KPN B.V.

Certification Practice Statement

DigiCert Trust Network

Version 4.3

Document Date: October 22, 2020
Publication Date: October 23, 2020

KPN B.V.
Fauststraat 1
P.O. Box 9105
7300 HN Apeldoorn
The Netherlands
https://certificaat.kpn.com

KPN Certification Practice Statement

Important – Acquisition Notice
On Oct 31, 2017, DigiCert Inc completed the acquisition of DigiCerts Website Security and related PKI solutions. As a result DigiCert is now the registered owner of the DPP Certificate Policy document and the PKI Services described within that document.

Trademark and Tradename Notices

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

DigiCert, the DigiCert Logo, and the Checkmark Logo are the registered trademarks of DigiCert Corporation or its affiliates in the U.S. and other countries.

Acknowledgement

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

Table of Contents

1 INTRODUCTION

This document is the KPN Certification Practice Statement (“CPS”). It describes the practices that KPN Certification Authorities (“KPN CAs”) employ in providing certification services that include, but are not limited to, issuing, managing, revoking and renewing certificates in accordance with the specific requirements of the DigiCert Certificate Policies (“CP”). KPN offers only Class 2 Certificates for end entity certificates, see Appendix 1.

The CP is the principal statement governing the DigiCert Public PKI (DPP). The CP establishes the business, legal, and technical requirements for approving, issuing, managing, using, revoking, and renewing, digital Certificates within the DPP and providing associated trust services. These requirements, called the “DPP Standards”, protect the security and integrity of the DPP, apply to all DPP Participants, and thereby provide assurances of uniform trust throughout the DPP. More information concerning the DPP and DPP Standards is available in the CP.

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

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

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

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

Name of Policy/Guideline/Requirement Standard	**Location of Source Document/Language**
DigiCert Certificate Policy version 5.0	https://www.digicert.com/legal-repository/
DigiCert Certificate Practice Statement 5.0	https://www.digicert.com/legal-repository/
CA/B Forum” Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates	https://cabforum.org/baseline-requirements-document/
Mozilla Root Store Policy	https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/
Mozilla CA/Forbidden or Problematic Practices	https://wiki.mozilla.org/CA/Forbidden_or_Problematic_Practices
KPN Security Policy	https://github.com/KPN-CISO/kpn-security-policy

1.1 Overview

1.1.1 CPS Purpose

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

This CPS describes, among other things:

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

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

- Ancillary security and operational documents that supplement the CP and this CPS by providing more detailed requirements, such as the KPN Security Policy, which sets forth security principles governing the DPP infrastructure,
- 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 DPP Standards to these DPP Participants and, in some cases, state specific practices for how they must meet DPP Standards.

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

1.1.2 CP/CPS Relationship

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

- securely managing the core infrastructure that supports the DPP, and

issuing, managing, revoking, and renewing DPP Certificates within KPN's Subdomain of the DPP, in accordance with the requirements of the CP/EDP and the DPP Standards.[1]

1.1.3 Status

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

Version	Document date	Changes
4.3	22-10-2020	Updates to include SC30, SC31, and SC33 requirements and practices from the CABF. Updates to include changes in new version of DigiCert Certificate Policy. Changes in CA hierarchy.
4.2	08-04-2020	Adjustments to clarify the distinction between the role of KPN and the Registration Authorities
4.1	31-03-2020	Updates to include new version of Mozilla Root Store Policy
4.0	30-10-2019	Complete revision of previous CPS version 3.7

1.2 Document Name and Identification

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

1.3 PKI Participants

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

1.3.1 Certification Authorities

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

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

[1] Although DigiCert CAs certify the CAs of Affiliates, the practices relating to an Affiliate are covered in the Affiliate's CPS such as this CPS for KPN and its customers.

1.3.2 Registration Authorities and Other Delegated Third Parties

A Registration Authority is an entity of the Issuing CA that performs identification and authentication of certificate applicants for end-user certificates. The RA also initiates or passes along revocation requests for certificates for end-user certificates on behalf of the Issuing CA. Validation of domains for S/MIME Certificates may not be delegated to a third party and is only validated by the RA of the Issuing CA. Issuing CAs, who enter into a contractual relationship with KPN, may operate their own RA and authorize the issuance of certificates by a KPN CA. RAs must abide by all the requirements of the DPP CP, the KPN CPS and the terms of their enterprise services agreement with KPN. RAs may, however implement more restrictive practices based on their internal requirements. KPN contractually obligates each Issuing CA to abide by the policies and industry standards that are applicable to that CA delegated responsibilities.

1.3.3 Subscribers

Subscribers under the DPP include all end users (including entities) of certificates issued by a DPP CA. A subscriber is the entity named as the end-user Subscriber of a certificate. End-user Subscribers may be individuals, organizations, or infrastructure components such as firewalls, routers, trusted servers or other devices used to secure communications within an Organization. In some cases certificates are issued directly to individuals or entities for their own use. However, there commonly exist other situations where the party requiring a certificate is different from the subject to whom the credential applies. For example, an organization may require certificates for its employees to allow them to represent the organization in electronic transactions/business. In such situations the entity subscribing for the issuance of certificates (i.e. paying for them, either through subscription to a specific service, or as the issuer itself) is different from the entity which is the subject of the certificate (generally, the holder of the credential). Two different terms are used in this CPS to distinguish between these two roles: “Subscriber”, is the entity which contracts with DigiCert for the issuance of credentials and; “Subject”, is the person to whom the credential is bound. The Subscriber bears ultimate responsibility for the use of the credential but the Subject is the individual that is authenticated when the credential is presented. When 'subject' is used, it is to indicate a distinction from the Subscriber. When “Subscriber” is used it may mean just the Subscriber as a distinct entity but it may also include the Subject. The context of its use in this CPS will invoke the correct understanding.

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

1.3.4 Relying Parties

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

1.3.5 Other Participants

No stipulation.

1.4 Certificate Usage

A digital Certificate (or Certificate) is formatted data that cryptographically binds an identified subscriber with a Public Key. A digital Certificate allows an entity taking part in an electronic transaction to prove its identity to other participants in such transaction. Digital Certificates are used in commercial environments as a digital equivalent of an identification card.

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

Organizational Certificates are issued to organizations after authentication that the Organization legally exists and that other Organization attributes included in the certificate (excluding non- verified subscriber information) are authenticated e.g. ownership of an Internet or e-mail domain. It is not the intent of this CPS to limit the types of usages for Organizational Certificates. While an organizational certificate may be used for other purposes, provided that a Relying Party is able to reasonably rely on that certificate and the usage is not otherwise prohibited by law, by the DigiCert CP, by any CPS (including this one) under which the certificate has been issued and any agreements with Subscribers.

1.4.1 Appropriate Certificate Uses

Certificates issued pursuant to this CPS may be used for all legal authentication, encryption and digital signature purposes, as designated by the key usage and extended key usage fields found within the Certificate. However, the sensitivity of the information processed or protected by a Certificate varies greatly, and each Relying Party must evaluate the application environment and associated risks before deciding on whether to use a Certificate issued under this CPS.

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

Table 1. Individual Certificate Usage

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

1.4.2 Prohibited Certificate Uses

Certificates shall be used only to the extent the use is consistent with applicable law, and in particular shall be used only to the extent permitted by applicable export or import laws. KPN Certificates are not designed, intended, or authorized for use or resale as control equipment in hazardous circumstances or for uses requiring fail-safe performance such as the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control systems, or weapons control systems, where failure could lead directly to death, personal injury, or severe environmental damage. CA Certificates may not be used for any functions except CA functions. In addition, end-user Subscriber Certificates shall not be used as CA Certificates.

KPN periodically re-keys Intermediate CAs. Third party applications or platforms that have an Intermediate CA embedded as a root certificate may not operate as designed after the Intermediate CA has been re-keyed. KPN therefore does not warrant the use of Intermediate CAs as root certificates and recommends that Intermediate CAs not be embedded into applications and/or platforms as root certificates.

1.5 CPS Administration

1.5.1 Organization Administering the Document

The KPN CPS is managed by a dedicated Policy Management Authority (PMA).

1.5.2 Contact Person

Information regarding this CPS and comments can be directed to:

KPN Security
Attn. Policy Management Authority
PO Box 9105
7300 HN Apeldoorn
pkio.servicedesk@kpn.com

To notify KPN of a service outage or report a suspected private key compromise, certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to certificates, please contact: pkio.servicedesk@kpn.com

1.5.3 Person Determining CPS Suitability for the Policy

The determination of the suitability of the CPS is part of the CPS approval process (see 1.5.4) of the PMA and is part of the assessment by the independent auditor (see 8).

1.5.4 CPS Approval Procedures

Changes to the KPN CPS are approved by the PMA, after consultation with the relevant stakeholders. Once approved, this document will be published in the Repository on https://certificaat.kpn.com/support/downloads/repository

As required by the Baseline Requirements, the CPS is reviewed at least once a year and given a higher version number.

1.6 Definitions and Acronyms

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

2 Publication and Repository Responsibilities

2.1 Repositories

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

Upon revocation of an end-user Subscriber's Certificate, KPN publishes notice of such revocation in the repository. KPN issues CRLs for its own CAs and customers within its Subdomain, pursuant to the provisions of this CPS.

2.2 Publication of Certificate Information

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

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

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

KPN will at all times publish a current version of:

- This CPS
- DPP CP and EDP
- Subscriber Agreements
- Relying Party Agreements
- Recent copies of its WebTrust reports.

The Repository permits Relying Parties to make online inquiries regarding revocation and other Certificate status information. KPN provides Relying Parties with information on how to find the appropriate repository to check Certificate status and, if OCSP (Online Certificate Status Protocol) is available, how to find the right OCSP responder.

KPN publishes the Certificates it issues on behalf of its own CAs and the CAs of customers in it's Subdomain. Upon revocation of an end-user Subscriber's Certificate, KPN shall publish notice of such revocation in the Repository. In addition, KPN issues Certificate Revocation Lists (CRLs) and, if available, provides OCSP services (Online Certificate Status Protocol) for its own CAs and the CAs of Service Centers within its Subdomain.

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

Certificates are published in accordance with Table 3 below.

Certificate Type	Publication Requirements
DPP PCA and DPP Issuing Root CA Certificates	Available to Relying Parties through inclusion in current browser software and as part of a Certificate Chain that can be obtained with the end-user Subscriber Certificate through the query functions described below.
Issuing CA Certificates	Available to Relying Parties as part of a Certificate Chain that can be obtained with the end-user Subscriber Certificate through the query functions described below.
Certificate of the KPN CA supporting Managed PKI Lite Certificates and CA Certificates of Managed PKI Customers	Available through query of the KPN LDAP directory server at directory.managedpki.com, only for customers enable this repository service.
End-User Subscriber Certificates	Available to Relying Parties through query functions in the KPN repository at: https://certificaat.kpn.com/repository/ Former KPN issued Certificates are available to Relying Parties through query functions in the DPP repository at: https://www.DigiCert.com/legal-repository/
End-User Subscriber Certificates issued through Managed PKI Customers	Made available through the query functions listed above, although at the discretion of the Managed PKI Customer, the Certificate may be accessible only via a search using the Certificate's serial number.

Table 3 – Certificate Publication Requirements

2.3 Time or Frequency of Publication

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

2.4 Access Controls on Repositories

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

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

3 Identification and Authentication

3.1 Naming

3.1.1 Types of Names

For s/MIME certs, certificates are issued with a non-null subject Distinguished Name (DN) that complies with ITU X.500 standards.

3.1.2 Need for Names to be Meaningful

Certificates contain names with commonly understood semantics permitting the determination of the identity of the subject (including intermediate CAs) of the Certificate.

3.1.3 Anonymity or Pseudonymity of Subscribers

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

3.1.4 Rules for Interpreting Various Name Forms

No stipulation.

3.1.5 Uniqueness of Names

The uniqueness of each subject name in a Certificate is enforced as follows:

Client Certificates	Requiring a unique email address or a unique organization name combined/associated with a unique serial integer.

The names of Subscribers shall be unique within a subordinate Issuer CA's and Customer's Sub-domain for a specific type of Certificate. Name uniqueness is not violated when multiple certificates are issued to the same entity.

3.1.6 Recognition, Authentication, and Role of Trademarks

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

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

No stipulation.

3.2.2 Authentication of Organizational Identity

An Issuer CA must take reasonable measures to verify that the entity submitting the request for a Certificate to be used to sign or encrypt email, controls the email account associated with the email address referenced in the Certificate, or was authorized by the email account holder to act on the account holder's behalf.
Issuer CAs and RAs shall check the accuracy of information sources and databases to ensure the data is considered accurate, including reviewing the database provider's terms of use.

If the request is for a Certificate that asserts an organizational affiliation between a human subscriber and an organization, the Issuer CA shall obtain documentation from the organization that recognizes the affiliation and obligates the organization to request revocation of the Certificate if that affiliation ends. See Sections 3.2.5, 4.9.1 and 9.6.1

Issuer CAs shall not delegate validation of the domain portion of an e-mail address in s/MIME certificates. The Issuer CA may rely upon validation the root CA has performed for an Authorized Domain Name as being valid domain names. If the Issuer CA is verifying the domain portion, then the Issuer CA must clearly specify in their applicable CPS how domains are verified, typically using a process the CA/B Forum authorized to meet this requirement.

3.2.3 Authentication of Individual Identity

For Issuing CAs that are not name constrained the Issuer CA verifies an individual's or organization's right to use or control an email address to be contained in a Certificate that will have the "Secure Email" EKU by sending an email message containing a Random Value to the email address to be included in the Certificate and receiving a confirming response through use of the Random Value to indicate that the Applicant and/or Organization owns or controls that same email address.

3.2.4 Non-Verified Subscriber Information

If an Issuing CA uses the Organization Unit (OU), the Issuing CA must follow a process for verifying that the OU does not contain an unverified name, trademark, or address.

3.2.5 Validation of Authority

The authority of the request is verified through the email address listed in the Certificate.

3.2.6 Criteria for Interoperation

KPN may provide interoperation services that allow another CA to be able to interoperate by unilaterally certifying that CA. CAs enabled to interoperate in this way will comply with this CPS as supplemented by additional policies when required.

KPN permits interoperation with another CA in circumstances where the CA:
• Enters into a contractual agreement with KPN;
• Operates under this CPS for the certificates it will issue;
• Passes a compliance assessment before being allowed to interoperate; and
• Passes an annual compliance assessment for ongoing eligibility to interoperate that meets the relevant requirements.

3.3 Identification and Authentication for Re-key Requests

Re-key is not supported.

3.3.1 Identification and Authentication for Routine Re-key

Not applicable.

3.3.2 Identification and Authentication for Re-key After Revocation

Not applicable.

3.4 Identification and Authentication for Revocation Request

The RA of the Issuing CA authenticates all revocation requests. The RA may authenticate revocation requests by referencing the Certificate's Public Key, regardless of whether the associated Private Key is compromised.

4 Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

Either the Applicant or an individual authorized to request Certificates on behalf of the Applicant may submit certificate requests. Applicants are responsible for any data that the Applicant or an agent of the Applicant supplies to the Issuing CA.

The Issuer CA is responsible for ensuring that the identity of each Applicant is verified in accordance with this CP and the applicable CPS prior to the issuance of any Certificate type per the applicable legal agreements. Applicants are responsible for submitting sufficient information and documentation for the Issuer CA or the RA to perform the required verification of identity prior to issuing a Certificate

4.1.2 Enrollment Process and Responsibilities

In no particular order, the enrollment process includes:
1. Submitting a certificate application;
2. Generating a Key Pair;
3. Delivering the Public Key of the Key Pair to the Issuing CA;
4. Agreeing to the applicable Subscriber Agreement.

KPN and the Issuer CAs are responsible for ensuring that the identity of each Applicant is verified in accordance with the DigiCert CP and this CPS prior to the issuance of any Certificate type per the applicable legal agreements. Applicants are responsible for submitting sufficient information and documentation for the Issuer CA and RA to perform the required verification of identity prior to issuing a Certificate.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

KPN and its Issuer CAs must identify and verify each Applicant in accordance with the applicable policies and standards listed in the Introduction of this CPS and the DigiCert CP. In cases where the certificate request does not contain all the necessary information about the Applicant, Issuer CAs shall obtain the remaining information from the Applicant or, having obtained it from a reliable, independent, third-party data source, confirm it with the Applicant. Issuer CAs and its RAs shall follow a documented procedure for verifying all data requested for inclusion in the Certificate by the Applicant.

KPN and the Issuer CAs ensure that all communication between the Issuer CA and an RA regarding certificate issuance or changes in the status of a Certificate are made using secure and auditable methods. If databases or other sources are used to confirm sensitive or confidential attributes of an individual subscriber, then that sensitive information shall be protected and securely exchanged in a confidential and tamper-evident manner, protected from unauthorized access, and tracked using an auditable chain of custody.

Issuer CAs shall develop, maintain, and implement documented procedures that identify and require additional verification activity for High Risk Certificate Requests prior to the Certificate's approval, as reasonably necessary to ensure that such requests are properly verified under the CABF Baseline

Requirements. KPN and its Issuer CAs create and maintain records sufficient to establish required verification tasks were followed.

4.2.2 Approval or Rejection of Certificate Applications

If the certificate application is successfully validated by the RA, the Issuing CA will approve the certificate application and issue the Certificate. KPN and Issuing CAs reject any certificate application that cannot be verified. KPN and the Issuing CA are not liable for any rejected Certificate and are not obligated to disclose the reasons for a rejection. Rejected Applicants may re-apply. Subscribers are required to check the Certificate's contents for accuracy prior to using the certificate.

KPN and its Issuer CAs follow industry standards in the Introduction of this CPS when approving and issuing Certificates. KPN and its Issuer CAs contractually require subscribers to verify the information in a Certificate prior to using the Certificate.

4.2.3 Time to Process Certificate Applications

Under normal circumstances, the RA of the Issuing CA verifies an Applicant's information and issues a digital Certificate within a reasonable time frame. Issuance time frames are greatly dependent on when the Applicant provides the details and documentation necessary to complete validation.

4.3 Certificate Issuance

4.3.1 CA actions during certificate issuance

The Issuer CA performs actions during the certificate issuance process in a secure manner. The Issuing CA confirms the source of a certificate request before issuance. Databases and CA processes occurring during certificate issuance are protected from unauthorized modification. After issuance is complete, the Certificate is stored in a database and sent to the Subscriber.

4.3.2 Notification to subscriber by the CA of issuance of certificate

The Issuing CA may deliver Certificates in any secure manner within a reasonable time after issuance. Generally, the Issuing CA delivers Certificates via SSCD or via email to the email address designated by the Subscriber during the application process.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

Subscribers are solely responsible for installing the issued Certificate. Certificates are considered accepted 30 days after the Certificate's issuance, or earlier upon use of the Certificate when evidence exists that the Subscriber used the Certificate.

4.4.2 Publication of the Certificate by the CA

KPN publishes all Issuing CA Certificates in its repository. The Issuing CA publishes end-entity Certificates by delivering them to the Subscriber.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

RAs may receive notification of a Certificate's issuance if an RA was as part of the Issuing CA involved in the issuance process.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

Use of the Private Key corresponding to the public key in the certificate is only permitted once the Subscriber agrees to the Subscriber Agreement and accepted the certificate. The certificate shall be used lawfully in accordance with DigiCert's Subscriber Agreement the terms of this CP and the relevant CPS.
Subscribers are contractually obligated to protect their Private Keys from unauthorized use or disclosure, discontinue using a Private Key after expiration or revocation of the associated Certificate, and use Certificates in accordance with their intended purpose.

4.5.2 Relying Party Public Key and Certificate Usage

Relying Parties may only use software that is compliant with X.509, IETF RFCs, and other applicable standards. KPN and the Issuing CAs do not warrant that any third party software will support or enforce the controls and requirements found herein.
A Relying Party should use discretion when relying on a Certificate and should consider the totality of the circumstances and risk of loss prior to relying on a Certificate. If the circumstances indicate that additional assurances are required, the Relying Party must obtain such assurances before using the Certificate. Any warranties provided by the Issuing CA are only valid if a Relying Party's reliance was reasonable and if the Relying Party adhered to the Relying Party Agreement set forth in the KPN repository.

A Relying Party should rely on a digital signature only if:
1. the digital signature was created during the operational period of a valid Certificate and can be verified by referencing a valid Certificate,
2. the Certificate is not revoked and the Relying Party checked the revocation status of the Certificate prior to the Certificate's use by referring to the relevant CRLs, and
3. the Certificate is being used for its intended purpose and in accordance with this CPS.

4.6 Certificate Renewal

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

4.6.1 Circumstances for Certificate Renewal

An Issuing CA may renew a Certificate if:
1. the associated Public Key has not reached the end of its validity period,
2. the Subscriber and attributes are consistent, and
3. the associated Private Key remains uncompromised.

Prior to the expiration of an existing Subscriber's Certificate, it is necessary for the Subscriber to renew the expiring certificate to maintain continuity of Certificate usage.

4.6.2 Who May Request Renewal

Only the certificate subject or an authorized representative of the certificate subject may request renewal of the Subscriber's Certificates.

4.6.3 Processing Certificate Renewal Requests

Renewal application requirements and procedures are generally the same as those used during the Certificate's original issuance as specified in section 3.2. The Issuing CA may refuse to renew a Certificate if it cannot verify any rechecked information. If an individual is renewing a client Certificate and the relevant information has not changed, then the Issuing CA does not require any additional identity vetting.

4.6.4 Notification of New Certificate Issuance to Subscriber

The Issuing CA may deliver the Certificate in any secure fashion, typically by email or by providing the Subscriber a hypertext link to a user id/password-protected location where the subscriber may log in and download the Certificate.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Renewed Certificates are considered accepted 30 days after the Certificate's renewal, or earlier upon use of the Certificate when evidence exists that the Subscriber used the Certificate.

4.6.6 Publication of the Renewal Certificate by the CA

The Issuing CA publishes a renewed Certificate by delivering it to the Subscriber.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

RAs may receive notification of a Certificate's renewal if the Issuing CA's RA was involved in the issuance process.

4.7 Certificate Re-Key

Re-keying a Certificate consists of creating a new Certificate with a new Public Key and serial number while keeping the subject information the same.
Re-key is not supported.

4.7.1 Circumstances for Certificate Re-Key

Not applicable.

4.7.2 Who May Request Certification of a New Public Key

Not applicable.

4.7.3 Processing Certificate Re-Keying Requests

Not applicable.

4.7.4 Notification of New Certificate Issuance to Subscriber

Not applicable.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

Not applicable.

4.7.6 Publication of the Re-Keyed Certificate by the CA

Not applicable.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

Not applicable.

4.8 Certificate Modification

4.8.1 Circumstances for Certificate Modification

Modifying a Certificate means creating a new Certificate for the same subject with authenticated information that differs slightly from the old Certificate (e.g., changes to email address or non-essential parts of names or attributes) provided that the modification otherwise complies with this CPS. The new Certificate may have the same or a different subject Public Key.
Certificate Modification is not supported. If the information contained in the Certificate is no longer accurate, the Subscriber must immediately revoke the Certificate. After revoking the Certificate, the Subscriber may apply for a new Certificate, if desired.

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

4.8.2 Who May Request Certificate Modification

Not applicable, see § 4.8.1.

4.8.3 Processing Certificate Modification Requests

Not applicable, see § 4.8.1.

4.8.4 Notification of New Certificate Issuance to Subscriber

Not applicable, see § 4.8.1.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

Not applicable, see § 4.8.1.

4.8.6 Publication of the Modified Certificate by the CA

Not applicable, see § 4.8.1.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

Not applicable, see § 4.8.1.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

KPN, the Issuing CA, or the Issuing CA's Registration Authority (RA) will revoke a Certificate within 24 hours after confirming one or more of the following occurred:

1. The Subscriber requests in writing that the Certificate be revoked;;
2. The Subscriber notifies KPN or the Issuing CA that the original Certificate request was not authorized and does not retroactively grant authorization;
3. KPN or the Issuing CA obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise; or
4. KPN or the Issuing CA obtains evidence that the validation of domain authorization or control for any FDQN or IP address in the Certificate should not be relied upon.

KPN or the Issuing CA may revoke a certificate within 24 hours and will revoke a Certificate within 5 days after confirming that one or more of the following occurred:

1. The Certificate no longer complies with the requirements of Sections 6.1.5 and 6.1.6 of the CA/B forum baseline requirements or any section of the Mozilla Root Store policy;
2. KPN or the Issuing CA obtains evidence that the Certificate was misused and/or used outside the intended purpose as indicated by the relevant agreement;
3. The Subscriber or the cross-certified CA breached a material obligation under the CP, this CPS, or the relevant agreement;
4. KPN or the Issuing CA confirms any circumstance indicating that use of a FQDN, IP address, or email address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name registrant and the Applicant has terminated, or the Domain Name registrant has failed to renew the Domain Name);
5. For code signing, the Application Software Supplier requests revocation and KPN or the Issuing CA does not intend to pursue an alternative course of action;
6. KPN or the Issuing CA confirms that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate FQDN;
7. KPN or the Issuing CA confirms a material change in the information contained in the Certificate;
8. KPN confirms that the Certificate was not issued in accordance with the CA/B forum requirements or relevant browser policy;
9. KPN or the Issuing CA determines or confirms that any of the information appearing in the Certificate is inaccurate;
10. KPN or the Issuing CA have the right to issue Certificates under the CA/B forum requirements expires or is revoked or terminated, unless KPN has made arrangements to continue maintaining the CRL Repository;
11. Revocation is required by the DigiCert CP and/or this CPS; or
12. KPN or the Issuing CA confirms a demonstrated or proven method that exposes the Subscriber's Private Key to compromise, methods have been developed that can easily calculate it based on the Public Key, or if there is clear evidence that the specific method used to generate the Private Key was flawed.

KPN or the Issuing CA may revoke any Certificate in its sole discretion, including if KPN or the Issuing CA believes that:

1. Either the Subscriber's or KPN or the Issuing CA obligations under the CP or this CPS are delayed or prevented by circumstances beyond the party's reasonable control, including computer or communication failure, and, as a result, another entity's information is materially threatened or compromised;
2. KPN or the Issuing CA received a lawful and binding order from a government or regulatory body to revoke the Certificate;
3. KPN or the Issuing CA ceased operations and did not arrange for another Certificate authority to provide revocation support for the Certificates;
4. The technical content or format of the Certificate presents an unacceptable risk to application software vendors, Relying Parties, or others; and
5. The Subscriber was added as a denied party or prohibited person to a blacklist or is operating from a destination prohibited under the laws of the United States.

4.9.2 Who Can Request Revocation?

Subscribers and Subjects can request the revocation of their own individual Certificates. In the case of organizational Certificates, a duly authorized representative of the organization shall be entitled to request the revocation of Certificates issued to the organization. A duly authorized representative of KPN or the Issuing CA/RA shall be entitled to request the revocation of an RA Administrator's Certificate. The entity that approved a Subscriber's Certificate Application shall also be entitled to revoke or request the revocation of the Subscriber's Certificate.

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

4.9.3 Procedure for Revocation Request

Entities submitting certificate revocation requests must list their identity and explain the reason for requesting revocation. KPN and the Issuer CA will authenticate and log each revocation request. KPN and the Issuer CA will always revoke a Certificate if the request is authenticated as originating from the Subscriber or the Affiliated Organization listed in the Certificate. If revocation or a problem report investigation is requested by someone other than an authorized representative of the Subscriber or Affiliated Organization through the contact method in section 1.5.2 or by directly contacting the Issuer CA, KPN or the Issuer CA investigate the alleged basis for the request.

4.9.3.1 Procedure for Requesting the Revocation of an end-user Subscriber Certificate

An end-user Subscriber requesting revocation is required to communicate the request to the Issuing CA approving the Subscriber's Certificate Application, who in turn will initiate revocation of the certificate promptly. The revocation request shall be in accordance with CPS § 3.4.

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

An Issuing CA requesting revocation of its CA Certificate is required to communicate the request to KPN. KPN will then revoke the CA Certificate. KPN may also initiate an Issuing CA Certificate revocation.

4.9.4 Revocation Request Grace Period

Revocation requests shall be submitted as promptly as possible within a commercially reasonable time. As mentioned earlier: if immediate revocation is necessary due to an emergency situation, it should be requested electronically, using the online / real time revocation service.

4.9.5 Time within Which CA Must Process the Revocation Request

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

4.9.6 Revocation Checking Requirements for Relying Parties

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

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

KPN shall provide Relying Parties with information on how to find the appropriate CRL, web-based repository, or OCSP responder (where available) to check for revocation status. Generally, this information is available from the Certificate itself.

4.9.7 CRL Issuance Frequency

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

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

4.9.8 Maximum Latency for CRLs

CRLs are posted to the repository within a commercially reasonable time after generation. This is generally done automatically within minutes of generation. However, it is always done within the legally allowed time (if applicable).

4.9.9 On-Line Revocation/Status Checking Availability

OCSP is not supported.

4.9.10 On-line revocation checking requirements

OCSP is not supported.

4.9.11 Other Forms of Revocation Advertisements Available

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

4.9.12 Special Requirements regarding Key Compromise

KPN uses commercially reasonable efforts to notify potential Relying Parties if it discovers, or has reason to believe, that there has been a Compromise of the private key of one of their own CAs or one of the CAs within their subdomains.

4.9.13 Circumstances for Suspension

Suspension of certificates is not supported by KPN.

4.9.14 Who can request suspension

Not applicable.

4.9.15 Procedure for suspension request

Not applicable.

4.9.16 Limits on suspension period

Not applicable.

4.10 Certificate Status Service

4.10.1 Operational characteristics

Certificate status information is available via CRL. OCSP is not supported.

The serial number of a revoked Certificate remains on the CRL until one additional CRL is published after the end of the Certificate's validity period. The CRL is published every 12 hours and valid for 24 hours.

The Status of certificates is available via CRL at KPN's website, Directory Service..

4.10.2 Service availability

Certificate Status Services are available 7 days a week, 24 hours a day.

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

4.10.3 Optional features

No stipulation.

4.11 End of Subscription

A Subscriber's subscription service ends if its Certificate expires or is revoked or if the applicable Subscriber Agreement expires..

4.12 Key Escrow and Recovery

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

Customers using a KPN key recovery service can escrow copies of the private keys of Subscribers whose Certificate Applications they approve. KPN does not store copies of Subscriber private keys but plays an important role in the Subscriber key recovery process.

4.12.1 Key Escrow and Recovery Policy and Practices

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

End-user Subscriber private keys shall only be recovered under the circumstances permitted within the KPN key recovery service, under which:

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

It is recommended that customers using Key Manager Service:

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

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Private keys are stored on the enterprise's premises in encrypted form. Each Subscriber's private key is individually encrypted with its own triple-DES symmetric key. A Key Escrow Record (KER) is generated, then the triple-DES key is combined with a random session key mask generated in hardware and destroyed. Only the resulting masked session key (MSK) is securely sent and stored at KPN. The KER (containing the end user's private key) and the random session key mask are stored in the Key Manager database on the enterprise premises.

Recovery of a private key and digital certificate requires the Managed PKI administrator to securely log on to the Managed PKI Control Center, select the appropriate key pair to recover and click a "recover" hyperlink. Only after an approved administrator clicks the "recover" link is the MSK for that key pair returned from the Managed PKI database operated out of KPN's secure data center. The Key Manager combines the MSK with the random session key mask and regenerates the triple-DES key which was used to originally encrypt the private key, allowing recovery of the end user's private key. As a final step, an encrypted PKCS#12 file is returned to the administrator and ultimately distributed to the end user.

5 Facility, Management, and Operational Controls

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

5.1 Physical Controls

KPN has described and implemented a Physical Security Policy. This policy meets the Security and Audit Requirements as specified in the DigiCert CP. An overview of the measures taken is described below.

5.1.1 Site Location and Construction

KPN's operations are conducted within a physically protected environment that deters, prevents, and detects unauthorized use of, access to, or disclosure of sensitive information and systems whether covert or overt. KPN also maintains disaster recovery facilities for its CA operations. KPN's disaster recovery facilities are protected by multiple tiers of physical security comparable to those of KPN's primary facility.

5.1.2 Physical Access

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

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

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

Access to HSMs and keying material is restricted in accordance with DPP's segregation of duties requirements. The opening and closing of cabinets or containers in these tiers is logged for audit purposes.

5.1.3 Power and Air Conditioning

KPN's secure facilities are equipped with primary and backup:

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

5.1.4 Water Exposures

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

5.1.5 Fire Prevention and Protection

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

5.1.6 Media Storage

All media containing production software and data, audit, archive, or backup information are stored within KPN facilities with appropriate physical and logical access controls designed to limit access to authorized personnel and protect such media from accidental damage (e.g. water, fire, and electromagnetic).

5.1.7 Waste Disposal

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

Media used to collect or transmit sensitive information are rendered unreadable before disposal. Cryptographic devices are physically destroyed or zeroized in accordance the manufacturers' guidance prior to disposal.

Other waste is disposed of in accordance with KPN's normal waste disposal requirements.

5.1.8 Off-site Backup

KPN performs routine backups of critical system data, audit log data, and other sensitive information. Offsite backup media are stored in a physically secure manner using KPN's disaster recovery facility.

5.2 Procedural Controls

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

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

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

5.2.1 Trusted roles

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

KPN considers the categories of personnel identified in this section as Trusted Persons having a Trusted Position. Persons seeking to become Trusted Persons by obtaining a Trusted Position must successfully complete the screening requirements set out in the Trusted Employee Policy.

5.2.2 Number of Persons Required per Task

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

5.2.3 Identification and authentication for each role

All personnel are required to authenticate themselves to CA systems before they are allowed access to systems necessary to perform their trusted roles.

5.2.4 Roles requiring separation of duties

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

5.3 Personnel Controls

5.3.1 Qualifications, experience, and clearance requirements

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

KPN has determined what knowledge and experience is needed for proper execution of each task. Because of the rapid developments in the specialism, this knowledge is actively maintained. KPN also registers the knowledge and experience of each of its employees.

5.3.2 Background check procedures

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

open to management if a (future) employee refuses to cooperate or if the result of the investigation is negative.

Other stipulations from the Trusted Employee Policy are:

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

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

5.3.3 Training requirements

As part of the annual Planning and Control cycle, a training plan is developed and after it is approved, the necessary budget for execution of the plan is made available. The implementation of the plan is closely monitored and the courses followed are registered. Professional training is stimulated wherever possible and where necessary it is made mandatory. Employees are also trained on the job. The training offered employees covers a wide range of knowledge so that, on the one hand, they can be widely deployed, while on the other hand, it is possible to offer them variation in the tasks they need to perform.

5.3.4 Retraining frequency and requirements

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

5.3.5 Job rotation frequency and sequence

Not applicable.

5.3.6 Sanctions for unauthorized actions

When an employee violates the internal or external rules and regulations, KPN management takes disciplinary actions in accordance with the KPN Collective Labor Agreement (CAO) and the disciplinary actions procedure.

5.3.7 Independent Contractor Requirements

In limited circumstances, independent contractors or consultants may be used to fill Trusted Positions. Any such contractor or consultant is held to the same functional and security criteria that apply to KPN employees in a comparable position. Independent contractors and consultants who have not completed or passed the background check procedures specified in CPS § 5.3.2 are permitted access to KPN's secure facilities only to the extent they are escorted and directly supervised by Trusted Persons at all times.

5.3.8 Documentation Supplied to Personnel

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

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

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

KPN manually or automatically logs the following significant events:
- CA key life cycle management events, including:
  - Key generation, backup, storage, recovery, archival, and destruction
  - Cryptographic device life cycle management events.
- CA and Subscriber certificate life cycle management events, including:
  - Certificate Applications, renewal, re-key, and revocation
  - Successful or unsuccessful processing of requests
  - Generation and issuance of Certificates and CRLs.
- Security-related events including:
  - Successful and unsuccessful PKI system access attempts
  - PKI and security system actions performed by KPN personnel
  - Security sensitive files or records read, written or deleted
  - Security profile changes
  - System crashes, hardware failures and other anomalies
  - Firewall and router activity
  - CA facility visitor entry/exit.

Log entries include the following elements:
- Date and time of the entry
- Serial or sequence number of entry, for automatic journal entries
- Identity of the entity making the journal entry
- Kind of entry.

5.4.2 Frequency of Processing Log

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

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

5.4.3 Retention Period for Audit-Log

Audit logs shall be retained on site for at least two (2) months after processing and thereafter archived in accordance with § 5.5.2. These audit logs are available to auditors upon request, as defined in section 8.

5.4.4 Protection of Audit-Log

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

5.4.5 Audit Log Backup Procedures

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

5.4.6 Audit Collection System (Internal vs. External)

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

5.4.7 Notification to Event-Causing Subject

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

5.4.8 Vulnerability Assessments

Events in the audit process are logged, in part, to monitor system vulnerabilities. Logical security vulnerability assessments ("LSVAs") are performed, reviewed, and revised following an examination of these monitored events. LSVAs are based on real-time automated logging data and are performed on a daily, monthly, and annual basis. An annual LSVA will be an input into an entity's annual Compliance Audit.

5.5 Records Archival

5.5.1 Types of Records Archived

KPN archives:

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

5.5.2 Retention Period for Archive

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

• Ten (10) years and six (6) months for Class 2 Certificates
• Seven (7) years after the expiry date or date of revocation for Qualified Certificates

5.5.3 Protection of Archive

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

5.5.4 Archive Backup Procedures

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

5.5.5 Requirements for Time-Stamping of Records

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

5.5.6 Archive Collection System (Internal or External)

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

5.5.7 Procedures to Obtain and Verify Archive Information

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

5.6 Key Changeover

Key Changeover is a responsibility of the Issuing CA.

5.7 Compromise and Disaster Recovery

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

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

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

5.7.1 Incident and Compromise Handling Procedures

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

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

5.7.2 Computing resources, software, and/or data are corrupted

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

KPN has fitted a complete backup facility for its CRL and online revocation service. The programs and data at the backup facility are identical to those in the production environment and it is possible to immediately switch to the backup facility when necessary (e.g. in case of a disaster). This kind of switch to the backup facility is regularly tested and the procedure is maintained. The backup facility is located at a different KPN location that has a similar level of security.

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

5.7.3 Entity Private Key Compromise Procedures

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

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

- The Certificate's revoked status is communicated to Relying Parties through the KPN repository,
- Commercially reasonable efforts will be made to provide additional notice of the revocation to all affected DPP Participants, and
- The CA will generate a new key pair, except where the CA is being terminated.

5.7.4 Business continuity capabilities after a disaster

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

KPN will restore all its services within one week.

5.8 CA or RA Termination

5.8.1 Termination of a KPN customer CA

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

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

5.8.2 Termination of a KPN CA

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

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

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

CA key pair generation is performed by multiple pre-selected, trained and trusted individuals using Trustworthy Systems and processes that provide for the security and required cryptographic strength for the generated keys. For PCA, Issuing Root CAs and all online KPN and Managed PKI Customer CAs the cryptographic modules used for key generation meet the requirements of FIPS 140-2 level 3.

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 DPP 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 Issuing CA for their RA using a FIPS 140-2 level 1 certified cryptographic module provided with their browser software.

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

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

6.1.2 Private Key Delivery to Subscriber

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

Where RA or end-user Subscriber key pairs are pre-generated by KPN on hardware tokens or SSCD's, such devices are distributed to the RA or end-user Subscriber using a commercial delivery service and tamper evident packaging. The data required to activate the device is communicated to the RA or end-user Subscriber using an out of band process. The distribution of such devices is logged by KPN.

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

6.1.3 Public Key Delivery to Certificate Issuer

End-user Subscribers and RAs submit their public key to KPN for certification electronically through the use of a PKCS#10 Certificate Signing Request (CSR) or other digitally signed package in a session secured by Secure Sockets Layer (SSL).

Where CA, RA, or end-user Subscriber key pairs are generated by KPN, this requirement is not applicable.

6.1.4 CA Public Key Delivery to Relying Parties

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

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

6.1.5 Key Sizes

Key pairs shall be of sufficient length to prevent others from determining the key pair's private key using cryptanalysis during the period of expected utilization of such key pairs.
DigiCert recommends the use of a minimum key size equivalent in strength to 2048 bit RSA (with a modulus size in bits divisible by 8) for Issuing CA and their RAs and end entity certificates key pairs. The KPN Standard for minimum key sizes is the use of key pairs equivalent in strength to 2048 bit RSA (with a modulus size in bits divisible by 8) for PCAs and CAs.

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

6.1.6 Public Key Parameters Generation and Quality Checking

Not applicable.

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

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

Refer to § 7.1.2.1.

6.2 Private Key Protection and Cryptographic Module engineering Controls

KPN has implemented a combination of physical, organizational, logical, and procedural controls to ensure the security of KPN and customer CA private keys.

Subscribers are required by contract to take necessary precautions to prevent the loss, disclosure, modification, or unauthorized use of private keys.

6.2.1 Cryptographic Module Standards and Controls

For PCA and Issuing Root CA key pair generation and CA private key storage, DigiCert and KPN use hardware cryptographic modules that are certified at or meet the requirements of FIPS 140-2 Level 3.

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

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

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

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

6.2.3 Private Key Escrow

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

6.2.4 Private Key Backup

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

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

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

6.2.5 Private Key Archival

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

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

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

6.2.6 Private Key Transfer Into or From a Cryptographic Module

KPN generates CA key pairs on the hardware cryptographic modules in which the keys will be used. In addition, KPN makes copies of such CA key pairs for routine recovery and disaster recovery

purposes. Where CA key pairs are backed up to another hardware cryptographic module, such key pairs are transported between modules in encrypted form.

6.2.7 Private Key Storage on Cryptographic Module

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

6.2.8 Method of Activating Private Key

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

6.2.8.1 Class 2 Certificates

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

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

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

6.2.8.2 Issuing CA's using a Cryptographic Module (with Automated Administration or with Managed PKI Key Manager Service)

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

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

6.2.8.3 Private Keys Held by Processing Centers

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

6.2.9 Method of Deactivating Private Key

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

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

6.2.10 Method of Destroying Private Key

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

6.2.11 Cryptographic Module Rating

See § 6.2.1

6.3 Other Aspects of Key Pair Management

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

6.3.1 Public Key Archival

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

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The Operational Period of a Certificate ends upon its expiration or revocation. The Operational Period for key pairs is the same as the Operational Period for the associated Certificates, except that they may continue to be used for decryption and signature verification. The maximum Operational Periods for KPN Certificates for Certificates issued on or after the effective date of this CPS are set forth in Table 7 below.

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

Certificate Issued By:	Validity Period
Public End-entity certificates	Maximum 2 years
Intermediate CAs	Maximum 10 years

Table 7 – Certificate Operational Periods

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.

Passwords must comply to the KPN Security Policy.

6.4.2 Activation Data Protection

KPN and the Issuer CAs protect data used to unlock Private Keys from disclosure using a combination of cryptographic and physical access control mechanisms. Activation data shall be:
• memorized;
• biometric in nature; or
• recorded and secured at the level of assurance associated with the activation of the cryptographic module, and shall not be stored with the cryptographic module.

KPN and the Issuer CAs requires personnel to memorize and not write down their password or share their passwords with other individuals. KPN and the Issuer CAs implement processes to temporarily lock access to secure CA processes if a certain number of failed log-in attempts occur as set forth in the KPN security policies.

End-user Subscribers shall protect the activation data for their private keys, if any, to the extent necessary to prevent the loss, theft, modification, unauthorized disclosure, or unauthorized use of such private key

6.5 Computer Security Controls

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

6.5.1 Specific Computer Security Technical Requirements

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

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

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

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

6.5.2 Computer Security Rating

The infrastructure of Processing Center used by KPN is positively audited against CEN TS 419 261:2015 *Security Requirements for Trustworthy Systems Managing Certificates and time-stamps*.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

Applications are developed and implemented by DigiCert in accordance with DigiCert systems development and DigiCert/ KPN change management standards. KPN also provides software to its customers for performing Issuing CA associated, RA and contractually bound CA functions. Such software is developed in accordance with DigiCert system development standards.

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

6.6.2 Security Management Controls

KPN has mechanisms and/or policies in place to control and monitor the configuration of its CA systems. DigiCert creates a hash of all software packages and DigiCert software updates.

This hash is used to verify the integrity of such software manually. Upon installation and periodically thereafter, KPN validates the integrity of its CA systems.

6.6.3 Life Cycle Security Controls

No stipulation.

6.7 Network Security Controls

KPN performs all its CA functions using networks secured in accordance with the KPN Security Policy and the Baselin Requirements Network and Certificate System Security Requirements to prevent unauthorized access and other malicious activity. KPN protects its communications of sensitive information through the use of encryption and digital signatures.

6.8 Time-stamping

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

Time and date information is based on one or more trusted time sources. KPN and Issuer CAs ensure that the accuracy of clocks used for time-stamping are within three minutes. Electronic or manual procedures may be used to maintain system time. Clock adjustments are auditable events, see Section 5.4.1.

7 Certificate, CRL and OCSP Profiles

7.1 Certificate Profile

KPN and Issuer CAs generate non-sequential Certificate serial numbers greater than zero (0) containing 128 bits of output from a CSPRNG.
See Annex 4.

7.1.1 Version Number(s)

KPN and Issuer CAs must issue X.509 version 3 Certificates.
See Annex 4.

7.1.2 Certificate Extensions

KPN and Issuer CAs use certificate extensions in accordance with applicable industry standards, including RFC 5280 and in accordance with the CA/B Forum Baseline Requirements. Issuer CAs shall not issue Certificates with a critical private extension. For Issuer CAs that are not used to issue TLS certificates, then the value id-kp-serverAuth must not be present. Other values may be present, but should not combine multiple independent usages (e.g. including idkp-timeStamping [RFC5280] with id-kp-codeSigning [RFC5280]).

Certificates must contain the ExtendedKeyUsage extension, aligning to Application Software Supplier granted trust bits and private PKI use cases. Certificates may not contain the anyEKU value. Subordinate CA Certificates created after January 1, 2019 for publicly trusted certificates, with the exception of cross-certificates that share a private key with a corresponding root certificate: must contain an EKU extension; and must not include the anyExtendedKeyUsage KeyPurposeId; and, must not include both the id-kp-serverAuth and id-kp-emailProtection KeyPurposeIds in the same certificate.

Technically Constrained Subordinate CA Certificates includes an Extended Key Usage (EKU) extension specifying all extended key usages for which the Subordinate CA Certificate is authorized to issue certificates. The anyExtendedKeyUsage KeyPurposeId shall not appear in the EKU extension of publicly trusted certificates.

For S/MIME, the subjectAltName extension is populated in accordance with RFC 5280.
See Annex 4.

7.1.3 Algorithm Object Identifiers

KPN and Issuer CAs sign Certificates using SHA-256 in accordance with the Mozilla Root Store Policy and the DigiCert CP section 7.1.3
See Annex 4.

7.1.4 Name Forms

KPN and Issuer CAs use distinguished names that are composed of standard attribute types, such as those identified in RFC 5280. KPN and the Issuer CAs shall include a unique serial number in each Certificate. The content of the Certificate Issuer Distinguished Name field must match the Subject DN of the Issuer CA to support name chaining as specified in RFC 5280, section 4.1.2.4. Certificates are populated with the Issuer Name and Subject Distinguished Name required under Section 3.1.1. Issuer DNs meet the requirements in the CAB forum baseline requirements. The Issuer CA shall restrict OU

fields from containing Subscriber information that is not verified in accordance with Section 3. Subject attributes must not contain only metadata such as '.', '-', and ' ' (i.e. space) characters, and/or any other indication that the value is absent, incomplete, or not applicable. The commonName attribute must be present and the contents should be an identifier for the certificate such that the certificate's Name is unique across all certificates issued by the issuing certificate.
See Annex 4.

7.1.5 Name Constraints

KPN and Issuer CAs may include name constraints in the nameConstraints field when appropriate.

Technically constrained Issuer CAs for KPN with id-kp-emailProtection extended key usage include the Name Constraints X.509v3 extension with constraints on rfc822Name, with at least one name in permittedSubtrees, each such name having its ownership validated according to section 3.2.2.4 of the Baseline Requirements.
See Annex 4.

7.1.6 Certificate Policy Object Identifier

When an Issuer CA or KPN issues a Certificate containing one of the policy identifiers set forth in the introduction of this CPS, it asserts that the Certificate is managed in accordance with the policy that is identified herein.
See Annex 4.

7.1.7 Usage of Policy Constraints Extension

No Stipulation.

7.1.8 Policy Qualifiers Syntax and Semantics

KPN and Issuer CAs may include brief statements in the Policy Qualifier field of the Certificate Policy extension. Certificates may contain a policy qualifier within the Certificate Policies extension. Generally, such Certificates contain a CPS pointer qualifier that points to the applicable Relying Party Agreement or the applicable CPS in order to meet the requirements of the Mozilla Root Store Policy and the DigiCert CP section 7.1.8.
See Annex 4.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No stipulation beyond what is stated in Annex 4.
See Annex 4.

7.2 CRL Profile

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

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

Table 12 – CRL Profile Basic Fields

For revoked issuing CAs, the CRLReason must be included and it cannot be unspecified (0) or certificateHold(6). If the reason for revocation is unspecified, KPN will omit the reasonCode entry extension, when technically not capable of issuance. If a reasonCode CRL entry extension is present, the CRLReason must indicate the most appropriate reason for revocation of the certificate. KPN specifies the following reason codes from RFC 5280, section 5.3.1 as appropriate for most instances when used in accordance with the practices in this section and this CPS:

- keyCompromise (1),
- cACompromise (2),
- affiliationChanged (3),
- superseded (4),
- cessationOfOperation (5).

If the reason is unspecified, then the Reason code is omitted from the CRL and OCSP in accordance with the baseline requirements.

7.2.1 Version Number(s)

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

7.2.2 CRL and CRL Entry Extensions

No stipulation.

7.3 OCSP profile

OCSP is not supported

7.3.1 Version number(s)

Not applicable

7.3.2 OCSP extensions

Not applicable

8 Compliance Audits and other Assessments

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

Issuing CAs which must comply to the Mozilla Root Store Policy are annually audited against WebTrust for Certification Authorities .

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

- KPN shall be entitled, within its sole and exclusive discretion, to perform at any time an "Exigent Audit/Investigation" on a Customer in the event KPN has reason to believe that the audited entity has failed to meet DPP 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 DPP.
- KPN shall be entitled to perform "Supplemental Risk Management Reviews" on a Customer following incomplete or exceptional findings in a Compliance Audit or as part of the overall risk management process in the ordinary course of business.

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

8.1 Frequency and Circumstances of Assessment

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

8.2 Identity/Qualifications of Assessor

KPN's and Issuing CA compliance audits are performed by a public accounting firm that is listed on webtrust.org. WebTrust auditors must meet the requirements of Section 8.2 of the CA/Browser Baseline Requirements.

8.3 Assessor's Relationship to Assessed Entity

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

8.4 Topics Covered by Assessment

The annual audits cover the business practices disclosure, the integrity of the PKI operations, and compliance with this CPS and referenced requirements. The annual audits verifies compliance with the DigiCert CP, this CPS, and any MOA between it and any other PKI.

The scope of the annual audits includes CA environmental controls, key management operations and Infrastructure/Administrative CA controls, certificate life cycle management and CA business practices disclosure.

8.5 Actions Taken as a Result of Deficiency

With respect to compliance audits , significant exceptions or deficiencies identified during the Compliance Audit will result in a determination of actions to be taken. Dependent of the deficiency this determination is made by KPN or the Issuing CA management with input from the auditor. KPN or the Issuing CA management is responsible for developing and implementing a corrective action plan. If KPN or the Issuing CA determines that such exceptions or deficiencies pose an immediate threat to the security or integrity of the DPP, 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 or the Issuing CA Management will evaluate the significance of such issues and determine the appropriate course of action.

8.6 Communications of Results

The results of each audit are reported to DigiCert within three months of completion of the audit report. DigiCert may submit copies of relevant audit compliance reports to various parties, such as Mozilla, Adobe, CA licensing bodies, etc.

9 Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

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

9.1.2 Certificate Access Fees

KPN and Customers do not charge a fee as a condition of making a Certificate available in a repository or otherwise making Certificates available to Relying Parties.

9.1.3 Revocation or Status Information Access Fees

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

9.1.4 Fees for Other Services

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

9.1.5 Refund policy

Not applicable.

9.2 Financial Responsibility

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

9.2.1 Insurance Coverage

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

9.2.2 Other Assets

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

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

9.2.3 Insurance or warranty coverage for end-entities

KPN provides a warranty to Subscribers according to the General Conditions. KPN provides a limited warranty to Relying Parties as described in the Relying Party Agreement (RPA).

9.3 Confidentiality of Business Information

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

9.3.1 Scope of Confidential Information

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

- CA application records, whether approved or disapproved,
- Certificate Application records,
- Private keys held by Customers using Managed PKI Key Manager and information needed to recover such Private Keys,
- Challenge Phrases,
- Transaction records (both full records and the audit trail of transactions),
- Audit trail records created or retained by KPN or a Customer,
- Audit reports created by KPN or a Customer (to the extent such reports are maintained), or their respective auditors (whether internal or public),
- Quality Management and Information Security Management System, such as
    - Contingency planning and disaster recovery plans, and
    - Security measures controlling the operations of DigiCert hardware and software and the administration of Certificate services and designated enrollment services.

9.3.2 Information Not Within the Scope of Confidential Information

Certificates, Certificate revocation and other status information, KPN repositories and information contained within them are not considered Confidential/Private Information. Information not expressly deemed Confidential/Private Information under § 9.3.1 shall be considered neither confidential nor private. This section is subject to applicable privacy laws.

9.3.3 Responsibility to Protect Confidential Information

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

9.4 Privacy of Personal Information

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

9.4.1 Privacy Plan

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

9.4.2 Information Treated as Private

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

9.4.3 Information Not Deemed Private

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

9.4.4 Responsibility to Protect Private Information

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

9.4.5 Notice and Consent to Use Private Information

Unless otherwise stated in this CPS, the applicable Privacy Policy or by agreement, private information will not be used without the consent of the party to whom that information applies. This section is subject to applicable privacy laws.

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

9.4.6 Disclosure pursuant to judicial or administrative process

9.4.6.1 Sharing Information Due to Legal Subpoena

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

9.4.6.2 Sharing Information in Relation to Private Law Argumentation

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

9.4.6.3 Sharing Information After a Request by the Owner

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

9.4.6.4 Making Certificate Revocation Information Public

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

9.4.7 Other Information Disclosure Circumstances

No Stipulation.

9.5 Intellectual Property Rights

The allocation of Intellectual Property Rights among KPN Subdomain Participants other than Subscribers and Relying Parties is governed by the applicable agreements among such KPN Subdomain Participants. The following subsections of § 9.5 apply to the Intellectual Property Rights in relation to Subscribers and Relying Parties.

9.5.1 Property Rights in Certificates and Revocation Information

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

9.5.2 Property Rights in the CPS

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

9.5.3 Property Rights in Names

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

9.5.4 Property Rights in Keys and Key Material

Key pairs corresponding to Certificates of CAs and end-user Subscribers are the property of the CAs and end-user Subscribers that are the respective Subjects of these Certificates, subject to the rights of enterprise Customers using Managed PKI Key Manager, regardless of the physical medium within which they are stored and protected, and such persons retain all Intellectual Property Rights in and to these key pairs.

Without limiting the generality of the foregoing, DPP's root public keys and the root Certificates containing them, including all PCA public keys and self-signed Certificates, are the property of DigiCert. DigiCert licenses software and hardware manufacturers to reproduce such root Certificates to place copies in trustworthy hardware devices or software.

Finally, Secret Shares of a CA's private key are the property of the CA, and the CA retains all Intellectual Property Right in and to such Secret Shares even though they cannot obtain physical possession of the those shares or the CA from KPN.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

See the General Conditions for this.

9.6.2 RA Representations and Warranties

See the General Conditions for this.

9.6.3 Subscriber Representations and Warranties

See the General Conditions for this.

9.6.4 Relying Party Representations and Warranties

See the General Conditions for this.

9.6.5 Representations and Warranties of Other Participants

No stipulation

9.7 Disclaimers of Warranties

See the General Conditions for this.

9.8 Limitations of Liability

See the General Conditions for this.

9.9 Indemnities

9.9.1 Indemnification by Subscribers

See the General Conditions for this.

9.9.2 Indemnification by Relying Parties

See the General Conditions for this.

9.10 Term and Termination

9.10.1 Term

The CPS becomes effective upon publication in the KPN repository. Amendments to this CPS become effective upon publication in the KPN repository.

9.10.2 Termination

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

9.10.3 Effect of Termination and Survival

Upon termination of this CPS, KPN Subdomain participants are nevertheless bound by its terms for all certificates issued for the remainder of the validity periods of such certificates.

9.11 Individual Notices and Communications with Participants

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

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

The aforementioned documents and much other information is available in the Electronic Repository. It is also always possible to ask questions or discuss other matters, see § 1.5.2.

KPN will notify DigiCert to inform Mozilla if:
1. Ownership or control of the CA certificates changes;
2. An organization other than the CA obtains control of an unconstrained intermediate certificate (as defined in section 5.3.2 of the Mozilla Root Store policy) that directly or transitively chains to KPN's included certificate(s);
3. Ownership or control of KPN's operations changes; or

4. There is a material change in KPN's operations (e.g., when the cryptographic hardware related to a certificate in Mozilla's root store is consequently moved from one secure location to another).

9.12 Amendments

9.12.1 Procedure for Amendment

KPN has the right to modify or make additions to this CPS. The functioning of the valid CPS is evaluated at least once a year by the KPN PMA. Clients and Relying Parties may submit remarks on CPS content to the KPN PMA, see § 1.5.2. Should changes to the CPS be necessary based on these remarks, the PMA will make the necessary changes in accordance with the change management process that has been set up for this purpose.

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

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

9.12.2 Notification Mechanism and Period

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

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

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

9.12.2.1 Comment Period

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

9.12.2.2 Mechanism to Handle Comments

The PMA shall consider any comments on the proposed amendments. The PMA shall either (a) allow the proposed amendments to become effective without amendment, (b) amend the proposed amendments and republish them as a new amendment when required, or (c) withdraw the proposed

amendments. The PMA is entitled to withdraw proposed amendments by providing notice in the Practices Updates and Notices section of the KPN Repository. Unless proposed amendments are amended or withdrawn, they shall become effective upon the expiration of the comment period.

9.12.3 Circumstances under Which OID Must be Changed

No stipulation.

9.13 Dispute Resolution Provisions

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

9.13.1 Disputes among KPN and Customers

Disputes among KPN Subdomain participants shall be resolved pursuant to provisions in the applicable agreements among the parties.

9.13.2 Disputes with End-User Subscribers or Relying Parties

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

9.14 Governing Law

Subject to any limits appearing in applicable law, the Dutch Law governs the enforceability, construction, interpretation, and validity of this CPS, irrespective of contract or other choice of law provisions and without the requirement to establish a commercial nexus in The Netherlands. This choice of law is made to ensure uniform procedures and interpretation for all KPN Subdomain Participants, no matter where they are located.

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

This CPS is subject to Dutch Law.

9.15 Compliance with Applicable Law

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

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

Not applicable.

9.16.2 Assignment

Not applicable.

9.16.3 Severability

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

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

Not applicable.

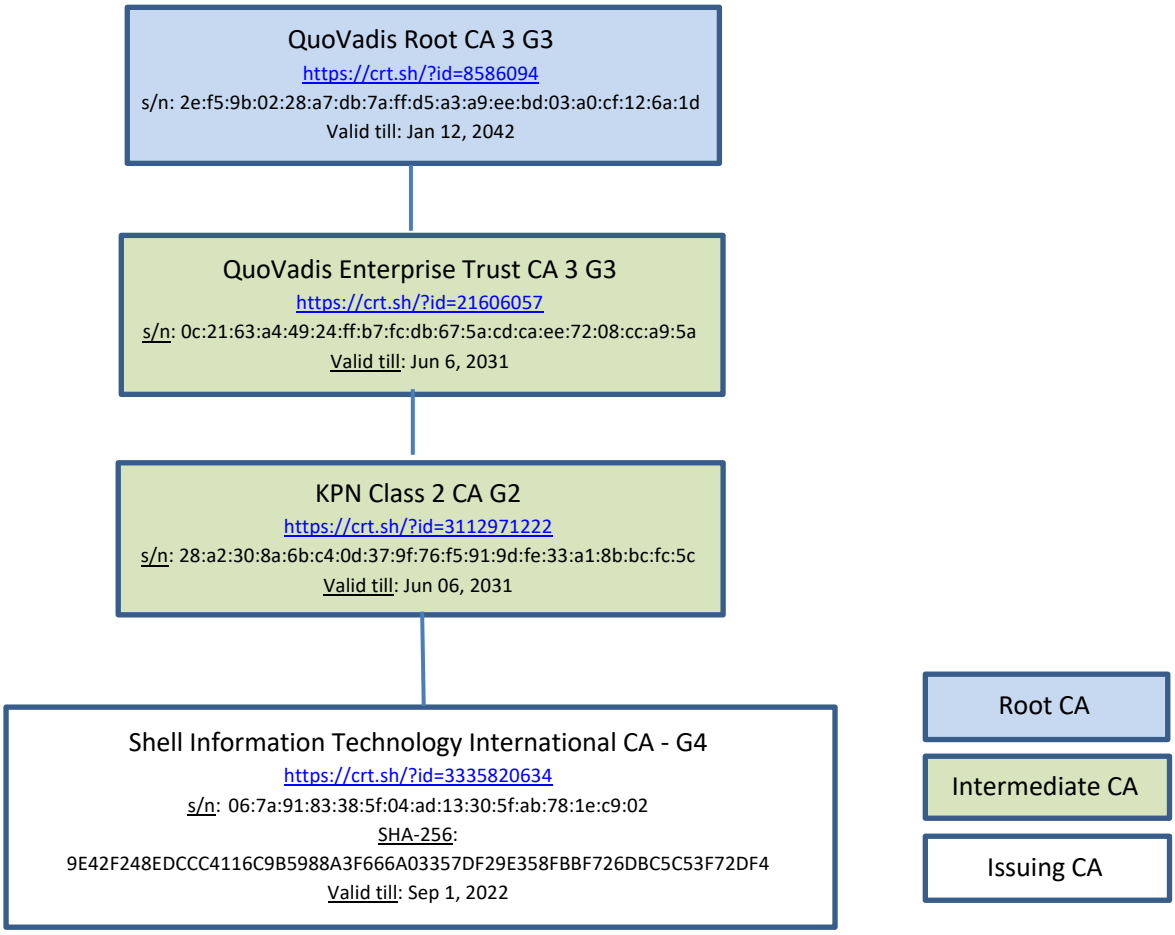
9.16.5 Force Majeure

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

9.17 Other Provisions

Not applicable.

Annex 1 CA model



Annex 2 Acronyms

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

Annex 3 Definitions

Definitions

Term	Definition
Administrator	A Trusted Person within the organization of a Processing Center, Service Center, Managed PKI Customer, or Gateway Customer that performs validation and other CA or RA functions.
Administrator Certificate	A Certificate issued to an Administrator that may only be used to perform CA or RA functions.
Affiliate	A leading trusted third party, for example in the technology, telecommunications, or financial services industry, that has entered into an agreement with VeriSign to be a VTN distribution and services channel within a specific territory.
Affiliate Audit Program Guide	A VeriSign document containing requirements for the Compliance Audits of Affiliates, including Certificate Management Control Objectives against which Affiliates will be audited.
Affiliate Practices Legal Requirements Guidebook	A VeriSign document setting forth requirements for Affiliate CPSs, agreements, validation procedures, and privacy policies, as well as other requirements that Affiliates must meet.

Term	Definition
Affiliated Individual	A natural person that is related to a Managed PKI Customer, Managed PKI Lite Customer, or Gateway Customer entity (i) as an officer, director, employee, partner, contractor, intern, or other person within the entity, (ii) as a member of a VeriSign registered community of interest, or (iii) as a person maintaining a relationship with the entity where the entity has business or other records providing appropriate assurances of the identity of such person.
Applicant	The Private Organization or Government Entity that applies for (or seeks renewal of) an EV Certificate naming it as the Subject.
Applicant Representative	An individual person employed by the Applicant for an EV certificate: (i) who signs and submits, or approves an EV Certificate Request on behalf of an Applicant, and/or (ii) who signs and submits a Subscriber Agreement on behalf of an Applicant.
Application Software Vendor	A developer of Internet browser software or other software that displays or uses certificates and distributes root certificates, such as KDE, Microsoft Corporation, Mozilla Corporation, Opera Software ASA, and Red Hat, Inc.
Automated Administration	A procedure whereby Certificate Applications are approved automatically if enrollment information matches information contained in a database.
Automated Administration Software Module	Software provided by VeriSign that performs Automated Administration.
Certificate	A message that, at least, states a name or identifies the CA, identifies the Subscriber, contains the Subscriber's public key, identifies the Certificate's Operational Period, contains a Certificate serial number, and is digitally signed by the CA.
Certificate Applicant	An individual or organization that requests the issuance of a Certificate by a CA.
Certificate Application	A request from a Certificate Applicant (or authorized agent of the Certificate Applicant) to a CA for the issuance of a Certificate.
Certificate Approver	[defined in Section 10]
Certificate Chain	An ordered list of Certificates containing an end-user Subscriber Certificate and CA Certificates, which terminates in a root Certificate.
Certificate Management Control Objectives	Criteria that an entity must meet in order to satisfy a Compliance Audit.
Certificate Policies (CP)	This document, which is entitled "VeriSign Trust Network Certificate Policies" and is the principal statement of policy governing the VTN.
Certificate Requester: [defined in Section 10]	
Certificate Revocation List (CRL)	A periodically (or exigently) issued list, digitally signed by a CA, of identified Certificates that have been revoked prior to their expiration dates in accordance with CP § 3.4. The list generally indicates the CRL issuer's name, the date of issue, the date of the next scheduled CRL issue, the revoked Certificates' serial numbers, and the specific times and reasons for revocation.
Certificate Signing Request	A message conveying a request to have a Certificate issued.
Certification Authority (CA)	An entity authorized to issue, manage, revoke, and renew Certificates in the VTN.
Certification Practice Statement (CPS)	A statement of the practices that VeriSign or an Affiliate employs in approving or rejecting Certificate Applications and issuing, managing, and revoking Certificates, and requires its Managed PKI Customers and Gateway Customers to employ.
Challenge Phrase	A secret phrase chosen by a Certificate Applicant during enrollment for a Certificate. When issued a Certificate, the Certificate Applicant becomes a Subscriber and a CA or RA can use the Challenge Phrase to authenticate the Subscriber when the Subscriber seeks to revoke or renew the Subscriber's Certificate.
Class	A specified level of assurances as defined within the CP. See CP § 1.1.1.
Client Service Center	A Service Center that is an Affiliate providing client Certificates either in the Consumer or Enterprise line of business.
Compliance Audit	A periodic audit that a Processing Center, Service Center, Managed PKI Customer, or Gateway Customer undergoes to determine its conformance with VTN Standards that apply to it.
Compromise	A violation (or suspected violation) of a security policy, in which an unauthorized disclosure of, or loss of control over, sensitive information may have occurred. With respect to private keys, a Compromise is a loss, theft, disclosure, modification, unauthorized use, or other compromise of the security of such private key.
Confidential/Private Information	Information required to be kept confidential and private pursuant to CP § 2.8.1.
Contract Signer: [defined in Section 10]	

Term	Definition
CRL Usage Agreement	An agreement setting forth the terms and conditions under which a CRL or the information in it can be used.
Customer	An organization that is either a Managed PKI Customer, Gateway Customer, or ASB Customer.
Demand Deposit Account	A deposit account held at a bank or other financial institution, the funds deposited in which are payable on demand. The primary purpose of demand accounts is to facilitate cashless payments by means of check, bank draft, direct debit, electronic funds transfer, etc. Usage varies among countries, but a demand deposit account is commonly known as: a checking account, a share draft account, a current account, or a checking account.
Enterprise, as in Enterprise Service Center	A line of business that an Affiliate enters to provide Managed PKI services to Managed PKI Customers.
Enterprise EV Certificate:	An EV Certificate that an Managed PKI for SSL Customer authorizes VeriSign to issue at third and higher domain levels that contain the domain that have been verified by VeriSign.
Enterprise RA	A Managed PKI for SSL customer that can request multiple valid EV Certificates for Domains and Organizations verified by VeriSign for domains at third and higher domain levels that contain a domain that was verified by VeriSign in the original EV Certificate, in accordance with the requirements of these Guidelines.
Enterprise Roaming Server	A server residing at the site of a Managed PKI Customer used in conjunction with the VeriSign Roaming Service to hold Roaming Subscribers' encrypted private keys and portions of symmetric keys used to encrypt and decrypt Roaming Subscribers' private keys.
EV Certificate:	A digital certificate that contains information specified in the EV Guidelines and that has been validated in accordance with the Guidelines.
EV OID	An identifying number, called an "object identifier," that is included in the certificatePolicies field of an EV certificate that: (i) indicates which CA policy statement relates to that certificate, and which, (ii) by pre-agreement with one or more Application Software Vendor, marks the certificate as being an EV Certificate.
Exigent Audit/Investigation	An audit or investigation by VeriSign where VeriSign has reason to believe that an entity's failure to meet VTN Standards, an incident or Compromise relating to the entity, or an actual or potential threat to the security of the VTN posed by the entity has occurred.
Extended Validation	Validation Procedures defined by the Guidelines for Extended Validation Certificates published by a forum consisting of major certification authorities and browser vendors.
Intellectual Property Rights	Rights under one or more of the following: any copyright, patent, trade secret, trademark, and any other intellectual property rights.
Intermediate Certification Authority (Intermediate CA)	A Certification Authority whose Certificate is located within a Certificate Chain between the Certificate of the root CA and the Certificate of the Certification Authority that issued the end-user Subscriber's Certificate.
Key Generation Ceremony	A procedure whereby a CA's or RA's key pair is generated, its private key is transferred into a cryptographic module, its private key is backed up, and/or its public key is certified.
Key Manager Administrator	An Administrator that performs key generation and recovery functions for a Managed PKI Customer using Managed PKI Key Manager.
Key Recovery Block (KRB)	A data structure containing a Subscriber's private key that is encrypted using an encryption key. KRBs are generated using Managed PKI Key Manager software.
Key Recovery Service	A VeriSign service that provides encryption keys needed to recover a Key Recovery Block as part of a Managed PKI Customer's use of Managed PKI Key Manager to recover a Subscriber's private key.
Managed PKI	VeriSign's fully integrated managed PKI service that allows enterprise Customers of VeriSign and its Affiliates to distribute Certificates to individuals, such as employees, partners, suppliers, and customers, as well as devices, such as servers, routers, and firewalls. Managed PKI permits enterprises to secure messaging, intranet, extranet, virtual private network, and e-commerce applications.
Managed PKI Administrator	An Administrator that performs validation or other RA functions for an Managed PKI Customer.
Managed PKI Control Center	A web-based interface that permits Managed PKI Administrators to perform Manual Authentication of Certificate Applications
Managed PKI Key Manager	A key recovery solution for those Managed PKI Customers choosing to implement key recovery under a special Managed PKI Agreement.
Managed PKI Key Management Service Administrator's Guide	A document setting forth the operational requirements and practices for Managed PKI Customers using Managed PKI Key Manager.
Manual Authentication	A procedure whereby Certificate Applications are reviewed and approved manually one-by-

Term	Definition
	one by an Administrator using a web-based interface.
NetSure Protection Plan	An extended warranty program, which is described in CP § 1.1.2.2.3.
Nonverified Subscriber Information	Information submitted by a Certificate Applicant to a CA or RA, and included within a Certificate, that has not been confirmed by the CA or RA and for which the applicable CA and RA provide no assurances other than that the information was submitted by the Certificate Applicant.
Non-repudiation	An attribute of a communication that provides protection against a party to a communication falsely denying its origin, denying that it was submitted, or denying its delivery. Denial of origin includes the denial that a communication originated from the same source as a sequence of one or more prior messages, even if the identity associated with the sender is unknown. Note: only an adjudication by a court, arbitration panel, or other tribunal can ultimately prevent repudiation. For example, a digital signature verified with reference to a VTN Certificate may provide proof in support of a determination of Non-repudiation by a tribunal, but does not by itself constitute Non-repudiation.
Offline CA	VeriSign PCAs, Issuing Root CAs and other designated intermediate CAs that are maintained offline for security reasons in order to protect them from possible attacks by intruders by way of the network. These CAs do not directly sign end user Subscriber Certificates.
Online CA	CAs that sign end user Subscriber Certificates are maintained online so as to provide continuous signing services.
Online Certificate Status Protocol (OCSP)	A protocol for providing Relying Parties with real-time Certificate status information.
Operational Period	The period starting with the date and time a Certificate is issued (or on a later date and time certain if stated in the Certificate) and ending with the date and time on which the Certificate expires or is earlier revoked.
PKCS #10	Public-Key Cryptography Standard #10, developed by RSA Security Inc., which defines a structure for a Certificate Signing Request.
PKCS #12	Public-Key Cryptography Standard #12, developed by RSA Security Inc., which defines a secure means for the transfer of private keys.
Policy Management Authority (PMA)	The organization within VeriSign responsible for promulgating this policy throughout the VTN.
Primary Certification Authority (PCA)	A CA that acts as a root CA for a specific Class of Certificates, and issues Certificates to CAs subordinate to it.
Processing Center	An organization (VeriSign or certain Affiliates) that creates a secure facility housing, among other things, the cryptographic modules used for the issuance of Certificates. In the Consumer and Web Site lines of business, Processing Centers act as CAs within the VTN and perform all Certificate lifecycle services of issuing, managing, revoking, and renewing Certificates. In the Enterprise line of business, Processing Centers provide lifecycle services on behalf of their Managed PKI Customers or the Managed PKI Customers of the Service Centers subordinate to them.
Public Key Infrastructure (PKI)	The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a Certificate-based public key cryptographic system. The VTN PKI consists of systems that collaborate to provide and implement the VTN.
Registration Authority (RA)	An entity approved by a CA to assist Certificate Applicants in applying for Certificates, and to approve or reject Certificate Applications, revoke Certificates, or renew Certificates.
Regulated Financial Institution	A financial institution that is regulated, supervised, and examined by governmental, national, state or provincial, or local authorities having regulatory authority over such financial institution based on the governmental, national, state or provincial, or local laws under which such financial institution was organized and/or licensed.
Relying Party	An individual or organization that acts in reliance on a certificate and/or a digital signature.
Relying Party Agreement	An agreement used by a CA setting forth the terms and conditions under which an individual or organization acts as a Relying Party.
Retail Certificate	A Certificate issued by VeriSign or an Affiliate, acting as CA, to individuals or organizations applying one by one to VeriSign or an Affiliate on its web site.
Roaming Subscriber	A Subscriber using the VeriSign Roaming Service whose private key is encrypted and decrypted with a symmetric key that is split between the VeriSign Roaming Server and an Enterprise Roaming Server.
RSA	A public key cryptographic system invented by Rivest, Shamir, and Adelman.
RSA Secure Server Certification Authority (RSA Secure Server CA)	The Certification Authority that issues Secure Server IDs.

Term	Definition
RSA Secure Server Hierarchy	The PKI hierarchy comprised of the RSA Secure Server Certification Authority.
Secret Share	A portion of a CA private key or a portion of the activation data needed to operate a CA private key under a Secret Sharing arrangement.
Secret Sharing	The practice of splitting a CA private key or the activation data to operate a CA private key in order to enforce multi-person control over CA private key operations under CP § 6.2.2.
Secure Server ID	A Class 3 organizational Certificate used to support SSL sessions between web browsers and web servers.
Secure Sockets Layer (SSL)	The industry-standard method for protecting Web communications developed by Netscape Communications Corporation. The SSL security protocol provides data encryption, server authentication, message integrity, and optional client authentication for a Transmission Control Protocol/Internet Protocol connection.
Security and Audit Requirements Guide	A VeriSign document that sets forth the security and audit requirements and practices for Processing Centers and Service Centers.
Security and Practices Review	A review of an Affiliate performed by VeriSign before an Affiliate is permitted to become operational.
Service Center	An Affiliate that does not house Certificate signing units for the issuance of Certificates for the purpose of issuing Certificates of a specific Class or type, but rather relies on a Processing Center to perform issuance, management, revocation, and renewal of such Certificates.
Subdomain	The portion of the VTN under control of an entity and all entities subordinate to it within the VTN hierarchy.
Subject	The holder of a private key corresponding to a public key. The term "Subject" can, in the case of an organizational Certificate, refer to the equipment or device that holds a private key. A Subject is assigned an unambiguous name, which is bound to the public key contained in the Subject's Certificate.
Subscriber	In the case of an individual Certificate, a person who is the Subject of, and has been issued, a Certificate. In the case of an organizational Certificate, an organization that owns the equipment or device that is the Subject of, and that has been issued, a Certificate. A Subscriber is capable of using, and is authorized to use, the private key that corresponds to the public key listed in the Certificate.
Subscriber Agreement	An agreement used by a CA or RA setting forth the terms and conditions under which an individual or organization acts as a Subscriber.
Superior Entity	An entity above a certain entity within a VTN hierarchy (the Class 1, 2, or 3 hierarchy).
Supplemental Risk Management Review	A review of an entity by VeriSign following incomplete or exceptional findings in a Compliance Audit of the entity or as part of the overall risk management process in the ordinary course of business.
Reseller	An entity marketing services on behalf of VeriSign or an Affiliate to specific markets.
Trusted Person	An employee, contractor, or consultant of an entity within the VTN responsible for managing infrastructural trustworthiness of the entity, its products, its services, its facilities, and/or its practices as further defined in CP § 5.2.1.
Trusted Position	The positions within a VTN entity that must be held by a Trusted Person.
Trustworthy System	Computer hardware, software, and procedures that are reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy. A trustworthy system is not necessarily a "trusted system" as recognized in classified government nomenclature.
VeriSign	Means, with respect to each pertinent portion of this CPS, VeriSign, Inc. and/or any wholly owned VeriSign subsidiary responsible for the specific operations at issue.
VeriSign Digital Notarization Service	A service offered to Managed PKI Customers that provides a digitally signed assertion (a Digital Receipt) that a particular document or set of data existed at a particular point in time.
VeriSign Repository	VeriSign's database of Certificates and other relevant VeriSign Trust Network information accessible on-line.
VeriSign Roaming Server	A server residing at VeriSign's Processing Center used in conjunction with the VeriSign Roaming Service to hold portions of symmetric keys used to encrypt and decrypt Roaming Subscribers' private keys.
VeriSign Roaming Service	The service offered by VeriSign that enables a Subscriber to download his or her private key and perform private key operations on different client terminals.
VeriSign Trust Network (VTN)	The Certificate-based Public Key Infrastructure governed by the VeriSign Trust Network Certificate Policies, which enables the worldwide deployment and use of Certificates by VeriSign and its Affiliates, and their respective Customers, Subscribers, and Relying Parties.
VTN Participant	An individual or organization that is one or more of the following within the VTN: VeriSign,

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

Annex 4 Certificates profiles

KPN Class 2 CA G2

Base Certificate

Base Certificate				Value
Version				2
Serial number				Unique Positive Integer
Issuer DN				c = **BM** o = **QuoVadis Limited** cn = **QuoVadis Enterprise Trust CA 3 G3**
Subject DN				c = **NL** o = **KPN B.V.** cn = **KPN Class 2 CA G2**
notBefore				**yymmdd000000Z(Key Ceremony Date)**
notAfter				**yymmdd000000Z (Cannot Exceed June 6, 2031)**
Signature Algorithm				sha256withRSAEncryption (1.2.840.113549.1.1.11)
Parameters				NULL

CA Key Pair Size: 4096 with RSA Public Exponent: Fermat 4 - 65537

The Distinguished Name (DN) fields cannot contain more than 64-characters including spaces

**If the CA is to be used for the KMS service, the Subject DN must be encoded with PrintableString. Characters such as "&" and "#" cannot be encoded using PrintableString.

CA Certificate Extensions

Standard Extensions	OID	Include	Criticality	Value
basicConstraints	{id-ce 19}	☒	**TRUE**	n/a
cA				Set
pathLenConstraint				1
keyUsage	{id-ce 15}	☒	**TRUE**	n/a
keyCertSign				Set
cRLSign				Set
authorityKeyIdentifier	{id-ce 35}	☒	**FALSE**	n/a
keyIdentifier				To be supplied during Key Ceremony
authorityCertIssuer				n/a
authorityCertSerialNumber				n/a
certificatePolicies	{id-ce 32}	☒	**FALSE**	n/a
policyIdentifiers				1.3.6.1.4.1.8024.0.3
policyQualifiers				n/a
CPSpointer				n/a
OID				1.3.6.1.5.5.7.2.1
value				https://www.quovadisglobal.com/QVRepository.aspx
new tag				IA5-string
UserNotice		☐		n/a
OID				1.3.6.1.5.5.7.2.2
Explicit Text				n/a
string type				UTF8
subjectKeyIdentifier	{id-ce 14}	☒	**FALSE**	Calculated per Method 1
extKeyUsage	{id-ce 37}	☒	**FALSE**	n/a
clientAuthentication				☒ 1.3.6.1.5.5.7.3.2
emailProtection				☒ 1.3.6.1.5.5.7.3.4
MS Smartcardlogin				☒ 1.3.6.1.4.1.311.20.2.2
DocumentSigning				☒ 1.3.6.1.4.1.311.10.3.12
Microsoft EFS				☒ 1.3.6.1.4.1.311.10.3.4
nameConstraints	{id-ce 30}	☐	**FALSE**	n/a
PermittedSubtrees				n/a
[1]Subtree				rfc822 =
[2]Subtree				rfc822 =
[3]Subtree				directoryName = C= , O=
crlDistributionPoints	{id-ce 31}	☒	**FALSE**	n/a
distributionPoint				n/a
FullName (URI)				http://crl.quovadisglobal.com/qventca3g3.crl
subjectAltName	{id-ce 17}	☒	**FALSE**	To be supplied during Key Ceremony
AuthorityInfoAccess	{id-pe 1}	☒	**FALSE**	n/a
accessMethod				1.3.6.1.5.5.7.48.1
accessLocation				http://ocsp.quovadisglobal.com

Shell Information Technology International CA - G4

Base Certificate

Base Certificate				Value
Version				2
Serial number				Unique Positive Integer
Issuer DN				c = **NL** o = **KPN B.V.** cn = **KPN Class 2 CA - G2**
Subject DN				c = **NL** o = **Shell Information Technology International B.V.** cn = **Shell Information Technology International CA - G4**
notBefore				**yymmdd000000Z(Key Ceremony Date)**
notAfter				**yymmdd000000Z(10 years)**
Signature Algorithm				sha256withRSAEncryption (1.2.840.113549.1.1.11)
Parameters				NULL

CA Key Pair Size: 2048 with RSA (Default) Public Exponent: Fermat 4 - 65537

The Distinguished Name (DN) fields cannot contain more than 64-characters including spaces

**If the CA is to be used for the KMS service, the Subject DN must be encoded with PrintableString. Characters such as "&" and "#" cannot be encoded using PrintableString.

CA Certificate Extensions

Standard Extensions	OID	Include	Criticality	Value
basicConstraints	{id-ce 19}	☒	TRUE	n/a
cA				Set
pathLenConstraint				0
keyUsage	{id-ce 15}	☒	TRUE	n/a
keyCertSign				Set
cRLSign				Set
authorityKeyIdentifier	{id-ce 35}	☒	FALSE	n/a
keyIdentifier				Calculated per Method 1
authorityCertIssuer				n/a
authorityCertSerialNumber				n/a
certificatePolicies	{id-ce 32}	☒	FALSE	n/a
policyIdentifiers				1.3.6.1.4.1.8024.0.3.2400.0
policyQualifiers				n/a
CPSpointer				n/a
OID				1.3.6.1.5.5.7.2.1
value				https://certificaat.kpn.com/CPS
new tag				IA5-string
UserNotice				n/a
OID				1.3.6.1.5.5.7.2.2
Explicit Text				https://certificaat.kpn.com/RPA
string type				UTF8
subjectKeyIdentifier	{id-ce 14}	☒	FALSE	Calculated per Method 1
extKeyUsage	{id-ce 37}	☒	FALSE	n/a
clientAuthentication				☒ 1.3.6.1.5.5.7.3.2
emailProtection				☒ 1.3.6.1.5.5.7.3.4
nameConstraints	{id-ce 30}	☒	FALSE	n/a
PermittedSubtrees				n/a
[1]Subtree				rfc822 = shell.com
[2]Subtree				rfc822 = .shell.com
[3]Subtree				rfc822 = lngcanada.ca
[4]Subtree				rfc822 = sakhalinenergy.ru
[5]Subtree				rfc822 = salympetroleum.ru
[6]Subtree				rfc822 = cri-criterion.com
[7]Subtree				rfc822 = basrahgas.com
[8]Subtree				rfc822 = bruneilng.com
crlDistributionPoints	{id-ce 31}	☒	FALSE	n/a
distributionPoint				n/a
FullName (URI)				http://crl.managedpki.com/KPNClass2CAG2/LatestCRL.crl
subjectAltName	{id-ce 17}	☒	FALSE	To be supplied during Key Ceremony
AuthorityInfoAccess	{id-pe 1}	☐	FALSE	n/a
accessMethod				1.3.6.1.5.5.7.48.1
accessLocation				<ocsp url>