

Equens Certificate Policy

WebServices and Connectivity

Final

H.C. van der Wyck

Classification: NON CONFIDENTIAL

Version 1.0 - 5 February 2008



Equens Certificate Policy

WebServices and Connectivity

Copyright © Equens N.V. and/or its subsidiaries. All rights reserved.

No part of this publication may be copied or reproduced, sold or transferred to any person, in whole or in part, in any manner or form or on any media, without the prior written permission of Equens. The recipient is, however, authorised to copy or reproduce this publication within its own organisation as may be reasonably necessary for the purpose for which it is supplied. Any such copy or reproduction will include the following: acknowledgement of the source, reference and date of the publication, and all notices set out on this page.

Equens was founded by Interpay Nederland
and Transaktionsinstitut für Zahlungsverkehrsdienstleistungen

Content

1	Introduction.....	6
1.1	Overview	7
1.2	Document name and identification.....	8
1.3	PKI participants	8
1.4	Certificate Usage.....	9
1.5	Policy administration	10
1.6	Definitions and acronyms	10
2	Publication and Repository Responsibilities.....	11
2.1	Repositories	11
2.2	Publication of certification information.....	11
2.3	Time or frequency of publication.....	11
2.4	Access controls on repositories.....	11
3	Identification and Authentication	12
3.1	Naming	12
3.2	Initial identity validation.....	13
3.3	Identification and authentication for re-key requests	14
3.4	Identification and authentication for revocation request	16
4	Certificate Life-Cycle Operational Requirements.....	17
4.1	Certificate Application	17
4.2	Certificate application processing.....	18
4.3	Certificate issuance	18
4.4	Certificate acceptance.....	19
4.5	Key pair and Certificate usage.....	19
4.6	Certificate renewal	20
4.7	Certificate re-key	21
4.8	Certificate modification	21
4.9	Certificate revocation and suspension.....	22
4.10	Certificate status services.....	26
4.11	End of subscription.....	26
4.12	Key escrow and recovery.....	26

5	Facility, Management and Operational Controls	27
5.1	Physical controls	27
5.2	Procedural controls.....	28
5.3	Personnel controls.....	29
5.4	Audit logging procedures.....	30
5.5	Records archival	31
5.6	Key changeover	31
5.7	Compromise and disaster recovery	31
6	Technical Security Controls.....	32
6.1	Key pair generation and installation	32
6.2	Private Key Protection and Cryptographic Module Engineering Controls ...	32
6.3	Other aspects of key pair management	34
6.4	Activation data	34
6.5	Computer security controls	35
6.6	Network security controls	35
6.7	Time-stamping	35
7	Certificate, CRL and OCSP Profiles	36
7.1	Certificate profile	36
7.2	CRL profile	38
7.3	OCSP profile.....	39
8	Compliance Audit and other Assessments.....	40
8.1	Frequency or circumstances of assessment	40
8.2	Identity/qualifications of assessor.....	40
8.3	Assessor's relationship to assessed entity	40
8.4	Topics covered by assessment	40
8.5	Actions taken as a result of deficiency.....	40
8.6	Communication of results	41

9	Other Business and Legal Matters	42
9.1	Fees	42
9.2	Financial responsibility	42
9.3	Confidentiality of business information	42
9.4	Privacy of personal information	43
9.5	Intellectual property rights	44
9.6	Representations and warranties	45
9.7	Disclaimers of warranties	46
9.8	Limitations of liability.....	46
9.9	Indemnities.....	46
9.10	Term and termination	47
9.11	Individual notices and communications with participants	47
9.12	Amendments	47
9.13	Dispute resolution provisions	48
9.14	Governing law	48
9.15	Compliance with applicable law	48
9.16	Miscellaneous provisions	48
9.17	Other provisions	49
	Annex 1 Acronyms and Definitions	50

1 Introduction

The Equens Private Public Key Infrastructure (PKI) is a private PKI with the objective to provide a secure infrastructure between Equens and the banks, and between Equens and bank clients i.e. the corporates. The Equens Private PKI is to enable and accommodate financial transactions and related financial information of web-applications using the Equens Portal via this secure infrastructure.

This document "Equens Certificate Policy" is the principal statement of policy governing this Equens Private PKI. The CP sets forth the business, legal, and technical requirements for approving, issuing, managing, using, revoking and renewing digital certificates to be used within this Private PKI, and providing associated trust services for all participants within this Private PKI.

These requirements protect the security and integrity of the Equens Private PKI and comprise a single set of rules that apply consistently Private PKI-wide, and thereby providing assurances of uniform trust throughout this Private PKI. The CP is not a legal agreement between Equens and Private PKI participants; rather, contractual obligations between Equens and Private PKI participants are established by means of agreements with such participants.

This document is targeted at:

- The Equens Private PKI service provider, Getronics PinkRocade, who has to operate in terms of their own Certificate Practice Statement (CPS) and to comply with the requirements laid down by this CP,
- The Registration Authority (RA) organisation at Equens which organisation is responsible for validating certificate requests and approving the issuing of certificates according to this CP,
- Private PKI Certificate Subscribers who need to understand how they are authenticated and what their obligations are Private PKI Certificate Subscribers
- Relying parties who need to understand how much trust to place in a private-PKI certificate, or a digital signature using that certificate.

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

1.1 Overview

This CP sets out the policies under which the Private PKI participants must operate.

In particular this CP is relevant for Getronics PinkRoccade that operates the Equens Private PKI Certificate Authority (CA) and provides the infrastructure for the Managed PKI Service for the Equens Private PKI. The Managed PKI Service enables the Managed PKI Equens RA (Registration Authority) at Equens to validate certificate requests, approve the issuing of certificates, request the revocation or renewal of Certificates according to the CP. The Managed PKI Administrator(s) at Equens are authorised to operate the Managed PKI Equens RA at Equens. Getronics PinkRoccade performs all the back-end Certificate issuance, management, revocation, and renewal functions.

1.1.1 Equens Certificate Policy Overview

Equens Private PKI offers according to the Equens Certificate Policy the following types of certificates depending on certificate usage and how the subscriber is authenticated by Equens:

- Organisational Managed PKI Certificates issued to organisations; these organisations can be the processor Equens, banks and bank clients (corporations),
- Class 3 Managed PKI Administrator Certificates.

Organisational Managed PKI Certificates are issued to devices to provide authentication; message, software, and content integrity; and confidentiality encryption. Organisational Managed PKI Certificates provide assurances of the identity of the Subscriber based on a confirmation that the Subscriber organisation does in fact exist, that the organisation has authorised the Certificate Application, and that the person submitting the Certificate Application on behalf of the Subscriber was authorised to do so.

The Class 3 Managed PKI Administrator Certificates are issued to the individuals responsible for operating the Managed PKI RA at Equens.

These types of Certificates are to be used for the Equens services called WebServices and Connectivity. These services consist currently of the following: WebServices offered by Equens at the Equens Portal (for example AIS (Advanced Information Service), SIB (Block Selected Direct Debit Mandates), etc. Payments from banks using transport channels such as I-Connect Direct Authorisation of payments (Fiattering) by banks using the transport-protocol/channel MQ, Payments from bank client using transport channel such as I-Connect 2 FTP.

WebServices will also use the following type of Certificate:

- Secure Server Class 3 organisational Certificates from the public VeriSign Trust Network (VTN) to be used as the Equens host Server SSL Certificate.

The management of Secure Server Certificates is according to the VeriSign Trust Network Certificate Policies, Version 2.3 and Getronics PinkRoccade CPS. The CP of the Equens Private PKI will therefore *not* describe the Certificate Policy of Secure Server Certificates.

1.2 Document name and identification

This document is the Equens Certificate Policy (CP). Equens acting as the policy-defining authority has *not* assigned an object-identifier value extension for the different types of certificates.

1.3 PKI participants

1.3.1 Certification authorities

The term Managed PKI Equens Certificate Authority (CA) is a term that refers to the entity, called Root Certificate Authority, authorized to issue public key certificates to end-user subscribers within the Equens Private PKI. This Root CA does not have a superior CA but has a self-signed root Certificate.

1.3.2 Registration authorities

The Managed PKI Equens Registration Authority (RA) is an entity that performs identification and authentication of certificate applicants for end-user certificates, initiates or passes along revocation requests for end-user certificates, and approves applications for renewal or re-keying certificates on behalf of the Equens Private PKI. Equens acts as RA for certificates that are being issued.

This is affected by the RA-Administrators at Equens using the Managed PKI Equens RA. The Managed PKI Equens RA consists of workstations for RA-Administrators at Equens, which are connected via a secured https-connection to the Managed PKI Equens CA.

1.3.3 Subscribers

Subscribers under the Equens Private PKI are all end-users (including entities) of certificates issued by the Managed PKI Equens CA. A subscriber is the entity named as the end-user Subscriber of a certificate. End-user Subscribers may be individuals, organisations, or infrastructure components such as firewalls, trusted servers or other devices used to secure communications within an Organisation. Two different terms are used in this CP to distinguish between two roles. The term "Subscriber" is the entity that has a contract with Equens for the issuance of the credentials in the certificate, and the term "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.

1.3.4 Relying parties

A Relying Party is an individual or an entity that acts in reliance of a certificate and/or a digital signature issued under the Equens Private PKI. A Relying Party may or may not also be a Subscriber within the Equens Private PKI.

1.3.5 Other participants

The Processing Centre of Getronics PinkRocade is an entity that facilitates the secure issuing of Certificates for the Equens Private PKI. It is responsible for the secure housing of among other things of cryptographic modules for the issuing of these certificates.

Getronics PinkRocade acts as the CA within the Equens Private PKI and performs all Certificate lifecycle services such as issuing, revoking and renewing of certificates upon the request of Equens acting as RA.

1.4 Certificate Usage

1.4.1 Appropriate certificate uses

The Equens Private PKI uses organisational certificates which are issued to Equens and either to banks or to bank clients as organisations. The certificates are issued only after it has been verified by Equens that the organisation legally exists and that the person who requests the certificate on behalf of the organisation is known at the organisation.

While the most common usages are included in the Table below, an organisational 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 this CP, by any CPS under which this certificate has been issued and any agreement with subscribers.

Certificate type	Issued to	Usage Content Signing	Usage Key Encryption for Secure SSL session
Organisational Managed PKI	Equens, Banks and Bank clients Specialized confirmation procedures using Managed PKI.	To be used for WebServices	To be used for Connectivity
Class 3 Administrator Certificates	Managed PKI Administrator	To validate the identity of MPKI Administrator	To validate the identity of MPKI Administrator

Table 1: Description of Certificates types

1.4.2 Prohibited certificate uses

The certificates are to be used only within the Equens Private PKI. Further the certificates shall be used only to the extent the use is consistent with applicable law, and to the extent permitted by Dutch export and import laws.

1.5 Policy administration

1.5.1 Organization administering the document

Equens Nederland B.V.
Postbus 30500
3503 AH Utrecht
The Netherlands

1.5.2 Contact person

The Equens Certificate Policy Manager
Equens Policy Management Authority
Department Equens Risk Management
c/o Equens Nederland B.V.
Postbus 30500
3503 AH Utrecht
The Netherlands
Tel.: 00 31 - (0)30 283 5111 / 6531
Web-site: http://www.equens.com/Support/Manuals/Connectivity_services.asp

1.5.3 Person determining CP suitability for the policy

The Equens Policy Management Authority (PMA) determines the suitability and applicability of this CP.

1.5.4 CP approval procedures

Approval of this CP and subsequent amendments shall be made by the PMA. Amendments shall either be in the form of a document containing an amended form of the CP or an update notice. Amended versions or notices shall be located at http://www.equens.com/Support/Manuals/Connectivity_services.asp.

Updates supersede any designated or conflicting provisions of the referenced version of the CP. The PMA shall determine whether changes to the CP require change in the Certificate Policy object identifiers corresponding to each type of Certificate.

1.6 Definitions and acronyms

See Appendix A for a table of acronyms and definitions.

2 Publication and Repository Responsibilities

2.1 Repositories

Getronics publishes, as part of their contract with Equens, Certificates for the Equens Private PKI based on the information provided by Managed PKI Equens RA. Getronics PinkRoccade publishes also in a repository as part of that same contract revocation information concerning such Certificates.

2.2 Publication of certification information

Getronics PinkRoccade hosts the following repository on behalf of the Equens Private PKI:

<https://mpki.pinkroccade.com/services/InterpayNederlandBV001/digitalidCenter.htm>

In this repository, Getronics PinkRoccade publishes the Certificates which are issued by the CA of Equens Private PKI and the Certificates of the CA itself.

Upon revocation of an end-user Subscriber's Certificate within the Equens Private PKI, Getronics PinkRoccade will publish notice of such revocation in this repository.

In addition Getronics PinkRoccade shall publish a Certificate Revocation List (CRL) regarding bankclient-type certificates in the following CRL-distributionpoint

<http://pki.pinkroccade.com/crl/InterpayNederlandBV001/LatestCRL.crl>.

2.3 Time or frequency of publication

Getronics PinkRoccade shall publish a Certificate Revocation List (CRL) at least once a day.

Whenever a CA-certificate is revoked, a CRL concerning the revocation of CA Certificates will be issued immediately. Expired certificates are removed from the CRL starting thirty (30) days after the Certificate's expiration. The CRL's are signed by the CA of the Equens Private PKI that issued the Certificate.

2.4 Access controls on repositories

Getronics PinkRoccade shall not intentionally use technical means of limiting access to the Certificates, Certificate status information, or CRL's related to the Equens Private PKI. Getronics PinkRoccade shall implement controls to prevent unauthorized persons from adding, deleting, or modifying repository entries.

Getronics PinkRoccade as an affiliate of Verisign shall require persons to agree to a Relying Party Agreement or CRL Usage Agreement as a condition to accessing Certificates, Certificate status information, or CRL's related to the Equens Private PKI.

3 Identification and Authentication

3.1 Naming

Unless where indicated otherwise in this CP, the relevant CPS or the content of the digital certificate, names appearing in Certificates issued under the Equens Private PKI are authenticated.

3.1.1 Types of names

The Certificates issued under the Equens Private PKI contain X.501 Distinguished Names in the Issuer and Subject fields.

The Equens Private PKI CA Distinguished Name consists of the following components specified in the Table below.

Attribute	Value
Country (C)	"NL"
Organisation (O)	"Interpay Nederland B.V."
Organisational Unit (OU)	Not used
State (S)	Not used
Locality (L)	Not used
Common Name (CN)	"Interpay Root CA"

Table 2: Equens Private PKI CA Distinguished Name

The end-user Subscriber Certificates issued under a CA for the Equens Private PKI contain a X.501 distinguished name in the Subject Name field and consist of the components specified in the Table below.

Attribute	Value
Country (C)	"NL"
Organisation (O)	Subscriber organisational name (for web server Certificates using http-based application)
Organisational Unit (OU)	Subscriber organisational unit
State (S)	Indicates the Subscriber Province
Locality (L)	Not used
Common Name (CN)	Domain name (for web server Certificates using http-based application)

Table 3: End-user Subscriber Certificates Distinguished Name

The Common Name (CN) component of the Subject distinguished name of the end-user Subscriber Certificates under the Equens Private PKI is authenticated.

3.1.2 Need for names to be meaningful

The end-user Subscriber Certificates issued by the Equens Private PKI CA contain names with commonly understood semantics permitting the determination of the identity of the organisation that is the Subject of the Certificate.

For such Certificates, pseudonyms of end-user Subscriber Certificates (names other than a Subscriber's true organisational name) are **not** permitted.

3.1.3 Anonymity or pseudonym of subscribers

See §3.1.2 above.

3.1.4 Rules for interpreting various name forms

No stipulation.

3.1.5 Uniqueness of names

The Managed PKI Equens RA ensures that Subject Distinguished Names are unique within the Equens Private PKI through automated components of the Subscriber enrolment process.

3.1.6 Recognition, authentication, and role of trademarks

Certificate Applicants shall not use names in their Certificate Applications that infringe upon the Intellectual Property Rights of others.

Getronics PinkRoccade acting as CA and Equens acting as RA do not verify whether a Certificate Applicant has Intellectual Property Rights in the name appearing in a Certificate Application or to arbitrate, mediate, or otherwise resolve any dispute concerning the ownership of any domain name, trade name, trademark, or service mark. Getronics PinkRoccade and Equens are entitled without liability to any Certificate Applicant to reject, or suspend any Certificate Application because of such dispute.

3.2 Initial identity validation

3.2.1 Method to prove possession of private key

The Equens Private PKI CA verifies the Certificate Applicant's possession of a private key through the use of a digitally signed certificate request pursuant to PKCS#10 (Certificate Signing Request).

3.2.2 Authentication of organization identity

See Getronics PinkRoccade CPS §3.1.9.1.1 Manual Authentication procedure for Organisational Managed PKI Certificates (and §3.1.8.2 Authentication of the identity of CA's and RA's).

3.2.3 Authentication of individual identity

See Getronics PinkRoccade CPS §3.1.9.3.1 Class 3 Administrator Certificates.

3.2.4 Non-verified subscriber information

Non-verified subscriber information includes:

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

3.2.5 Validation of authority

See Getronics PinkRoccade CPS §3.1.9.3.1 Class 3 Administrator Certificates.

3.2.6 Criteria for interoperation

The Equens Private PKI is a private PKI that is only used for services provided by Equens to entities within this private PKI. Therefore, the Equens Private PKI cannot provide interoperation services that allow a non-Equens Private PKI CA to unilaterally certify the Managed PKI Equens PKI CA in order to interoperate with that CA.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

Prior to the expiration of an existing Subscriber's Certificate, it is necessary for the Subscriber to obtain a new certificate to maintain continuity of Certificate's usage. The Equens Private PKI requires for end-user Subscriber Certificates that the Subscriber generates a new key pair to replace the expiring key pair (technically defined as "rekey"). However for other type Certificates, the Equens Private PKI permits that a new certificate is requested for an existing key pair (technically defined as "renewal"). The Table below describes the requirements for routine rekey and renewal.

Certificate Type	Routine Rekey and Renewal Requirements
Organisational Managed PKI (within 30 days before and 30 days after Certificate expiration)	The Managed PKI process at Equens authenticates Subscribers seeking Certificate replacement through the use of a Challenge Phrase. As part of the initial registration process, Subscribers choose and submit a Challenge Phrase with their enrolment information. Upon rekey of a Certificate within the specified timeframe, if a Subscriber correctly submits the Subscriber's Challenge Phrase (or equivalent thereof) with the Subscriber's enrolment information, <i>or</i> proves possession of the private key, and the enrolment information (including contact information) has not changed, a new Certificate is automatically issued. After rekeying in this fashion and on at least alternative instances of subsequent rekeying or renewal, the Equens Private PKI shall reconfirm the identity of the Subscriber in accordance with the requirements specified in the Getronics PinkRocade CPS §3.1.8.1 for the authentication of an original Certificate Application.
Organisational Managed PKI (beyond 30 days after Certificate expiration)	In this scenario, the requirements as specified in §3.2 for the authentication of an original Certificate Application are used for replacing an end-user Subscriber certificate.
Class 3 Administrator Certificates	For this type of Certificates, Subscriber key pairs are browser generated as part of the online enrolment process. The Subscriber does not have the option to submit an existing key pair for renewal. Accordingly for this type of certificates only rekey is supported.

Certificate Type	Routine Rekey and Renewal Requirements
CA Certificates	Renewal of CA Certificates is permitted as long as the cumulative certified lifetime of the CA key pair does not exceed the applicative maximum CA key pair lifetime specified in the Getronics PinkRoccade CPS §6.3.2. The CA's may also be rekeyed in accordance with the CPS §4.7. Accordingly, for CA Certificates both rekey and certificate renewal are supported. The renewal requests are created and approved by authorised Getronics PinkRoccade personnel through a controlled process that requires the participation of multiple trusted individuals.

Table 4: Routine Rekey and Renewal requirements per Certificate type

3.3.2 Identification and authentication for re-key after revocation

Rekey after revocation is not permitted if:
 Revocation occurred because the Certificate was issued to a person other than the one named as the Subject of the Certificate,
 The certificate was issued without the authorisation of the person named as the Subject of such Certificate, or
 The entity approving the Subscriber's Certificate Application discovers or has reason to believe that a material fact in the Certificate application is false.

Subject to the foregoing paragraph, End-user Subscriber's Certificates such as Organisational Managed PKI Certificates for banks and bankclients which have been revoked, may be replaced (i.e. rekeyed) in accordance with the table below.

Timing	Requirement
Prior to Certificate expiration	For replacement of an organisational or individual Certificate following revocation of the Certificate, the RA-process at Equens verifies that the person seeking certificate replacement, is in fact the Subscriber (for individuals) or an authorised organisational representative (for organisation) through the use of a Challenge Phrase as described in §3.3.1. Other than this procedure, the requirements for the validation of an original Certificate Application as defined in §3.2 are used for replacing a certificate following revocation. Such Certificates contain the same Subject distinguished name as the Subject distinguished name of the Certificate being replaced.
After Certificate expiration	In this scenario, the requirements as specified in §3.2 for the authentication of an original Certificate Application are used for replacing an end-user Subscriber certificate.

Table 5: Replacement revoked end-user Certificates

3.4 Identification and authentication for revocation request

Revocation procedures ensure prior to any revocation of a Certificate that the revocation has in fact been requested by the Certificate's Subscriber, Equens acting as RA, or Getronics PinkRocade acting as CA. Acceptable procedures for authenticating Subscriber revocation requests include:

- Having the Subscriber submit the Subscriber's Challenge Phrase and revoking the Certificate automatically if it matches the Challenge Phrase on record.
- Receiving a message purporting to be from the Subscriber that requests revocation and contains a digital signature verifiable with the Certificate to be revoked, and
- Communication with the Subscriber providing reasonable assurances in light of the Class of Certificate that the person or organisation requesting revocation is in fact the Subscriber. Depending on the circumstances such communication may include one or more of the following: telephone, facsimile, e-mail, postal mail, or courier service.

The Equens Private PKI CA authenticates the identity of Administrators via access control using SSL and client authentication before permitting them to perform revocation functions.

The requests by Equens using a Managed PKI system to revoke a CA certificate are authenticated by Getronics PinkRocade to ensure that the revocation has in fact been requested by the Managed PKI Equens CA.

4 Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who can submit a certificate application

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

- Any individual who is the subject of the certificate,
- Any authorised individual of an organisation or entity,
- Any authorised individual of Getronics PinkRoccade as CA,
- Any authorised individual of Equens as RA

4.1.2 Enrolment process and responsibilities

4.1.2.1 End-user Certificate Subscribers

All end-user Certificate Subscribers shall manifest assent to the relevant Subscriber Agreement (*verify Legal/M&S*) that contains representations and warranties described in §9.6.3 and undergo an enrolment process consisting of:

- Completing a Certificate Application and providing true and correct information,
- Generating, or arranging to have generated a key pair in accordance with Getronics PinkRoccade CPS §6.1,
- Delivering his, her, or its public key through the Managed PKI Equens as RA to Getronics PinkRoccade as CA in accordance with Getronics PinkRoccade CPS §6.1.3,
- Demonstrating to the Equens Private PKI CA in accordance with §3.2.1 possession of the private key corresponding to the public key delivered to the Managed PKI Equens RA.

4.1.2.2 CA Certificates

Equens as Subscriber of the Equens Private PKI CA Certificate with CommonName "Interpay Root CA" for the Equens Private PKI enters into a contract with Getronics PinkRoccade that issues the CA. The CA Certificate Applicants from Equens provides their credentials as required by the Getronics PinkRoccade CPS §3.1.8.2 to demonstrate their identity and provide contact information during the contracting process. During this contracting process or at the latest prior to the Key Generation Ceremony to create a CA key pair for the Equens Private PKI, Equens shall cooperate with Getronics PinkRoccade to determine the appropriate distinguished name and the content of the Equens Private PKI CA Certificates to be issued to Equens. For these CA's within the Equens Private PKI certificate requests are created and approved by authorised Getronics PinkRoccade personnel through a controlled process that requires the participation of multiple trusted individuals.

4.1.2.3 Managed PKI Equens RA Certificates

Getronics PinkRoccade operates an Administrative CA which issues certificates to Managed PKI Equens personnel (Managed PKI Administrators) who process Certificate Applications on behalf of the Managed PKI Equens RA.

For the Managed PKI Equens RA as subscriber to the relevant Administrative CA the requirements for Class 3 Administrator Certificates specified in §4.1.2.1 apply.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

The Managed PKI Equens RA shall perform identification and authentication of all Subscriber information in terms of Section 3.2.

4.2.2 Approval or rejection of certificate applications

If the identification and authentication of all required Subscriber information in terms of Section 3.2 is successful, the Managed PKI Equens RA will approve a Certificate Application.

The Managed PKI Equens RA will reject a Certificate Application if:

- Identification and authentication of all required Subscriber information in terms of Section 3.2 cannot be completed, or
- The Subscriber fails to furnish supporting documentation upon request, or
- The Subscriber fails to respond to notices within a specified time, or
- Equens as RA believes that issuing a certificate to the Subscriber may bring the Equens Private PKI into disrepute.

4.2.3 Time to process certificate applications

The Managed PKI RA and CA together will process Certificate Applications within a reasonable time of receipt. There is no time stipulation to complete the processing of a Certification Application unless indicated in the Subscriber Agreement, Equens CPS or other agreement between Equens Private PKI participants.

4.3 Certificate issuance

4.3.1 Issuance of End-user Subscriber Certificates

4.3.1.1 CA actions during certificate issuance

A Certificate is created and issued by the Managed PKI CA following the approval of a Certificate Application by the Managed PKI Equens RA. The Managed PKI CA creates and issues to a Certificate Applicant a Certificate based on the information in a Certification Application following the receipt from the Managed PKI Equens RA to issue such a Certificate.

4.3.1.2 Notification to Subscriber by the CA of issuance of certificate

The Managed PKI CA issuing Certificates to end-user Subscribers shall notify Subscribers through the Managed PKI Equens that they have created such Certificates, and provide Subscribers the Certificates via a message sent to the Subscriber containing the Certificate as described in §3.2.

4.3.2 Issuance of Equens Private PKI CA and RA Certificates

Getronics PinkRoccade authenticates the identity of the Equens CA and RA Applicant in accordance with the Getronics PinkRoccade CPS §3.1.8.2 and, upon approval issues the Certificates needed to perform the CA and/or RA functions for the Equens Private PKI. Before Getronics PinkRoccade enters into a contract with Equens under Getronics PinkRoccade CPS §4.1.2, the identity of the Equens CA and RA Applicant is confirmed based on credentials presented. The execution of such a contract indicates the complete and final approval of the application by Getronics PinkRoccade. The decision to approve or reject application of the Equens

application is solely at the discretion of Getronics PinkRoccade. Following such approval, Getronics PinkRoccade issues the Certificate(s) to the Equens Private PKI CA and corresponding Managed PKI Equens RA.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

The Managed PKI Equens RA sends the Subscriber a PIN which the Subscriber enters into the enrolment web page to obtain the Certificate. Downloading all the Certificates in the CA Chain including the CA Certificate by the Subscriber constitutes acceptance of all the Certificates in the CA Chain.

4.4.2 Publication of the Certificate by the CA

The Managed PKI CA publishes the Certificates they issue in a public accessible repository for the Equens Private PKI.

The CA Certificate of the Equens Private PKI is not published but downloaded in the Certificate Chain.

4.4.3 Notification of certificate issuance by the CA to other entities

The Managed PKI Equens RA automatically receives notification from the Managed PKI CA of the actual issuance of the Certificates that have been approved by the Managed PKI Equens RA. The issued Certificates are available at the repository for the Equens Private PKI.

The CA Certificates are automatically downloaded in the CA Chain.

4.5 Key pair and Certificate usage

4.5.1 Subscriber private key and certificate usage

Use of the Private key corresponding to the public key in the Certificate shall only be permitted once the Subscriber has agreed to the Equens Subscriber Agreement and accepted the Certificate. The Certificate shall be used lawfully in accordance with the Subscriber Agreement in terms of this CP and the relevant CPS.

Certificate use must be consistent with the KeyUsage field extensions included in the Certificate (e.g. if Digital Signature is not enabled then the Certificate must not be used for signing).

Subscribers shall protect their private keys from unauthorised use and shall discontinue use of the private key following expiration or revocation of the Certificate.

4.5.2 Relying party public key and certificate usage

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

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

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

- The appropriateness of the use of the Certificate for any given purpose and determine that the Certificate will, in fact be used for an appropriate purpose that is not prohibited or otherwise restricted by this CP,

- that the certificate is being used in accordance with the KeyUsage field extensions included in the certificate (e.g. if Digital Signature is not enabled then the certificate may not be relied upon for validating a Subscriber's signature),
- the status of the certificate and all the CA's in the chain of the Equens Private PKI that issued the certificate. If any of the Certificates in the Certificate Chain have been revoked, the Relying party is solely responsible to investigate whether reliance on a digital signature performed by the end-user Subscriber Certificate prior to the revocation of a Certificate in the Certificate Chain is reasonable. Any such reliance is made solely at the risk of the Relying Party.

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

4.6 Certificate renewal

Certificate renewal is the issuance of a new certificate to the Subscriber without changing the existing key pair. The Equens Private PKI permits renewal for CA Certificates but not for end-user Subscriber Certificates.

4.6.1 Circumstance for certificate renewal

Prior to the expiration of an existing CA Certificate, it is necessary to renew the Certificate to maintain continuity of Certificate usage. A certificate may also be renewed after expiration.

4.6.2 Who may request renewal

The request of renewal of CA Certificates follows the same procedure as generation of CA certificates as described in Getronics PinkRocade CPS 3.1.8.2.

4.6.3 Processing certificate renewal requests

See § 3.3 of this CP. Renewal of the CA certificate is done according to Getronics PinkRocade CPS §4.7 and 6.3.2.

4.6.4 Notification of new certificate issuance to subscriber

See §4.3.2.

4.6.5 Conduct constituting acceptance of a renewal certificate

See §4.4.1.

4.6.6 Publication of the renewal certificate by the CA

See §4.4.2.

4.6.7 Notification of certificate issuance by the CA to other entities

See §4.4.3

4.7 Certificate re-key

Certificate re-key is the application for the issuance of a new certificate with a new key pair to replace the expiring key pair. The Equens Private PKI requires Certificate re-key for end-user Subscriber Certificates and for CA Certificates.

4.7.1 Circumstance for certificate re-key

Prior to the expiration of an existing end-user Subscriber Certificates and/or CA Certificate, it is necessary to renew the Certificate to maintain continuity of Certificate usage. A Certificate may also be renewed after expiration.

4.7.2 Who may request certification of a new public key

Only the subscriber for an individual Class 3 Managed PKI Administrator Certificate or an authorised representative for an Organisational Managed PKI Certificate may request Certificate re-key.

4.7.3 Processing certificate re-keying requests

See §4.1.2 and 4.2.

4.7.4 Notification of new certificate issuance to subscriber

See §4.3.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

See §4.4.1.

4.7.6 Publication of the re-keyed certificate by the CA

See §4.4.2.

4.7.7 Notification of certificate issuance by the CA to other entities

See §4.4.3.

4.8 Certificate modification

4.8.1 Circumstance for certificate modification

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

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

4.8.2 Who may request certificate modification

See §4.1.1.

4.8.3 Processing certificate modification requests

See §4.1.2 and 4.2.

4.8.4 Notification of new certificate issuance to subscriber

See §4.3.

4.8.5 Conduct constituting acceptance of modified certificate

See §4.4.1.

4.8.6 Publication of the modified certificate by the CA

See §4.4.2.

4.8.7 Notification of certificate issuance by the CA to other entities

See §4.4.3.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

4.9.1.1 Circumstances for Revoking End-User Subscriber Certificates

Reasons for revocation of an end-user Subscriber Certificate are:

- Equens or a Subscriber has reason to believe or strongly suspects that there has been a Compromise of a Subscriber's private key,
- Equens has reason to believe that the Subscriber has materially breached a material obligation, representation, or warranty under the applicable Subscriber Agreement,
- The Subscriber Agreement with the Subscriber has been terminated,
- Equens or the Subscriber of the Certificate has reason to believe that the Certificate was issued in a manner not materially in accordance with the procedures required by the applicable CPS, the Certificate was issued to a person other than the one named as the Subject of the Certificate, or the Certificate was issued without the authorization of the person named as the Subject of such Certificate,
- Equens or the Subscriber of the Certificate has reason to believe that a material fact in the Certificate Application is false,
- Equens or Getronics PinkRoccade determines that a material prerequisite to Certificate Issuance was neither satisfied nor waived,
- The information within the Certificate is incorrect or has changed, or
- The Subscriber requests revocation of the Certificate in accordance with Getronics PinkRoccade CPS §4.9.3.1,
- The private key is corrupt.

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

(Equens Subscriber Agreements require end-user Subscribers to immediately notify Getronics PinkRoccade of a known or suspected compromise of its private key in accordance with the procedures in Getronics PinkRoccade CPS § 4.4.3.1.)

4.9.1.2 Circumstances for Revoking CA or RA Certificates

Getronics PinkRoccade will revoke CA or RA Certificates of the Equens Private PKI if:

- Getronics PinkRoccade discovers or has reason to believe that there has been a compromise of the relevant CA or RA private key,
- The agreement between Equens with Getronics PinkRoccade with respect to the Equens Private PKI has been terminated,

- Getronics PinkRoccade discovers or has reason to believe that the Certificate was issued in a manner not materially in accordance with the procedures required by this Equens CP and CPS, the Certificate was issued to an entity other than the one named as the Subject of the Certificate, or the Certificate was issued without the authorization of the entity named as the Subject of such Certificate,
- Getronics PinkRoccade determines that a material prerequisite to Certificate issuance was neither satisfied nor waived, or
- The Managed PKI Equens requests revocation of the Certificate of the Equens Private PKI CA or RA.

Getronics PinkRoccade requires that the Managed PKI Equens notify Getronics PinkRoccade when revocation is required in accordance with the procedures in Getronics PinkRoccade CPS § 4.4.3.3.

4.9.2 Who can request revocation

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

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

- The Managed PKI Equens RA which approved the Subscriber's Certificate Application may request the revocation of any end-user Subscriber or Administrator Certificates in accordance with 4.9.1.1.
- For the Organisational Managed PKI Certificates, only a duly authorized representative of the organization is entitled to request the revocation of Certificates issued to the organization.
- The duly authorized representative of the Managed PKI Equens RA whose Administrator received an Administrator Certificate is entitled to request the revocation of an Administrator's Certificate.

4.9.2.2 Who Can Request Revocation of a CA or RA Certificate

The following entities may request revocation of a CA or RA Certificate of the Equens Private PKI:

- Getronics PinkRoccade may initiate the revocation of the Equens Private PKI CA or RA Certificate in accordance with CPS § 4.9.1.2.
- The Managed PKI Equens RA is entitled, through their duly authorized representatives, to request the revocation of the relevant CA and RA Certificates belonging to the Equens Private PKI.

4.9.3 Procedure for revocation request

For Managed PKI customers, the end-user Subscriber is required to communicate the request to the Managed PKI Administrator who will communicate the revocation request to Getronics PinkRoccade for processing. Communication of such revocation request shall be in accordance with the Getronics PinkRoccade CPS § 3.4.

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

The end-user Subscriber requesting revocation is required to communicate the request to the Managed PKI Administrator who will communicate the revocation request to the Equens Private PKI CA at Getronics PinkRoccade for processing. In case the Managed PKI Equens RA initiates revocation of an end-

Equens Certificate Policy

WebServices and Connectivity

user Subscriber Certificate upon its own initiative, it will instruct as such the Equens Private PKI CA at Getronics PinkRoccade to revoke the Certificate. Prior to the revocation of a Certificate, the Equens Private PKI CA verifies that the revocation has been requested by the Certificate's Subscriber, or by the Managed PKI Equens RA. Acceptable procedures for authenticating Subscriber revocation requests include:

- Having the Subscriber submit the Subscriber's Challenge Phrase and revoking the Certificate automatically if it matches the Challenge Phrase on record,
- Receiving a message purporting to be from the Subscriber that requests revocation and contains a digital signature verifiable with reference to the Certificate to be revoked, and
- Communication with the Subscriber providing reasonable assurances in light of the Class of Certificate that the person or organization requesting revocation is, in fact the Subscriber. Depending on the circumstances, such communication may include one or more of the following: telephone, facsimile, e-mail, postal mail, or courier service.

The Equens Private PKI CA and RA shall process the revocation requests and reports upon receipt. The Equens Private PKI CA at Getronics PinkRoccade authenticates the identity of Administrators via access control using SSL and client authentication before permitting them to perform revocation functions. The Subscriber whose Certificate was revoked shall be informed of the revocation. Certificates that are revoked shall not be reinstated as valid Certificates. Certificates that are revoked will not be reinstated as valid Certificates.

(Managed PKI Equens using the Automated Administration Software Module may submit bulk revocation requests to Getronics PinkRoccade. Such requests are authenticated via a request digitally signed with the private key in the Managed PKI Equens Automated Administration hardware token.)

4.9.3.2 Procedure for Requesting the Revocation of the Equens Private PKI CA or RA Certificate

The Equens Private PKI CA or RA requesting revocation of its CA or RA Certificate is required to communicate the request to Getronics PinkRoccade. This request is authenticated by Getronics PinkRoccade to ensure that the revocation has in fact been requested by the Managed PKI Equens. Getronics PinkRoccade will then revoke the Certificate.

Getronics PinkRoccade may also initiate revocation of the Equens Private PKI CA or RA Certificate.

4.9.4 Revocation request grace period

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

4.9.5 Time within which Equens Private PKI CA must process the revocation request

Commercially reasonable steps are taken to process revocation requests without delay by the Managed PKI Equens CA.

4.9.6 Revocation checking requirement for relying parties

Relying Parties must check the status of Certificates on which they wish to rely.

The Equens Private PKI CA communicates via a CRL-distributionpoint in the Certificate the specific repository for the Equens Private PKI where CRL's are posted: <http://pki.pinkroccade.com/crl/InterpayNederlandBV001/LatestCRL.crl>

4.9.7 CRL issuance frequency (if applicable)

The Equens Private PKI CA publishes CRL's showing the revocation of Certificates for the Equens Private PKI. CRL's for the Equens Private PKI CA that issue end-user Subscriber Certificates are published at least once per day. Expired Certificates are removed from the CRL starting thirty (30) days after the Certificate's expiration. CRL's are signed by the Equens Private PKI CA that issued the Certificate. A new CRL may be published before the stated time of the next CRL to be issued.

4.9.8 Maximum latency for CRLs (if applicable)

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

4.9.9 On-line revocation/status checking availability

In addition to publishing CRLs, the Equens Private PKI CA provides Certificate status information through web-based query functions accessible through the Equens Private PKI repository at:

<https://mpki.pinkroccade.com/services/InterpayNederlandBV001/digitalidCenter.htm>

4.9.10 On-line revocation checking requirements

If a Relying Party does not check the status of a Certificate on which the Relying Party wishes to rely by consulting the most recent relevant CRL, the Relying Party must check Certificate status using the applicable method specified in §4.9.9.

4.9.11 Other forms of revocation advertisements available

Not applicable.

4.9.12 Special requirements regarding key compromise

Equens shall be notified by Getronics PinkRocade, as responsible party for operating the Managed PKI Equens CA, of an actual or suspected Equens Private PKI CA private key Compromise using commercially reasonable efforts. Equens shall commercially reasonable efforts to notify Relying Parties of the Equens Private PKI if it discovers or is being notified or has reason to believe that there has been a Compromise of the private key of the Managed PKI Equens CA.

4.9.13 Circumstances for suspension

The Equens Private PKI does not offer suspension services for CA or end-user Subscriber Certificates.

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 services

4.10.1 Operational characteristics

As described in §4.9.6 and 4.9.9 the Managed PKI CA provides the status of certificates via a CRL through the repository mentioned in the Certificate as CRL-distribution point, or at the Equens Private PKI LDAP directory for web-based query functions.

4.10.2 Service availability

The Managed PKI CA shall provide Certificate Status Services 24*7 hours without scheduled intervention.

4.10.3 Optional features

Not applicable.

4.11 End of subscription

A Subscriber may end a subscription for his Certificate of the Equens Private PKI by:

- Allowing his Certificate to expire without renewing or re-keying that Certificate, or
- Revoking of his Certificate before certificate expiration without replacing the Certificates.

4.12 Key escrow and recovery

It is not possible within the Equens Private PKI to escrow the private keys of the Equens Private PKI CA and RA, and/or end-user Subscribers.

4.12.1 Key escrow and recovery policy and practices

Not applicable.

4.12.2 Session key encapsulation and recovery policy and practices

Not applicable.

5 Facility, Management and Operational Controls

As Getronics PinkRoccade is responsible for operation of the Managed PKI Equens CA, it will be referred for the relevant policies for these items to the Getronics PinkRoccade CPS Chapter 5.

With respect to the Managed PKI Equens RA roles and functions under the responsibility of Equens, it is referred to the "Equens Netherlands Information Security Policy".

5.1 Physical controls

5.1.1 *Site location and construction*

See Getronics PinkRoccade CPS §5.1.1 for operation of the Managed PKI Equens CA.

The RA operations at Equens are performed in zone 1 according to "Equens Information Security Policy, Guideline for the Physical Security of the Equens Premises".

5.1.2 *Physical access*

See Getronics PinkRoccade CPS §5.1.2 for operation of the Managed PKI Equens CA.

The RA operations at Equens are performed in zone 1 according to "Equens Information Security Policy, Guideline for the Physical Security of the Equens Premises".

5.1.3 *Power and air conditioning*

See Getronics PinkRoccade CPS §5.1.3 for operation of the Managed PKI Equens CA.

The power and air conditioning of the area where the RA operations at Equens are, shall be according to the requirements for zone 1 as defined in "Equens Information Security Policy, Guideline for the Physical Security of the Equens Premises".

5.1.4 *Water exposures*

See Getronics PinkRoccade CPS §5.1.4 for operation of the Managed PKI Equens CA.

Measures to prevent water exposures in the area where the RA operations at Equens take place, shall be according to the requirements for zone 1 as defined in "Equens Information Security Policy, Guideline for the Physical Security of the Equens Premises".

5.1.5 *Fire prevention and protection*

See Getronics PinkRoccade CPS §5.1.5 for operation of the Managed PKI Equens CA.

Equens Certificate Policy

WebServices and Connectivity

Measures to prevent and to protect against fire in the area where the RA operations at Equens take place, shall be according to the requirements for zone 1 as defined in "Equens Information Security Policy, Guideline for the Physical Security of the Equens Premises".

5.1.6 Media storage

See Getronics PinkRoccade CPS §5.1.6 for operation of the Managed PKI Equens CA.

The storage of the Certificate Applications with the related identification data, the generated enrolment data by the RA Administrators at Equens shall be according to "Equens Information Security Policy, Guideline Media".

5.1.7 Waste disposal

See Getronics PinkRoccade CPS §5.1.7 for operation of the Managed PKI Equens CA.

The RA Administrators at Equens shall dispose media with data which is not anymore useful for the RA operations according to "Equens Information Security Policy, Guideline Media and Guideline for the Disposal and Destruction of Paper".

5.1.8 Off-site backup

See Getronics PinkRoccade CPS §5.1.8 for operation of the Managed PKI Equens CA.

Equens has an off-site backup for its RA operations.

5.2 Procedural controls

5.2.1 Trusted roles

The trusted roles that may materially affect:
the validation of information in Certificate Applications,
the acceptance, rejection, or other processing of Certificate Applications,
revocation requests, or renewal requests, or enrolment information,
or the handling of Subscriber information or requests,
are managed by Equens.

Persons seeking to fulfil a trusted role at Equens must successfully complete the screening requirements of the Equens Netherlands Information Security Policy.

The trusted roles that may materially affect:
the issuance or revocation of Subscriber Certificates and CA Certificates, including
personnel having access to restricted portions of its repository,
are managed by Getronics PinkRoccade.

Persons seeking to fulfil a trusted role at Getronics PinkRoccade must successfully complete the screening requirements of its CPS §5.3.

5.2.2 Number of persons required per task

See Getronics PinkRoccade CPS §5.2.2 with respect to the operation of the Equens Private PKI CA and its related trusted roles.

The trusted roles and related tasks mentioned in §5.2.1 which are managed by Equens deal with the operation of the Managed PKI Equens RA. Each task is done by one person. The roles as mentioned in §5.2.1 are separated between two departments within Equens.

5.2.3 Identification and authentication for each role

See Getronics PinkRoccade CPS §5.2.3 which is relevant also for the operation of the RA-workstations and related roles managed by Equens.

5.2.4 Roles requiring separation of duties

See Getronics PinkRoccade CPS §5.2.2 with respect to the operation of the Equens Private PKI CA and the trusted role managed by Getronics PinkRoccade.

The trusted roles and related tasks mentioned in §5.2.1 which are to be managed by Equens deals with the operation of the Managed PKI Equens RA. Each task is done by one person. The roles as mentioned in §5.2.1 are separated between two departments within Equens.

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

See Getronics PinkRoccade CPS §5.3.1 with respect to trusted personnel required for the trusted roles for operating the Equens Private PKI CA.

The "Equens Information Security Policy, Guideline Pre Employment Screening" describe the policies with respect to trusted personnel required for the trusted roles for operating the Managed PKI Equens RA at Equens.

5.3.2 Background check procedures

See Getronics PinkRoccade CPS §5.3.2 with respect to trusted personnel required for the trusted roles for operating the Managed PKI Equens CA.

The "Equens Information Security Policy, Guideline Pre Employment Screening" describe the policies with respect to trusted personnel required for the trusted roles for operating the Managed PKI Equens RA at Equens.

5.3.3 Training requirements

See Getronics PinkRoccade CPS §5.3.3 with respect to trusted personnel required for the trusted roles for operating the Managed PKI Equens CA.

The manager(s) of the trusted personnel required for the trusted roles for operating the Managed PKI Equens RA at Equens is/are responsible for having specific training requirements. These are defined in so called 'Flexi-matrix' between the manager and the personnel.

5.3.4 Retraining frequency and requirements

See Getronics PinkRoccade CPS §5.3.4 with respect to trusted personnel required for the trusted roles for operating the Managed PKI Equens CA.

The manager(s) of the trusted personnel required for the trusted roles for operating the Managed PKI Equens RA at Equens is/are responsible for updating having specific training requirements. These are updated in so-called 'flexi-matrix'.

Equens Certificate Policy

WebServices and Connectivity

5.3.5 Job rotation frequency and sequence

No stipulation.

5.3.6 Sanctions for unauthorized actions

See Getronics PinkRoccade CPS §5.3.6 with respect to trusted personnel required for the trusted roles for operating the Managed PKI Equens CA.

The "Equens Information Security Policy, chapter 'Employees and clients', §1.7.2 Sanctions" describe the process at Equens in case of unauthorised actions at the Managed PKI Equens RA.

5.3.7 Independent contractor requirements

See Getronics PinkRoccade CPS §5.3.7 with respect to trusted personnel required for the trusted roles for operating the Managed PKI Equens CA.

The "Equens Information Security Policies, chapter 'Employees and clients', §1.6. Security requirements for relationships / third parties" describe the requirements for independent contractors at the Managed PKI Equens RA.

5.3.8 Documentation supplied to personnel

See Getronics PinkRoccade CPS §5.3.8 with respect to trusted personnel required for the trusted roles for operating the Managed PKI Equens CA.

The Equens personnel involved in the operation of the Managed PKI Equens RA are supplied with the Equens Nederland Information Security Policy and Guidelines.

5.4 Audit logging procedures

5.4.1 Types of events recorded

See Getronics PinkRoccade CPS §4.5.1.

5.4.2 Frequency of processing log

See Getronics PinkRoccade CPS §4.5.2.

5.4.3 Retention period for audit log

See Getronics PinkRoccade CPS §4.5.3.

5.4.4 Protection of audit log

See Getronics PinkRoccade CPS §4.5.4.

5.4.5 Audit log backup procedures

See Getronics PinkRoccade CPS §4.5.5

5.4.6 Audit collection system (internal vs. external)

See Getronics PinkRoccade CPS §4.5.6.

5.4.7 Notification to event-causing subject

See Getronics PinkRoccade CPS §4.5.7.

5.4.8 Vulnerability assessments

See Getronics PinkRoccade CPS §4.5.8.

5.5 Records archival

5.5.1 Types of records archived

See Getronics PinkRoccade CPS §4.6.1.

5.5.2 Retention period for archive

See Getronics PinkRoccade CPS §4.6.2.

5.5.3 Protection of archive

See Getronics PinkRoccade CPS §4.6.3.

5.5.4 Archive backup procedures

See Getronics PinkRoccade CPS §4.6.4.

5.5.5 Requirements for time-stamping of records

See Getronics PinkRoccade CPS §4.6.5.

5.5.6 Archive collection system (internal or external)

The archive collection system related to the Equens Private PKI CA is internal to Getronics PinkRoccade. Getronics PinkRoccade shall assist the Managed PKI Equens RA in preserving an audit trail related to Certificate Applications and the processing of them.

5.5.7 Procedures to obtain and verify archive information

See Getronics PinkRoccade CPS §4.6.3.

5.6 Key changeover

See Getronics PinkRoccade CPS §4.7.

5.7 Compromise and disaster recovery

See Getronics PinkRoccade CPS §4.8.

5.7.1 Incident and compromise handling procedures

See Getronics PinkRoccade CPS §4.8.1.

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

See Getronics PinkRoccade CPS §4.8.1.

5.7.3 Entity private key compromise procedures

See Getronics PinkRoccade CPS §4.8.3.

5.7.4 Business continuity capabilities after a disaster

See Getronics PinkRoccade CPS §4.8.2 and 4.8.4.

5.7.5 CA or RA termination

See Getronics PinkRoccade CPS §4.9.

6 Technical Security Controls

6.1 Key pair generation and installation

6.1.1 Key pair generation

See Getronics PinkRoccade CPS §6.1.1.

6.1.2 Private key delivery to subscriber

Within the Equens Private PKI the end-user Subscriber key pairs are generated by the end-user Subscriber themselves; therefore private key delivery is not applicable.

6.1.3 Public key delivery to certificate issuer

See Getronics PinkRoccade CPS §6.1.3.

6.1.4 CA public key delivery to relying parties

When the end-user Subscriber accepts its Certificate, the CA Certificate including its public key, of the Equens Private PKI is downloaded to the Subscriber in the Certificate Chain together with the end-user Subscriber's Certificate.

6.1.5 Key sizes

The key pairs within the Equens Private PKI of the Class 3 Administrator Certificates for the Managed PKI Equens RA and of all end-user Subscribers Certificates are 1024 bit RSA.

The key pair of the Equens Private PKI CA is 2048 bit RSA.

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)

See Getronics PinkRoccade CPS §6.1.9.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

See Getronics PinkRoccade CPS §6.2.

6.2.1 Cryptographic module standards and controls

See Getronics PinkRoccade CPS §6.2.1 in general and §6.2.1.1 with respect to the Equens Private PKI CA.

6.2.2 Private key (n out of m) multi-person control

See Getronics PinkRoccade CPS §6.2.2.

6.2.3 Private key escrow

Getronics PinkRoccade does not escrow Equens Private PKI CA, Managed PKI Equens RA or end-user Subscriber private keys with any third party for purposes of access by law enforcement.

6.2.4 Private key backup

See Getronics PinkRoccade CPS §6.2.4.

6.2.5 Private key archival

When the Equens Private PKI CA key pairs reach the end of their validity period, these CA key pairs will be archived for a period of at least 5 years. These archived CA key pairs will be securely stored using hardware cryptographic modules that meet the requirements of CPS § 6.2.1. Procedural controls prevent the archived CA key pairs from being returned to production use. Upon the end of the archive period, the archived CA private keys will be securely destroyed in accordance with CPS § 6.2.9.

Getronics PinkRoccade does not archive copies of RA-Administrator and Subscriber private keys.

6.2.6 Private key transfer into or from a cryptographic module

See Getronics PinkRoccade CPS §6.2.6.

6.2.7 Private key storage on cryptographic module

The private key(s) of the Equens Private PKI CA held on cryptographic modules are stored in encrypted form.

6.2.8 Method of activating private key

All participants in the Equens Private PKI are required to protect the activation data for their private keys against loss, theft, modification, unauthorized disclosure, or unauthorized use. Depending on the participant, the following requirements apply.

6.2.8.1 End-user Subscriber with Organisational Managed PKI Certificates and private key

The following methods are used to protect a Subscriber Organisational Managed PKI private key:

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 Administrators of the Managed PKI Equens RA

The following method is used to protect an Administrator's private key:

A smart card to authenticate the Administrator before the activation of the private key, which includes a PINcode to operate the private key; and

Take commercially reasonable measures for the physical protection of the Administrator's Workstation to prevent use of the workstation and its associated private key without the Administrator's authorization.

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

6.2.9 Method of deactivating private key

See Getronics PinkRoccade CPS §6.2.8.

6.2.10 Method of destroying private key

See Getronics PinkRoccade CPS §6.2.9.

6.2.11 Cryptographic Module Rating

See Getronics PinkRoccade CPS §6.2.1 in general and §6.2.1.1 with respect to the Managed PKI Equens CA.

6.3 Other aspects of key pair management

6.3.1 Public key archival

See Getronics PinkRoccade CPS 6.3.1.

6.3.2 Certificate operational periods and key pair usage periods

See Getronics PinkRoccade CPS 6.3.2.

6.4 Activation data

6.4.1 Activation data generation and installation

The activation data (Secret Shares), used to protect tokens containing the Equens Private PKI CA private keys, is generated by Getronics PinkRoccade in accordance with the requirements of Getronics PinkRoccade CPS §6.2.2 and the Key Ceremony Reference Guide. The creation and distribution of Secret Shares is logged.

The PINcode related to the smart card to authenticate the Administrator before the activation of its private key, is generated by Getronics PinkRoccade and shall be distributed by Getronics PinkRoccade to Equens using means according to ISO 9564-1.

Equens strongly recommends that end-user Subscriber's choose passwords for activating their private key which meet the requirements set out in the "Equens Guideline Authentication".

6.4.2 Activation data protection

The trusted Getronics PinkRoccade employees called "Shareholders" in Getronics PinkRoccade CPS §6.2.2, are required to safeguard their Secret Shares and sign an agreement acknowledging their Shareholder responsibilities.

The RA-Administrators at Equens store their private keys in encrypted form through the use of a smart card with a PINcode to activate the private key. The End-user Subscriber stores their private keys in encrypted form on their Workstation and protects their private keys through the use of a password.

6.4.3 Other aspects of activation data

See §6.4.1 and 6.4.2 above.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

See Getronics PinkRocade CPS §6.5.1 with respect to the Managed PKI CA systems.

6.5.2 Computer security rating

No stipulation. Life cycle technical controls

6.5.3 System development controls

See Getronics PinkRocade CPS §6.6.1 with respect to the Managed PKI CA systems.

6.5.4 Security management controls

See Getronics PinkRocade CPS §6.6.2.

6.5.5 Life cycle security controls

No stipulation.

6.6 Network security controls

See Getronics PinkRocade CPS §6.7.

6.7 Time-stamping

Not applicable.

7 Certificate, CRL and OCSP Profiles

7.1 Certificate profile

This Equens CP §7.1 defines the Equens Private PKI Certificate Profile and Certificate content requirements for the Equens Private PKI Certificates issued under this CP.

The Equens Private PKI Certificates conform to (a) ITU-T Recommendation X.509 (1997): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, June 1997 and (b) RFC 2459: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, January 1999 (RFC 2459).

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

Field	Value or Value constraint
Version	See §7.1.1
Serial Number	Unique value per Issuer DN
Signature Algorithm	Name of the algorithm used to sign the certificate (See §7.1.3)
Issuer DN	See §7.1.4
Valid From	Universal Coordinate Time base. Synchronized to Master Clock of U.S. Naval Observatory. Encoded in accordance with RFC 2459
Valid To	Universal Coordinate Time base. Synchronized to Master Clock of U.S. Naval Observatory. Encoded in accordance with RFC 2459. The validity period will be set in accordance with the constraints specified in §6.3.2
Subject DN	See §7.1.4
Subject Public Key	Encoded in accordance with RFC 2459 using algorithms specified in CPS §7.1.3 and key lengths specified in §6.1.5
Signature	Generated and encoded in accordance with RFC 2459

Table 6: Certificate Profile Basic Fields

7.1.1 Version number(s)

The Equens Private PKI CA and RA and end-user Subscriber Certificates are X.509 Version 3 Certificates.

7.1.2 Certificate extensions

The Equens Private PKI CA populates the X.509 Version 3 Certificates, used in the Equens Private PKI, with the extensions as required by the following par's 7.1.2.1-7.1.2.8.

7.1.2.1 Key Usage

The Equens Private PKI CA populates the X.509 Version 3 Certificates, used in the Equens Private PKI, with the extensions in accordance with §6.1.7. The criticality field of this extension is set to FALSE.

7.1.2.2 Certificate Policies Extension

As the Equens Private PKI X.509 Version 3 end-user Subscribers Certificates does *not* use the Certificate Policies extension, this sub-paragraph is not applicable.

7.1.2.3 Subject Alternative Names

No stipulation.

7.1.2.4 Basic Constraints

The Equens Private PKI CA populates X.509 Version 3 CA Certificates with a BasicConstraints extension with the Subject Type set to CA. End-user Subscriber Certificates are also populated with a BasicConstraints extension with the Subject Type equal to End Entity. The criticality of the Basic Constraints extension is set to FALSE.

The CA Certificate issued to the Equens Private PKI CA issuing end-user Subscriber Certificates has a pathLenConstraint field set to a value of 0 indicating that only an end-user Subscriber Certificate may follow in the Certification path.

7.1.2.5 Extended Key Usage

Not applicable.

7.1.2.6 CRL Distribution Points

The Organisational Managed PKI end-user Subscriber Certificates of the Equens Private PKI use the cRLDistributionPoints extension containing the URL of the location where a Relying Party can obtain a CRL to check the CA Certificate's status. The criticality field of this extension is set to FALSE.

7.1.2.7 Authority Key Identifier

VeriSign and thereby also Getronics PinkRoccade populate the Authority Key Identifier extension, called "sleutel-ID van CA", of X.509 Version 3 end user Subscriber Certificates issued by the VeriSign Commercial Software Publishers CA. The Authority Key Identifier is composed of the 160-bit SHA-1 hash of the public key of the Equens Private PKI CA issuing the Certificate. The criticality field of this extension is set to FALSE.

7.1.2.8 Subject Key Identifier

The Equens Private PKI CA populates X.509 Version 3 Certificates with a subjectKeyIdentifier extension, called "identificatie van het onderwerp", whereby the keyIdentifier based on the public key of the Subject of the Certificate is generated. Where this extension is used, the criticality field of this extension is set to FALSE.

7.1.3 Algorithm object identifiers

The Equens Private PKI X.509 Certificates are signed with sha1RSA (OID: 1.2.840.113549.1.1.5) in accordance with RFC 2459.

7.1.4 Name forms

The Equens Private PKI CA populates Certificates with an Issuer and Subject Distinguished Name in accordance with §3.1.1.

The Equens Private PKI CA does *not* include within end-user Subscriber Certificates for the Equens Private PKI an additional Organizational Unit field or a Certificate Policy Extension which contains a notice stating that the terms of use of the Certificate are set forth in a URL which is a pointer to the applicable Relying Party Agreement.

As the Equens Private PKI is a private and not a public PKI, the terms of use of the Certificates are agreed between the participants of the Equens Private PKI themselves.

7.1.5 Name constraints

No stipulation.

7.1.6 Certificate policy object identifier

As the Equens Private PKI X.509 Version 3 end-user Subscribers Certificates does *not* use the Certificate Policies extension, this paragraph is not applicable.

7.1.7 Usage of Policy Constraints extension

No stipulation.

7.1.8 Policy qualifiers syntax and semantics

As the Equens Private PKI X.509 Version 3 end-user Subscribers Certificates does *not* use the Certificate Policies extension, this paragraph is not applicable.

7.1.9 Processing semantics for the critical Certificate Policies extension

As the Equens Private PKI X.509 Version 3 end-user Subscribers Certificates does *not* use the Certificate Policies extension, this paragraph is not applicable.

7.2 CRL profile

The Equens Private PKI CA issues CRL's that conform to RFC 2459. At a minimum, these CRL's contain the basic fields and contents specified in the Table 7 below:

Field	Value or Value constraint
Version	See §7.2.1.
Signature Algorithm	Algorithm used to sign the CRL. The CRL's are signed using md5RSA (OID: 1.2.840.113549.1.1.4) in accordance with RFC 2459.
Issuer	Issuer Entity who has signed and issued the CRL. The CRL Issuer Name is in accordance with the Issuer Distinguished Name requirements specified in §7.1.4.
Effective Date	Issue date of the CRL. The CRL's are effective upon issuance.

Field	Value or Value constraint
Next Update	Date by which the next CRL will be issued. The Next Update date for the CRL's is set as follows: 10 days from the Effective Date for the Equens Private PKI CA certificate and at least one day for end-user certificates. CRL issuance frequency is in accordance with the requirements of §4.9.7.
Revoked Certificates	Listing of revoked Certificates, including the Serial Number of the revoked Certificate and the Revocation Date

Table 7: CRL Profile Basic Fields

7.2.1 Version number(s)

The Equens Private PKI CA issues X.509 Version 1 CRL's.

7.2.2 CRL and CRL entry extensions

No stipulation.

7.3 OCSP profile

As the Equens Private PKI does not support OCSP, this paragraph is not applicable.

7.3.1 Version number(s)

Not applicable.

7.3.2 OCSP extensions

Not applicable.

8 Compliance Audit and other Assessments

8.1 Frequency or circumstances of assessment

The Equens Private PKI CA which is operated by Getronics PinkRoccade is required by Equens to be audited. The requirements for the audit are those for non-qualified certificates as specified in ETSI TS 102 042 Policy requirements for certification authorities issuing public key certificates. This is done every year. The Managed PKI Equens RA which is operated by Equens including the procedures to verify the identity of party requesting a certificate, is audited by the Internal Audit department of Equens and by its external auditor. The frequency is at least once every three years.

Other important assessments done by Equens NL is to have its core activities, which are the processing of payments and cards transactions, certified according to IS 27001, Information Security Management System. Equens NL received the certificate in April 2007. This certification deals also with the systems and its procedures regarding the delivery of payments such the described PKI-system. Every year a re-assessment is done in order to have the certificate renewed.

8.2 Identity/qualifications of assessor

With respect to the assessment of the CA-system at Getronics PinkRoccade, the assessment is done by the external auditor of Getronics PinkRoccade.

With respect to the assessment of the RA-system and related procedures at Equens, the assessment is done by the internal and external auditor of Equens. The assessor of the IS 27001 certificate for having Information Security Management System at Equens is an external auditor.

8.3 Assessor's relationship to assessed entity

See §8.2.

8.4 Topics covered by assessment

The topics covered by the assessment at Getronics PinkRoccade are described in its CPS §2.7.4.

The topics covered by the assessment at Equens are the RA environmental controls, the operations and procedures verifying certificate-requests and validity of issued certificates, and the infrastructure/administrative RA controls.

8.5 Actions taken as a result of deficiency

Actions by Getronics PinkRoccade in case of deficiency are specified in its CPS §2.7.5.

With respect to compliance audits of Equens, any significant exceptions or deficiencies identified during the Compliance Audit will result in an action plan authorised by the Board of Directors and senior management. This action plan is made by Equens management with input from the auditor. Equens management is responsible for developing and implementing the corrective action plan. If Equens determines that such exceptions or deficiencies pose an immediate threat to the RA-infrastructure, a corrective action plan will be developed and implemented as

soon as possible within a commercially reasonable period of time. For less serious exceptions or deficiencies, Equens Management will evaluate the significance of such issues and determine the appropriate course of action.

Currently Equens has established a project to address the minor-conformities stated by the external auditor when Equens received its IS 27001 certificate.

8.6 Communication of results

The results of the assessor are communicated via the Board of Directors to the manager of the centre Risk Management. The manager of the centre Risk Management is responsible for coordinating the necessary actions to be taken within other centres, such as Operations and to have all necessary information available for the relevant centres where actions have to take place.

The manger of Risk Management together with the BoD will verify that the requested actions are implemented.

9 Other Business and Legal Matters

9.1 Fees

The Certificates issued to end-user Subscriber's in the Equens Private PKI is part of the total service offering provided by Equens to its clients. Therefore, Equens will charge its clients no specific fee for an end-user Subscriber Certificate.

9.1.1 Certificate issuance or renewal fees

Not applicable.

9.1.2 Certificate access fees

Not applicable.

9.1.3 Revocation or status information access fees

Not applicable.

9.1.4 Fees for other services

Not applicable.

9.1.5 Refund policy

Not applicable.

9.2 Financial responsibility

9.2.1 Insurance coverage

Equens as Managed PKI RA and Getronics PinkRoccade as provider of the Equens Private PKI CA and Managed PKI infrastructure shall 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. Getronics PinkRoccade maintains such errors and omissions insurance coverage.

9.2.2 Other assets

Equens as Managed PKI RA and Getronics PinkRoccade as provider of the Equens Private PKI CA and Managed PKI infrastructure 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

Not applicable.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

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

- CA application records, whether approved or disapproved,
- Certificate Application records,

- Private keys held by RA customers using PKI Key Manager and information needed to recover such Private Keys,
- Transactional records (both full records and the audit trail of transactions),
- Audit trail records created or retained by Equens, an Affiliate or a Customer,
- Audit trails created by Equens, an Affiliate or a Customer (to the extent such reports are maintained), or their respective auditors (whether internal or public),
- Contingency planning and disaster recovery plans, and
- Security measures controlling the operations of Equens or Affiliate hardware and software and the administration of Certificate services and designated enrolment services.

9.3.2 Information not within the scope of confidential information

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

9.3.3 Responsibility to protect confidential information

Participants receiving private information shall secure it from compromise and disclosure to third parties and shall comply with all applicable privacy laws.

9.4 Privacy of personal information

9.4.1 Privacy plan

Equens and Affiliates shall implement a privacy policy in accordance with the applicable legislation. Equens and Affiliates shall not disclose or sell the names of Certificate Applicants or other identifying information about them, subject to Section 9.3.2 and to the right of a terminating CA to transfer such information to a successor CA.

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 CRL's is treated as private.

9.4.3 Information not deemed private

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

9.4.4 Responsibility to protect private information

Participants receiving private information shall secure 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 where otherwise stated in this CP, 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.

9.4.6 Disclosure pursuant to judicial or administrative process

Participants acknowledge that Equens and the Affiliate shall be entitled to disclose Confidential/Private information if, in good faith, Equens or the Affiliate believes that:

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

This section is subject to applicable privacy laws.

9.4.7 Other information disclosure circumstances

Privacy policies shall contain provisions relating to the disclosure of Confidential/Private Information to the person disclosing it to Equens or the Affiliate. This section is subject to applicable privacy laws.

9.5 Intellectual property rights

The allocation of Intellectual Property Rights among Participants other than Subscribers and Relying Parties shall be governed by the applicable agreements between such Participants. The following paragraphs of Section 9.5 apply to the Intellectual Property Rights in relation to Subscribers and Relying Parties.

Equens retains all Intellectual Property Rights in and to the Certificates and revocation information that they issue. Equens, Affiliates, and Customers shall 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. Equens, Affiliates, 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.

Participants acknowledge that Equens retains all Intellectual Property Rights in and to this CP.

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.

Key pairs corresponding to Certificates of CA's and end-user Subscribers are the property of the CA's and end-user Subscribers that are the respective Subjects of these Certificates, subject to the rights of 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, Equens' root public keys and root Certificates containing them, including self-signed Certificates are the property of Equens.

9.6 Representations and warranties

9.6.1 CA representations and warranties

Equens warrants that:

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

Subscriber Agreements may include additional representations and warranties.

9.6.2 RA representations and warranties

Equens' RAs warrant that:

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

Subscriber Agreements may include additional representations and warranties.

9.6.3 Subscriber representations and warranties

Subscriber warrants that:

- Each digital signature created using the private key corresponding to the public key listed in the Certificate is the digital signature of the Subscriber and the Certificate has been accepted and is operational (not expired or revoked) at the time the digital signature is created,
- Their private key is protected and that no unauthorized person has ever had access to the Subscriber's private key,
- All representations made by the Subscriber in the Certificate Application the Subscriber submitted are true,
- All information supplied by the Subscriber and contained in the Certificate is true,
- The certificate is being used exclusively for authorized and legal purposes, consistent with all material requirements of this CP and the applicable CPS, and
- The Subscriber is an end-user Subscriber and not a CA, and is not using the private key corresponding to any public key listed in the Certificate for purposes of digitally signing any Certificate (or any other format of certified public key) or CRL, as a CA or otherwise.

Subscriber Agreements may include additional representations and warranties.

9.6.4 Relying party representations and warranties

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

Relying Party Agreements may include additional representations and warranties.

9.6.5 Representations and warranties of other participants

No stipulation.

9.7 Disclaimers of warranties

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

9.8 Limitations of liability

To the extent permitted by applicable law, Subscriber Agreements and Relying Party Agreements shall limit Equens' and the applicable Affiliate's liability outside such agreement. Limitations of liability shall include an exclusion of indirect, special, incidental and consequential damages. They shall also include the following liability caps limiting Equens' and the Affiliate's liability concerning a specific Certificate according to the relevant agreement.

9.9 Indemnities

To the extent permitted by applicable law, Subscriber is required to indemnify Equens for:

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

The applicable Subscriber Agreement may include additional indemnity obligations.

To the extent permitted by applicable law, Relying Party Agreements shall require Relying Parties to indemnify Equens for:

- The Relying Party's failure to perform the obligations of a Relying Party,
- The Relying Party's reliance on a Certificate that is no reasonably under the circumstances, or
- The Relying Party's failure to check the status of such Certificate to determine if the Certificate is expired or revoked.

The applicable Relying Party Agreement may include additional indemnity obligations.

9.10 Term and termination

9.10.1 Term

The CP becomes effective upon publication in the Equens repository. Amendments to this CP become effective upon publication in the Equens repository

9.10.2 Termination

This CP 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 CP, 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 parties, participants shall use commercially reasonable methods to communicate with each other, taking into account the criticality and subject matter of the communication.

9.12 Amendments

9.12.1 Procedure for amendment

Amendments to this CP may be made by Equens. Amendments shall either be in the form of a document containing an amended form of the CP or an update. Amended versions or updates shall be linked to the Equens repository. Updates supersede any designated or conflicting provisions of the referenced version of the CP. Equens shall determine whether changes to the CP require a change in the CP object identifiers of the CP.

9.12.2 Notification mechanism and period

Equens reserves the right to amend the CP without notification for amendments that are not material, including without limitations correction of typographical errors, changes to URLs, and changes to contact information. The decision to designate amendments as material or non-material shall be within Equens' sole discretion.

Equens shall send Affiliates notice of material amendments to the CP proposed by Equens. The notice shall state the text of the proposed amendment and the

comment period. Proposed amendments to the CP shall also appear in the repository.

Notwithstanding anything in the CP to the contrary, if Equens believes material amendments to the CP are necessary immediately to stop or prevent a breach of the security, Equens shall be entitled to make such amendments by publication in the repository. Such amendments will be effective immediately upon publication. Within a reasonable time after publication, Equens shall provide notice to Affiliates of such amendments.

9.12.3 *Circumstances under which OID must be changed*

If Equens determines that a change is necessary in the object identifier corresponding to a CP, the amendment shall contain new object identifiers for the CP. Otherwise, amendments shall not require a change in CP object identifier.

9.13 *Dispute resolution provisions*

Disputes among one or more of Equens, Affiliates and/or Customers shall be resolved pursuant to provisions in the applicable agreements among the parties.

To the extent permitted by applicable law, Subscriber Agreements and Relying Party Agreements shall contain a dispute resolution clause.

9.14 *Governing law*

Subject to any limitations appearing in applicable law, the laws of The Netherlands, shall govern the enforceability, construction, interpretation, and validity of this CP, unless contract or other choice of law provisions but without the requirement to establish a commercial domicile in The Netherlands.

9.15 *Compliance with applicable law*

This CP is subject to applicable national, state, local and foreign laws, rules, regulations, ordinances, decrees, and orders including, but not limited to, restrictions on exporting or importing software, hardware, or technical information.

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 CP is held to be unenforceable by a court of law or other tribunal having authority, the remainder of the CP shall remain valid.

9.16.4 *Enforcement (attorneys' 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 Equens and the applicable Affiliate.

9.17 Other provisions

Not applicable

Annex 1 **Acronyms and Definitions**

Acronym	Definition
CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
OCSP	Online Certificate Status Protocol
PKCS	Public-Key Cryptography Standard
PKI	Public Key Infrastructure
PMA	Policy Management Authority
RA	Registration Authority
RFC	Request for comment

Table 8: Acronyms and Definitions