the Certificate issued to the CA by KPN,
- The preservation of the CA's archives and records for the time periods required in CPS § 4.6,
- The continuation of Subscriber and customer support services,
- The continuation of revocation services, such as the issuance of CRLs or the maintenance of online status checking services,

- The revocation of unexpired unrevoked Certificates of end-user Subscribers and subordinate CAs, if necessary,
- 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 CA's private key and the hardware tokens containing such private key, and
- Provisions needed for the transition of the CA's services to a successor CA.

5 Physical, Procedural, and Personnel Security Controls

KPN has implemented the KPN Physical Security Policy, which supports the security requirements of this CPS.

5.1 Physical Controls

5.1.1 Site Location and Construction

KPN's Service Center operations are conducted within KPN's facilities in Den Haag, the Netherlands, which meet the requirements of VeriSign's Security and Audit Requirements. All KPN Service Center operations are conducted within a physically protected environment designed to deter, prevent, and detect covert or overt penetration.

5.1.2 Physical Access

KPN Service Center systems are protected by a minimum of four tiers of physical security, with access to the lower tier required before gaining access to the higher tier.

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

The physical security system includes additional tiers for key management security which serves to protect both online and offline storage of CSUs and keying material. Areas used to create and store cryptographic material enforce dual control, each through the use of two factor authentication including biometrics. Online CSUs are protected through the use of locked cabinets. Offline CSUs are protected through the use of locked safes, cabinets and containers. Access to CSUs and keying material is restricted in accordance with VeriSign'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

Affiliate has take reasonable precautions to minimize the impact of water exposure to KPN systems.

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 is stored within KPN facilities or in a secure off-site storage facility with appropriate physical and logical access controls designed to limit access to authorized personnel and protect such media from accidental damage (e.g., water, fire, and electromagnetic).

5.1.7 Waste Disposal

Sensitive documents and materials are shredded before disposal. Media used to collect or transmit sensitive information are rendered unreadable before disposal. Cryptographic devices are physically destroyed or zeroized in accordance with 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.

5.2 Procedural Controls

5.2.1 Trusted Roles

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

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

Trusted Persons include, but are not limited to:

- Customer service personnel,
- Cryptographic business operations personnel,
- Security personnel,
- System administration personnel,
- Designated engineering personnel, and
- Executives that are designated to manage infrastructural trustworthiness.

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 of CPS § 5.3.

5.2.2 Number of Persons Required Per Task

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

These internal control procedures are designed to ensure that at a minimum, two trusted personnel are required to have either physical or logical access to the device. Access to CA cryptographic hardware is strictly enforced by multiple Trusted Persons throughout its lifecycle, from incoming receipt and inspection to final logical and/or physical destruction.

Once a module is activated with operational keys, further access controls are invoked to maintain split control over both physical and logical access to the device. Persons with physical access to modules do not hold “Secret Shares” and vice versa. Requirements for CA private key activation data and Secret Shares are specified in CPS § 6.2.7.

Other manual operations such as the manual validation and issuance of Class 3 Certificates require the participation of at least 2 Trusted Persons, or a combination of at least one trusted person and an automated validation and issuance process.

5.2.3 Identification and Authentication for Each Role

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

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

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

5.3 Personnel Controls

5.3.1 Background, Qualifications, Experience, and Clearance Requirements

Personnel seeking to become Trusted Persons must present proof of the requisite background, qualifications, and experience needed to perform their prospective job responsibilities competently and satisfactorily, as well as proof of any government clearances, if any, necessary to perform certification services under government contracts. Background checks are repeated at least every 5 years for personnel holding Trusted Positions.

5.3.2 Background Check Procedures

Prior to commencement of employment in a Trusted Role, KPN conducts background checks which include (but are not limited to) the following:

- Confirmation of previous employment,
- Check of professional reference,
- Confirmation of the highest or most relevant educational degree obtained,
- Search of criminal records (local, state or provincial, and national) by means of a 'Verklaring van goed gedrag' issued by the major of the Secretary of Justice of the Dutch Government,
- Search of Social Security Administration records.

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

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

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

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

5.3.3 Training Requirements

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

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

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

5.3.4 Retraining Frequency and Requirements

KPN provides refresher training and updates to its personnel to the extent and frequency required to ensure that such personnel maintain the required level of proficiency to perform their job responsibilities competently and satisfactorily. Periodic security awareness training is provided on an ongoing basis.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

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

5.3.7 Contracting Personnel Requirements

In limited circumstances, independent contractors or consultants may be used to fill Trusted Positions. Any such contractor or consultant is held to the same functional and security criteria that apply to a KPN employees in a comparable position.
Independent contractors and consultants who have not completed 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.

5.3.8 Documentation Supplied to Personnel

KPN personnel involved in the operation of KPN's PKI services are required to read this CPS, the VTN CP, and the KPN Security Policy. KPN provides its employees the requisite training and other documentation needed to perform their job responsibilities competently and satisfactorily.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

CA key pair generation is performed by multiple pre-selected, trained and trusted individuals using Trustworthy Systems and processes that provide for the security and required cryptographic strength for the generated keys. For PCA and Issuing Root CAs, the cryptographic modules used for key generation meet the requirements of FIPS 140-1 level 3. For other CAs (including KPN CAs and Managed PKI Customer 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 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.

Managed PKI 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 certified cryptographic module.

Generation of end-user Subscriber key pairs is generally performed by the Subscriber. For Class 1 Certificates, Class 2 Certificates, and Class 3 code/object signing Certificates, the Subscriber typically uses a FIPS 140-1 level 1 certified cryptographic module provided with their browser software for key generation. For server Certificates, the Subscriber typically uses the key generation utility provided with the web server software.

6.1.2 Private Key Delivery to Entity

End-user Subscriber key pairs are typically generated by the end-user Subscriber; therefore in such cases, 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 smart cards, such devices are distributed to the RA or end-user Subscriber using a commercial delivery service and tamper evident packaging. The required activation data required to activate the device is communicated to the RA or end-user Subscriber using an out of band process. The distribution of such devices is logged by KPN.

Where end-user Subscriber key pairs are pre-generated by Managed PKI Customers on hardware tokens or smart cards, such devices are distributed to the end-user Subscriber using a commercial

delivery service and tamper evident packaging. The required activation data required to activate the device is communicated to the RA or end-user Subscriber using an out of band process. The distribution of such devices is logged by the Managed PKI Customer.

For Managed PKI 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 Users

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, 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. .

6.1.5 Key Sizes

KPN CA key pairs are at least 1024 bit RSA, except for the legacy RSA Secure Server CA whose key pair is 1000 bit RSA. VeriSign's third generation (G3) PCAs have 2048 bit RSA key pairs. KPN recommends that Registration Authorities and end-user Subscribers generate 1024 bit RSA key pairs, but currently permits the use of 512 bit RSA key pairs to support certain legacy applications and web servers.

6.1.6 Public Key Parameters Generation

Not applicable.

6.1.7 Parameter Quality Checking

Not applicable.

6.1.8 Hardware/Software Key Generation

KPN generates its CA pairs keys in appropriate hardware cryptographic modules in accordance with CPS § 6.2.1. RA and end-user Subscriber key pairs may be generated in hardware or software.

6.1.9 Key Usage Purposes

For X.509 Version 3 Certificates, KPN generally populates the KeyUsage extension of Certificates in accordance with RFC 3280[29]: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, April 2002. The KeyUsage extension in VeriSign X.509 Version 3 Certificates is populated in accordance with Table 15 below with the following exceptions:

- The KeyUsage extension is not used for Global Server IDs, Class 1 individual Certificates and Class 2 individual Certificates.
- The criticality of the KeyUsage extension is set to TRUE for the KPN Class 3 Managed PKI Authentication Services Bureau CA.
- Setting the nonrepudiation bit for dual key pair signature Certificates through Managed PKI Key Manager is permissible.
- The criticality of the KeyUsage extension may be set to TRUE for other Certificates in the future.

		CAs	Class 3 Server End-User Subscribers; Automated Administration tokens	Dual Key Pair Signature (Managed PKI Key Manager)	Dual Key Pair Encipherment (Managed PKI Key Manager)	Code/Object Signing End-User Subscribers	Class 1 and 2 End-User Subscribers
Criticality		*FALSE*	*FALSE*	*FALSE*	*FALSE*	*FALSE*	*FALSE*
0	digitalSignature	Clear	Set	Set	Clear	Set	Set
1	nonRepudiation	Clear	Clear	Clear	Clear	Clear	Clear
2	keyEncipherment	Clear	Set	Clear	Set	Clear	Set
3	dataEncipherment	Clear	Clear	Clear	Clear	Clear	Clear
4	keyAgreement	Clear	Clear	Clear	Clear	Clear	Clear
5	keyCertSign	Set	Clear	Clear	Clear	Clear	Clear
6	CRLSign	Set	Clear	Clear	Clear	Clear	Clear
7	encipherOnly	Clear	Clear	Clear	Clear	Clear	Clear
8	decipherOnly	Clear	Clear	Clear	Clear	Clear	Clear

Table 15 – Settings for KeyUsage Extension

Certain CA and end-user Subscriber Certificates are X.509 Version 1 Certificates (see CPS § 7.1.1) and thus do not support the use of the KeyUsage extension. In addition, KPN did not use the KeyUsage extension for WTLS Certificates.

6.2 Private Key Protection

KPN has implemented a combination of physical, logical, and procedural controls to ensure the security of KPN, Managed PKI Customer, and ASB Customer CA private keys. Logical and

[29] RFC 3280 replaced RFC 2459.

procedural controls are described in CPS § 6.2. Physical access controls are described in CPS § 5.1.2. Subscribers are required by contract to take necessary precautions to prevent the loss, disclosure, modification, or unauthorized use of private keys.

6.2.1 Standards for Cryptographic Modules

For PCA and Issuing Root CA key pair generation and CA private key storage, VeriSign and KPN use hardware cryptographic modules that are certified at or materially meet the requirements of FIPS 140-1 Level 3. For other CAs, KPN uses hardware cryptographic modules that are certified to at least FIPS 140-1 Level 2.

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 CPS § 6.4.2.

6.2.3 Private Key Escrow

KPN does not escrow CA, RA or end-user Subscriber private keys with any third party for purposes of access by law enforcement. CA private signature keys shall not be escrowed by a third party.

Managed PKI Customers using Managed PKI Key Management 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 as described in CPS §1.1.2.3.2.

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 CPS § 6.2.1. CA private keys are copied to backup hardware cryptographic modules in accordance with CPS § 6.2.6.

Modules containing onsite backup copies of CA private keys are subject to the requirements of CPS §§ 5.1, 6.2.1. Modules containing disaster recovery copies of CA private keys are subject to the requirements of CPS § 4.8.2.

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

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 CPS § 6.2.1. 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 CPS § 6.2.9.

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

6.2.6 Private Key Entry into 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 Method of Activating Private Key

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

6.2.7.1 End-User Subscriber Private Keys

This section applies the VTN Standards for protecting activation data for end-user Subscribers' private keys to KPN's Subdomain. In addition, Subscribers have the option of using enhanced private key protection mechanisms available today including the use of smart cards, biometric access devices, and other hardware tokens to store private keys. The use of two factor authentication mechanisms (e.g., token and passphrase, biometric and token, or biometric and passphrase) is encouraged.

6.2.7.1.1 Class 1 Certificates

The VTN Standard for Class 1[30] private key protection is for Subscribers to take commercially reasonable measures for the physical protection of the Subscriber's workstation to prevent use of the workstation and its associated private key without the Subscriber's authorization. In addition, KPN recommends that Subscribers use a password in accordance with CPS § 6.4.1 or security of equivalent strength to authenticate the Subscriber before the activation of the private key, which includes, for instance, a password to operate the private key, a Windows logon or screen saver password, or a network logon password.

6.2.7.1.2 Class 2 Certificates

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

- Use a password in accordance with CPS § 6.4.1 or security of equivalent strength to authenticate the Subscriber before the activation of the private key, which includes, for

[30] KPN currently is not offering Class 1 Certificates.

instance, a password to operate the private key, a Windows logon or screen saver password, a network logon password, or a password in conjunction with the KPN Roaming Service; 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.

6.2.7.1.3 Class 3 Certificates Other Than Administrator Certificates

The VTN Standard for Class 3 private key protection (other than Administrators) is for Subscribers to:

- Use a smart card, other cryptographic hardware device, biometric access device, password (in conjunction with the KPN Roaming Service), or security of equivalent strength to authenticate the Subscriber before the activation of the private key; and
- Take commercially reasonable measures for the physical protection of the Subscriber's workstation to prevent use of the workstation or server and its associated private key without the Subscriber's authorization.

Use of a password along with a smart card, other cryptographic hardware device, or biometric access device in accordance with CPS § 6.4.1 is recommended. When deactivated, private keys shall be kept in encrypted form only.

6.2.7.2 Administrators' Private Keys

6.2.7.2.1 Administrators

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

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

Use of a password along with a smart card, biometric access device, in accordance with CPS § 6.4.1 is recommended to authenticate the Administrator before the activation of the private key.

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

6.2.7.2.2 Managed PKI Administrators using a Cryptographic Module (with Automated Administration or with Managed PKI Key Manager Service)

The VTN 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 CPS § 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.

6.2.7.3 Private Keys Held by KPN

KPN CA private keys are activated by a threshold number of Shareholders supplying their activation data (stored on secure media) in accordance with CPS § 6.2.2. For KPN's offline CAs, the CA private key is activated for one session (e.g., for the certification of a Subordinate CA or an instance where a PCA signs a CRL) after which it is deactivated and the module is returned to secure storage. For KPN's online CAs, the CA private key is activated for an indefinite period and the module remains online in the production data center until the CA is taken offline (e.g., for system maintenance). KPN Shareholders are required to safeguard their Secret Shares and sign an agreement acknowledging their Shareholder responsibilities.

6.2.8 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 smart card from the smart card reader depending upon the authentication mechanism employed by the user. In all cases, end-user Subscribers have an obligation to adequately protect their private key(s) in accordance with CPS §§ 2.1.3, 6.4.1.

6.2.9 Method of Destroying Private Key

At the conclusion of a KPN's CA's operational lifetime, one or more copies of the CA private key are archived in accordance with CPS § 6.2.5. Remaining copies of the CA private key are securely destroyed. In addition, archived CA private keys are securely destroyed at the conclusion of their archive periods. CA key destruction activities require the participation of multiple trusted individuals.

Where required, KPN destroys CA private keys in a manner that reasonably ensures that there are no residuals remains of the key that could lead to the reconstruction of the key. KPN utilizes the zeroization function of its hardware cryptographic modules and other appropriate means to ensure the complete destruction of CA private keys. When performed, CA key destruction activities are logged.

6.3 Other Aspects of Key Pair Management

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 Usage Periods for the Public and Private Keys

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 private keys may continue to be used for decryption and public keys may continue to be used for 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 16 below.

In addition, KPN 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:	*Class 1*	*Class 2*	*Class 3*
PCA self-signed (1024 bit)	Up to 30 years	Up to 30 years	Up to 30 years
PCA self-signed (2048 bit)	Up to 50 years	Up to 50 years	Up to 50 years
Self-signed Issuing Root CAs	N/A	N/A	Up to 10 years
PCA to CA	Up to 10 years	Up to 10 years	Up to 10 years
CA to Subordinate CA	Up to 5 years	Up to 5 years	Up to 5 years
CA to end-user Subscriber	Up to 2 years	Normally up to 2 years, but up to 5 years under the conditions described below	Normally up to 2 years, but up to 5 years under the conditions described below
CA to end-user organizational automated administration certificate	N/A	N/A	Up to 5 years

Table 16 – Certificate Operational Periods

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 smart card,
- Subscribers are annually required to undergo reauthentication procedures under CPS § 3.1.9,

- Subscribers shall annually prove possession of the private key corresponding to the public key within the Certificate,
- If a Subscriber is unable to complete reauthentication procedures under CPS § 3.1.9 successfully or is unable to prove possession of such private key when required by the foregoing, the CA shall automatically revoke the Subscriber's Certificate.

VeriSign also operates the RSA Secure Server CA as a legacy self-signed issuing root CA which is part of the VeriSign 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 16 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 Managed PKI 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.

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.

6.4.3 Other Aspects of Activation Data

See CPS § 6.4.1 and 6.4.2.

6.5 Computer Security Controls

KPN performs all CA and RA functions using Trustworthy Systems that meet the requirements of VeriSign's Security and Audit Requirements Guide. Managed PKI 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 use 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 require 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 operations group having a valid business reason for such access.

6.5.2 Computer Security Rating

VeriSign'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 VeriSign Processing Center Security Target. VeriSign may, from time to time, evaluate new releases of the Processing Center software under the Common Criteria.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

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

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

6.6.2 Security Management Controls

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

6.6.3 Life Cycle Security Ratings

No stipulation.

6.7 Network Security Controls

KPN performs all its CA and RA functions using networks secured in accordance with the VeriSign 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 Cryptographic Module Engineering Controls

Cryptographic modules used by KPN and VeriSign meet the requirements specified in CPS § 6.2.1.

7 Certificate and CRL Profile

7.1 Certificate Profile

CPS § 7.1 defines KPN's Certificate Profile and Certificate content requirements for VTN Certificates issued under this CPS.

Except for WTLS Certificates[31], 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 3280[32]: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, April 2002 ("RFC 3280").
Not all certificate services allow the use of UTF8String encoding of DirectoryString.

WTLS Certificates conform to the Wireless Application Protocol: WAP Certificate and CRL Profiles Specification, Proposed Version dated March 9, 2000. KPN will conform to the finalized version of the specification when approved by the WAP Forum within one year of its publication[33].

At a minimum, KPN X.509 and WTLS Certificates contain the basic X.509 Version 1 fields and indicated prescribed values or value constraints in Table 17 below:

Field	*Value or Value constraint*
Version	See CPS §7.1.1. Not applicable for WTLS Certificates.
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 U.S. Naval Observatory. Encoded in accordance with RFC 3280.
Valid To	Universal Coordinate Time base. Synchronized to Master Clock of U.S. Naval Observatory. Encoded in accordance with RFC 3280. The validity period will be set in accordance with the constraints specified in CPS § 6.3.2.
Subject DN	See CPS § 7.1.4
Subject Public Key	Encoded in accordance with RFC 3280 using algorithms specified in CPS § 7.1.3 and key lengths specified in CPS § 6.1.5.
Signature	Generated and encoded in accordance with RFC 3280.

Table 17 – Certificate Profile Basic Fields

7.1.1 Version Number(s)

KPN CA and end-user Subscriber Certificates are X.509 Version 3 Certificates with the following exceptions:

[31] WTLS certificates are no longer available through KPN.
[32] RFC 3280 replaced RFC 2459.
[33] WAP and WTLS certificates are no longer available through KPN.

- VeriSign root CA certificates, including the VeriSign PCAs and other VeriSign root CAs, are X.509 Version 1 Certificates.
- Certain legacy VeriSign Issuing CA certificates are X.509 Version 1 Certificates, including.
- Certain Secure Server Certificates are X.509 Version 1 Certificates where the specific web server does not support the use of X.509 Version 3 Certificates.
- VeriSign G2 PCA Certificates where issued in WAP format to support KPN's wireless PKI services.
- Any WTLS User and WTLS Server Certificates still in existence which are issued in WAP format.

7.1.2 Certificate Extensions

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

KPN currently does not use extensions for WTLS Certificates.

7.1.2.1 Key Usage

Where X.509 Version 3 Certificates are used, KPN populates the KeyUsage extension of in accordance with CPS § 6.1.9. The criticality field of this extension is generally set to FALSE.

7.1.2.2 Certificate Policies Extension

KPN X.509 Version 3 end-user Subscribers Certificates use the Certificate Policies extension. The CertificatePolicies extension is populated with the applicable object identifier for the VTN 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 is set to FALSE.

7.1.2.3 Subject Alternative Names

No stipulation.

7.1.2.4 Basic Constraints

KPN populates X.509 Version 3 CA Certificates with a BasicConstraints extension with the Subject Type set to CA. End-user Subscriber Certificates are also populated with a BasicConstraints extension with the Subject Type equal to End Entity. The criticality of the Basic Constraints extension is generally set to FALSE for End-Entity Certificates and TRUE for CA Certificates The criticality of this extension may be set to TRUE for additional Certificates in the future.

KPN X.509 Version 3 CA Certificates issued to 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 the online CAs of Managed PKI Customers and KPN CAs, issuing end-user Subscriber Certificates 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 18 below. For other types of Certificates, KPN does not usually use the Extended Key Usage extension.

Certificate Type	*Certificate Type*
Certification Authority (CA)	Class 3 International Server CA
OCSP Responder	Class 1-3 Public Primary OCSP Responders Secure Server OCSP Responder
Class 3 Web Server Certificates	Secure Server IDs Global Server IDs
Individual Certificates	Class 1 Individual Certificates Class 2 Individual Certificates

Table 18 – Certificates Using the Extended Key Usage Extension

For the Certificates, KPN populates the ExtendedKeyUsage extension in accordance with Table 19 below.

	Class 3 International Server CA	OCSP Responders	Secure Server IDs	Global Server IDs	Authenticated Content Signing Certificates	Class 1 and 2 Individual Certificates
Criticality	*FALSE*	*FALSE*	*FALSE*	*FALSE*	*FALSE*	*FALSE*
ServerAuth	Set	Clear	Set	Set	Clear	Clear
ClientAuth	Set	Clear	Set	Set	Clear	Set
CodeSigning	Clear	Clear	Clear	Clear	Set	Clear
EmailProtection	Clear	Clear	Clear	Clear	Clear	Set
IpsecEndSystem	Clear	Clear	Clear	Clear	Clear	Clear
IpsecTunnel	Clear	Clear	Clear	Clear	Clear	Clear
IpsecUser	Clear	Clear	Clear	Clear	Clear	Clear
TimeStamping	Clear	Clear	Clear	Clear	Clear	Clear
OCSP Signing	Clear	Set	Clear	Clear	Clear	Clear
Microsoft Server Gated Crypto (SGC) OID: 1.3.6.1.4.1.311.10.3.3	Clear	Clear	Clear	Set	Clear	Clear
Netscape SGC - OID: 2.16.840.1.113730.4.1	Set	Clear	Clear	Set	Clear	Clear
VeriSign SGC Identifier for CA Certificates – OID: 2.16.840.1.113733.1.8.1	Set	Clear	Clear	Clear		Clear

Table 19 – Settings for ExtendedKeyUsage Extension

7.1.2.6 CRL Distribution Points

Most KPN 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. The use of CRL Distribution Points will be supported for other KPN CA Certificates and end user Subscriber Certificates in the future.

7.1.2.7 Authority Key Identifier

VeriSign 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 160-bit SHA-1 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. The use of Authority Key Identifier extension may be supported for other VeriSign CAs and end user Subscriber Certificates in the future.

7.1.2.8 Subject Key Identifier

Where KPN populates X.509 Version 3 VTN Certificates with a subjectKeyIdentifier extension, the keyIdentifier based on the public key of the Subject of the Certificate is generated. Where this extension is used, the criticality field of this extension is set to FALSE.

7.1.3 Algorithm Object Identifiers

KPN X.509 Certificates are signed with sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5) or md5WithRSAEncryption (OID: 1.2.840.113549.1.1.4) in accordance with RFC 3279. VeriSign signed certain legacy CA and end user Subscriber Certificates with md2WithRSAEncryption (OID: 1.2.840.113549.1.1.2).

KPN WTLS Certificates still in existence are signed with sha1RSA (OID: 1.2.840.113549.1.1.5) or ecdsa-with-SHA1 (OID: 1.2.840.10045.1).

7.1.4 Name Forms

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

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

7.1.5 Name Constraints

No stipulation.

7.1.6 Certificate Policy Object Identifier

Where the Certificate Policies extension is used, Certificates contain the object identifier for the Certificate Policy corresponding to the appropriate Class of Certificate as set forth in CPS § 1.2. For legacy Certificates issued prior to the publication of the VTN CP which include the Certificate Policies extension, Certificates refer to the VeriSign CPS.

7.1.7 Usage of Policy Constraints Extension

No stipulation.

7.1.8 Policy Qualifiers Syntax and Semantics

KPN populates X.509 Version 3 VTN Certificates with a policy qualifier within the CertificatePolicies extension. Generally, such Certificates contain a CPS pointer qualifier that points to the applicable Relying Party Agreement or the VeriSign 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 Policy Extension

No stipulation.

7.2 CRL and OCSP Profile

KPN issues CRLs that conform to RFC 3280[34]. At a minimum, KPN CRLs contain the basic fields and contents specified in Table 20 below:

Field	*Value or Value constraint*
Version	See CPS §7.2.1.
Signature Algorithm	Algorithm used to sign the CRL. VeriSign CRLs are signed using sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5) or md5RSAWithRSAEncryption (OID: 1.2.840.113549.1.1.4) or md2RSA (OID: 1.2.840.113549.1.1.2) in accordance with RFC 3279.
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. KPN CRLs are effective upon issuance.
Next Update	Date by which the next CRL will be issued. CRL issuance frequency is in accordance with the requirements of CPS § 4.4.9.
Revoked Certificates	Listing of revoked certificates, including the Serial Number of the revoked Certificate and the Revocation Date.

Table 20 – CRL Profile Basic Fields

KPN's OCSP responders conform with RFC2560.

[34] RFC 3280 replaced RFC 2459.

7.2.1 Version Number(s)

KPN issues both X.501 Version1 and Version 2 CRLs. KPN's OCSP responders implement Version 1 of the OCSP specification as defined by RFC2560, with the exception of including nonce as one of the requestExtensions in requests.

7.2.2 CRL and CRL Entry Extensions

No stipulation.

8 Specification Administration

8.1 Specification Change Procedures

Amendments to this CPS shall be made by KPN and approved by the VeriSign Practices Development group. Amendments shall either be in the form of a document containing an amended form of the CPS or an update. 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.

8.1.1 Items that Can Change Without Notification

KPN reserves 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. KPN's decision to designate amendments as material or non-material shall be within KPN's sole discretion.

8.1.2 Items that Can Change with Notification

KPN shall make material amendments to the CPS in accordance with this CPS § 8.1.2.

8.1.2.1 List of Items

Material amendments are those changes that KPN, under CPS § 8.1.1, considers to be material.

8.1.2.2 Notification Mechanism

KPN's Policy Management Authority will post proposed amendments to the CPS in the Practices Updates and Notices section of the KPN Repository, which is located at: https://certificaat.kpn.com/repository. KPN solicits proposed amendments to the CPS from other KPN Subdomain Participants. If KPN considers such an amendment desirable and proposes to implement the amendment, KPN shall provide notice of such amendment in accordance with this section.

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

8.1.2.3 Comment Period

Except as noted under CPS § 8.1.2.2, 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 KPN Policy Management Authority up until the end of the comment period.

8.1.2.4 Mechanism to Handle Comments

The KPN Policy Management Authority will consider any comments on the proposed amendments. KPN will either (a) allow the proposed amendments to become effective without amendment, (b) amend the proposed amendments and republish them as a new amendment under CPS § 8.1.2.2, or (c) withdraw the proposed amendments. KPN 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 under CPS § 8.1.2.3.

8.1.3 Changes Requiring Changes in the Certificate Policy OID or CPS Pointer

See CP § 8.1.3.

8.2 Publication and Notification Policies

8.2.1 Items Not Published in the CPS

Security documents considered confidential by VeriSign and the Affiliates are not disclosed to the public. Confidential security documents include the documents identified in CPS § 1.1(a) Table 1 as documents that are not available to the public.

8.2.2 Distribution of the CPS

This CPS is published in electronic form within the KPN Repository at https://certificaat.kpn.com/repository. The CPS is available in the KPN Repository in Adobe Acrobat pdf. The CPS is available in paper form from the KPN Policy Management Authority upon requests sent to: mailto:pma.en@kpn.com.

8.3 CPS Approval Procedures

Not applicable.

Date of publication
1 June 2004

Version
2.0

Annex A Acronyms and Definitions

1.1 Table of Acronyms

Acronym	Term
ANSI	The American National Standards Institute.
ASB	Authentication Service Bureau.
B2B	Business-to-business.
BIS	The United States Bureau of Industry and Science of the United States Department Commerce.
BXA	The United States Bureau of Export Administration of the United States Department of Commerce (which has been replaced by the BIS).
CA	Certification Authority.
CP	Certificate Policy.
CPS	Certification Practice Statement.
CRL	Certificate Revocation List.
EAL	Evaluation assurance level (pursuant to the Common Criteria).
EDI	Electronic Data Interchange.
EDIFACT	EDI for Administration, Commerce, and Transport (standards established by the United Nations Economic Commission for Europe).
FIPS	United State Federal Information Processing Standards.
ICC	International Chamber of Commerce.
KRB	Key Recovery Block.
LSVA	Logical security vulnerability assessment.
OCSP	Online Certificate Status Protocol.
OFX	Open Financial Exchange.
PCA	Primary Certification Authority.
PIN	Personal identification number.
PKCS	Public Key Cryptography Standard.
PKI	Public Key Infrastructure.
PMA	Policy Management Authority.
RA	Registration Authority.
RFC	Request for comment.
SAS	Statement on Auditing Standards (promulgated by the American Institute of Certified Public Accountants).
S/MIME	Secure Multipurpose Internet Mail Extensions.
SSL	Secure Sockets Layer.
VTN	VeriSign Trust Network.
WAP	Wireless Application Protocol.
WTLS	Wireless Transport Layer Security.

1.2 Definitions

Term	Definition
Administrative Certification Authority (Administrative CA)	A type of KPN CA that issues Certificates to KPN RAs, Managed PKI Customer personnel (Managed PKI Administrators), Affiliate Administrators, and Automated Administration servers.
Administrator	A Trusted Person within the organization of a Processing Center, Service Center, Managed PKI 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.
Affiliated Individual	A natural person that is related to a given 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.
ASB Customer	An entity that contracts with VeriSign or an Affiliate to obtain Authentication Service Bureau services. An ASB Customer is a CA, and is named as such within the Certificates issued by its CA, but it outsources all CA functions to an ASB Provider.
ASB Provider	An entity (either VeriSign or an Affiliate) that offers Authentication Service Bureau services to ASB Customers. An ASB Provider acts as an outsourcing provider of back-end functions for an ASB Customer and as an RA for the ASB Customer.
Authentication Service Bureau	A service within the VTN by which VeriSign or an Affiliate performs most front-end RA and all back-end CA functions on behalf of an organization.
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

Term	Definition
	Certificate Applicant) to a CA for the issuance of a Certificate.
Certificate Chain	An ordered list of Certificates containing an end-user Subscriber Certificate and CA Certificates, which terminates in a root Certificate.
Certificate Management Control Objectives	Criteria that an entity must meet in order to satisfy a Compliance Audit.
Certificate Policies (CP)	The document entitled "VeriSign Trust Network Certificate Policies" and is the principal statement of policy governing the VTN.
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 CPS § 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 to employ. In the context of this CPS, "CPS" refers to this document.
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. The distinctions are summarized in CPS § 1.1.1.
Class 2 Individual ASB Certificate	A Class 2 individual Certificate issued by an ASB Provider on behalf of an ASB Customer CA.
Class 3 Organizational ASB Certificate	A Class 3 organizational Certificate issued by an ASB Provider on behalf of an ASB Customer CA.
Client OnSite Customer	See Managed PKI Customer.
Client OnSite Lite Customer	See Managed PKI Lite Customer.
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, or Managed PKI 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

Term	Definition
	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 CPS § 2.8.1.
Consumer, as in Consumer Service Center	A line of business that an Affiliate enters to provide client Retail Certificates to Certificate Applicants.
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, or ASB Customer.
Digital Receipt	A data object created in connection with the VeriSign Digital Notarization Service offered by KPN and digitally signed by the Time-Stamping Authority that includes the hash of a document or set of data and a time-stamp showing that the document or data existed at a certain time.
Electronic Data Interchange (EDI)	The computer-to-computer exchange of business transactions, such as purchase orders, invoices, and payment advices in accordance with applicable standards.
Electronic Data Interchange Certificate[35] (EDI Certificate)	A Class 3 organizational Certificate that allows for digital signatures on Electronic Data Interchange messages and for the encryption of EDI messages.
Enterprise, as in Enterprise Service Center	A line of business that an Affiliate enters to provide Managed PKI services to Managed PKI Customers.
Enterprise Roaming Server	A server residing at the site of a Managed PKI Customer used in conjunction with the VeriSign Roaming Service offered by KPN to hold Roaming Subscribers' encrypted private keys and portions of symmetric keys used to encrypt and decrypt Roaming Subscribers' private keys.
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.
Global Server ID	A Class 3 organizational Certificate used to support SSL sessions between web browsers and web servers that are encrypted using strong cryptographic protection consistent with applicable export laws.
Global Server OnSite	See Managed PKI for SSL Premium Edition.
Global Server OnSite Customer	See Managed PKI for SSL Premium Edition Customer.

[35] EDI certificates are no (longer) part of KPN's service offering.

Term	Definition
Go Secure!	A suite of plug-and-play services building on Managed PKI services and designed to accelerate e-commerce applications.
Infrastructure Certification Authority (Infrastructure CA)	A type of KPN CA that issues Certificates to components of the KPN infrastructure supporting certain KPN services. Infrastructure CAs do not issue CA, RA, or end-user Subscriber Certificates.
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 Ceremony Reference Guide	A document describing Key Generation Ceremony requirements and practices.
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 provided by KPN 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.
KPN Physical Security Policy	*The highest-level document describing KPN's security policies.*
KPN Repository	*KPN's database of Certificates and other relevant VeriSign Trust Network information accessible on-line.*
KPN Subdomain Participants	*An individual or organization that is one or more of the following within the KPN's Subdomain of the VTN: KPN, a Customer, a Reseller, a Subscriber, or a Relying Party.*
Managed PKI	VeriSign's fully integrated Managed PKI service offered by KPN that allows enterprise Customers of KPN 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 a Managed PKI Customer.
Managed PKI	A document setting forth the operational requirements and

Term	Definition
Administrator Handbook	practices for Managed PKI Customers.
Managed PKI Agreement	An agreement under which an organization becomes a Managed PKI Customer and agrees to be bound by this CPS.
Managed PKI Certificate	A Certificate whose Certificate Application was approved by a 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 Customer	An organization that has obtained Managed PKI services from KPN, whereby the organization becomes a CA within the VTN to issue client Certificates. Managed PKI Customers outsource back-end functions of issuance, management, and revocation to KPN, but retain for themselves the RA functions of approving or rejecting Certificate Applications and initiating revocations and renewals of Certificates.
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.
Managed PKI Lite	A type of Managed PKI service that permits an organization to become a Registration Authority within the VTN to assist a VeriSign CA to issue client Certificates.
Managed PKI Lite Customer	An organization that has obtained Managed PKI Lite services from VeriSign or an Affiliate, whereby the organization becomes a Registration Authority within the VTN to assist a VeriSign CA to issue client Certificates. This CA delegates to Managed PKI Lite Customers the RA functions of approving or rejecting Certificate Applications and initiating revocations and renewals of Certificates.
Managed PKI for SSL	A type of Managed PKI service that permits an organization to become an RA within the VTN to assist a VeriSign CA to issue Secure Server IDs within designated domains. This CA delegates to Managed PKI Customers the RA functions of approving or rejecting Certificate Applications and initiating revocations and renewals of Secure Server IDs.
Managed PKI for SSL Customer	An organization that has obtained Managed PKI for SSL services from VeriSign or an Affiliate.
Managed PKI for SSL Premium Edition	A type of Managed PKI service that permits an organization to become an RA within the VTN to assist a VeriSign CA to issue Global Server IDs within designated domains. This CA delegates to Managed PKI Customers the RA functions of approving or rejecting Certificate Applications and initiating revocations and renewals of Global Server IDs.

Term	Definition
Managed PKI for SSL Premium Edition Customer	An organization that has obtained Managed PKI for SSL Premium services from VeriSign or an Affiliate.
Manual Authentication	A procedure whereby Certificate Applications are reviewed and approved manually one-by-one by an Administrator using a web-based interface.
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.
Online Certificate Status Protocol (OCSP)	A protocol for providing Relying Parties with real-time Certificate status information.
OnSite	See Managed PKI.
OnSite Administrator	See Managed PKI Administrator.
OnSite Administrator's Handbook	See Managed PKI Administrator Handbook.
OnSite Agreement	See Managed PKI Agreement. .
OnSite Certificate	See Managed PKI Certificate.
OnSite Control Center	See Managed PKI Control Center.
OnSite Key Manager	See Managed PKI Key Manager.
OnSite Key Management Service Administrator's Guide	See Managed PKI Management Service Administrator's Guide.
OnSite Lite	See Managed PKI Lite.
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

Term	Definition
	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.
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 KPN, acting as CA, to individuals or organizations applying one by one to KPN 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.
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.

Term	Definition
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 CPS § 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.
Server Gated Cryptography	A technology that permits web servers that have been issued a Global Server ID to create an SSL session with a browser that is encrypted using strong cryptographic protection.
Server OnSite	See Managed PKI for SSL.
Server OnSite Customer	See Managed PKI for SSL Customer.
Server Service Center	A Service Center that is an Affiliate providing Secure Server Ids and Global Server Ids either in the Web Site or Enterprise line of business.
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.

Term	Definition
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.
Time-Stamping Authority	The VeriSign entity that signs Digital Receipts as part of the VeriSign Digital Notarization Service.
Time-Stamping Authority CA	The VeriSign CA that issued a special Class 3 organizational Certificate to the Time-Stamping Authority used to verify the digital signatures on Digital Receipts.
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 CPS § 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 Digital Notarization Service offered by KPN[36]	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 Roaming Server offered by KPN	A server residing at KPN's Processing Center used in conjunction with the VeriSign Roaming Service offered by KPN to hold portions of symmetric keys used to encrypt and decrypt Roaming Subscribers' private keys.
VeriSign Roaming Service offered by KPN	The service offered by KPN that enables a Subscriber to download his or her private key and perform private key operations on different client terminals.
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.

[36] KPN currently is not offering VeriSigns Digital Notarization Service.

Term	Definition
VeriSign Trust Network (VTN)	The Certificate-based Public Key Infrastructure governed by the VeriSign Trust Network Certificate Policy, 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, an Affiliate, a Customer, 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.
Web Host	An entity hosting the web site of another, such as an Internet service provider, a systems integrator, a Reseller, a technical consultant, and application service provider, or similar entity.
Web Host Program	A program that allows Web Hosts to enroll for Secure Server IDs and Global Server IDs on behalf of end-user Subscribers who are customers of the Web Hosts.
Web Site, as in Web Site Service Center	A line of business that an Affiliate enters to provide Secure Server ID and Global Server ID Retail Certificates one by one to Certificate Applicants.
Wireless Application Protocol (WAP)	A standard for the presentation and delivery of wireless information and telephony services on mobile phones and other wireless terminals.
Wireless Transport Layer Security (WTLS)	A protocol that protects the communication of applications that operate using the Wireless Application Protocol, such as communications between a wireless handset and a server.
Wireless Transport Layer Security Certificate (WTLS Certificate)	A Class 3 organizational Certificate whose format is defined as part of the Wireless Application Protocol, which authenticates a Wireless Transport Layer Security server to a WTLS client and facilitates encrypted communication between the WTLS server and the WTLS client[37].

[37] WTLS Certificates are no longer part of KPN's service offering.