Certification Practice Statement PKIoverheid

Effective Date: September 10, 2019
Version: 1.0

QuoVadis TrustLink B.V.
Nevelgaarde 56
3436 ZZ Nieuwegein
Tel: +31 302324320
Fax: +31 302324329

Version Control

Author	Date	Version	Comment
QuoVadis PMA	10 September 2019	1.0	English version consolidating all prior Dutch versions below.

Previous documents

Author	Date	Version	Comment
QuoVadis PMA	12 July 2019	1.8	Certification Practice Statement PKIoverheid Domeinen Organisatie (G2), Organisatie Persoon (G3)
QuoVadis PMA	12 July 2019	1.9	Certification Practice Statement PKIoverheid Domeinen Organisatie (G2), Organisatie services(G3)
QuoVadis PMA	12 July 2019	1.7	Certification Practice Statement PKIoverheid Burger
QuoVadis PMA	12 July 2019	1.9	Certification Practice Statement PKIoverheid Domeinen Organisatie (G2), Organisatie services /server (G3)
QuoVadis PMA	12 July 2019	1.7	Certification Practice Statement PKIoverheid EV
QuoVadis PMA	12 July 2019	1.3	Certification Practice Statement PKIoverheid Domeinen Private Services G1
QuoVadis PMA	12 July 2019	1.3	Certification Practice Statement PKIoverheid Domeinen Private Services Server G1
QuoVadis PMA	12 July 2019	1.3	Certification Practice Statement PKIoverheid Domeinen Private Personen G1

CONTENTS

1. INTRODUCTION

QuoVadis TrustLink B.V., a subsidiary of DigiCert Inc., is a Company incorporated in the Netherlands, trading under the name QuoVadis. QuoVadis is a leading international provider of Certificates. QuoVadis was founded in 1999 and has offices in The Netherlands, Switzerland, the United Kingdom and Bermuda. QuoVadis TrustLink B.V is certified as a Trust Service Provider ("TSP") and has also joined PKIoverheid .

PKIoverheid (also "PKIo") is an initiative of the Dutch government and forms a framework with requirements and agreements that enables the use of an Electronic Signature, electronic Authentication and confidential electronic communication, based on Certificates with a high level of reliability.

The requirements that are placed on the Trusted Service Provider (TSP) for Issuing and managing these Certificates are described in the PKI Requirements Program for the government (Programma van Eisen, PvE) (http://www.logius.nl). These requirements are referred to as the Programme of Requirements or "POR" in this Certification Practice Statement ("CPS").

In this CPS the RFC 3647 Standard is followed as much as possible, this RFC can be found within the Internet Technology Task Force Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, see https://ietf.org. According to the RFC, this document is divided into nine parts that cover the security controls, practices, Certificate profiles and procedures for Certificate Issuance.

1.1. OVERVIEW

This CPS describes the practices and procedures that are employed in the life-cycle management containing generation, Issuance and revocation of PKIoverheid Certificates. The publication of version 1.0 of this English Certificate Practice Statement for PKIoverheid renders all the previous Dutch versions (as mentioned under 'previous versions' in Version Control) obsolete.

Personal Certificates and Personal Certificates for Registered Professionals are EU Qualified Certificates issued to natural persons according to Regulation (EU) No 910/2014. The Certificate Policy for Qualified Certificates is in this case aligned with the Qualified Certificate Policy for natural persons (QCPn-qscd).

QuoVadis conforms to the current version of the Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates published at http://www.cabforum.org. In the event of any inconsistency between this document and those requirements, those requirements take precedence over this document.

QuoVadis is evaluated against multiple requirements, including PKIoverheid Programma van Eisen parts 3a (Organisatie & Organisatie Persoon), 3b (Service), 3c (Burger), 3e (Server - Organisatie Services), 3f (EV, Extended Validation), 3g (Private Service), 3h (Server - Private Services), 3i (Private Persoon), ETSI 319 411-1 and 319 411-2, ISO27001:2013, WebTrust for Certification Authorities, WebTrust for Baseline Requirements, WebTrust for Extended Validation, WebTrust for Code Signing. Please see our website for details.

1.1.1. Intended audience

This document is intended for:

- Subscribers
- Certificate Holders
- Certificate Managers
- Relying Parties

1.1.2. Relationship between CP and CPS, coverage of the CPS

QuoVadis issues Subscriber Certificates under the following hierarchies:

Root CA: Staat der Nederlanden Root CA - G2 **Domain CA: Staat der Nederlanden Organisatie CA – G2**		
Issuing CA	**Profile Name**	**OID**
QuoVadis CSP - PKIoverheid CA - G2	Personal User Authentication G2	2.16.528.1.1003.1.2.5.1
QuoVadis CSP - PKIoverheid CA - G2	Personal User Non-Repudiation G2	2.16.528.1.1003.1.2.5.2
QuoVadis CSP - PKIoverheid CA - G2	Personal User Encryption G2	2.16.528.1.1003.1.2.5.3
QuoVadis CSP - PKIoverheid CA - G2	Organisation Service Authentication G2	2.16.528.1.1003.1.2.5.4
QuoVadis CSP - PKIoverheid CA - G2	Organisation Service Encryption G2	2.16.528.1.1003.1.2.5.5
QuoVadis CSP - PKIoverheid CA - G2	Organisation Service Server G2	2.16.528.1.1003.1.2.5.6

With the exception of Organisation Service Server G2 Certificates, the G2 hierarchy is no longer being used for certificate issuance.

Root CA: Staat der Nederlanden Root CA – G3 **Domain CA: Staat der Nederlanden Organisatie Persoon CA - G3**		
Issuing CA	**Profile Name**	**OID**
QuoVadis PKIoverheid Organisatie Persoon CA - G3	Personal Organisation Authentication G3	2.16.528.1.1003.1.2.5.1
QuoVadis PKIoverheid Organisatie Persoon CA - G3	Personal Organisation Non-Repudiation G3	2.16.528.1.1003.1.2.5.2
QuoVadis PKIoverheid Organisatie Persoon CA - G3	Personal Organisation Encryption G3	2.16.528.1.1003.1.2.5.3

Root CA: Staat der Nederlanden Root CA – G3 **Domain CA: Staat der Nederlanden Burger CA - G3**		
Issuing CA	**Profile Name**	**OID**
QuoVadis PKIoverheid Burger CA - G3	Personal Citizen Authentication G3	2.16.528.1.1003.1.2.3.1
QuoVadis PKIoverheid Burger CA - G3	Personal Citizen Non-Repudiation G3	2.16.528.1.1003.1.2.3.2
QuoVadis PKIoverheid Burger CA - G3	Personal Citizen Encryption G3	2.16.528.1.1003.1.2.3.3

Root CA: Staat der Nederlanden Root CA – G3 **Domain CA: Staat der Nederlanden Organisatie Services CA - G3**		
Issuing CA	**Profile Name**	**OID**
QuoVadis PKIoverheid Organisatie Server CA - G3	Organisation Service Server G3	2.16.528.1.1003.1.2.5.6

Root CA: Staat der Nederlanden EV Root CA Intermediate CA: Staat der Nederlanden EV Intermediair CA		
Issuing CA	**Profile Name**	**OID**
QuoVadis PKIoverheid EV CA	PKIOverheid Qualified Website authentication	2.16.528.1.1003.1.2.7
QuoVadis PKIoverheid EV CA	PKIOverheid EV SSL	2.16.528.1.1003.1.2.7

Root CA: Staat der Nederlanden Private Root CA - G1 Domain CA: Staat der Nederlanden Private Personen CA – G1		
Issuing CA	**Profile Name**	**OID**
QuoVadis PKIoverheid Private Personen CA - G1	Private Personal Authentication	2.16.528.1.1003.1.2.8.1
QuoVadis PKIoverheid Private Personen CA - G1	Private Personal Non-Repudiation	2.16.528.1.1003.1.2.8.2
QuoVadis PKIoverheid Private Personen CA - G1	Private Personal Encryption	2.16.528.1.1003.1.2.8.3

Root CA: Staat der Nederlanden Private Root CA - G1 Intermediate CA: QuoVadis PKIoverheid Private Services CA – G1		
Issuing CA	**Profile Name**	**OID**
QuoVadis PKIoverheid Private Services CA – G1	Private Services – Authentication	2.16.528.1.1003.1.2.8.4
QuoVadis PKIoverheid Private Services CA – G1	Private Services – Encryption	2.16.528.1.1003.1.2.8.5

Root CA: Staat der Nederlanden Private Root CA - G1 Intermediate CA: QuoVadis PKIoverheid Private Services CA – G1		
Issuing CA	**Profile Name**	**OID**
QuoVadis PKIoverheid Private Services CA – G1	Private Services – Server	2.16.528.1.1003.1.2.8.6

1.2. DOCUMENT NAME AND IDENTIFICATION

This Certificate Practice Statement is identified as:

- Title: Certificate Practice Statement for PKIoverheid Certificates

1.3. PKI PARTICIPANTS

The following groups are part of the User community:

1.3.1. Certificate Authorities

Trusted Root and Intermediate CAs are owned and operated by the Government of the Netherlands under the PKIoverheid Regime.

PKIoverheid is the name for the PKI designed for trustworthy electronic communication within and with the Dutch government for which a national PKI certificate hierarchy has been created. This national hierarchy

consists of 4 root CAs and multiple domain CAs (sub-CAs) with each issuing Trust Service Providers (TSP) CA certificates. The TSPs are responsible for issuing certificates to end-users.

Issuing CAs and Their Obligations

- Issuing CAs are operated by QuoVadis as authorised by the Policy Authority to participate within the PKI to issue, revoke and otherwise manage Digital Certificates.
- Issuing CAs are required to act in accordance with their respective Issuing CA Agreements and to be bound by the terms of this CPS.
- Generally, Issuing CAs will be authorised to issue and manage the types of Digital Certificates relevant to that Issuer as supported by this CPS.
- An Issuing CA may, but shall not be obliged to, detail its specific practices and other requirements in a policy or practices statement adopted by it following approval by the QuoVadis Policy Authority. Within the PKI all Issuing CAs are responsible for the management of Digital Certificates issued by them. Digital Certificate Management includes all aspects associated with the application, issue and revocation of Digital Certificates, including any required identification and authentication processes included in the Digital Certificate application process
- Issuing CAs are required to ensure that all aspects of the services they offer and perform within the QuoVadis PKI are in compliance at all times with this CP/CPS.

Issuing CAs are required to ensure that;

- FIPS 140-3 or equivalent cryptographic modules are used for CA Private Key management.
- Private Keys are used only in connection with the signature of Digital Certificates and Certificate Revocation Lists.
- Enforce multi-factor authentication for all accounts capable of directly causing certificate issuance.
- All administrative procedures related to personnel and procedural requirements, as well as physical and technological security mechanisms, are maintained in accordance with this CPS.
- They comply at all times with all compliance audit requirements.
- They follow a privacy policy in accordance with this CPS .

1.3.2. Registration Authorities

The QuoVadis Registration Authority in Nieuwegein is responsible for identification and registration of the Subscriber and Certificate Manager and the revocation of issued Certificates. In certain cases, QuoVadis uses the services provided by the AMP Group, based in Houten or uses appropriately trained employees from other group companies to establish identities of the Applicant.

Certificate requests can be made using hardcopy forms to the Registration Authority or can be filed online via https://www.quovadisglobal.nl where a request module runs that is hosted at our Data Centre in Switzerland.

1.3.3. Subscribers, Certificate Holder, Certificate Manager

Subscribers can be a natural person, a natural person with a registered profession or a natural person in association with a legal person – a legal Representative of an organisation.

The Certificate Holder is the entity stated in the subject field of the Certificate, and the holder of the Private Key. Holders of Personal Certificates are natural persons. Holders of Server Certificates are organisations. The Certificate Manager is a Representative of an organisation, it is also the holder of the Private Key.

1.3.3.1. Obligations and Responsibilities

- Exercise sole and complete control and use of the Private Key that corresponds to the Certificate Holder's Public Key. In the case of legal persons, the private key must be maintained and used under the control of the Certificate Holder and is recommended to be used only for electronic seals.
- If the policy requires the use of a Qualified Electronic Signature Creation Device (QSCD), digital signatures must only be created by a QSCD.

- For Qualified certificates issued to natural persons, it is recommended that the Certificate Holder's key pair is only used for electronic signatures.

1.3.4. Relying Parties

A relying party is any natural or legal person who is a recipient data signed or protected by a Certificate, who acts in confidence on that Certificate and relies upon the trusted status of the Certificate. Relying Parties must assess the status of the Certificate before acting on communications with the Subscriber.

1.4. CERTIFICATE USAGE

1.4.1. Permitted Certificate Usage

The Certificates within PKIoverheid that are issued by the QuoVadis CAs may be used for the purposes explained in this document, in the Terms and Conditions and as identified in the Key Usage field of the Certificate. Reference is made below to the Programma of Requirements (POR/PVE) sections (https://www.logius.nl/english/pkioverheid).

3a: Personal and Professional Certificates (including Certificates for Registered Professionals)

- Authentication Certificate: can be used to reliably authenticate the identity of a user
- Digital Signatures: can be used to digitally sign documents
- Encryption: can be used for securing trusted information/details which are exchanged in electronic form. This can be both exchanges between people and people exchanging with automated systems.

3b: Organisation / Organisation services

- Authentication Certificate: can be used to reliably authenticate the identity of a device or service
- Encryption can be used for securing trusted information/details which are exchanged in electronic form. This can be both exchanges between device or service and device or service exchanging with automated systems.
- Non-repudiation Certificate: can be used to digitally sign documents as a Legal person.

3c: Citizen

- Authentication Certificate: can be used to reliably authenticate the identity of a user
- Digital Signatures: can be used to digitally sign documents
- Encryption: can be used for securing trusted information/details which are exchanged in electronic form. This can be both exchanges between people and people exchanging with automated systems.

3e: Organisation / Organisation Services

- Server Certificate: can be used to identify a website and secure communication between a browser and the webserver. It can also be used to secure communication between two devices or services.

3f: Extended Validation

- Server EV Certificate: can be used to identify a website and secure communication between a browser and the webserver where it displays information of the owner of the domain name. It can also be used to secure communication between two devices or services.

3g: Private Services

- Authentication Certificate: can be used to reliably authenticate the identity of a device or service
- Encryption can be used for securing trusted information/details which are exchanged in electronic form. This can be both exchanges between device or service and device or service exchanging with automated systems.

3h: Private Server

- Server Certificate: can be used to identify a website and secure communication between a browser and the webserver. It can also be used to secure communication between two devices or services.

3i: Private Person

- Authentication Certificate: can be used to reliably authenticate the identity of a user

- Digital Signatures: can be used to digitally sign documents
- Encryption: can be used for securing trusted information/details which are exchanged in electronic form. This can be both exchanges between people and people exchanging with automated systems.

1.4.2. Prohibited Certificate Usage

Certificates issued under this CPS may not be used other than as described above.

1.5. POLICY ADMINISTRATION

The QuoVadis CPS is managed by its Policy Management Authority. Information regarding this CPS and comments can be directed to:

QuoVadis TrustLink B.V.
attn. Policy Authority
Nevelgaarde 56 Noord
3436 ZZ Nieuwegein
The Netherlands

Tel:	+31 30 232 4320	Fax:	+31 30 232 4329
Website:	http://www.quovadisglobal.nl	E-mail:	info.nl@quovadisglobal.com

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1. REPOSITORY

QuoVadis has an electronic Repository (dissemination service) that is available through:

- https://quovadisglobal.com/Repository.aspx
- https://quovadisglobal.nl/Beheer/Documenten.aspx

All Repository information is publicly available in read-only format and is available 24 by 7.

2.2. PUBLICATION OF INFORMATION

The Repository contains:

- The CPS
- PKI Disclosure Statement
- Terms and Conditions, Privacy Statement
- Certificates for Certificate Holders (only with consent of the Certificate Holder)

The location of the Repository, Certificate Revocation List ("CRL") and the Online Certificate Status Protocol ("OCSP") responders are also in the corresponding field of the Certificate profiles as stated in this CPS.

2.3. FREQUENCY OF PUBLICATION

Updates of this CPS and other documents are published as soon as possible when updates are made to the documents.

QuoVadis publishes a list of revoked Certificates, this list is automatically updated every 10 (ten) minutes. The response is valid for a maximum of 24 (twenty-four) hours. The OCSP is updated immediately when a Certificate is revoked, OSCP responses are valid for a maximum of 8 (eight) hours. All OSCP responses conform to RFC6960.

3. IDENTIFICATION & AUTHENTICATION

3.1. INITIAL IDENTITY VALIDATION

The x.501 name standard is used to define the assignment of Certificates; a distinguished name (DN) is specified in each issued Certificate.

Personal Certificates

Field	Description	Max. length
CN - Common name	Full name of the Subscriber	64
C - Country	Two-digit country code for the location	2
GN – Given Name	Official given name(s) of the Subscriber per the Legal ID	64
S - Surname	Official surname(s) of the Subscriber per the Legal ID	64

Personal Certificates with Legal person

Field	Description	Max. length
CN - Common name	Full name of the Subscriber	64
C - Country	Two-digit country code for the location	2
GN – Given Name	Official given name(s) of the Subscriber per the Legal ID	64
S - Surname	Official surname(s) of the Subscriber per the Legal ID	64
O - Organisation Name	Name of the Organisation	64

Personal Certificates for Registered Professionals

Field	Description	Max. length
CN - Common name	Full name of the Subscriber	64
C - Country	Two-digit country code for the location	2
GN – Given Name	Official given name(s) of the Subscriber per the Legal ID	64
S - Surname	Official surname(s) of the Subscriber per the Legal ID	64
T- Title	Official registered profession(al) title of the Subscriber	64
O - Organisation Name	GN – Given Name + S - Surname	64

Services Certificates – G1

Field	Description	Max. length
CN - Common name	FQDN to which the Certificate and keypair are assigned or Non-FQDN	64
O - Organisation Name	Name of the Organisation	64
C - Country	Two-digit country code for the location	2
Serial number	Chamber of Commerce number for the Organisation	64

Server Certificates – G2 & G3

Field	Description	Max. length
CN - Common name	FQDN to which the Certificate and keypair are assigned	64
O - Organisation Name	Name of the Organisation	64
serial number	Chamber of Commerce number for the Organisation	64
C - Country	Two-digit country code for the location	2
L- Locality	Place the Organisation is located	128
ST- State	State or province the Organisation is located	128
OU – Organisational Unit (optional)	Department of the Organisation	64

Extended Validation

Field	Description	Max. length
Subject	Certificate	
BusinessCategory	Must contain either: Private Organisation Government Entity Business Entity	fixed
CN - Common name	Full name of the Subscriber	64
O - Organisation Name	Name of the Organisation	64
C - Country	Two-digit country code for the location	2
L- Locality	Place the Organisation is located	128
ST- State	State or province the Organisation is located	128
serial number	Chamber of Commerce number for the Organisation	64
PublicKeyInfo	Public Key	
OU – Organisational Unit (optional)	Department of the Organisation	64
StreetAdress	Address where the Subscriber is located	180
PostalCode	Postal code where the Subscriber is located	16
JuridsictionOfIncorporationCountryName	Two-digit country code of the country of jurisdiction for the Certificate	2

Private Services Server

Field	Description	Max. length
Subject	Certificate	
BusinessCategory	Must contain either: • Private Organisation • Government Entity • Business Entity	fixed
CN - Common name	FQDN to which the Certificate and keypair are assigned or Non-FQDN	64
O - Organisation Name	Name of the Organisation	64
C - Country	Two-digit country code for the location	2
L- Locality	Place the Organisation is located	128
ST- State	State or province the Organisation is located	128
serial number	Chamber of Commerce number for the Organisation	64
PublicKeyInfo	Public Key	
OU – Organisational Unit (optional)	Department of the Organisation	64
StreetAdress	Address where the Subscriber is located	180
PostalCode	Postal code where the Subscriber is located	16
JuridsictionOfIncorporationCountryName	Two-digit country code of the country of jurisdiction for the Certificate	2

The naming of the Distinguished Name in the Certificates based on the tables above, should result names which are meaningful, unambiguous, and unique and allows any relying party to identify the Subscriber.

Anonymous Certificates, or the use of a pseudonym is not permitted.

Certificate Applicants shall not use names which infringe upon the intellectual property rights of others.

QuoVadis is not required to and does not determine whether a Certificate Applicant has intellectual property rights, and therefore does not mediate, arbitrate or try to resolve any dispute regarding the ownership of any intellectual property or trademarks.

QuoVadis reserves the right, without liability, to reject any application for a Certificate.

3.2. INITIAL IDENTITY VALIDATION

After being contacted by an Applicant, QuoVadis either sends a standard template to the Applicant by email or advises the Applicant to submit information via a website link. The client is responsible for accurate completion of the form either in hardcopy or online. A QuoVadis representative checks the forms and if complete, the documents are scanned. (If applicable a professional registrar is contacted to verify application-data.) An appointment is made to perform the Face-to-Face vetting, after the Face-to-Face vetting has been completed a QuoVadis employee reviews the documents for completeness and correctness. The identity vetting may also be performed by the company AMP or by trained employees of other QuoVadis group companies.

The procedures described in this CPS and internal procedures manuals are carried out in order to verify information and issue a certificate to the applicant following which the Applicant becomes a client. ("Abonnee")

When applicable, QuoVadis will guide the Applicant through the following steps:

Personal details

QuoVadis verifies the personal details of the Applicant with the details on the Legal Identity Document provided by the Applicant. This includes the full legal name(s), date of birth and gender.

E-mail address

Verification of the Applicant's control of an e-mail address to be included in the certificate is done in the first contact being made from QuoVadis to the Applicant, by sending in e-mail with instructions, documents and forms needed for application by the Applicant or automatically using the TrustLink Enterprise portal.

Legal Identity Document

Verification of the Applicant is done by verifying the Legal Identity Document (LID). QuoVadis has multiple processes that use the LID; the Applicant can send a copy of the LID, can take a picture of the LID during the registration or use an NFC-capable phone to read the NFC chip in the LID.

Face-to-Face identification

Part of the registration process is a Face-to-Face or physical identification of the natural person applying for the Certificate. Face-to-Face identity vetting is performed for all the individuals who are listed on the applicable PKIoverheid application forms. During the Face-to-Face vetting process the Applicant must place their signature on a copy of the LID as provided by QuoVadis -or a third party acting on behalf of QuoVadis-.

Note: Dutch Driving Licenses are considered acceptable Legal Identity Documents, but on Dutch Driving Licenses, not all names are fully written. As fully written names are mandatory for the Issuance of Certificates within PKIoverheid and eIDAS, Dutch Drivers Licenses are not accepted by QuoVadis for validation purposes.

Terms and Conditions, privacy statement

During registration, the Applicant is required to agree with the applicable Terms and Conditions as well as the Privacy Statement.

Professional Registration (where applicable)

Verification of the natural person in the applicable professional registrar is done when applicable for the specific Certificate that is applied for.

General verifications

When applicable, QuoVadis will verify:

- whether the Subscriber is an existing and legal organisation;
- whether the organisation name included in the Certificate is correct and complete and corresponds to the organisation name notified by the Subscriber;
- whether the address of the organisation provided by the Subscriber is correct and complete and that it is also the address where it carries out its work;
- whether the general telephone number of the organisation provided by the Subscriber is correct and complete;
- or, if it appears that the Subscriber's organisation has been in existence for less than three years, the Subscriber has an active current account;
- may not be older than 13 months otherwise the data must be requested and verified again. In those cases where the information sources have not been updated or adjusted in the last 13 months, the most recent version must be assumed;
- the ownership of the domain and its organisation.

3.2.1. Method to prove possession of Private Key

QuoVadis ensures that the Subscriber delivers the Certificate signing request (CSR) in a secure manner. The delivery must take place safely, as follows:

- inputting the CSR on the specially developed application TrustLink Enterprise (TLE) from QuoVadis using an SSL connection which uses a PKIoverheid SSL Certificate or equivalent or;
- Inputting the CSR on the HTTPS website of the QuoVadis which uses a PKIoverheid SSL Certificate or equivalent or;
- sending the CSR via e-mail with a qualified Electronic Signature from the Certificate Manager which uses a PKIoverheid qualified Certificate or equivalent or;
- inputting or sending a CSR in a manner at least equivalent to the above ways

3.2.2. Authentication of the Organisation Identity

QuoVadis verifies that the Subscriber is an existing and legal organisation.

As proof that it is an existing and legal organisation, QuoVadis will request and verify at least the following supporting documents:

- For organisations within the Netherlands, a recently certified extract (maximum 1 month old) from the Trade Register of the Chamber of Commerce or a law, articles of association, or a general administrative order, in which the Authorised Representative (or representation) is specified;
- For organisations outside the Netherlands, the National Trade Register or equivalent or a law, articles of association, or a general administrative order, in which the Authorised Representative (or representation) is specified;
- For private law organisations with and without legal personality, a recently certified extract (maximum 1 month old) from the Trade Register of the Chamber of Commerce.

QuoVadis checks that a legal organisation is not included in the most recent EU list of banned terrorists and organisations published by the European Council before certificate issuance (list of persons, groups and entities referred to in Articles 2, 3 and 4 of Common Position 2001/931/CFSP on the application of specific measures to combat terrorism.) These lists can be found via the web page: https://www.consilium.europa.eu/nl/policies/fight-against-terrorism/terrorist-list/. QuoVadis will not issue a Certificate to an organisation on this list.

3.2.2.1. Verification of the name of the organisation

QuoVadis verifies that the organisation name which is included in the Certificate is correct and complete and corresponds to the organisation name registered by the Subscriber.

As proof of the correctness of the given official organisation name, QuoVadis will request and verify at least the following supporting documents:

- For organisations within the Netherlands a recently certified extract (maximum 1 month old) from the Trade Register of the Chamber of Commerce or, if registration in the Trade Register has not yet taken place, a copy of the relevant page from the most recent version of the State Almanac where the address of the relevant Netherlands organisation is stated;
- For private law organisations with and without legal personality, a recently certified extract (maximum 1 month old) from the Trade Register of the Chamber of Commerce. Furthermore, the evidence submitted must distinguish the organisational entity from any other organisations with the same name. In general, the official name of the organisation is also stated in an extract from the Trade Register of the Chamber of Commerce.

3.2.2.2. Verification of the address of the organisation

QuoVadis verifies that the address the organisation provided by the Subscriber is correct and complete and that it is also the address where it carries out its work.

Address is only understood to mean street name, house number (possibly with addition) postal code and city.

As proof of the correctness and existence of the provided address and that it is also the address where the organisation carries out its work, QuoVadis will request and verify at least the following supporting documents:

- For organisations within the Netherlands a recently certified extract (maximum 1 month old) from the Trade Register of the Chamber of Commerce or, if registration in the Trade Register has not yet taken place, a copy of the relevant page from the most recent version of the State Almanac where the address of the relevant State organisation is stated.
- For private law organisations with and without legal personality, a recently certified extract (maximum 1 month old) from the Trade Register of the Chamber of Commerce.

If the address in the supporting documents matches the address of the request, QuoVadis will regard this as sufficient proof that this is also the address where the organisation carries out its work.

If the address in the supporting documents does not match, QuoVadis will visit the provided location of the Subscriber and record its findings in a report. The report must include at least the following:

- Whether the address of the location of the Subscriber exactly matches the address of the request.
- The nature of the buildings/location of the Subscriber and whether this is the location where the organisation is likely to perform its work.
- Whether permanent signs are present that identify the location of the Subscriber.
- One or more photos of the outside of the Subscriber's premises (on which, the signposts and street address plate, if existing, are present) and the reception desk or office workspace of the Subscriber.

Alternatively, QuoVadis will also accept a statement from an external auditor or civil-law notary confirming the address provided and that this is the address where the organisation performs its work.

3.2.2.3. Verification of the telephone number of the organisation

QuoVadis verifies that the general telephone number of the organisation provided by the Subscriber is correct and complete.

As proof of correctness and the existence of the provided general telephone number of the organisation, QuoVadis will:

- call the relevant telephone number and verify that the Subscriber can indeed be reached at the telephone number provided; and
- verify the general telephone number of the organisation in the most recent version of the (online) Telephone Directory, or by means of a certified extract (maximum 1 month old) from the Trade Register of the Chamber of Commerce; or
- receive a statement from an external auditor or notary confirming the provided general telephone number of the Subscriber

3.2.2.4. Verification of the age of the organisation

If, based on the requested data, it appears that the Subscriber's organisation has been in existence for less than three years (calculated from the date of registration of the Trade Register, or the date of publication of the law or general administrative order until the date of the (EV) SSL Certificate request), then QuoVadis will verify that the Subscriber is able to participate in business transactions because it has an active/current bank account.

As proof of correctness and the existence of the provided payment account, QuoVadis requests and verifies at least one of the following supporting documents:

- A statement from a financial institution, which is licensed in the Netherlands by the DNB [the Netherlands Bank] and falls under the Dutch deposit guarantee scheme, which shows that the Subscriber has an active current account.
- A statement from an external auditor that the Subscriber has an active current account with a financial institution that is licensed in the Netherlands by DNB and falls under the Dutch deposit guarantee scheme.
- For organisations incorporated and doing business other than the Netherlands, proof of a banking relationship with a duly regulated financial institution is acceptable.

3.2.2.5. Unverified data

During the registration procedure, forms are used that serve as registration of the data provided by the Subscriber. This contains data which serves for correspondence purposes and/or that can optionally be included in the Certificate. For example, the address details of a branch of the organisational entity or the name of the department (OU).

3.2.3. Validation of the Domain Authorisation

QuoVadis verifies that the Subscriber is the registered owner of the domain name (FQDN), if applicable, or that the Subscriber is exclusively Authorised by the registered domain name owner to use the domain name on behalf of the registered domain name owner.

This verification will not be outsourced by QuoVadis to Registration Authorities or other parties.

If the Subscriber indicates that it is the registered owner of the domain name provided in the request, QuoVadis will:

- verify that the domain name is registered with a registrar or domain administrator, such as SIDN (Foundation for Internet Domain Registration in the Netherlands), affiliated with Internet Corporation for Assigned Names and Numbers (ICANN), or an organisation that is part of Internet Assigned Numbers Authority (IANA) and;
- make use of a WHOIS service, part of an organisation connected to or part of ICANN or IANA, which provides the data via HTTPS or the CSP must use a command line program, if a WHOIS service is used that offers data via HTTP and;
- verify in the WHOIS service, the name, home address and the administrative contact person of the organisation and compare this data with the verified Subscriber data and record that there is no inconsistency between both sets of data and;
- verify that the domain name does not appear on a spam and/or phishing blacklist. QuoVadis uses at least http://www.phishtank.com for this purpose.
- verify if it is a domain name of a Fortune 500 company or
- verify if it is a domain name with a second level domain equal to a second level domain of the top 500 domain names worldwide and the Netherlands specifically.

If the domain name is of a Fortune 500 company or concerns a second level domain that is equal to a second level domain of the top 500 domain names worldwide and in the Netherlands, approval must be given by the management for publication

If the domain name appears on phishtank or another trustworthy blacklist that has been consulted, QuoVadis will handle the request for the relevant services Certificate with extra care during the verification process. If a 100% phish status comes back on the FQDN that is being requested, the Certificate will not be issued.

The data used to verify that the Subscriber is the registered owner of the domain name (FQDN) provided in the request may not be older than 13 months, otherwise the data must be requested and verified again.

If the Subscriber indicates that it is exclusively Authorised by the registered domain name owner to use the domain name on behalf of the registered domain name owner, then QuoVadis will, in addition to performing the above checks:

- request a statement from the registered domain name owner (e.g. by e-mail or telephone) in which the registered domain name owner must confirm that the Subscriber has the exclusive right of use for the domain name (FQDN) and;
- request and verify a written and signed statement from a civil-law notary or external auditor stating the domain name (FQDN) for which the Subscriber, on behalf of the registered domain name owner, has been granted the exclusive right of use and;
- verify that the domain name (FQDN) is not a generic Top Level Domain (gTLD) or country code Top Level Domain (ccTLD). For these domain names, only the Subscriber may register as a registered domain name owner.

A statement from the registered domain name owner or notary or external accountant may not be older than 13 months.

The validation of the FQDN is in accordance with section 3.2.2.4 of the Baseline Requirements.

For every FQDN included in a Certificate QuoVadis confirms that, from the date of issue of the Certificate, the Applicant is the domain name registrant or controls the FQDN through:

1. Direct communication with the domain name registrant by e-mail, facsimile or post with the domain name registrar. Performed in accordance with BR section 3.2.2.4.2 with a random value (valid up to at most 30 days after generation)
2. Direct communication with the domain name registrant by calling their telephone number and by receiving an answer to confirm the request of the Applicant for verification of the FQDN. The telephone number used must be the number that is mentioned by the domain name registrar. Performed in accordance with BR section 3.2.2.4.3;
3. Communication by e-mail with the manager of the domain by making use of an e-mail address that uses 'admin@', 'manager@', 'webmaster@', 'hostmaster@' or 'postmaster@', ensuring that it regards the domain name manager. Performed in accordance with BR section 3.2.2.4.4;
4. Inclusion by the Applicant of the FQDN of a stipulated Random Value on its website in the URL "domain.tld/well-known/pki-validation" or IP via "xx.xx.xx.xx/well-known/pki-validation". Performed in accordance with BR section 3.2.2.4.6;
5. Confirmation of ownership by having the Applicant includes a stipulated Random Value (which starts with an underscore) in a DNS record of the requested Authorisation Domain Name. Performed in accordance with BR section 3.2.2.4.7;
6. Confirmation of the control of the Applicant over the FQDB by demonstrating management of an IP address that is returned by a DNS search for A- or AAAA records for the FQDN, performed in accordance with BR sections 3.2.2.5 and 3.2.2.4.8;
7. Confirmation that the Applicant is the domain contact for the basic domain name (on the conditions that the CA or RA is also the domain name registrar or a branch of the registrar), performed in accordance with BR section 3.2.2.4.12;
8. Confirmation of the control of the Applicant over the FQDN by sending a stipulated Random Value to a DNS CAA e-mail contact by e-mail and by subsequently receiving a confirming reaction with the help of the Random Value. The relevant CAA Resource Record Set is found with the help of the search algorithm defined in RFC 6844, section 4, as changed by Errata 5065, performed in accordance with BR section 3.2.2.4.13;

9. Confirmation of the control by the Applicant over the FQDN by sending a Random Value to the DNS TXT Record e-mail contact by e-mail for the authorisation domain name for the FQDN and by subsequently receiving a confirming response with the help of the Random Value, performed in accordance with BR section 3.2. 2.4.14;
10. Confirmation of the control of the Applicant over the FQDN by calling the telephone number of the Domain Contact and by receiving a confirming answer to validate the Authorised Domain Name. A telephone conversation can confirm the control over multiple Authorised domain names on the condition that the same domain contact telephone number is mentioned for every verified domain name that is verified and they provide a confirming answer for every Authorised domain name, performed in accordance with BR section 3.2.2.4.15; and
11. Confirmation of the control of the Applicant over the FQDN by calling the telephone number of the DNS TXT Record Phone Contact and by receiving a confirming answer to validate the Authorised Domain Name. Every telephone conversation can confirm the control over multiple Authorised Domain Names on the condition that the same telephone number of the DNS TXT Record Phone is mentioned for every verified domain name that is verified and they provide a confirming reaction for every Authorised Domain Name, performed in accordance with BR section 3.2.2.4.16.

IP Address

For each IP Address listed in a Certificate, QuoVadis confirms that, as of the date the Certificate was issued, the Applicant controlled the IP Address by:

1. Having the Applicant demonstrate practical control over the IP Address by confirming the presence of a Request Token or Random Value contained in the content of a file or webpage in the form of a meta tag under the "/.well-known/pkivalidation" directory on the IP Address, performed in accordance with BR Section 3.2.2.5.1;
2. Confirming the Applicant's control over the IP Address by sending a Random Value via email, fax, SMS, or postal mail and then receiving a confirming response utilizing the Random Value, performed in accordance with BR Section 3.2.2.5.2;
3. Performing a reverse-IP address lookup and then verifying control over the resulting Domain Name, as set forth above and in accordance with BR Section 3.2.2.5.3;
4. After July 31, 2019, QuoVadis will not perform IP Address validations using the any-other-method method of BR Section 3.2.2.5.4;
5. Confirming the Applicant's control over the IP Address by calling the IP Address Contact's phone number, as identified by the IP Address Registration Authority, and obtaining a response confirming the Applicant's request for validation of the IP Address, performed in accordance with BR Section 3.2.2.5.5;
6. Confirming the Applicant's control over the IP Address by performing the procedure documented for an "http-01" challenge in draft 04 of "ACME IP Identifier Validation Extension," available at https://tools.ietf.org/html/draft-ietfacme-ip-04#section-4, performed in accordance with BR Section 3.2.2.5.6; or
7. Confirming the Applicant's control over the IP Address by performing the procedure documented for a "tls-alpn-01" challenge in draft 04 of "ACME IP Identifier Validation Extension," available at https://tools.ietf.org/html/draft-ietfacme-ip-04#section-4, performed in accordance with BR Section 3.2.2.5.7.

High risk domains

QuoVadis maintains a list of *High-Risk Domains* and has implemented technical controls to prevent the issue of Certificates to certain domains. QuoVadis follows documented procedures that identify and require additional verification activity for high risk Certificate requests, prior to the approval of the Certificate.

3.2.4. Authentication of the Authorised Representative

QuoVadis will verify who the Authorised Representative (or Representation) of the Subscriber is.

As proof of correctness and the existence of the Authorised Representative (or Representation) provided by the Subscriber, QuoVadis will request and verify at least one of the following supporting documents:

- For entities within the Netherlands, a recently certified extract (maximum 1 month old) from the Trade Register of the Chamber of Commerce or, if registration in the Trade Register has not yet taken place, a copy of the relevant page from the most recent version of the State Almanac (http://staatsalmanak.sdu.nl), on which the Competent Representative (or Representation) is stated;
- For organisations within the business world, a recently certified extract (maximum 1 month old) from the Trade Register of the Chamber of Commerce in which the Authorised Representative (or Representation) is stated.

QuoVadis checks to confirm that the Competent Representative is not on the then current EU list of banned terrorists and organisations:

https://www.consilium.europa.eu/nl/policies/fight-against-terrorism/terrorist-list/

3.2.4.1. Verification of the identity of the Certificate Holder

QuoVadis will verify the identity and, if applicable, specific properties of the Certificate Manager, in accordance with Dutch laws and regulations. Proof of identity is checked by verification of the physical appearance of the person.

This check must take place again, every 13 months, unless the contract with the Subscriber explicitly deviates from this by e.g. It states that the Certificate Manager retains his or her role until such time as this is revised by the Subscriber, or until the agreement expires or is terminated. In the appointment form for the Certificate Manager, QuoVadis includes the above deviation as standard.

3.2.4.2. Verification of Certificate Manager

The Certificate Manager is a person whose identity must be determined, in some cases in conjunction with an organisational entity by QuoVadis.

Evidence must be submitted to QuoVadis of:

- full name, including surname, given name, initials or other first name (s) (if applicable) and inserts (if applicable);
- date and place of birth, an appropriate national registration number, or other characteristics of the Certificate Manager that can be used to distinguish, insofar as possible, the person from other persons with the same name;
- proof that the Certificate Manager is entitled to receive a Certificate for a Certificate Holder on behalf of the legal entity or other organisational entity. This proof may not be older than 13 months, otherwise the data must be requested and verified again, unless the contract with the Subscriber explicitly states that the Certificate Manager retains his or her authorisation until such time as this is revised by the Subscriber or until the time that the agreement expires or is terminated.

3.2.4.3. Non-verified Subscriber information

Non-verified Subscriber information includes the Organisational Unit (OU) as mentioned in this CPS. QuoVadis does not verify this information nor any intellectual property rights of the Applicants.

3.2.5. Authorisation of the Certificate Holder (Service)

3.2.5.1. Verification of authorisation of the Certificate Holder (Service)

QuoVadis will check that:

- the proof that the Certificate Holder is Authorised on behalf of the Subscriber to request and receive a Certificate is authentic;
- whether the Certificate Manager has obtained permission from the Subscriber to perform actions assigned to him (if the Certificate Manager performs the registration process).

Note: The Certificate Manager who takes over actions from the Certificate Holder does not necessarily have to be the same person as the system manager or personnel officer. It is also permitted that the knowledge of the activation data of the key material (e.g. PIN) is shared by different persons, if required by the management

organisation. However, it is recommended that the number of people who know the PIN is kept as low as possible and to take measures that restrict access to the PIN.

3.2.5.2. Accountability of the Subscriber

In the agreement between the Subscriber and QuoVadis, the Subscriber agrees that if relevant changes occur in the relationship between the Subscriber and Certificate Manager and/or service, it is responsible for immediately communicating this to QuoVadis. If the service ceases to exist, this must be done by means of a revocation request.

3.2.6. Data Source Accuracy

Documents relied upon for the verification of identity may not be older than 1 (one) to 3 (three) months, at the time of the Certificate Issuance. This includes:

- Chamber of Commerce information (or comparable) - 1 (one) month
- Domain name check and validation – 3 (three) months
- Identification checks – 3 (three) months
- Blacklist & Phishing check – 3 (three) months

If the document is older, QuoVadis will request updated documents from the Applicant. QuoVadis imposes time limits to ensure the accuracy and reliability of information.

For Server Certificate applications, all other documents used in the application process (ID validation for example) should not be older than 825 (eight hundred and twenty-five) days. When data is older, verification must take place again.

3.3. IDENTIFICATION & AUTHENTICATION FOR RE-KEY REQUESTS

QuoVadis does not re-key Certificates. When a Subscriber requests new keys, new Certificates need to be issued.

3.4. IDENTIFICATION & AUTHENTICATION FOR REVOCATION REQUEST(S)

QuoVadis will revoke a Digital Certificate upon receipt of a valid request. A revocation request should be promptly and directly communicated to the Issuing CA and the Registration Authority that approved or acted in connection with the issue thereof.

The Certificate Holder may be required to submit the revocation request via the QuoVadis Support Line or directly over an Internet connection. The Certificate Holder, Registration Authority or Issuing CA may be required to provide a shared secret or pass phrase that will be used to activate the revocation process.

Digital Certificate revocation requests may also be issued by contacting the administrators of the Issuing CA or Registration Authority directly.

The Certificate Holder, organisation or where applicable, an appropriately authorised regulatory or professional body may request revocation by contacting the Issuing CA and providing adequate proof of identification in accordance with this QuoVadis CP/CPS or an equivalent method.

QuoVadis maintains a continuous 24/7 ability to internally respond to any high priority Certificate Problem Report and will take such action as deemed appropriate based on the nature of such a report. This may include, but not be limited to, the revocation of a Certificate that is the subject of such a complaint.

Certificate Holders may also revoke their Certificates via the Trust/Link system.

If the Subscriber wishes to revoke the Certificate(s), then the following options are applicable:

3.4.1. TrustLink Certificate Management Portal

Each Certificate Holder who has received a Certificate directly from the TrustLink portal has credentials to log in, select the certificate to revoke and select a reason for revocation. The system confirms the real time revocation by message display and email confirmation. Where the Certificate is issued via a subsidiary system, that system communicates with TrustLink to revoke the certificate. Duly authorised Client

Administrators may additionally request revocation of certificates which have been issued for subscribers in their organisation.

3.4.2. Telephone

Telephonic communication using a pre-existing shared secret, password or other information associated with Certificate Holder's account with the Certification Authority following appropriate Identification.

3.4.3. E-mail

Revocation requests solely via e-mail are not accepted for PKIoverheid Certificates.

3.4.4. Professional Bodies

In certain cases, namely where a PKIoverheid professional certificate showing the Certificate Holder's affiliation with a designated professional body, for example lawyer/accountant/doctor; the associated professional body may request revocation when a member is no longer allowed to work or is no longer capable of working in that profession. In these circumstances appropriate procedures to confirm authorisation of the request are made prior to revocation.

3.4.5. Professional Bodies

In certain cases, a Government or Industry Supervisory Body may request revocation when a Certificate Holder's entitlement to use certain fields in a certificate, for example when a PSD2 qualifier is expired or revoked. In these circumstances appropriate procedures to confirm authorisation of the request are made prior to revocation.

4. CERTIFICATE LIFECYCLE

4.1. CERTIFICATE APPLICATION

4.1.1. Who can apply for a Certificate

Only an Authorised Representative of the Subscriber can apply for a Subscriber registration. By signing the Subscriber registration, the Authorised Representative authorises one or more contacts mentioned in the forms to apply for, install, manage and revoke Certificates and to authorise other contacts on behalf of the Subscriber.

The Applicant is responsible to provide correct and up-to-date data, as required for the generation and Issuance of Certificates as well as the correct usage of the Certificates. By agreeing to the Terms and Conditions of both QuoVadis, the PKIoverheid framework and the Privacy Statement and signing the contracts, the Applicant also agrees to all underlying documents (the CPS, CP and others). If any of the required information for the Issuance of Certificates is missing, incomplete or produces a negative outcome, QuoVadis will reject the application for a Certificate.

Subscribers have obligations regarding usage of the Certificate(s), which are set out in the Terms and Conditions documents and the contracts.

4.2. PROCESSING A REQUEST

Prior to Issuing a Certificate, various verification procedures are carried out during the registration process (see paragraph 3.2). QuoVadis can only make approval assessments based on the information provided by the Applicant. The Applicant has the obligation to ensure all information provided is accurate and complete at the time of application, QuoVadis provides no guarantees to the Issuance of Certificates.

QuoVadis processes Certificate application information on a "best efforts" basis, usually on the day of receipt. Completion of the certification Issuing process is dependent on the availability of both parties (QuoVadis and Applicant) to make an appointment for the Face-to-Face identity check. The total processing time from identification of the Applicant to Issuance of a Certificate is approximately three (3) to five (5) working days.

Subject to the applicant providing all required information including but not limited to any and all data that is required by QuoVadis to process and supply the certificate, including successful (domain)validation

information and a conforming Certificate Signing Request (CSR) as well as appropriate Organisation and Certificate Manager identity and authorisation data, all valid, non-expired certificates can be replaced within 5 days.

4.3. CERTIFICATE ISSUANCE, CERTIFICATE ACCEPTANCE

QuoVadis follows the processes outlined in this CPS document for the Issuance of Certificates in accordance with the legal and regulatory requirements as described in paragraph 1.1.

After Issuing a Certificate, the Certificate Holder or Certificate Manager must explicitly confirm the handover of the key material belonging to the QuoVadis issued Certificate. Acceptance of Certificates is deemed to have taken place after completion of the Certificate issue via TrustLink Enterprise.

To reiterate: With the acceptance of the Certificate and its use, the Certificate Holder or Certificate Manager has agreed with

- What is contained in this CPS;
- The General Terms and Conditions, the PKIoverheid Terms and Conditions, the Privacy Policy and the Terms and Conditions of the contracts signed;
- The obligation to adequately secure (access to) the Private Key corresponding to the public key included in the Certificate. Where applicable, to use the SSCD/QSCD carefully and to take reasonable precautions to prevent loss, theft, modification or unauthorised use of the Certificate/Private Key.

The Certificate Holder or Certificate Manager is obliged to check the data included in the Certificate for correctness prior to acceptance of the Certificate. In the off chance that the Certificate is not entirely accurate, the Certificate Holder or Certificate Manager must adjust it during the issue process, or if it subsequently transpires that the information in the Certificate is incorrect, make a request for revocation immediately. The acceptance of the Certificate contents is confirmed by downloading or using the Certificate issued.

After the successful Issuance of the Certificate, the Applicant is known as the Subscriber.

4.4. KEY PAIR & CERTIFICATE USAGE

As described in this CPS the Subscriber agrees with all applicable Terms and Conditions, the Relying Parties on their hand must ensure that:

- the Certificate is used in accordance with its intended use;
- the Certificate is used in accordance with any Key-Usage field extensions;
- the Certificate is valid at the time that it is relied upon by consulting the Certificate status information in the CRL, or via the OCSP protocol.

In addition, it is stated that the Subscriber itself will ensure timely replacement, in the case of an impending expiry of validity, and emergency replacement in the case of compromise and / or other types of emergency with regard to the Certificate or the Certificates from which it is derived. The Subscriber is expected to take adequate measures to guarantee the continuity of the use of Certificates.

The validity of a Certificate should not be confused with the authority of the Certificate Holder to perform a certain transaction on behalf of an organisation. PKIoverheid does not regulate appropriateness of reliance. A relying party must gain assurance itself that it is appropriate to rely on the certificate for a particular transaction by another means.

4.5. REPORTING PROBLEMS AND CERTIFICATE TRANSPARENCY

In the case of problems with the Certificate, subscribers can contact QuoVadis by phone using the support line (+31 30 2324320) during normal Dutch office working hours. An emergency number can be used (+1 615 2293456) for critical issues or email to support@quovadisglobal.com for non-emergencies (revocation per mail is not possible). The support team will take appropriate action.

QuoVadis fulfils the requirements for Certificate Transparency as set in 4.5.2-pkio145 by publication of pre-certs and issued Certificates to appropriate directories.

4.6. CERTIFICATE RENEWAL

Renewal of a Certificate means reissuance of the Certificate using the same key pair. QuoVadis does not support Renewal; key pairs must always expire at the same time as the associated Certificate. QuoVadis makes reasonable efforts to notify Certificate Holders of the imminent expiration of a Certificate. Identification and Authentication procedures are generally the same for replacement Certificates as for a new application.

4.7. CERTIFICATE RE-KEY

QuoVadis does not re-key Certificates. In the event of a certificate expiration a new certificate request must be submitted and following the procedures set out in this CPS a new certificate and new key pair will be generated.

4.8. CERTIFICATE MODIFICATION

QuoVadis does not provide Certificate Modification. QuoVadis may reissue or replace a valid Certificate when the Certificate Holder's common name, organisation name, device name, or geographic location changes. Modified information must undergo the same Identification and Authentication procedures as for a new Certificate.

4.9. REVOCATION AND SUSPENSION OF CERTIFICATES

The revocation of a Certificate ensures that it is declared invalid and that this status is included in the Certificate status information. Once a Certificate has been withdrawn, it can no longer receive the status 'valid'. QuoVadis does not support certificate suspension.

4.9.1. Circumstances leading to revocation

Certificates will be revoked when:

- the Subscriber indicates that the original request for a Certificate was not allowed and the Subscriber does not grant permission retroactively;
- QuoVadis has sufficient evidence that the Subscriber's Private Key (corresponding to the public key in the Certificate) has been compromised, or there is a suspicion it has been compromised, there is an inherent security weakness, or that the Certificate has been misused in another way. A key is considered compromised in the case of unauthorised access or suspected unauthorised access to the Private Key, lost or presumably lost Private Key or SSCD/QSCD, stolen or presumably stolen key or SSCD/QSCD or destroyed key or SSCD/QSCD;
- a Subscriber does not fulfil its obligations as stated in the CP, or the corresponding CPS of QuoVadis or the agreement that QuoVadis has entered into with the Subscriber;
- QuoVadis is informed or otherwise becomes aware that the use of the domain name in the Certificate is no longer legally permitted (e.g. by a court decision);
- QuoVadis is informed or otherwise becomes aware of a material change in the information contained in the Certificate.
- QuoVadis determines that the Certificate has not been issued in accordance with the CP or the associated CPS of QuoVadis or the agreement that QuoVadis has entered into with the Subscriber;
- QuoVadis determines that information in the Certificate is incorrect or misleading;
- QuoVadis ceases its activities and the CRL and OCSP services are not undertaken by another TSP;
- the technical content of the Certificate entails an irresponsible risk for Subscribers, Relying Parties and third parties (e.g. browser parties)

In addition, Certificates can be withdrawn as a measure to prevent or combat an emergency. As emergency is certainly considered an attack or suspected attack on the Private Key of QuoVadis with which Certificates are signed.

QuoVadis is the determinant of the requirements for revocation which can be exercised at its sole discretion.

4.9.2. Who may request a revocation

The following parties may apply for the revocation of an end-user Certificate:

- The Certificate Manager
- The Subscriber
- QuoVadis as a TSP
- Any other interested party/person.

4.9.3. Procedure for a request for revocation

QuoVadis will revoke a Certificate upon receipt of a valid request. A revocation request must be notified to QuoVadis immediately after a circumstance as mentioned above in section 4.9.1 occurs.

The Subscriber or the Certificate Manager can personally contact the Registration Authority, submit a revocation request by telephone via the QuoVadis support line. The Subscriber and the Certificate Manager may be asked to authenticate themselves.

The online revocation facility via the QuoVadis website TrustLink Enterprise is available 24 hours a day, 7 days a week via https://tl.quovadisglobal.com. The QuoVadis support line +31 (0) 30 232 4320 is also available outside office hours via +1 651 229 3456. The Registration Authority at the office of QuoVadis +31 30 232 4320 is only available during office hours. In the case of system defects, service activities, or other factors that are beyond the scope of QuoVadis, QuoVadis will do everything possible to ensure that the unavailability of the revocation facility will not last longer than four (4) hours. In the case of unavailability, the Registration Authority has the option of having a Certificate revoked directly via an emergency procedure on the QuoVadis PKIoverheid CA environments.

The status of the certificate is updated immediately following revocation in the QuoVadis CRL and OSCP responders and published within 5 minutes.

4.9.4. Availability of the revocation management service

The maximum time which the availability of the revocation management services must be restored is set at 4 (four) hours.

4.9.5. Recording the reason for revocation

QuoVadis will record the reason for the revocation of a Certificate in all circumstances using the codes included in RFC 5280.

4.9.6. Certificate Status Information

QuoVadis uses an OCSP and a CRL to make the Certificate status information available.

4.9.7. Availability of the revocation management service

The online revocation facility via the QuoVadis website TrustLink Enterprise is available 24 hours a day, 7 days a week via https://tl.quovadisglobal.com. The QuoVadis support line +31 (0) 30 232 4320 is also available outside office hours via +1 651 229 3456. The Registration Authority at the office of QuoVadis +31 30 232 4320 is only available during office hours. In the case of system defects, service activities, or other factors that are beyond the scope of QuoVadis, QuoVadis will do everything possible to ensure that the unavailability of the revocation facility will not last longer than four (4) hours. In the case of unavailability, the Registration Authority has the option of having a Certificate revoked directly via an emergency procedure on the QuoVadis PKIoverheid CA environments.4.9.8 Validity of CRL

A CRL is valid for a maximum of 72 hours and is generated every 12 hours. If a revocation has taken place, the CRL will be generated within 5 minutes.

4.9.8. Issuing subordinate CA

If there is an Issuing subordinate CA under the QuoVadis CA, then:

- QuoVadis uses an OCSP and a CRL to make the Certificate status information related to the Issuing subordinate CA available;
- QuoVadis establishes the reason for the revocation of the Issuing subordinate CA Certificate;

4.9.9. Duration for processing a revocation request

The maximum duration between the receipt of a revocation request or revocation report and the change of the revocation status information, which is available to all Relying Parties, is set at four hours.

This duration applies to all types of Certificate status information (CRL and OCSP)

4.9.10. Duration for processing a revocation request in the case of an Issuing subordinate CA

In the case of an Issuing subordinate CA, the maximum period between the decision to revoke an Issuing subordinate CA (established in a report) and the change of the revocation status information that is available to all Relying Parties is set at 72 hours.

4.9.11. OCSP and CRL Services

With regard to its OCSP and CRL services, QuoVadis has appropriate server capacity with which a commercially acceptable response time can be achieved on the basis of queries of all outstanding QuoVadis Certificates.

4.9.12. Check conditions for consulting Certificate status information

An end-user consulting the Certificate status information must verify the Authenticity of this information by checking the Electronic Signature with which the information was signed and the corresponding certification path.

4.9.13. Availability of check conditions

The obligation to check conditions is included by QuoVadis in the user conditions that are made available to the Relying Parties.

4.9.14. Frequency of Issuance of the Certificate Revocation List (CRL)

QuoVadis will update and re-issue the CRL for end-user Certificates at least once every 7 calendar days and the date of the “Next Update” field will not be more than 10 calendar days after the date in the field “Effective Date”.

4.9.15. Online revocation/status check

QuoVadis offers Online Certificate Status Protocol (OCSP) checks. The URL for the OCSP responder can be found within the Authority Information Access extension of the Certificate.

4.9.16. Signing the online revocation/status check

OCSP responses of QuoVadis are digitally in accordance with RFC 6960, signed by either:

- the private (CA) key with which the Certificate for which the status is requested is also signed;
- the Private Key of a responder designated by TSP who has an OCSP-Signing Certificate signed for this purpose by the private (CA) key with which the Certificate of which the status is requested is also signed;
- If QuoVadis opts for the second option, the OCSP-Signing Certificate that the responder has at its disposal fulfils the following additional condition (see RFC6960 and the requirements of the PoR part 3e, 4.9.9.4):
- The OCSP-Signing Certificate is also provided with the extension id-pkix-ocsp-nocheck which is not marked as "critical" and has the value "NULL"

4.9.17. OCSP Response

Apart from the publication of CRLs QuoVadis also offers Certificate status information using Online Certificate Status Protocol ("OCSP). The layout of the OCSP response is in accordance with IETF RFC 6960.

OCSP validation is an online validation method in the course of which QuoVadis sends an electronically signed message to the relying party (OCSP response) after the relying party has sent a specific request for status information (OCSP request) to the OCSP service (OCSP responder) of QuoVadis. The requested status of the relevant Certificate is mentioned in the OCSP response.

The status can have the following values: good, revoked or revoked with reason CertificateHold.

If an OCSP response is, for any reason whatsoever, is not received or is malformed then this cannot result in a conclusion regarding the status of the Certificate. The URL of the OCSP with which the revocation status of a Certificate can be validated is mentioned in the Certificate.

An OCSP response may not always sent and signed by the OCSP responder for which the status is requested. A Relying Party must verify the signature under the OCSP response with the Certificate that is also sent in the OCSP response.

To clarify what is stated in IETF RFC 6960, QuoVadis does not use pre-calculated OCSP responses (precomputed responses).

4.9.18. Updating OCSP Service

QuoVadis updates the OCSP service at least once every 3 (three) calendar days. The maximum expiry period for the OCSP responses is 7 (seven) calendar days.

4.9.19. Supported methods for OCSP responses

QuoVadis supports the GET and POST methods in offering OCSP responses according to RFC5019. Http-based OCSP requests can use both the GET and the POST method for submitting a request.

As required by the BR (all TLS/SSL Certificates) or other industry requirements then QuoVadis OCSP responder shall not react to a request for the status of a Certificate that has not been issued yet with a "good" status

4.9.20. Supported OCSP responses

If the QuoVadis OCSP responder receives a status request from a Certificate that has not been issued, the responder will not respond with the status "good". QuoVadis records such requests to the responder as part of the security procedure and will act upon them, if necessary.

4.9.21. Suspension of Certificates

Within the PKIoverheid, QuoVadis does not support suspension of Certificates for its services.

4.9.22. Operational characteristics

QuoVadis will maintain appropriate server capacity that guarantees a response time of 10 seconds or less under normal circumstances for OCSP and CRL services.

4.9.23. Certificate Status Service

The maximum time within which the availability of the revocation status information will be recovered is set at 4 (four) hours.

5. PHYSICAL, PROCEDURAL AND PERSONAL SECURITY

5.1. PHYSICAL SECURITY

QuoVadis appropriately manages and implements the physical security measures to restrict access to the hardware and software used for CA operations.

5.1.1. Site location

QuoVadis operations facilities are especially designed for computer operations and as such have been built to meet the security requirements that apply to QTSPs. The main datacenter in Bermuda has been independently certified. Applicable norms and standards for security features include measures against:

- fire (according to standard DIN 4102 F90) with an automatic FM200 extinguishing system;
- smoke and humidity (according to DIN 18095 standard);
- robbery and vandalism (ET2 according to standard DIN 18103);
- electromagnetic influences and radiation (such as an electromagnetic pulse).

QuoVadis has a certified BS-EN 1047 classification and an ISO9000/1/2 liability insurance.

The RA activities are performed by QuoVadis TrustLink B.V., established in Nieuwegein. In certain cases, QuoVadis uses the identification services of AMP Group B.V. as well as the services of appropriately trained employees of other QuoVadis group companies.

5.1.2. Physical access

QuoVadis allows physical access to its secure operational environment only to Authorised persons. Controls have been implemented for physical access to the CA operations facilities. The physical access of persons within the secure environment is stored in a log file and periodically evaluated. Physical access to the secure environment is controlled by a combination of access passes and biometric identification.

Access to the QuoVadis TrustLink B.V. office is controlled. Access is permitted to employees with an electronic key system. Visitors to the office must be accompanied by a member of the QuoVadis staff.

5.1.3. Power supply and cooling

The secure environment is connected to the regular standard power supply. All components are further connected to a UPS unit in order to prevent uncontrolled unavailability of critical systems during the possible electricity failure.

5.1.4. Water

Measures have been taken against flooding within the secure environment. The area is located on a higher floor with raised floors. The walls are also sealed, and the location complies with the safety requirements as set forth in DIN 18095.

5.1.5. Fire protection and prevention

The protected environment offers fire protection according to the guidelines of DIN 4102 F9, by means of an automatic extinguishing system.

5.1.6. Media Storage

All magnetic media containing information regarding the QuoVadis PKIoverheid services, including backup files, are stored in storage facilities, cabinets and fireproof safes with fire and electromagnetic interruption (EMI) resistance. These are located in the secure environment or at a secure external storage location.

5.1.7. Waste Processing

Paper documents and magnetic media that contain confidential QuoVadis or commercially sensitive information are securely destroyed by:

- In the case of magnetic media:
  - Inflicting irreparable physical damage or the complete destruction of the relevant data-carrier;
  - Use of a suitable device for deleting or overwriting the information; and
- In the case of printed information, the document is shredded or destroyed in a suitable manner.

5.1.8. External Backup

An external location is used for storing backup software and data. The external location:

- is available to Authorised personnel 24 hours a day, 7 days a week for the purpose of retrieving software and data;
- has adequate physical security measures (for example, software and data are stored in fireproof safes and storage is behind doors with access control, in environments that are only accessible to Authorised personnel).

5.2. PROCEDURAL SECURITY

QuoVadis guarantees that physical and technical security procedure are complied with in accordance with this CPS and other relevant internal operational documents.

It is business policy that QuoVadis does not delegate PKI operations to other organisations, barring the establishment of identity, in certain instances.

5.2.1. Vulnerability assessments

Baseline assessments, as well as constant threats and risk vulnerabilities are performed on all components of the QuoVadis PKIoverheid CA environment, including the material, the physical location, the documents, the data, the software, the personnel, the administrative processes and the communications.

QuoVadis' systems are assessed via internal and external vulnerability scans and penetration tests. These tests, as well as other risk analysis assessments, are carried out in accordance with a predetermined schedule and as needed in the case of a new vulnerability. Penetration tests are carried out by the Dutch Government Agencies at least annually. All foreseeable internal and external threats are assessed with both the risk analysis and compliance teams of both QuoVadis and DigiCert when they arise, or at least once per year. When significant changes to the infrastructure or applications are made, the risk and compliance teams are involved.

QuoVadis develops, implements, maintains and evaluates an information security plan based on the risk analysis. This plan describes a coherent set of appropriate administrative, organisational, technical and physical measures and procedure with which QuoVadis guarantees the availability, exclusivity and integrity of all PKIoverheid processes, requests and the data used for this

5.2.2. Trusted Roles

To ensure high security, the responsibilities are divided among multiple roles and persons. This has been achieved by, among other things, creating separate roles and accounts on the various components of the CA system, and each role has limited authorisations. Supervision can only be carried out by a person who is not directly involved in the Issuance of Certificates (for example, a Security or Administrative Officer who views system records or audit logs to ensure that other people act within their responsibilities and within the applicable Security Policy).

The applicable roles are:

- Certification Authority Officers (CAO) who are responsible for CA hardware and software and the generation and signing of the issue of CA keys.
- Registration Authority Officers (RA) who are responsible for executing the functions of the Registration Authority and the interface with QuoVadis.
- QuoVadis Chief Security Officer (CSO) who is responsible for verifying the integrity of the QuoVadis PKIoverheid CA's
- CA and its configuration and operations.
- System administrator (SYS) responsible for managing the QuoVadis systems, including installing, configuring and maintaining the systems.
- Data Protection Officer (DPO) who is responsible for the handling of all security incidents involving Person Data breach or leakage.

- System and Internal auditors who are authorised to view archives and audit logs of QuoVadis systems for the purpose of auditing.

5.2.3. Number of people required per task

QuoVadis ensures that the number of staff available for tasks is adequate to meet demand, but more so adequate to ensure that all security, risk and compliancy regulations are met.

QuoVadis maintains the segregation of duties between employees who control the issue of Certificates and employees who approve the Issuance of the Certificate.

CA key pair generation and initialisation requires the active participation of at least two Trusted Roles, on a case-by-case basis. Such sensitive actions also require the active participation and supervision of higher management.

5.2.4. Identification and Authentication for every role

Employees in Trusted Roles undergo extra screening and training, all employees are screened, verified and authenticated; including Face-to-Face checks and identification checks.

Employees in Trusted Roles use a Certificate issued by QuoVadis, stored on an SSCD/QSCD, to identify him/herself for operational steps on the various systems used for Issuing and managing PKIoverheid Certificates. A detailed record is kept of all access rights held by employees.

5.2.5. Roles that require a separation of duties

Privileges are assigned based on the tasks for the role, and a *need-to-know* and *least privilege* principle for access, rather than a default permission.

Transactions related to the issue of CA roles are separated between M from N employees, where M is equal to or greater than 2 (an M-of-N person check means that there is a minimum of "M" persons from a total of "N" persons who are authorised to perform the task). The implementation and maintenance of the system audit logs are separate from the people who operate such systems.

5.2.6. Optional Management and security

In addition to an audit carried out by an accredited auditor, QuoVadis may carry out periodic audits at its external suppliers of core PKIoverheid services to ensure that these suppliers have implemented and operationalised the relevant requirements of the PKIoverheid POR. QuoVadis may choose whether to conduct its own audit or to make use of existing audit results, such as those of the formal certification audits, the various internal and external audits, third party announcements and compliance reports.

QuoVadis is also entitled to inspect the underlying evidence such as audit files, relevant to the performance of PKIoverheid core services.

5.3. PERSONAL SECURITY

All employees, in trusted roles must have a clean and complete background check. Confidentiality agreements must be signed before commencing work, Declarations of Conduct from the Dutch Ministry of Justice are required for many roles.

QuoVadis is not liable for the conduct of employees who are outside the performance of their duties and over which QuoVadis has no control, including but not limited to (corporate) espionage, sabotage, criminal conduct.

5.3.1. Identity check and employee screening

The identity of the employee must be established face to face by a personnel officer or other appropriate resources from QuoVadis based on a valid passport, a valid identity card or a valid driver's license.

For determining the reliability of the employee, QuoVadis carries out at least the following actions:

- checking the correctness and completeness of the employment history stated by the employee;
- checking the correctness of the references provided by the employee;

- checking the correctness of the highest or most relevant training stated by the employee;
- requesting a Declaration of Conduct (VOG) from the employee.

5.3.2. Confidentiality statement

All employees and contractors are subject to confidentiality provisions included in their employment contracts or staff handbooks. All employees are required to complete online periodic training exercises which reiterate their confidentiality and security obligations.

5.3.3. Professional knowledge, experience and qualifications

Before Issuing services Server Certificates, QuoVadis will:

- train all personnel involved in checking and approving a services Server Certificate, whereby general knowledge about PKI, Authentication and verification policies and procedures with regard to the control and approval process and threats including phishing and other social engineering tactics, are covered;
- have all staff sit and successfully pass an internal exam;
- keep records of the training(s) and the exam and guarantee that the skills of the personnel concerned remain at the right level.

5.3.4. Documentation provided to staff

QuoVadis provides the staff with all necessary manuals, descriptions of procedures and training materials that are necessary to fulfil the function and role.

5.4. LOGGING PROCEDURES

QuoVadis is required under industry standards and best practice to log events and to store critical logs on servers other than those servers generating the log events in a secure manner. Due to the number of servers and transactions QuoVadis evaluates critical logging events and systems prior to implementation of logging procedures. The ethos of log management is to establish the who/what/when of data transactions.

5.4.1. Types of events recorded

The types of data recorded by QuoVadis include, but are not limited to:

- Lifecycle events
  - Key generation, backup, storage, recovery, archival and destruction
  - Cryptographic device lifecycle management events
- Certificate lifecycle events
  - Certificate requests and revocation
  - Verification activities
  - Date, time, contact persons, phone numbers and verification their verification
  - Acceptance (and rejection) of Certificate requests
  - Issuance of the Certificates
  - Generation of CRL's and OCSP's
- Security events
  - Access attempts
  - System actions performed
  - Profile changes
  - System Activity
  - Firewall and router activity
  - Entries to and from the QuoVadis controlled areas

All log entries provide at least the following:

- Source addresses (IP addresses if available)
- Target addresses (IP addresses if available)
- Time and date
- User ID's (if available)
- Name of the event
- Description of the event

QuoVadis determines which data it stores based on its risk analysis.

5.4.2. Retention of audit logs

QuoVadis log files for events related to Lifecycle events and Certificate lifecycle events are retained for a period of 7 years before deletion.

Log files for events related to Security events are retained for a period of 18 months before deletion.

All logfiles are back upped daily. The logfiles are stored in such a way that the integrity and accessibility of the data is guaranteed.

5.4.3. Security of audit logs

The relevant collected logs are regularly analysed for attempts to compromise the integrity of any part of the PKIoverheid service.

Only CA officers and auditors may view the complete audit logs. QuoVadis decides if the specific audit logs should also be viewed by others, as needed in certain situations, and then makes those logs available. Consolidated logs are protected against modification and/or destruction.

5.4.4. Notification concerning logging

When an event is logged, there is no need to notify the person, organisational entity, device, or request that performed or triggered the event.

5.5. ARCHIVING OF DOCUMENTS

5.5.1. Nature of archived data

QuoVadis archives documentation in accordance with its document access control policy and only makes it accessible after an authorised request.

For each Certificate, the archive contains the information related to activities concerning the creation, the issue, the use, the revocation, the period of validity and the renewal. This documentation file contains all the relevant evidence, including:

- Audit logs;
- Certificate requests and all related actions and forms;
- Content of issued Certificates;
- Proof of Acceptance Certificate and signed agreements
- Revocation requests and all related actions and records;
- Published Certificate Revocation Lists;
- Audit findings as discussed within this CPS.

5.5.1.1. Storage of information

QuoVadis stores all information used to verify the identity of the Subscriber and Certificate Manager, including reference numbers from the documentation used for verification, as well as limitations on validity.

5.5.1.2. Phishing

QuoVadis maintains a registration of all revoked Certificates and rejected requests for Certificates in connection with the suspicion of phishing or possible other abuse, at the discretion of QuoVadis. QuoVadis reports this to Phishtank.

5.5.1.3. Retention period for the archive

QuoVadis will, after the validity of the Certificate has expired, store all information regarding the request and possible revocation of the Certificate and all data used to verify the identity of the Certificate Subscriber, Authorised Representative and Certificate Manager for at least 7 years after the expiration date of the certificate.

5.5.2. Protection of the archive

The archives are adequately protected against modification or destruction. Access to the archive is limited. Only CA Officers, the QuoVadis Chief Security Officer and Auditors may view the entire archive. The contents of the archives will not be released in their entirety, except when required by law or by order of a court order or other legally competent authority.

5.5.3. Backup Procedures related to the archive

QuoVadis maintains and implements backup procedures such that, in case of the loss or destruction of the primary archives, a full set of spare copies is immediately available.

5.5.4. Requirements for time stamping of data

QuoVadis supports timestamping for all its data. All logged events that are recorded within the service of QuoVadis include the date and time of the time the event occurred. The date and time of the timestamp are based on the system time at which the QuoVadis PKIoverheid CA system is operating. QuoVadis uses procedures to ensure that all systems that are operational within the PKIoverheid (CA) environment rely on a reliable time source.

5.5.5. Archiving system

The QuoVadis archiving system is used exclusively as an internal system.

5.5.6. Procedures to obtain and verify the archive information

Only CA Officers, the QuoVadis Chief Security Officer and Auditors may view the entire archive. The contents of the archives will not be released in their entirety, except when required by law or by order of a court order or other legally competent authority. QuoVadis can decide to release logs of individual transactions when requested to do so by the Subscriber or its Representatives. A reasonable contribution to the administrative costs per request will be charged for this.

5.6. KEY CHANGEOVER

Changing the public key of the CA is based on a procedure established for this purpose. At the end of the lifespan of the CA Private Key, QuoVadis stops using this Private Key for signing public keys and only uses the expiring Private Key to sign CRLs and OSCP Responder Certificates associated with that Private Key.

A new CA signing key pair is issued and then all Certificates and CRLs issued from that moment on are signed with the new Private Key. This means that both old and new CA key pairs can be active simultaneously.

5.7. COMPROMISE AND DISASTER RECOVERY

5.7.1. Disaster management

QuoVadis has implemented procedures to minimise the consequence of disasters as much as possible. These measures include a Disaster Recovery Program and a Key Compromise Plan. As an example: Compromise of QuoVadis' Private Key is considered a disaster. QuoVadis will inform Relying Parties, Subscribers, Certificate Holders and Certificate Managers as soon as possible of the compromise of QuoVadis' Private Key by

publishing information about this on its website. QuoVadis will also send an e-mail to the affected parties listed above as well as the Government Policy Authority immediately.

5.7.2. Business continuity

QuoVadis has a Business Continuity Plan (BCP) to ensure continuity when a disaster occurs. The aim of the plan is to ensure the orderly recovery of business operations, communication to Subscribers and Relying Parties as well as the continuity of services for the affected Subscribers. The BCP includes all criteria as required per the CA/Browser Forum Baseline Requirements. The BCP is a confidential document and has been audited and approved by external auditors.

5.8. CA OR RA TERMINATION

If QuoVadis is forced to terminate the service, the negative consequences of this termination will be kept to a minimum.

QuoVadis specifies the procedures which are followed when terminating the provision of Certificate services. The procedures must have at least the following objectives:

- that any disruption caused by the termination of the QuoVadis certification service is limited to a minimum
- that archived documents from QuoVadis are retained
- that immediate reporting is provided to Subscribers, Certificate Holders, Relying Parties and other relevant parties within PKIoverheid
- that the revocation process of all Certificates issued by QuoVadis remains operational at the time of termination
- that relevant state bodies, including the PA PKIoverheid are informed within the framework of applicable laws and regulations

Wherever possible, the revocation of Certificates will be scheduled in conjunction with the scheduled issue of new Certificates by a TSP that takes over the activities of QuoVadis within PKIoverheid.

Wherever possible, the TSP that takes over the activities of QuoVadis within the PKIoverheid should use procedures, guidelines and obligations similar to those used by QuoVadis. The TSP that takes over the activities of QuoVadis within PKIoverheid must also issue Certificates to all Certificate Holders whose Certificates have been withdrawn. This requires that Subscriber and the Certificate Holders must conform to the procedures and requirements of the new TSP. The new TSP will, in any case, be responsible for making the Certificate status information available for six months, keeping the revocation management service (revocation facility) operational and storing the archived registration documents.

6. TECHNICAL SECURITY MEASURES

6.1. KEY PAIR GENERATION AND INSTALLATION

6.1.1. Key pair generation

The key of the QuoVadis PKIoverheid CA was generated and is stored within a cryptographic module that at least fulfils the standards FIPS 140-2 level 3 and/or Common Criteria EAL4 AUGMENTED (EAL4 +). The keys for the authorising Registration Officers are generated on a Signature Creation Device (SSCD / QSCD), a secure means for generating an Electronic Signature.

For relevant European Qualified Certificates of type QCP-n-qscd or QCP-l-qscd, the Certificate Holder Private Keys are generated and stored on a Qualified Electronic Signature/ Seal Creation Device (QSCD) which meets the requirements laid down in Annex II of Regulation (EU) No 910/2014 and is certified to the appropriate standards.

In some cases, QuoVadis generates and manages private keys on behalf of the Certificate Holder. This is signified by the presence of the 0.4.0.19431.1.1.3 OID in certificate policies. This OID is the EUSCP: EU SSASC Policy 'eu-remote-qscd' OID defined in ETSI TS 119 431-1. See chapter 7.1 Certificate profiles.

QuoVadis monitors the QSCD certification status up to the end of the validity period of the Certificate and takes appropriate measures in case of a change in the said status, for instance through expiry of the certification validity period or early revocation of the said certification. As a first step the QuoVadis Policy Management Authority (PMA) is informed of the said change in status and it will, based on the then observed situation, implement potential further measures.

6.1.1.1. Generation of key pairs for the TSP sub CA

The algorithm and the length of the cryptographic keys used to generate the keys for the TSP sub CA must fulfil the requirements set in the list of recommended cryptographic algorithms and key lengths, as defined in ETSI TS 119 312.

6.1.1.2. Generation of key pairs of the Certificate Holders

The keys of Certificate Holders (or data for creating Electronic Signatures) are generated within the requirements specified in EN 419 211 for QSCD's or CWA 14169 for SSCD's (transition rule eIDAS 51)"Secure signature creation devices (EAL 4+)" or equivalent security criteria.

6.1.1.3. Algorithm of key pairs of the Certificate Holders

With exception of the certificate policy Private Service Server QuoVadis is not permitted with in the POR to generate and deliver the Private Key (PKCS #12)..

6.1.1.4. Key pairs managed on behalf of the Certificate Holders

In the case of Qualified certificates, where QuoVadis manages the keys on behalf of the Certificate Holder, QuoVadis ensures:

where the policy requires the use of a Qualified Signature Creation Device (QSCD) then the signatures are only created by the QSCD;

in the case of natural persons, the Certificate Holders' private key is maintained and used under their sole control and used only for electronic signatures; and

in the case of legal persons, the private key is maintained and used under their control and used only for electronic seals.

6.1.2. Delivery of the Private Key to the Certificate Holder

Certificate Holders are responsible for the generation of the Private Keys which they request in their Certificate, unless explicitly agreed with QuoVadis. QuoVadis does not offer key generation, escrow, restore or backup facilities where Key Usage includes Server Authentication.

For some Certificates types, QuoVadis generates and manages private keys on behalf of the Certificate Holder. Where the policy requires the use of a Qualified Signature Creation Device (QSCD) then the signatures shall only be created by the QSCD. In the case of natural persons, the Certificate Holders' private key is maintained and used under their sole control and used only for electronic signatures. In the case of legal persons, the private key is maintained and used under their control and used only for electronic seals

6.1.3. Delivery of a public key

Public keys for Certificates that are generated within an SSCD/QSCD are submitted to the QuoVadis PKIoverheid CA by means of a PKCS#10 request for certification. Public keys for Services Certificates that are not generated within the SSCD/QSCD, but on location of the applicant, must be provided in a safe and reliable manner, such as by means of a Certificate Signing Request (PKCS # 10).

6.1.4. CA Public Key distribution to trusted parties

The public keys of the QuoVadis PKIoverheid CA within the PKIoverheid, as well as the intermediate CAs and the Root CAs of the Dutch State are recorded on the SSCD/QSCD. The Root CA of the Dutch State are included as root Certificates of the PKI for the Government in the popular browsers and/or in the operating systems.

6.1.5. Key length

The minimal key length for the QuoVadis PKIoverheid CAs is 2048-bits. QuoVadis supports higher-bits keys for certain Certificates as determined by customer request. The Keys are based on sha256WithRSAEncryption.

6.1.6. Purpose of key use (as referred to in X.509 v3)

Keys may only be used for the purposes described in this CPS. The QuoVadis PKIoverheid CA Private Keys may only be used for signing public keys (Certificates) and CRLs/OCSP responses.

6.2. PRIVATE KEY PROTECTION

6.2.1. Standards and controls of the cryptographic module (HSM)

The Private Keys of QuoVadis PKIoverheid CAs are generated and stored in a cryptographic module that complies with (at least) FIPS 140-2 level 3 and/or EAL 4+ security standards.

The HSM modules are always stored in a secure environment and are subject to strict security procedures throughout the entire life cycle.

For relevant Qualified Certificates of type QCP-n-qscd or QCP-l-qscd, the Certificate Holder Private Keys are generated and stored on a Qualified Electronic Signature/ Seal Creation Device (QSCD) which meets the requirements laid down in Annex II of the eIDAS Regulation and is certified to the appropriate standards.

In some cases, QuoVadis generates and manages private keys on behalf of the Certificate Holder and operates the QSCD in accordance with Annex II of the eIDAS Regulation. This will be signified by the presence of the 0.4.0.19431.1.1.3 OID in certificate policies. This OID is the EUSCP: EU

SSASC Policy 'eu-remote-qscd' OID defined in ETSI TS 119 431-1. See chapter 7.1 Certificate profiles.

6.2.2. Private Key (N out of M) "Multi-person" control

Access to the HSMs is limited to persons in Relying Roles and takes place based on prepared smart cards with a corresponding passphrase. These smart cards and passphrases have been assigned to several people in Relying Roles. Such required presence of multiple persons before gaining access ("N out of M" multi-person control) ensures that not one single person can have total control over a critical component within the infrastructure.

6.2.3. Escrow of the Private Key

QuoVadis does escrow Private Keys.

6.2.4. Private Key backup

Private Keys of Certificate Holders under this CPS are not backed up by QuoVadis. .

6.2.5. Archiving of the Private Key

QuoVadis does not archive any Private Keys of Certificate Holders under this CPS.

6.2.6. Access to Private Keys in the cryptographic module

The keys of the QuoVadis PKIoverheid CAs are stored in an HSM (see 6.2.1) They are stored in an encrypted state (whereby an encryption key is used in order to make a "cryptographic package" for the key). The Private Key may never exist in plaintext form outside the cryptographic module. When the Private Key is transported between two cryptographic modules, they must be transferred form one module to the other in a decoded state, under strict security measures. Access to the key material is exclusively obtained in the presence of multiple persons in Relying Roles, as described in 6.2.2.

6.2.7. Storage of Private Key in a cryptographic module

The Private Keys which are stored in a cryptographic module are secured throughout their entire life cycle.

6.2.8. Activation methods for a Private Key

The activation of the Private Keys of the QuoVadis PKIoverheid CAs is described in 6.2.2

6.2.9. Methods for deactivation of the Private Key

The Private Key of the operational QuoVadis PKIoverheid CAs is not normally deactivated but remains in production in the secure environment. Other cryptographic modules are deactivated after use, for example, by means of a manual logout procedure or a passive timeout. Cryptographic Modules that are not in use are deleted and stored.

6.2.10. Method for the destruction of the Private Key

Private Keys of the QuoVadis PKIoverheid CAs are destroyed when they are no longer needed, or when the Certificates with which they correspond have expired or have been withdrawn.

When the validity period of a key pair expires, or in other cases where destruction is required, the QuoVadis authorised personnel will destroy the Private Key (for example, by re-initialising or zeroing the Cryptographic Module or by inflicting physical damage (e.g. with a metal shredder). Such destruction is always documented.

6.2.11. Cryptographic classification of the module and SSCD/QSCDs

For relevant Qualified Certificates, in accordance with the eIDAS Regulation, the Certificate Holder Private Keys are generated and stored on a Qualified Electronic Signature Creation Device (QSCD) meets the requirements laid down in Annex II of the eIDAS Regulation and is certified to the appropriate standards. Where QuoVadis manages the QSCD on behalf of the Certificate Holder, QuoVadis operates the QSCD in accordance with Annex II of the eIDAS Regulation

QuoVadis verifies that QSCDs are certified as a QSCD in accordance requirements laid down in

Annex II of the eIDAS Regulation. QuoVadis monitors this certification status and takes appropriate measures if the certification status of a QSCD changes on a regular basis. The QSCD certification status and evidence of the QuoVadis monitoring are in scope of the external eIDAS/ ETSI conformity assessments

6.2.11.1. Conformity CWA14169 or EN 419 211

QuoVadis may issue and recommends QuoVadis SSCD/QSCDs that have been certified according to another protection profile against the Common Criteria (ISO/IEC 15408) at EAL4+, EN 419 211 or that have a comparable level of reliability. This must be determined by a testing laboratory that is accredited for performing Common Criteria evaluations.

QuoVadis can otherwise demonstrate compliance with CWA 14169 (for SSCD) or ETSI EN 419 211 (for QSCDs).

6.3. OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1. Period of use for keys and Certificates

Periods for use of the public and Private Keys are the same as the period of use of the Certificate that links the public key to a Certificate Holder. When the end-user Certificates are issued, the remaining validity of the QuoVadis CA used is always longer than the specified validity of the Certificate for the Certificate Holder. The maximum validity of end-user Certificates is 3 (three) years. An overview of the current validity of the different QuoVadis CAs is as follows:

PKIoverheid Intermediates	**Valid to:**	**G1 / G2 / G3**
QuoVadis PKIoverheid EV CA	5-Dec-22	G1

QuoVadis CSP - PKIoverheid CA - G2	23-Mar-20	G2
QuoVadis CSP Burger CA - G2	23-Mar-20	G2
QuoVadis PKIoverheid Burger CA - G3	11-Nov-28	G3
QuoVadis PKIoverheid Organisatie Persoon CA - G3	11-Nov-28	G3
QuoVadis PKIoverheid Organisatie Server CA - G3	11-Nov-28	G3
QuoVadis PKIoverheid Organisatie Services CA - G3	11-Nov-28	G3
QuoVadis PKIoverheid Private Personen CA - G1	11-Nov-28	G1
QuoVadis PKIoverheid Private Services CA - G1	11-Nov-28	G1
TRIAL QuoVadis CSP - PKIoverheid TEST CA - G2	23-Mar-20	G2

6.3.1. Certificate operational periods and key pair usage periods

Private keys that are used by a certificate holder and issued under this CPS must not be used for more than two (2) years.

After November 1, 2019 certificates which are issued under the Issuing Certificate Authorities in the table below will not be valid for more than 397 days.

Issuing CA	**Profile Name**	**OID**
QuoVadis CSP - PKIoverheid CA - G2	Organisation Service Server G2	2.16.528.1.1003.1.2.5.6
QuoVadis PKIoverheid Organisatie Server CA - G3	Organisation Service Server G3	2.16.528.1.1003.1.2.5.6
QuoVadis PKIoverheid EV CA	PKIOverheid Qualified Website authentication	2.16.528.1.1003.1.2.7
QuoVadis PKIoverheid EV CA	PKIOverheid EV SSL	2.16.528.1.1003.1.2.7

In the case of certificate replacement where the previous certificate is to be revoked because of an issue listed in section 4.9.1.1. of the Baseline Requirements the private key will not be reused, unless the revocation is caused by a violation of subsection 7 (Certificate not issued in accordance with these Requirements or the CA Certificate Policy or Certification Practice Statement).

6.4. ACTIVATION DATA

Please see chapter 3.2

6.5. COMPUTER SECURITY

6.5.1. All computer equipment and systems are under strict security measures:

- Dual control on all CA-systems
- Multifactor Authentication on systems
- Multifactor Authentication for online portals and interfaces
- Usage of encryption Certificates (SSL/TLS) on all systems
- Separation of duties and trusted roles
- Separation of networks, domains and core services
- Usage of x.509 Certificates for administrators

6.6. TECHNICAL LIFE CYCLE CONTROL MEASURES

6.6.1. Control measures for system development

QuoVadis uses standard products from accredited suppliers who fulfil the security classifications required by the PKIoverheid Programme of Requirements (see 6.1 and 6.2).

QuoVadis follows the Certificate of Issuing and Management Components (CIMC) Family of Protection Profiles (Common Criteria), which sets the requirements for components that issue, revoke and manage public key Certificates, such as X.509 public key Certificates. CIMC is based on the Criteria/ISO IS15408 standards.

Software developed by QuoVadis and used for use in services within PKIoverheid is developed in a controlled environment which fulfils strict safety requirements. The software developed within QuoVadis itself and used within one of the core PKI services must fulfil the applicable requirements for reliable systems as included in CEN TS 419261.

6.6.2. Control measures for security development

All QuoVadis systems and networks are monitored, managed and controlled to ensure integrity and correct operation. There are procedures and schedules in place for the systems and their related maintenance. Regular systems and monitoring checks are carried out by the responsible team(s). Additionally, automated processes are in place to alert trusted personal in case activities outside the set boundaries would occur.

6.6.3. Life cycle security measures

All hardware and software used for the QuoVadis services within the PKIoverheid must be purchased and delivered in such a way that the risk of unauthorised actions is kept to a minimum.

During operations, QuoVadis uses a configuration management procedure for the installation and continuous maintenance of the CA systems. When the CA software is first loaded, it provides a method for verifying the software on the system, including the following:

- the software developer/supplier
- changes prior to installation
- the version intended for use

The QuoVadis periodically verifies the integrity of the CA's software and the configuration of the CA systems

6.7. NETWORK SECURITY

QuoVadis performs all technical actions described in this CPS using secure networking measures. These measures are in place to prevent and circumvent unauthorised and/or malicious activity. Strict access controls are in place for all systems, furthermore encryption and digital signitures are used to protect data. The controls in place are preventive, detective, repressive and corrective in nature. The controls include regular vulnerability scans, at least monthly, as well as penetration tests that are done at least annually.

6.8. TIME STAMPING

QuoVadis does not provide time stamps within the PKIoverheid framework.

7. CERTIFICATE PROFILES

QuoVadis only uses approved Certificate Profiles for the Issuance of PKI Certificates, all profiles are detailed in this document as the CPS describes the approved Certificate Profiles for all Certificates from PKIoverheid Issuing CAs.

7.1. SERIAL NUMBER GENERATION

The serial number of all certificates issued under this CPS complies with the following requirements:

a) The value of the serial number is not 0 (zero)
b) The value of the serial number is not negative

c) The value of the serial number is unique for each certificate issued
d) The serial number has a minimum length of 96 bits (12 octets)
e) The serial number contains at least 64 bits of random data
f) The random data is generated by a Cryptographically Secure Pseudorandom Number Generator
g) The serial number is no longer than 160 bits (20 octets)

7.2. ECC CERTIFICATES

QuoVadis can select one of the following options for the Signature field in a Certificate:

- sha256WithRSAEncryption: 1.2.840.113549.1.1.11
- ecdsa-with-SHA256: 1.2.840.10045.4.3.2

7.3. QUOVADIS PKIOVERHEID ORGANISATIE PERSOON CA - G3

7.3.1. Personal Organisation Authentication G3

Basic Contents	**Value**	**Demarcation**
Subject.CommonName	CommonName	Required
Subject.givenname	Given Name	Required
Subject.surname	Surname	Required
Subject.SerialNumber	SerialNumber	Required
Subject.OrganisationName	OrganisationName	Required
Subject.organisationalUnitName	OrganisationalUnitName	Optional / Prohibited for Profession Certificates
Subject.title	Title	Optional
Subject.CountryName	Country	Required
Subject.PublicKeyInfo	RSA (2048 bit)	Required
Extensions		**Fixed**
KeyUsage (CRITICAL)	Digital Signature	Fixed
extKeyUsage	Client Authentication Document Signing E-Mail Protection	Required
CertPolicyID	2.16.528.1.1003.1.2.5.1	Fixed
subjectAltName.Rfc822Name	Rfc822 email address	Optional - Used for e-mail signing (Outlook)
subjectAltName.User Principle Name (MS UPN)	user@domain (used for Single Sign on)	Optional
subjectAltName.User Principle Name (MS UPN)	MS UPN in the format: .<unique identifier>@2.16.528.1.1003.1.3.5.2.1	Required
CRLDistributionPoints	http://crl.quovadisglobal.com/pkiopersong3.crl	Fixed
AuthorityInfoAccess	http://uw.ocsp.quovadisglobal.com http://trust.quovadisglobal.com/pkiopersong3.crt	Fixed

7.3.2. Personal Organisation Non-Repudiation G3

Basic Contents	Value	Demarcation
Subject.CommonName	CommonName	Required
Subject.givenname	Given Name	Required
Subject.surname	Surname	Required
Subject.SerialNumber	SerialNumber	Required
Subject.OrganisationName	OrganisationName	Required
Subject.organisationalUnitName	OrganisationalUnitName	Optional / Prohibited for Profession Certificates
Subject.title	Title	Optional
Subject.CountryName	Country	Required
Subject.PublicKeyInfo	RSA (2048 bit)	Required
Extensions		**Fixed**
KeyUsage(CRITICAL)	Non-Repudiation	Fixed
extKeyUsage	Document Signing E-Mail Protection	Required/ optional
CertPolicyID	2.16.528.1.1003.1.2.5.2 0.4.0.19431.1.1.3 'eu-remote-qscd' EUSCP: EU SSASC Policy (ETSI TS 119 431-1)	Fixed Only included when QuoVadis generates & manages private keys on behalf of Cert holder on a QSCD.
subjectAltName.Rfc822Name	Rfc822 email address	Optional - Used for e-mail signing (Outlook)
subjectAltName.User Principle Name (MS UPN)	MS UPN in the format: .<unique identifier>@2.16.528.1.1003.1.3.5.2.1	Required
CRLDistributionPoints	http://crl.quovadisglobal.com/pkiopersong3.crl	Fixed
AuthorityInfoAccess	http://uw.ocsp.quovadisglobal.com http://trust.quovadisglobal.com/pkiopersong3.crt	Fixed
QC Statements	Id-etsi-qcs-QcCompliance { id-etsi-qcs 1 } 0.4.0.1862.1.1 Id-etsi-qct-eseal { id-etsi-qct-esign } 0.4.0.1862.1.6.1 Id-etsi-qcs-QcSSCD { id-etsi-qcs 4 } 0.4.0.1862.1.4 Id-etsi-qcs-QcPDS { id-etsi-qcs 5 } 0.4.0.1862.1.5	Fixed

7.3.3. Personal Organisation Encryption G3

Basic Contents	Value	Demarcation
Subject.CommonName	CommonName	Required
Subject.givenname	Given Name	Required

Subject.surname	Surname	Required
Subject.SerialNumber	SerialNumber	Required
Subject.OrganisationName	OrganisationName	Required
Subject.organisationalUnitName	OrganisationalUnitName	Optional / Prohibited for Profession Certificates
Subject.title	Title	Optional
Subject.CountryName	Country	Required
Subject.PublicKeyInfo	RSA (2048 bit)	Required
Extensions		**Fixed**
KeyUsage (CRITICAL)	Key Encipherment Data Encipherment	Fixed
extKeyUsage	Encrypting File System E-Mail Protection	Required
CertificatePolicies	2.16.528.1.1003.1.2.5.3	Fixed
subjectAltName.Rfc822Name	Rfc822 email address	Optional - Used for e-mail signing (Outlook)
subjectAltName.User Principle Name (MS UPN)	MS UPN in the format: .<unique identifier>@2.16.528.1.1003.1.3.5.2.1	Required
CRLDistributionPoints	http://crl.quovadisglobal.com/pkiopersong3.crl	Fixed
AuthorityInfoAccess	http://uw.ocsp.quovadisglobal.com http://trust.quovadisglobal.com/pkiopersong3.crt	Fixed

7.4. QUOVADIS CSP - PKIOVERHEID CA - G2

7.4.1. Personal User Authentication G2

Basic Contents	**Value**	**Demarcation**
Subject.CommonName	CommonName	Required
Subject.givenname	Given Name	Required
Subject.surname	Surname	Required
Subject.SerialNumber	SerialNumber	Required
Subject.OrganisationName	OrganisationName	Required
Subject.organisationalUnitName	OrganisationalUnitName	Optional / Prohibited for Profession Certificates
Subject.title	Title	Optional
Subject.CountryName	Country	Required
Subject.PublicKeyInfo	RSA (2048 bit)	Required
Extensions		**Fixed**
KeyUsage (CRITICAL)	Digital Signature	Fixed
extKeyUsage	Client Authentication Document Signing E-Mail Protection	Required

CertPolicyID	2.16.528.1.1003.1.2.5.1	Fixed
subjectAltName.Rfc822Name	Rfc822 email address	Optional - Used for e-mail signing (Outlook)
subjectAltName.User Principle Name (MS UPN)	user@domain (used for Single Sign on)	Optional
subjectAltName.User Principle Name (MS UPN)	MS UPN in the format: .<unique identifier>@2.16.528.1.1003.1.3.5.2.1.	Required
CRLDistributionPoints	http://crl.quovadisglobal.com/qvocag2.crl	Fixed
AuthorityInfoAccess	http://ocsp.quovadisglobal.com http://trust.quovadisglobal.com/qvocag2.crt	Fixed

7.4.2. Personal User Non-Repudiation G2

Basic Contents	**Value**	**Demarcation**
Subject.CommonName	CommonName	Required
Subject.givenname	Given Name	Required
Subject.surname	Surname	Required
Subject.SerialNumber	SerialNumber	Required
Subject.OrganisationName	OrganisationName	Required
Subject.organisationalUnitName	OrganisationalUnitName	Optional / Prohibited for Profession Certificates
Subject.title	Title	Optional
Subject.CountryName	Country	Required
Subject.PublicKeyInfo	RSA (2048 bit)	Required
Extensions		**Fixed**
KeyUsage(CRITICAL)	Non-Repudiation	Fixed
extKeyUsage	Document Signing E-Mail Protection	Required/ optional
CertPolicyID	2.16.528.1.1003.1.2.5.2 0.4.0.19431.1.1.3 'eu-remote-qscd' EUSCP: EU SSASC Policy (ETSI TS 119 431-1)	Fixed Only included when QuoVadis generates & manages private keys on behalf of Cert holder on a QSCD.
subjectAltName.Rfc822Name	Rfc822 email address	Optional - Used for e-mail signing (Outlook)
subjectAltName.User Principle Name (MS UPN)	MS UPN in the format: .<unique identifier>@2.16.528.1.1003.1.3.5.2.1	Required
CRLDistributionPoints	http://crl.quovadisglobal.com/qvocag2.crl	Fixed
AuthorityInfoAccess	http://ocsp.quovadisglobal.com http://trust.quovadisglobal.com/qvocag2.crt	Fixed
QC Statements	Id-etsi-qcs-QcCompliance { id-etsi-qcs 1 } 0.4.0.1862.1.1	Fixed

	Id-etsi-qct-eseal { id-etsi-qct-esign } 0.4.0.1862.1.6.1 Id-etsi-qcs-QcSSCD { id-etsi-qcs 4 } 0.4.0.1862.1.4 Id-etsi-qcs-QcPDS { id-etsi-qcs 5 } 0.4.0.1862.1.5	

7.4.3. Personal User Encryption G2

Basic Contents	**Value**	**Demarcation**
Subject.CommonName	CommonName	Required
Subject.givenname	Given Name	Required
Subject.surname	Surname	Required
Subject.SerialNumber	SerialNumber	Required
Subject.OrganisationName	OrganisationName	Required
Subject.organisationalUnitName	OrganisationalUnitName	Optional / Prohibited for Profession Certificates
Subject.title	Title	Optional
Subject.CountryName	Country	Required
Subject.PublicKeyInfo	RSA (2048 bit)	Required
Extensions		**Fixed**
KeyUsage (CRITICAL)	Key Encipherment Data Encipherment	Fixed
extKeyUsage	Encrypting File System E-Mail Protection	Required Required
CertificatePolicies	2.16.528.1.1003.1.2.5.3	Fixed
subjectAltName.Rfc822Name	Rfc822 email address	Optional - Used for e-mail signing (Outlook)
subjectAltName.User Principle Name (MS UPN)	MS UPN in the format: .<unique identifier>@2.16.528.1.1003.1.3.5.2.1	Required
CRLDistributionPoints	http://crl.quovadisglobal.com/qvocag2.crl	Fixed
AuthorityInfoAccess	http://ocsp.quovadisglobal.com http://trust.quovadisglobal.com/qvocag2.crt	Fixed

7.4.4. Personal User Encryption G2

Basic Contents	**Value**	**Demarcation**
Subject.CommonName	CommonName	Required
Subject.SerialNumber	SerialNumber	Optional
Subject.OrganisationName	OrganisationName	Required
Subject.organisationalUnitName	OrganisationalUnitName	Optional / Prohibited for Profession Certificates
Subject.CountryName	Country	Required

Subject.PublicKeyInfo	RSA (2048 bit)	Required
Extensions		**Fixed**
KeyUsage (CRITICAL)	Digital Signature	Fixed
extKeyUsage	Client Authentication Document Signing E-Mail Protection	Required
CertPolicyID	2.16.528.1.1003.1.2.5.4	Fixed
subjectAltName.Rfc822Name	Rfc822 email address	Optional - Used for e-mail signing (Outlook)
subjectAltName.User Principle Name (MS UPN)	user@domain (used for Single Sign on)	Optional
subjectAltName.User Principle Name (MS UPN)	MS UPN in the format: .<unique identifier>@2.16.528.1.1003.1.3.5.2.1.	Required
CRLDistributionPoints	http://crl.quovadisglobal.com/qvocag2.crl	Fixed
AuthorityInfoAccess	http://ocsp.quovadisglobal.com http://trust.quovadisglobal.com/qvocag2.crt	Fixed

7.4.5. Organisation Service Encryption G2

Basic Contents	**Value**	**Demarcation**
Subject.CommonName	CommonName	Required
Subject.SerialNumber	SerialNumber	Required
Subject.OrganisationName	OrganisationName	Required
Subject.organisationalUnitName	OrganisationalUnitName	Optional / Prohibited for Profession Certificates
Subject.CountryName	Country	Required
Subject.PublicKeyInfo	RSA (2048 bit)	Required
Extensions		**Fixed**
KeyUsage (CRITICAL)	Key Encipherment Data Encipherment	Fixed
extKeyUsage	Encrypting File System E-Mail Protection	Required Required
CertificatePolicies	2.16.528.1.1003.1.2.5.5	Fixed
subjectAltName.Rfc822Name	Rfc822 email address	Optional - Used for e-mail signing (Outlook)
subjectAltName.User Principle Name (MS UPN)	MS UPN in the format: .<unique identifier>@2.16.528.1.1003.1.3.5.2.1	Required
CRLDistributionPoints	http://crl.quovadisglobal.com/qvocag2.crl	Fixed
AuthorityInfoAccess	http://ocsp.quovadisglobal.com http://trust.quovadisglobal.com/qvocag2.crt	Fixed

7.4.6. Organisation Service Server G2

Basic Contents	Value	Demarcation
Subject.CommonName	CommonName (e.q. fully qualified domain name)	Required
Subject.SerialNumber	SerialNumber	Required
Subject.OrganisationName	OrganisationName	Required
Subject.organisationalUnitName	OrganisationalUnitName	Optional / Prohibited for Profession Certificates
Subject.stateOrProvinceName	State or province	Required
Subject.localityName	City	Required
Subject.CountryName	Country	Required
Subject.PublicKeyInfo	RSA (2048 bit)	Required
Extensions		**Fixed**
KeyUsage (CRITICAL)	Digital Signature Key Encipherment	Fixed
extKeyUsage	Server Authentication Client Authentication	Fixed
CertificatePolicies	2.16.528.1.1003.1.2.5.6	Fixed
SignedCertificate-TimestampList	Certificate Transparency related (1.3.6.1.4.1.11129.2.4.2)	Fixed as per 1-7-2017
subjectAltName.dNSName	Name that identifies the server.	Required
subjectAltName.IPAddress	Contains a public IP address	Optional
CRLDistributionPoints	http://crl.quovadisglobal.com/qvocag2.crl	Fixed
AuthorityInfoAccess	http://ocsp.quovadisglobal.com http://trust.quovadisglobal.com/qvocag2.crt	Fixed

7.5. QUOVADIS PKIOVERHEID ORGANISATIE SERVICES CA - G3

7.5.1. Organisation Services Authentication G3

Basic Contents	Value	Demarcation
Subject.CommonName	CommonName	Required
Subject.SerialNumber	SerialNumber	Optional
Subject.OrganisationName	OrganisationName	Required
Subject.organisationIdentifier	3 character legal person identity type reference (e.g. NTR or VAT); 2 character ISO 3166 [2] country code; hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8)); and identifier (according to country and identity type reference).	Required

	Company registration number	
Subject.organisationalUnitName	OrganisationalUnitName	Optional / Prohibited for Profession Certificates
Subject.CountryName	Country	Required
Subject.PublicKeyInfo	RSA (2048 bit)	Required
Extensions		**Fixed**
KeyUsage (CRITICAL)	Digital Signature	Fixed
extKeyUsage	Client Authentication Document Signing EmailProtection	Fixed
CertificatePolicies	2.16.528.1.1003.1.2.5.4	Fixed
subjectAltName.User Principle Name (MS UPN)	user@domain (used for Single Sign on)	Optional
subjectAltName.User Principle Name (MS UPN)	<Service ID>@2.16.528.1.1003.1.3.5.2.1 (Where <Service ID> is the relevant ID number of the Service)	Required
subjectAltName.rfc822Name	Rfc822 email address	Optional - Used for e-mail signing (Outlook)
CRLDistributionPoints	http://crl.quovadisglobal.com/pkioservicg3.crt	Fixed
AuthorityInfoAccess	http://uw.ocsp.quovadisglobal.com http://trust.quovadisglobal.com/pkioservicg3.crt	

7.5.2. Organisation Service Encryption G3

Basic Contents	**Value**	**Demarcation**
Subject.CommonName	CommonName	Required
Subject.SerialNumber	SerialNumber	Optional
Subject.OrganisationName	OrganisationName	Required
Subject.organisationIdentifier	3 character legal person identity type reference (e.g. NTR or VAT); 2 character ISO 3166 [2] country code; hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8)); and identifier (according to country and identity type reference). Company registration number	Required
Subject.organisationalUnitName	OrganisationalUnitName	Optional / Prohibited for Profession Certificates
Subject.CountryName	Country	Required
Subject.PublicKeyInfo	RSA (2048 bit)	Required
Extensions		**Fixed**

KeyUsage (CRITICAL)	Key Encipherment Data Encipherment	Fixed
extKeyUsage	Email Protection Encrypting File System	Fixed
CertificatePolicies	2.16.528.1.1003.1.2.5.5	Fixed
subjectAltName.User Principle Name (MS UPN)	<Service ID>@2.16.528.1.1003.1.3.5.2.1 (Where <Service ID> is the relevant ID number of the Service)	Required
subjectAltName.rfc822Name	Rfc822 email address	Optional - Used for e-mail signing (Outlook)
CRLDistributionPoints	http://crl.quovadisglobal.com/pkioservicg3.crt	Fixed
AuthorityInfoAccess	http://uw.ocsp.quovadisglobal.com http://trust.quovadisglobal.com/pkioservicg3.crt	Fixed

7.5.3. Organisation Service Seal G3

Basic Contents	**Value**	**Demarcation**
Subject.CommonName	CommonName (commonly used name of the Subject)	Required
Subject.SerialNumber	SerialNumber	Optional
Subject.OrganisationName	OrganisationName	Required
Subject.organisationalUnitName	OrganisationalUnitName	Optional / Prohibited for Profession Certificates
Subject Organisation Identifier	3 character legal person identity type reference (e.g. NTR or VAT); 2 character ISO 3166 [2] country code; hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8)); and identifier (according to country and identity type reference). Company registration number	Required
Subject.localityName	City	Optional
Subject.stateOrProvinceName	State or province	Optional
Subject.PublicKeyInfo	RSA (2048 bit) / System Generated	Fixed
Subject Serial Number	Serial number	Required
Extensions		**Fixed**
KeyUsage (CRITICAL)	Non repudiation	Fixed
extKeyUsage	Document Signing EmailProtection	Fixed
CertificatePolicies	2.16.528.1.1003.1.2.5.7	Fixed

	Policy Identifier=0.4.0.19431.1.1.3 'eu-remote-qscd' EUSCP: EU SSASC Policy (ETSI TS 119 431-1)	Only included when QuoVadis generates & manages private keys on behalf of Cert holder on a QSCD
subjectAltName.User Principle Name (MS UPN)	<Service ID>@2.16.528.1.1003.1.3.5.2.1 (Where <Service ID> is the relevant ID number of the Service)	Holder Variable
CRLDistributionPoints	http://crl.quovadisglobal.com/pkioservicg3.crt	Fixed
AuthorityInfoAccess	http://uw.ocsp.quovadisglobal.com http://trust.quovadisglobal.com/pkioservicg3.crt	Fixed
QC Statements	Id-etsi-qcs-QcCompliance { id-etsi-qcs 1 } 0.4.0.1862.1.1 Id-etsi-qct-eseal { id-etsi-qcs-QcType 2 } 0.4.0.1862.1.6.2 Id-etsi-qcs-QcSSCD { id-etsi-qcs 4 } 0.4.0.1862.1.4 Id-etsi-qcs-QcPDS { id-etsi-qcs 5 } 0.4.0.1862.1.5 ld-etsi-gcs SymanticsID-legal } { id-etsi-qcs-Symantics-identifiers 2 } 0.4.0.194121.1.2	Fixed

7.6. QUOVADIS PKIOVERHEID BURGER CA - G3

7.6.1. Personal Citizen Authentication G3

Basic Contents	**Value**	**Demarcation**
Subject.commonName	Subject Common Name	Required
Subject.surname	Surname	Required
Subject.givenName	Given name	Required
Subject.serialNumber	Serial Number	Required
Subject.countryName	Country Name	Required
Subject.publicKeyInfo	RSA (2048 bit)	Required
Extensions		**Fixed**
KeyUsage (CRITICAL)	Digital Signature	Fixed
extKeyUsage	Client authentication Document Signing E-Mail Protection	Required/optional
CertificatePolicies	2.16.528.1.1003.1.2.3.1	Fixed
subjectAltName.Rfc822Name	Rfc822 email address	Optional - Used for e-mail signing (Outlook)

subjectAltName.Principle Name (MS UPN)	MS UPN in the format: .<unique identifier>@2.16.528.1.1003.1.3.5.2.1	Required
CRLDistributionPoints	http://crl.quovadisglobal.com/pkioburgerg3.crl	Fixed
AuthorityInfoAccess	http://uw.ocsp.quovadisglobal.com http://trust.quovadisglobal.com/pkioburgerg3.crl	Fixed

7.6.2. Personal Citizen Non-Repudiation G3

Basic Contents	**Value**	**Demarcation**
Subject.commonName	Subject Common Name	Required
Subject.surname	Surname	Required
Subject.givenName	Given name	Required
Subject.serialNumber	Serial Number	Required
Subject.countryName	Country Name	Required
Subject.publicKeyInfo	RSA (2048 bit)	Required
Extensions		**Fixed**
KeyUsage (CRITICAL)	Non-Repudiation	Fixed
extKeyUsage	Document Signing E-Mail Protection	Required
CertificatePolicies	2.16.528.1.1003.1.2.3.2 0.4.0.19431.1.1.3 'eu-remote-qscd' EUSCP: EU SSASC Policy (ETSI TS 119 431-1)	Fixed Only included when QuoVadis generates & manages private keys on behalf of Cert holder on a QSCD.
subjectAltName.Rfc822Name	Rfc822 email address	Optional - Used for e-mail signing (Outlook)
subjectAltName.User Principle Name (MS UPN)	MS UPN in the format: <unique identifier>@2.16.528.1.1003.1.3.3.3.1	Required
CRLDistributionPoints	http://crl.quovadisglobal.com/pkioburgerg3.crl	Fixed
AuthorityInfoAccess	http://uw.ocsp.quovadisglobal.com http://trust.quovadisglobal.com/pkioburgerg3.crt	Fixed
QC Statements	Id-etsi-qcs-QcCompliance { id-etsi-qcs 1 } 0.4.0.1862.1.1 Id-etsi-qct-eseal { id-etsi-qct-esign } 0.4.0.1862.1.6.1 Id-etsi-qcs-QcSSCD { id-etsi-qcs 4 } 0.4.0.1862.1.4 Id-etsi-qcs-QcPDS { id-etsi-qcs 5 } 0.4.0.1862.1.5	Fixed

7.6.3. Personal Citizen Encryption G3

Basic Contents	Value	Demarcation
Subject.commonName	Subject Common Name	Required
Subject.surname	Surname	Required
Subject.givenName	Given name	Required
Subject.serialNumber	Serial Number	Required
Subject.countryName	Country Name	Required
Subject.publicKeyInfo	RSA (2048 bit)	Required
Extensions		**Fixed**
KeyUsage (CRITICAL)	Key Encipherment Data Encipherment	Fixed
extKeyUsage	Encrypting File System E-Mail Protection	Required
CertificatePolicies	2.16.528.1.1003.1.2.3.3	Fixed
subjectAltName.Rfc822Name	Rfc822 email address	Optional - Used for e-mail signing (Outlook)
subjectAltName.UserPrinciple Name (MS UPN)	MS UPN (in format: <unique identifier>@2.16.528.1.1003.1.3.3.3.1	Required
CRLDistributionPoints	http://crl.quovadisglobal.com/pkioburgerg3.crl	Fixed
AuthorityInfoAccess	http://ocsp.quovadisglobal.com http://trust.quovadisglobal.com/pkioburgerg3.crt	Fixed

7.7. QUOVADIS PKIOVERHEID ORGANISATIE SERVER CA – G3

7.7.1. Organisation Service Server G3

Basic Contents	Value	Demarcation
Subject.CommonName	CommonName (e.q. fully qualified domain name)	Required
Subject.SerialNumber	SerialNumber	Required
Subject.OrganisationName	OrganisationName	Required
Subject.organisationalUnitName	OrganisationalUnitName	Optional
Subject.stateOrProvinceName	State or province	Required
Subject.localityName	City	Required
Subject.CountryName	Country	Required
Subject.PublicKeyInfo	RSA (2048 bit)	Required
Extensions		**Fixed**
KeyUsage (CRITICAL)	Digital Signature Key Encipherment	Fixed
extKeyUsage	Server Authentication Client Authentication	Fixed

CertificatePolicies	2.16.528.1.1003.1.2.5.6	Fixed
SignedCertificate-TimestampList	Certificate Transparency related (1.3.6.1.4.1.11129.2.4.2)	Fixed as per 1-7-2017
subjectAltName.dNSName	Name that identifies the server.	Required
subjectAltName.IPAddress	Contains a public IP address	Optional
CRLDistributionPoints	http://crl.quovadisglobal.com/pkioserverg3.crl	Fixed
AuthorityInfoAccess	http://ocsp.quovadisglobal.com http://trust.quovadisglobal.com/pkioserverg3.crt	Fixed

7.8. QUOVADIS PKIOVERHEID EV CA

7.8.1. PKIOverheid EV SSL

Basic Contents	**Value**	**Demarcation**
Subject.CommonName	Fully Qualified Domain Name	Required
Subject.SerialNumber	SerialNumber	Required
Subject.OrganisationName	OrganisationName	Required
Subject.organisationalUnitName	OrganisationalUnitName (If a Government entity without NTR registration: must contain overheidsorganisatie)	Optional/Required
Subject.stateOrProvinceName	State or province	Required
Subject.localityName	City	Required
Subject.CountryName	Country	Required
Subject.businessCategory	"Private Organisation", "Government Entity", "Business Entity", or "Non-Commercial Entity"	Required
Subject.jurisdictionOfIncorporationCountryName	Country of Incorporation. FIXED VALUE = NL	Fixed
Subject.serialNumber	Registration Number	Required
Subject.PublicKeyInfo	RSA (2048 bit) / System Generated	Required
Extensions		**Fixed**
KeyUsage (CRITICAL)	Digital Signature Key Encipherment	Fixed
extKeyUsage	Server Authentication Client Authentication	Fixed
CertificatePolicies	2.16.528.1.1003.1.2.7	Fixed
SignedCertificate-TimestampList	Certificate Transparency related (1.3.6.1.4.1.11129.2.4.2)	Fixed as per 1-7-2017
Subject.Altname.dNSname	DNSName	Required
CRLDistributionPoints	http://crl.quovadisglobal.com/pkioevg2.crl	Fixed

AuthorityInfoAccess	http://ocsp.quovadisglobal.com http://trust.quovadisglobal.com/pkioevg2.crt	Fixed

7.8.2. PKIOverheid Qualified Website Authentication

Basic Contents	**Value**	**Demarcation**
Subject.CommonName	Fully Qualified Domain Name	Required
Subject.SerialNumber	SerialNumber	Required
Subject.OrganisationName	OrganisationName	Required
Subject.organisationIdentifier	Refer to: CA/Browser Forum Ballot SC17	Optional
Subject.organisationalUnitName	OrganisationalUnitName (If a Government entity without NTR registration: must contain overheidsorganisatie)	Optional/Required
Subject.stateOrProvinceName	State or province	Required
Subject.localityName	City	Required
Subject.CountryName	Country	Required
Subject.businessCategory	"Private Organisation", "Government Entity", "Business Entity", or "Non-Commercial Entity"	Required
Subject.jurisdictionOfIncorporationCountryName	Country of Incorporation. FIXED VALUE = NL	Fixed
Subject.serialNumber	Registration Number	Required
Subject.PublicKeyInfo	RSA (2048 bit) / System Generated	Required
Extensions		**Fixed**
KeyUsage (CRITICAL)	Digital Signature Key Encipherment	Fixed
extKeyUsage	Server Authentication Client Authentication	Fixed
CertificatePolicies	0.4.0.194112.1.4 1.3.6.1.4.1.8024.0.2.100.1.2 2.16.528.1.1003.1.2.7 2.23.140.1.1	Fixed
SignedCertificate-TimestampList	Certificate Transparency related (1.3.6.1.4.1.11129.2.4.2)	Fixed as per 1-7-2017
subjectAltName.dNSName	dNSName	Required
CRLDistributionPoints	http://crl.quovadisglobal.com/pkioevg2.crl	Fixed
AuthorityInfoAccess	http://ocsp.quovadisglobal.com http://trust.quovadisglobal.com/pkioevg2.crt	Fixed
QC Statements	Id-etsi-qcs-QcCompliance { id-etsi-qcs 1 } 0.4.0.1862.1.1	Fixed

	Id-etsi-qct-web { id-etsi-qcs-QcType 3 } 0.4.0.1862.1.6.3 Id-etsi-qct-web QC Type 6 { id-etsi-qcs-QcType 6 } 0.4.0.1862.1.6.3 Id-etsi-qcs-QcPDS { id-etsi-qcs 5 } 0.4.0.1862.1.5 ld-etsi-gcs SymanticsID-legal } { id-etsi-qcs-Symantics-identifiers 2 } 0.4.0.194121.1.2	

7.9. QUOVADIS PKIOVERHEID PRIVATE SERVICES CA - G1

7.9.1. Private Services – Authentication

Basic Contents	**Value**	**Demarcation**
Subject.CommonName	If FQDN it should be registered, else a name that identifies the server/service. Internal domain name allowed.	required
Subject.SerialNumber	SerialNumber	Required
Subject.OrganisationName	OrganisationName	Required
Subject.organisationalUnitName	OrganisationalUnitName	Optional
Subject.CountryName	Country	Required
Subject.PublicKeyInfo	RSA (2048 bit) / System Generated	Required
Extensions		**Fixed**
KeyUsage (CRITICAL)	Digital Signature	Fixed
extKeyUsage	Client Authentication Document Signing E-Mail Protection	Required
CertificatePolicies	2.16.528.1.1003.1.2.8.4	Fixed
subjectAltName.Rfc822Name	Rfc822 email address	Optional - Used for e-mail signing (Outlook)
subjectAltName.User Principle Name (MS UPN)	user@domain (used for Single Sign on)	Optional
subjectAltName.Principle Name (MS UPN)	MS UPN in the format: .<unique identifier>@2.16.528.1.1003.1.3.5.2.1	Required
CRLDistributionPoints	http://crl.quovadisglobal.com/pkioprivservg1.crl	Fixed
AuthorityInfoAccess	http://sl.ocsp.quovadisglobal.com http://trust.quovadisglobal.com/pkioprivserv.crt	Fixed

7.9.2. Private Services – Encryption

Basic Contents	Value	Demarcation
Subject.CommonName	If FQDN it should be registered, else a name that identifies the server/service. Internal domain name allowed	required
Subject.SerialNumber	SerialNumber	Required
Subject.OrganisationName	OrganisationName	Required
Subject.organisationalUnitName	OrganisationalUnitName	Optional
Subject.CountryName	Country	Required
Subject.PublicKeyInfo	RSA (2048 bit) / System Generated	Required
Extensions		**Fixed**
KeyUsage (CRITICAL)	Key Encipherment Data Encipherment	Fixed
extKeyUsage	Encrypting File System E-Mail Protection	Required
CertificatePolicies	2.16.528.1.1003.1.2.8.5	Fixed
subjectAltName.Rfc822Name	Rfc822 email address	Optional - Used for e-mail signing (Outlook)
subjectAltName.User Principle Name (MS UPN)	user@domain (used for Single Sign on)	Optional
subjectAltName.Principle Name (MS UPN)	MS UPN in the format: .<unique identifier>@2.16.528.1.1003.1.3.5.2.1	Required
CRLDistributionPoints	http://crl.quovadisglobal.com/pkioprivservg1.crl	Fixed
AuthorityInfoAccess	http://sl.ocsp.quovadisglobal.com http://trust.quovadisglobal.com/pkioprivserv.crt	Fixed

7.9.3. Private Services – Server

Basic Contents	Value	Demarcation
Subject.CommonName	If FQDN it should be registred, else a name that identifies the server/service. Internal domain name allowed	Required
Subject.SerialNumber	SerialNumber	Required
Subject.OrganisationName	OrganisationName	Required
Subject.organisationalUnitName	OrganisationalUnitName	Optional
Subject.CountryName	Country	Required
Subject.PublicKeyInfo	RSA (2048 bit) / System Generated	Required
Extensions		**Fixed**
KeyUsage (CRITICAL)	Digital Signature Key encipherment	Fixed
extKeyUsage	Client Authentication	Required

	Server Authentication	
CertificatePolicies	2.16.528.1.1003.1.2.8.6	Fixed
subjectAltName.Rfc822Name	Rfc822 email address	Optional - Used for e-mail signing (Outlook)
subjectAltName.dNSname	If FQDN is used it must be in first SAN DNS field. Otherwise usage of this field is prohibited	Required/prohibited
subjectAltName.ipadress	Only public IP adresses	Optional
subjectAltName.Principle Name (MS UPN)	MS UPN in the format: .<unique identifier>@2.16.528.1.1003.1.3.5.2.1	Required
CRLDistributionPoints	http://crl.quovadisglobal.com/pkioprivservg1.crl	Fixed
AuthorityInfoAccess	http://sl.ocsp.quovadisglobal.com http://trust.quovadisglobal.com/pkioprivserv.crt	Fixed

7.10. QUOVADIS PKIOVERHEID PRIVATE PERSONEN CA - G1

7.10.1. Private Personal Authentication

Basic Contents	**Value**	**Demarcation**
Subject.CommonName	CommonName	Required
Subject.givenname	Given Name	Required
Subject.surname	Surname	Required
Subject.SerialNumber	SerialNumber	Required
Subject.OrganisationName	OrganisationName	Required
Subject.OrganisationUnit	OrganisationUnitName	optional
Subject.CountryName	Country	Required
Subject.Title	Title	Optional
Subject.PublicKeyInfo	RSA (2048 bit)	Required
Extensions		**Fixed**
KeyUsage (CRITICAL)	Digital Signature	Fixed
extKeyUsage	Client Authentication Document Signing E-Mail Protection	Required
CertificatePolicies	2.16.528.1.1003.1.2.8.1	Fixed
subjectAltName.Rfc822Name	Rfc822 email address	Optional - Used for e-mail signing (Outlook)
subjectAltName.User Principle Name (MS UPN)	user@domain (used for Single Sign on)	Optional
subjectAltName.User Principle Name (MS UPN)	MS UPN in the format: .<unique identifier>@2.16.528.1.1003.1.3.5.2.1	Required
CRLDistributionPoints	http://crl.quovadisglobal.com/pkioprivpersg1.crl	Fixed

AuthorityInfoAccess	http://uw.ocsp.quovadisglobal.com http://trust.quovadisglobal.com/pkioprivpersg1.crt	Fixed

7.10.2. Private Personal Non-Repudiation

Basic Contents	**Value**	**Demarcation**
Subject.CommonName	CommonName	Required
Subject.givenname	Given Name	Required
Subject.surname	Surname	Required
Subject.SerialNumber	SerialNumber	Required
Subject.OrganisationName	OrganisationName	Required
Subject.organisationalUnitName	OrganisationalUnitName	Optional / Prohibited for Profession Certificates
Subject.title	Title	Optional
Subject.CountryName	Country	Required
Subject.PublicKeyInfo	RSA (2048 bit)	Required
Extensions		**Fixed**
KeyUsage(CRITICAL)	Non-Repudiation	Fixed
extKeyUsage	Document Signing E-Mail Protection	Required/ optional
CertPolicyID	2.16.528.1.1003.1.2.8.2	Fixed
subjectAltName.Rfc822Name	Rfc822 email address	Optional - Used for e-mail signing (Outlook)
subjectAltName.User Principle Name (MS UPN)	MS UPN in the format: .<unique identifier>@2.16.528.1.1003.1.3.5.2.1	Required
CRLDistributionPoints	http://crl.quovadisglobal.com/pkioprivpersg1.crl	Fixed
AuthorityInfoAccess	http://uw.ocsp.quovadisglobal.com http://trust.quovadisglobal.com/pkioprivpersg1.crt	Fixed
QC Statements	Id-etsi-qcs-QcCompliance { id-etsi-qcs 1 } 0.4.0.1862.1.1 Id-etsi-qct-eseal { id-etsi-qct-esign } 0.4.0.1862.1.6.1 Id-etsi-qcs-QcSSCD { id-etsi-qcs 4 } 0.4.0.1862.1.4 Id-etsi-qcs-QcPDS { id-etsi-qcs 5 } 0.4.0.1862.1.5	Fixed

7.10.3. Private Personal Encryption

Basic Contents	**Value**	**Demarcation**
Subject.CommonName	CommonName	Required
Subject.givenname	Given Name	Required

Subject.surname	Surname	Required
Subject.SerialNumber	SerialNumber	Required
Subject.OrganisationName	OrganisationName	Required
Subject.organisationalUnitName	OrganisationalUnitName	Optional / Prohibited for Profession Certificates
Subject.title	Title	Optional
Subject.CountryName	Country	Required
Subject.PublicKeyInfo	RSA (2048 bit)	Required
Extensions		**Fixed**
KeyUsage (CRITICAL)	Key Encipherment Data Encipherment	Fixed
extKeyUsage	Encrypting File System E-Mail Protection	Required
CertificatePolicies	2.16.528.1.1003.1.2.8.3	Fixed
subjectAltName.Rfc822Name	Rfc822 email address	Optional - Used for e-mail signing (Outlook)
subjectAltName.User Principle Name (MS UPN)	MS UPN in the format: .<unique identifier>@2.16.528.1.1003.1.3.5.2.1	Required
CRLDistributionPoints	http://crl.quovadisglobal.com/pkioprivpersg1.crl	Required
AuthorityInfoAccess	http://uw.ocsp.quovadisglobal.com http://trust.quovadisglobal.com/pkioprivpersg1.crt	Fixed

7.11. CERTIFICATE PROFILE – CRL

Basic Contents	**Value**	**Demarcation**
Issuer.CountryName	NL	Fixed
Issuer.OrganisationName	QuoVadis Trustlink BV	Fixed
Issuer.OrgIdentifier	NTRNL-30237459	Fixed
Issuer.CommonName	Common name of the relevant issuer	Fixed
Effective date	Date	Required
Next update	Date	Required
revokedCertificates	List of revoked Certificates	Required
CRL Extensions		**Fixed**
KeyIdentifier	Key ID	Fixed
CRL Number	CRL Number	Required

7.12. CERTIFICATE PROFILE – OCSP

The OCSP certificate profile below provides an overview of the certificate profile as issued in accordance with the PKIoverheid Program of Requirements, part 3a.

Basic Contents	**Value**	**Demarcation**
SignatureAlgorithm	sha256RSA	Fixed

Issuer.CountryName	NL	Fixed
Issuer.OrganisationName	QuoVadis Trustlink BV	Fixed
Issuer.OrganisationName	NTRNL-30237459	Fixed
Issuer.CommonName	Common name of the relevant issuer	Fixed
Validity.NotBefore	10 years	Required
Validity.NotAfter	10 years	Required
Subject.CommonName	QuoVadis OCSP Authority Signature	Required
Subject.OrganisationName	QuoVadis Limited	Required
Subject.OrganisationUnitName	OCSP Responder	Optional
Subject.CountryName	BM	Required
Subject.PublicKeyInfo	RSA (2048 bit) / System Generated	Required
Extensions		**Fixed**
KeyUsage (CRITICAL)	Digital Signature	Fixed
CertificatePolicies	The OID for OCSP certificates (for all domains) under the G2 is: 2.16.528.1.1003.1.2.5.4. The OID for OCSP certificates under the G3 is as follows: - Organisation Person: 2.16.528.1.1003.1.2.5.1 - Organisation Services: 2.16.528.1.1003.1.2.5.4 - Organisation Servier: 2.16.528.1.1003.1.2.5.6 - Citizen: 2.16.528.1.1003.1.2.3.1 - Autonomous Devices: 2.16.528.1.1003.1.2.6.1 The OID for OCSP certificates under the EV is 2.16.528.1.1003.1.2.7 The OID for OCSP certificates under the Private Root is as follows: - Private Services/server: 2.16.528.1.1003.1.2.8.4 - Private Persons: 2.16.528.1.1003.1.2.8.1	Fixed
extKeyUsage (CRITICAL)	OCSP Signing ocspNoCheck is present	Fixed

8. CONFORMITY EVALUATION

QuoVadis is a TSP as referred to in regulation EU 910/2014 (the eIDAS framework). Being a TSP within the PKIoverheid framework, QuoVadis must comply to the requirements described within the framework as defined in the *Programma van Eisen (PvE).*

QuoVadis is compliant to the applicable requirements of the following standards, requirements and regulations:

- ETSI EN 319 411-1 and 391 411-2

- eIDAS – EU 910/2014
- CA/Browser Forum Network and Certificate System Security Requirements
- CA/Browser Forum Baseline requirements
- GDPR – EU 2016/679
- PKIoverheid Programma van Eisen (PvE)
    - PvE part 3 – General requirements
    - PvE part 3 – Additional requirements
    - PvE part 3a – Organisatie (G2) + Organisatie Persoon (G3)
    - PvE part 3b – Organisatie Services (G1 & G3)
    - PvE part 3c – CSP Burger CA (G2 & G3)
    - PvE part 3e – Organisatie Server CA (G3)
    - PvE part 3f – EV CA (G3)
    - PvE part 3g – Private Services (G1)
    - PvE part 3h – Private Server (G1)
    - PvE part 3i – Private Persoon (G1)

QuoVadis is supervised by the Dutch Governmental Organisation *Agentschap Telecom* for compliance with the EU Regulation on Electronic Signatures. (910/2014 eIDAS)

BSI Group Nederland audits QuoVadis against ETSI EN 319411-1, 319411-2 and standards on an annual basis. During the audits compliance with national laws, regulations and standards are reviewed. BSI Group Nederland is accredited by UKAS for assessments under ISO17065 and the requirements defined in ETSI EN 319403.

External auditors are independent and have no business interests or business affiliation with QuoVadis, DigiCert or affiliated companies.

The scope of the audit concerns the following subjects and processes:

- Registration service
- Certificate Generation Service
- Dissemination Service
- Revocation Management Service
- Revocation Status Service
- Subject Device Provision Service
- Network Security
- Logical and Physical Access
- Logging and Monitoring
- Human Resource Security
- Business Continuity Management
- Compliance

For any non-conformities are found during an audit, QuoVadis drafts a Corrective Action Plan (CAP) proposing corrective measures. The certifying institution must grant approval to the CAP.

QuoVadis conducts internal audits in which the follow-up of corrective actions is checked. Finally, during a subsequent certification audit, the implementation of the corrective measure is checked by the certifying institution.

9. GENERAL AND LEGAL PROVISIONS

9.1. RATES

All applicable rates are available upon request. Rates for Issuing Certificates vary greatly, based on volume and Certificate types. The Subscriber may receive a request for payment prior to or following certificate issuance depending on contractual terms.

Some Products (Certificates) described in this CPS are subject to a Face-to-Face check, where the identity and the Legal Identity Document supplied by the Applicant is verified in person. QuoVadis may charge a fee for this service.

Additional services can be provided to the Subscriber if requested, these additional requests are preceded by a price-quote before the delivery of services takes place. In cases where the Subscriber wishes to renew the Certificate, the Subscriber will be invoiced for a new Certificate with all applicable additional fees.

When Certificates need to be replaced repeatedly at the request of the Subscriber, QuoVadis reserves the right to charge an extra/administrative fee. This fee will be proportionate to the amount of work and/or costs to the repeated replacement of the Certificates.

9.2. FINANCIAL RESPONSIBILITY

QuoVadis has a financial department, responsible for all financially related tasks and operations. QuoVadis uses the services of an international financial services accounting firm, including periodic audits.

QuoVadis has made adequate arrangements to cover liabilities – including product liability – related to this service. The coverage is $10'000,000 (ten million US Dollars). The corporate liability insurance is taken out with an insurance company that has at least an "A" rating with a known rating agency. More details about liability and insurance are in the Terms and Conditions and the contractual agreements between the Subscriber, Relying Parties and QuoVadis.

QuoVadis does not provide for any other undertakings, guarantees and/or commitments than those explicitly provided for in the Terms and Conditions and the contractual agreements.

9.3. CONFIDENTIALITY OF BUSINESS-SENSITIVE DATA

Any personal or company information in the possession of QuoVadis, related to the request of the Certificate Holder and the issue of Certificates, is considered confidential and will not be released without prior permission from the relevant party, unless otherwise required by legislation or requirements of this CPS.

Information in Certificates or that is stored in the electronic storage facility is not considered to be confidential unless required by statutes or special agreements. QuoVadis, Subscribers, Certificate Holders, Relying Parties and all others are responsible for protecting confidential business information that they possess.

9.4. CONFIDENTIALITY OF PERSONAL INFORMATION

QuoVadis is compliant with Data Protection laws and European regulations that are in force for the protection of data. QuoVadis is registered with the Dutch Data Protection Authority as being responsible for processing personal data for the purpose of Certificate services. QuoVadis has an information Security Policy which is regularly reviewed and audited. The policy identifies the data, information and measures necessary to protect it. The QuoVadis Data Protection Officer oversees all aspects of data privacy and reports to the Executive Board of the Parent Company.

All information regarding Certificate Holders that is not publicly available through the content of issued Certificates, CRLs or from the electronic storage location is treated as confidential. All registration records are considered and treated as confidential information.

Certificate Holders explicitly agree with the relocation of personal data, in the form of data recorded in the Certificate fields, outside the Netherlands and may or may not agree with the publication of the Certificate in the electronic Repository that makes the Certificate information publicly available to Relying Parties who search within the electronic Repository with the appropriate query string. Personal data obtained during the registration process that is not included in the Certificate will not be moved outside the Netherlands.

Except for the revocation reasons included in a CRL, the detailed reason for revoking a Certificate is considered confidential information, the only exception being the revocation of the QuoVadis PKIoverheid CA's:

- The compromise of the Private Key of a QuoVadis PKIoverheid CA, in which case a disclosure that the Private Key has been compromised may be published;
- The cancellation of a QuoVadis PKIoverheid CA, in which case prior disclosure of the cancellation may be published.

No confidential data in the possession of QuoVadis will be released to investigative authorities or officers, unless Dutch legislation and regulations require this by means of a court order.

9.5. INTELLECTUAL PROPERTY RIGHTS

All intellectual property rights including all copyrights on Certificates and QuoVadis documents (electronic or in other form) are and will remain the property of QuoVadis. To avoid confusion, documents signed or encrypted with a QuoVadis Certificate are not considered QuoVadis documents in relation to this paragraph, and QuoVadis is not responsible for the content of such documents or notes.

Private and public keys are the property of the Subscriber and Certificate Holder.

QuoVadis guarantees to its Subscribers and Certificate Holders that the Certificates issued by the same and carriers of the private and public key, including the thereto-pertaining and delivered equipment and documentation, do not infringe intellectual property rights, including copyrights, trademark rights and used software that are vested in its suppliers.

9.6. LIABILITY AND GUARANTEES

9.6.1. Liabilities of QuoVadis

QuoVadis hereby declares that:

i. It has taken reasonable steps to verify the information contained in a Certificate for accuracy at the time of issue

ii. Certificates will be withdrawn if QuoVadis suspects or has been notified that the content of a Certificate is no longer accurate, or that the key associated with a Certificate has been compromised in any way.

QuoVadis is only liable in respect to Certificate Holders or Relying Parties for immediate loss resulting from the violation by QuoVadis of provisions of this CSP or of any other liability under agreement, tort or otherwise, including liability for negligence up to the maximum amount included in chapter 9.8, for any event or series of related events (in a 12-month period).

QuoVadis excludes all liability for damage that occurs if the Certificate is not used in accordance with the intended Certificate use, as described in chapter 1.4 of this CPS.

QuoVadis can, at the direction of the PA of the PKI for the Government, include restrictions on its use in the signature Certificate, provided the relevant restrictions are clear to third parties. QuoVadis is not liable for damage resulting from the use of a signature Certificate in violation of such an included restriction.

QuoVadis does not accept any form of liability for damage suffered by Relying Parties, with the following exceptions:

- QuoVadis is, in principle, liable in accordance with Article 6.19b, first to third paragraphs, of the Dutch Civil Code, on the understanding that:
  a) "a Qualified Certificate as referred to in Article 1.1. section ss Telecommunications Act" is read as follows: "an Authentication Certificate"
  b) "Signatory": is read as: "Certificate Holder";
  c) "Electronic Signatures" is read as: "Authentication characteristics".
- QuoVadis is, in principle, liable in accordance with Article 6.19b, first to third paragraphs, of the Dutch Civil Code, on the understanding that:

a) “a Qualified Certificate as referred to in Article 1.1. section ss Telecommunications Act” is read as follows: "an EV SSL Certificate";
b) "Signatory": is read as: “Certificate Holder”;
c) "creating Electronic Signatures" is read as: "creating Encrypted Data";
d) "verifying Electronic Signatures" is read as: "decrypting Encrypted Data".
e) “a Qualified Certificate as referred to in Article 1.1. section ss Telecommunications Act” is read as follows: "a Server Certificate";
f) "Signatory": is read as: “Certificate Holder”;
g) "creating Electronic Signatures" is read as: "verifying Authentication characteristics and creating Encrypted Data";
h) "verifying Electronic Signatures" is read as: "decrypting Authentication characteristics and Encrypted Data".

9.6.2. Liability of Subscribers and Certificate Holders

Certificate Holders guarantee that:

- the Private Key is protected and there has never been access for another person
- all representations made by the Certificate Holder are correct
- all information in the Certificate is correct and accurate
- the Certificate is used in accordance with the intended, authorised and lawful use in accordance with this CPS
- they request immediate revocation of the Certificate in the case that: (a) any information contained in the Certificate is or becomes inaccurate or inaccurate, or (b) the Private Key corresponding to the public key in the Certificate is (presumably) abused or compromised.

9.6.3. Liability of the Relying Parties

Relying parties guarantee that:

- they will collect sufficient information about a Certificate and its holder to make a decision based on good information about the extent to which a Certificate can be relied on.
- they are solely responsible for making the decision to rely on a Certificate (except for the provisions in 9.6.1)
- they bear the legal consequences as a result of failure to act in accordance with the obligations of relying parties in accordance with this CPS.
- They have checked to certificate status against the QuoVadis OCSP or relevant CRL

9.7. EXCLUSION OF GUARANTEES

To the extent permitted by applicable law, this CPS, the Certificate Holder Agreement and any other contractual documentation applicable within the PKI for Government excludes guarantees from QuoVadis.

9.8. LIMITATION OF LIABILITY

9.8.1. Limitations of the liability of QuoVadis

Under no circumstances will QuoVadis be responsible for any loss of profit, loss of sales or turnover, loss or damage to reputation, loss of contracts, loss of customers, loss of use of any software or data, loss or use of any computer or other equipment (unless directly the result of a breach of this CPS), time of management or other personnel, losses or liabilities in connection with or in relation to other contracts, indirect damage or loss, consequential damage or loss, special loss or damage, and within this section, "loss" means both a partial loss of or decrease in value, and full or total loss.

QuoVadis' liability as regards a particular person regarding damage that occurs in any way under, on behalf of, within or in relation to this CPS, Certificate Holder Agreement, the applicable contract or related

agreement, whether in contract, warranty, tort or any other legal theory , is, subject to what is set forth below, limited to actual damage suffered by this person. QuoVadis will not be liable for indirect, consequential, incidental, special, exemplary or punitive damages in respect of any person, even if QuoVadis has been advised of the possibility of such damages, regardless of how such damage or responsibility occurred, whether in unlawful act, negligence, justice, contract, statute, customary law or otherwise. As a condition for participation within the PKI for the Government (including, without limitation, the use of or reliance on Certificates), any person who participates within the PKI for the Government irrevocably agrees that they do not wish to claim or otherwise seek, for example, consequential, special, incidental or punitive damages and irrevocably confirms to QuoVadis the acceptance of the aforementioned as a condition and incentive to allow this person to participate in the PKI for the Government.

9.8.2. Exclusion of liability

QuoVadis will in no way be liable for any loss concerning or arising from one (or more) of the following circumstances or causes:

- If the Certificate, held by the claimant or otherwise subject to any claim, has been compromised by unauthorised disclosure or use of the Certificate, or any password or activation data that controls access thereto;
- If the Certificate, held by the claimant or otherwise subject to any claim, is issued as a result of misrepresentation, error or fact, or negligence of any person, entity or organisation;
- If the Certificate held by the claimant or otherwise subject to any claim has expired or has been withdrawn before the date of any circumstances leading to any claim;
- If the Certificate, held by the claimant or otherwise subject to any claim, has been changed or altered in any way or used in any way other than permitted by the terms of this CPS and/or the relevant Certificate Holder Agreement or any applicable law - or regulations;
- If the Private Key, corresponding to the Certificate held by the claimant or otherwise subject to any claim, is compromised;
- If the Certificate, held by the claimant is issued in a manner that is in violation of any applicable law or regulation;
- Computer hardware or software, or mathematical algorithms, have been developed that tend to make public key cryptography or asymmetric crypto systems uncertain, provided that QuoVadis uses commercially reasonable practices to protect against security breaches caused by such hardware, software or algorithms;
- Power failures, power outages, or other power outages, provided that QuoVadis uses commercially reasonable methods to protect against such disruptions;
- Failure of one or more computer systems, communication infrastructure, processing, or storage media or mechanisms or any sub-component of the aforementioned, not under the exclusive control of QuoVadis and/or its subcontractors; or
- One or more of the following events: a natural disaster or force majeure (including, without limitation, flood, earthquake, or other natural or weather-related cause); a work disruption; war, insurrection or overt military hostilities; conflicting legislation or state action, prohibition, embargo or boycott; riots or civil disturbances; fire or explosion; catastrophic epidemic; trade embargo; restriction or impediment (including, without limitation, export controls); any lack of availability or integrity of telecommunications; legal coercion, including any decision made by a court of competent jurisdiction to which QuoVadis is subject; and any event or circumstance or set of circumstances that fall outside the control of QuoVadis.

9.8.2.1. Restriction of Certificate Loss

Without prejudice to another provision of this chapter, QuoVadis' liability for breach of its obligations under this CPS, except for QuoVadis fraud or wilful misconduct, will be subject to a monetary limit determined by the type of Certificate held by the claimant.

The loss limitations apply to the life cycle of a certain Certificate with the intention that the loss limitations reflect the total possible cumulative liability of QuoVadis per Certificate per year (regardless of the number of requirements per Certificate). This limitation applies regardless of the number of transactions or causes of action with respect to a particular Certificate in any year of that Certificate's life cycle.

9.8.3. Limitation of liability of QuoVadis

QuoVadis has introduced several measures to reduce or limit its liabilities in the case that protective means fail to:

- prevent misuse of these sources by authorised personnel;
- prohibit access to these sources by unauthorised individuals;

These measures include, but are not limited to:

- identifying unforeseen events and applicable remedial actions in a business continuity plan and Disaster Recovery Plan;
- regularly performing system data backups;
- performing a backup of the current working software and certain software configuration files;
- storing all backups in secure local and decentralised facilities;
- maintaining a secure decentralised facility for other material needed for disaster recovery;
- periodically testing local and decentralised backups to ensure that the information is recoverable in the case of a failure;
- periodically reviewing the business continuity plan and Disaster Recovery Plan, including the identification analysis, evaluation and prioritisation of risks; and
- periodic monitoring of uninterrupted power supply.

9.8.4. Requirements regarding the liability of QuoVadis

9.8.4.1. Notification Period

QuoVadis will have no obligations in accordance with any claim for breach of its obligations unless the claimant informed QuoVadis within ninety (90) days after the claimant knew or should have reasonably known of the claim, and in no case more than three years after the expiry of the Certificate that the claimant held.

9.8.4.2. Restrictive actions and disclosure of supporting information

As a condition for payment of QuoVadis regarding any claim under the terms of this CPS, a claimant will do and perform all further actions and acts, and perform and deliver all such agreements, instruments and documents that QuoVadis reasonably requests for a claim for loss made by the claimant.

9.9. DAMAGE COMPENSATION

The provisions and obligations regarding compensation are included in the relevant contractual documentation.

9.10. CPS VALIDITY PERIOD

9.10.1. Term

This CPS is valid from the date and time of publication on the QuoVadis Repository. Revisions to the CPS are valid from the date and time of publication in the QuoVadis Repository.

9.10.2. Termination

This CPS will remain valid until it has been revised or replaced by another version.

9.10.3. Effect of termination and survival

The provisions within this CPS survive the termination or revocation of a Certificate Holder or relying party within the PKI for the Government regarding all acts based on the use of or reliance on a Certificate or other participation within the PKI for the Government. Any such termination or revocation will not act in such a way as to prejudice or influence any right to action or remedy that were due to any person up to and including the date of revocation or termination.

9.11. INDIVIDUAL NOTIFICATION AND COMMUNICATION WITH INVOLVED PARTIES

QuoVadis may use E-mail, mail, fax and web pages are available means to notify parties as required by this CPS, unless specifically provided otherwise.

Participants may Electronic mail, mail and fax are valid means to provide any information required by this CPS to QuoVadis unless specifically noted in this CPS (for example, regarding revocation requests).

9.12. CHANGES

9.12.1. Change procedure

Changes to this CPS will be in the form of a modified CPS or replacement CPS. Updated versions of this CPS will replace designated or conflicting provisions of the stated version of the CPS.

There are two possible types of policy change:

- the issue of a new CPS; or
- a change or adjustment of a policy in the existing CPS.

The only changes that may be made to this CPS without reporting are editorial or typographical corrections that have no consequences for any participants within the PKI for the Government.

9.12.2. Notification of changes

The new or modified CPS is published in the electronic Repository, on the website http://www.quovadisglobal.nl/repository.aspx.

If a policy change has consequences for Certificate Holders, QuoVadis will make the change known to its registered Subscribers and/or Certificate Holders by means of a notification in accordance with the provisions of this CPS.

If there is an intention to change the CA structure, QuoVadis submits this information to the PA.

9.13. DISPUTE SETTLEMENT

Any controversy or requirement between two or more participants within the PKI for the Government (with QuoVadis as a participant within the PKI for the Government), arising from or related to this CPS, will be submitted to a competent court.

9.14. APPLICABLE LEGISLATION

All agreements entered into by QuoVadis are governed by Dutch law, unless otherwise specified.

9.15. COMPLIANCE WITH RELEVANT LEGISLATION

QuoVadis is a Certification Service Provider under the Telecommunications Act and conforms to the applicable laws and regulations that relate to that role.

9.16. OTHER PROVISIONS

Any provisions within this CPS that is declared invalid or unenforceable will not apply. This is without prejudice to the applicability of the remaining provisions in this CPS.

In accordance with the subscriber agreement the issuance of certificates which include the ServerAuth extended key use are subject to the Baseline Requirements QuoVadis will inform all subscribers every six

months that certificates may revoked because of those conditions and within the timespan defined in the Baseline Requirements section 4.9.1.1.

10. ANNEX A – DEFINITIONS AND ABBREVIATIONS

For definitions and abbreviations regarding this CPS, please refer to the SoR, part 4, managed by Logius located at:

https://www.logius.nl/sites/default/files/public/bestanden/English/PKIoverheid/Program-Requirements-EN-part4_0.pdf