Certification Practice Statement PKIoverheid

Effective Date: 29 April, 2020
Version: 1.2

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.
QuoVadis PMA	20 March 2020	1.1	Revisions and edits to entire CPS, including structural changes for RFC 3647, Mozilla Policy 2.7 and Ballot SC2.
QuoVadis PMA	29 April	1.2	CAA Records Update and minor formatting changes.

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

CONTENTS

1. INTRODUCTION

This document is the QuoVadis Trustlink B.V. Certification Practice Statement for PKIoverheid. 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") for the issuance of Certificates from the PKIoverheid Root.

1.1 OVERVIEW

This CPS describes the practices and procedures that are employed in the life-cycle management of Certificates, including the generation, Issuance and revocation of PKIoverheid Certificates. The publication of version 1.1 of this English Certificate Practice Statement for PKIoverheid renders all the previous English and Dutch versions (as mentioned under 'previous versions' in Version Control) obsolete.

The Dutch Government are the Policy Authority (PA) for PKIoverheid issued Certificates and impose strict requirements on TSPs to be able to issue any publicly trusted Certificate from their Root. The requirements are known as the "Programma van Eisen" (PvE) which means Program of Requirements. These are maintained and managed by the Government department Logius. The requirements are publicly available via the website from Logius [www.logius.nl].
This document is structured per RFC 3647 and divided into 9 parts which cover all aspects of the issuance and management of Certificates. 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 and ISO27001:2013. Please see our website for details.

1.1.1 Intended audience

This document is intended for:

- Subscribers
- Certificate Managers
- Relying Parties

1.2 DOCUMENT NAME AND IDENTIFICATION

This document is the QuoVadis Trustlink B.V. "Certificate Practice Statement for PKIoverheid Certificates".
QuoVadis issues the following Subscriber Certificates in the following hierarchies from PKIoverheid;

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

NOTE: 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

Root CA: Staat der Nederlanden EV Root CA Intermediate CA: Staat der Nederlanden EV Intermediair CA		
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

1.3 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 Scheme. 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 comply 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 (RA) 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 and 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 Subscriber 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. Subscribers of Server Certificates are organisations. The Certificate Manager is a Representative of an organisation and is also the holder of the Private Key.

1.3.3.1 Obligations and Responsibilities Of Subscribers

Subscribers agree to the following obligations in applying for, using and managing a Certificate issued by QuoVadis under PKIoverheid;

a) The obligation to provide the TSP with accurate and complete information in accordance with the requirements of the present document, particularly with regards to registration;

b) The obligation for the key pair to be only used in accordance with any limitations notified to the subscriber and the subject if the subject is a natural or legal person;
c) The prohibition of unauthorized use of the subject's private key;
d) If the Subscriber has generated their own keys, then;
    a. The recommendation to generate the subject keys using an algorithm as specified in ETSI TS 119 312 for the uses of the certified key as identified in the CP;
    b. The recommendation to use the key length and algorithm as specified in ETSI TS 119 312 for the uses of the certified key as identified in the CP during the validity time of the certificate;
e) If the Subscriber or Subject generates the subject's keys and certificate key usage is for Non-repudiation (signing), Digital Signatures or Key Encipherment, then;
    a. When the Subject is a natural person there is an obligation for the subject's private key to be maintained under the Subject's sole control;
    b. When the Subject is a legal person there is an obligation for the subject's private key to be maintained under the Subject's sole control;
f) The obligation to only use the Subject's private keys for cryptographic functions within the secure cryptographic device;
g) The obligation to notify the TSP, without delay, if any of the following occur up to the end of the Certificate validity period;
    a. If the Subject's private key has been lost, stolen, potentially compromised;
    b. Where control over the Subject's private key has been lost due to compromise of activation data (e.g. PIN code) or other reasons;
    c. Where there are inaccuracies or changes to the Certificate content, as notified to the Subscriber or Subject;
h) The obligation, following compromise of the Subject's private key, to immediately and permanently discontinue use of this key, except for key decipherment, and;
i) The obligation, in case of being informed that the Subject's Certificate has been revoked, or that the issuing CA has been compromised, to ensure that the private key is no longer used by the Subject.

1.3.4 Relying Parties

A Relying Party is any natural or legal person who is a recipient of data signed or protected by a Certificate, who acts in reliance on that Certificate and relies upon the trusted status of the Certificate. QuoVadis recommend the following;

a) To verify the validity, suspension or revocation of the Certificate using current revocation status information as indicated to the relying party;
b) To take account of any limitations on the usage of the certificate indicated to the relying party either in the Certificate or Terms of Use as supplied;
c) To take any other precautions prescribed in agreements or elsewhere.

Revocation is covered in 4.9.1and 4.9.3 of this CPS.

1.3.5 Other Participants

No stipulation.

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 (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

1.5.1 Organisation Administering the Document

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

1.5.2 Contact Person

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

1.5.2.1 Revocation Reporting

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 case of suspected Private Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates or this document, Subscribers, Relying Parties, Application Software Suppliers, and other third parties can contact QuoVadis directly.
Revocation procedures are also described in this CPS in 4.9.1 and 4.9.3.

1.5.3 Person Determining CPS Suitability for the Policy

The QuoVadis Policy Management Authority (PMA) determines the suitability and applicability of this CPS based on the results and recommendations received from an independent auditor (see Section 8).

1.5.4 CPS Approval Procedures

This CPS is reviewed and approved at least on an annual basis, and if any significant changes in the provision of PKIoverheid Certificates occurs.

1.6 DEFINITIONS AND ACRONYMS

Definitions and acronyms are provided at the end of this document in Chapter 10.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 REPOSITORY

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

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

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

2.2 PUBLICATION OF INFORMATION

The Repository contains:

- The CPS
- PKI Disclosure Statement
- Terms and Conditions, Privacy Statement
- Certificates for Subscribers (only with the consent of the Subscriber)
- 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 TIME OR 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 a minimum of every 12 hours, where the response is valid for 72 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.

2.4 ACCESS CONTROLS ON REPOSITORIES

Read-only access to the repository is unrestricted. Logical and physical controls prevent unauthorised write access to repositories.

3 IDENTIFICATION & AUTHENTICATION

3.1 NAMING

3.1.1 Types of Names

3.1.1.1 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

3.1.2 Need for Names to be Meaningful

QuoVadis uses Distinguished Names in the Certificates based on the tables above, to create names which are meaningful, unambiguous, and unique and allows any Relying Party to identify the Subscriber.

3.1.3 Anonymity or Pseudonymity of Subscribers

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

3.1.4 Rules for Interpreting Various Name Forms

Distinguished Names in Certificates are interpreted using X.500 standards.

3.1.5 Uniqueness of Names

No stipulation.

3.1.6 Recognition, Authentication and Role of Trademarks

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

QuoVadis may use any legal means of communication or investigation to ascertain the identity of an organisational or individual applicant. QuoVadis may refuse to issue a Certificate in its sole discretion.

The applicant begins the application on the QuoVadis website: https://www.quovadisglobal.nl/. Depending on the type of Certificate required the applicant will submit information via the website registration or will be sent a standard application form. A QuoVadis representative is responsible for the processing of applications, however, a professional registrar may be consulted (where needed) to verify application data. Identity vetting may also be performed by AMP by trained employees on behalf of QuoVadis, specifically for the Face-to-face checks.

For all Certificate applications a series of checks and validation actions will be carried out. The table below shows the types of checks and validations carried out per Certificate;

Certificate Type	Checks and Validations Performed
PKIo Personal Organisation Certificates **Domain CA: Staat der Nederlanden Organisatie Persoon CA - G3**	• Individual Identity Checks • Organisation Checks • Certificate Signing Request (CSR)
PKIo Professional Certificate (Beroepscertificaat) **Staat der Nederlanden Burger CA - G3**	• Individual Identity Checks • Professional check • CSR
PKIo Services Server Certificates **Staat der Nederlanden Organisatie Services CA - G3**	• Individual Identity Checks • Authorised Person Checks • Organisation Checks • Fully Qualified Domain Name Checks (FQDN) • CSR
PKIo Extended Validation Certificates **Staat der Nederlanden EV Intermediair CA**	• Individual Identity Checks • Authorised Person Checks • FQDN Checks • Organisation Checks • CSR
PKIo Qualified Website Authentication **Staat der Nederlanden EV Intermediair CA**	• Individual Identity Checks • Authorised Person Checks • FQDN Checks • Organisation Checks • CSR
PKIo Private Root Personal **Staat der Nederlanden Private Personen CA – G1**	• Individual Identity Checks • CSR
PKIo Private Root Server Services **QuoVadis PKIoverheid Private Services CA – G1**	• Individual Identity Checks • Authorised Person Checks • FQDN (if applicable0 • CSR

All certificate OIDs are listed in 1.2 of this document where the names refer to the names in the table above.

Once all checks are performed and successful a Certificate can be issued. Once a Certificate is issued an applicant becomes a subscriber.

3.2.1 Method to prove possession of Private Key

QuoVadis ensures that the applicant delivers the Certificate signing request (CSR) in a secure manner. For PKIo Certificates a CSR is required. 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 applicant 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 in the Netherlands a certified extract from the Kamer van Koophandel (KvK) Trade Register. Extracts may not be older than 1 month old.
- For Organisations outside of the Netherlands the following may be used where the Authorised Representative is shown;
- Trade Registers or equivalent
- Article of Association
- Generation Administrative Order

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

For Organisations in the Netherlands in the application a certified extract from the Kamer van Koophandel (KvK) Trade Register. Extracts may not be older than 1 month old.

For Organisations outside of the Netherlands the following may be used where the Authorised Representative is shown;

- Trade Registers or equivalent
- Article of Association
- Generation Administrative Order

3.2.2.2 Verification of the address of the organisation

QuoVadis verifies that the address the organisation provided by the applicant 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, building 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 check the information with the Trade Register Information collected (above in 3.2.2.1) for a match.

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

The nature of the buildings/location of the applicant 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 applicant.

One or more photos of the outside of the applicant's premises (on which, the signposts and street address plate, if existing, are present) and the reception desk or office workspace of the applicant.

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 applicant 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 applicant 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 applicant.

3.2.2.4 Verification of the age of the organisation

If, based on the requested data, it appears that the applicant'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 applicant 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 Validation of Domain Authorisation and Control

For each FQDN listed in a Certificate, QuoVadis confirms that, as of the date the Certificate was issued, the Applicant either is the Domain Name Registrant or has control over the FQDN by:

i) Communicating directly with the Domain Name Registrant via email, fax or postal mail provided by the Domain Name Registrar. Performed in accordance with BR section 3.2.2.4.2 using a Random Value (valid for no more than 30 days from its creation)

ii) Communicating directly with the Domain Name Registrant by calling their phone number and obtaining a response confirming the Applicant's request for validation of the FQDN. The phone number used must be the number listed by the Domain Name Registrar. Performed in accordance with BR section 3.2.2.4.3;

iii) Communicating with the Domain's administrator using a constructed email address created by pre-pending 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' to the Authorisation Domain Name. Performed in accordance with BR section 3.2.2.4.4;

iv) Confirming the Applicant's control over the requested Authorisation Domain Name (which may be prefixed with a label that begins with an underscore character) by confirming the presence of an agreed-upon Random Value in a DNS record. Performed in accordance with BR section 3.2.2.4.7;

v) Confirming the Applicant's control over the FQDN through control of an IP address returned from a DNS lookup for A or AAAA records for the FQDN, performed in accordance with BR Sections 3.2.2.5 and 3.2.2.4.8;

vi) Confirming that the Applicant is the Domain Contact for the Base Domain Name (provided that the CA or RA is also the Domain Name Registrar or an Affiliate of the Registrar), performed in accordance with BR Section 3.2.2.4.12;

vii) Confirming the Applicant's control over the FQDN by sending a Random Value via email to a DNS CAA Email Contact and then receiving a confirming response utilising the Random Value. The relevant CAA Resource Record Set is found using the search algorithm defined in RFC 8659 performed in accordance with BR Section 3.2.2.4.13;

viii) Confirming the Applicant's control over the FQDN by sending a Random Value via email to the DNS TXT Record Email Contact for the Authorisation Domain Name for the FQDN and then receiving a confirming response utilising the Random Value, performed in accordance with BR Section 3.2.2.4.14;

ix) Confirming the Applicant's control over the FQDN by calling the Domain Contact's phone number and obtaining a confirming response to validate the authorised Domain Name. Each phone call can confirm control of multiple authorised Domain Names provided that the same Domain Contact phone number is listed for each authorised Domain Name being verified and they provide a confirming response for each authorised Domain Name, performed in accordance with BR Section 3.2.2.4.15;

x) Confirming the Applicant's control over the FQDN by calling the DNS TXT Record Phone Contact's phone number and obtaining a confirming response to validate the authorised Domain Name. Each phone call can confirm control of multiple authorised Domain Names provided that the same DNS TXT Record Phone Contact phone number is listed

for each authorised Domain Name being verified and they provide a confirming response for each authorised Domain Name, performed in accordance with BR Section 3.2.2.4.16;

xi) Confirming the Applicant's control over the requested FQDN by confirming the presence of an agreed-upon Random Value under the "/.well-known/pki-validation" directory. Performed in accordance with BR section 3.2.2.4.18; and

xii) Confirming the Applicant's control over a FQDN by validating domain control of the FQDN using the ACME HTTP Challenge method, performed in accordance with BR Section 3.2.2.4.19.

QuoVadis verifies an Applicant's or Organisation's right to use or control of an email address to be contained in a Certificate that will have the "Secure Email" EKU by doing one of the following:

i) By verifying domain control over the email Domain Name using one of the procedures listed in this section; or

ii) by sending an email message containing a Random Value to the email address to be included in the Certificate and receiving a confirming response within a limited period of time that includes the Random Value to indicate that the Applicant controls that same email address.

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

3.2.2.6 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. 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;
4. 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

5. 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.

3.2.3 Authentication of Individual Identity

3.2.3.1 Natural Person

The following checks are carried out for a natural person;

- Personal Details: The personal details are verified using the details on a Legal Identity Document. This includes full legal name(s) and date of birth.
- Email address: Verification of the applicant's control over the email address is carried out by the first contact. The applicant is manually sent an email with instructions, documents and forms required for the registration, or automatically when 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 check: 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 of Use and Privacy Statement: During registration, the Applicant is required to agree with the applicable Terms of Use as well as the Privacy Statement.

- **PROFESSION CHECK**

Verification of the natural person in the applicable professional registrar is done when applicable for the specific Certificate that is applied for. QuoVadis currently issue Certificates for the following professions;

- Advocate/Lawyer
- Notary
- Court Bailiff

- Registered Accountant
- Administration-Accountant Consultant

3.2.3.2 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 Organisations in the Netherlands a certified extract from the Kamer van Koophandel (KvK) Trade Register. Extracts may not be older than 1 month old at the time of certificate request.
- For Organisations outside of the Netherlands the following may be used where the Authorised Representative is shown;
    - Trade Registers or equivalent
    - Article of Association
    - Generation Administrative Order

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/

3.2.3.3 Verification of the identity of the Certificate Subscriber

QuoVadis will verify the identity and, if applicable, specific properties of the Certificate Manager, in accordance with Dutch laws and regulations, as described in 3.2.3.1. 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.

3.2.3.4 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:

1 full name, including surname, given name, initials or other first name (s) (if applicable) and inserts (if applicable);

2 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;

3 proof that the Certificate Manager is entitled to receive a Certificate for a Subcriber 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 Non-verified Subscriber information

Non-verified Subscriber information may include the Organisational Unit (OU) as mentioned in this CPS.

3.2.4.1 Authorisation of the Certificate Subscriber (Service)

No stipulation.

3.2.4.2 Verification of authorisation of the Subscriber (Service)

QuoVadis will check that:

- the proof that the Certificate Manager is Authorised on behalf of the Subscriber to request and receive a Certificate;
- 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 Subscriber 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.

3.2.4.3 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.

3.2.4.4 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:

- Trade Register information which is not older than 1 month old at the time of Certificate request.
- Domain name check and validation – 3 (three) months
- Identification checks – 3 (three) months
- Blacklist & Phishing check – 3 (three) months

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. Certificate

3.4 IDENTIFICATION & AUTHENTICATION FOR REVOCATION REQUEST(S)

All revocation requests are authenticated by QuoVadis or the RA responsible for issuing the Certificate. QuoVadis may authenticate revocation requests by referencing the Certificate's Public Key, regardless of whether the associated Private Key is compromised. A Subscriber may request that their Certificate be revoked by:

• Authenticating to TrustLink Certificate Management Portal and requesting revocation via that system;

• Applying in person to the RA, Issuing CA or QuoVadis supplying either original proof of identification in the form of a valid Driving License or Passport;

• Telephonic communication using a pre-existing shared secret, password or other information associated with Subscriber's account with the CA following appropriate Identification.

3.4.1 Professional Bodies

In certain cases, namely where a PKIoverheid professional Certificate showing the Subscriber'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.

3.4.2 Professional Bodies

In certain cases, a Government or Industry Supervisory Body may request revocation when a Subscriber's entitlement to use certain fields in a Certificate. 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 Submit a Certificate Application

Only an Authorised Representative of the Subscriber can apply for a Subscriber Certificate. 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 documentation and the contracts.

QuoVadis does not issue Certificates to entities on a government denied list maintained by the United States or that are located in a country with which the laws of the United States prohibit doing business.

4.2 CERTIFICATE APPLICATION PROCESSING

4.2.1 Performing Identification and Authentication Functions

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.

4.2.2 Approval or Rejection of Certificate Applications

After receiving a Certificate application QuoVadis will assess the information for completeness and will check if all of the information meets the requirements as laid out in this CPS.

QuoVadis, in its sole discretion, may refuse to issue a Certificate, without incurring any liability for loss or damages arising out of such refusal. QuoVadis reserves the right not to disclose the reason for any refusal.

4.2.3 Time to Process Certificate Applications

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.

4.2.4 Certificate Authority Authorisation (CAA)

Prior to issuing TLS/SSL Digital Certificates, QuoVadis checks for CAA records for each dNSName in the subjectAltName extension of the Digital Certificate to be issued. If the QuoVadis Digital Certificate is issued, it will be issued within the TTL of the CAA record, or 8 hours, whichever is greater.
When processing CAA records, QuoVadis processes the issue, issuewild, and iodef property tags as specified in RFC 6844 as amended by Errata 5065 (Appendix A). QuoVadis may not act on the contents of the iodef property tag. QuoVadis will not issue a Digital Certificate if an unrecognized property is found with the critical flag.

CAA checking is optional for Certificates where CAA was checked prior to the creation of a corresponding CT pre-certificate that was logged in at least 2 public CT log servers.
DNS access failure can be treated as permission to issue when the failure is proven to be outside QuoVadis infrastructure, was retried at least once, and the domain zone does not have a DNSSEC validation chain to the ICANN root. QuoVadis documents potential issuances that were prevented by a CAA record, and may not dispatch reports of such issuance requests to the contact stipulated in the CAA iodef record(s), if present. QuoVadis supports mailto: and https: URL schemes in the iodef record.

The CAA identifying domains for Cas recognized by QuoVadis are:
"quovadisglobal.com", "pkioverheid.nl", "digicert.com", digicert.ne.jp", "cybertrust.ne.jp", "Symantec.com", "Thawte.com", "geotrust.com", "rapidssl.com", "digitalcertvalidation.com" (with reseller-specific licensed prefixes) and any domain containing those identifying domains as suffixes (e.g. example.digicert.com).

4.3 CERTIFICATE ISSUANCE

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 Subscriber 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.

4.4 CERTIFICATE ACCEPTANCE

After Issuing a Certificate, the Subscriber 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, all Subscriber obligations are as described in 1.3.3.1.

The Subscriber 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 Subscriber 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.

4.5 KEY PAIR & CERTIFICATE USAGE

As described in this CPS the Subscriber agrees with all applicable Terms of Use, 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 Subscriber 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.

4.5.1 Relying Party Public Key and Certificate Usage

Relying Parties may only use software that is compliant with X.509, IETF RFCs, and other applicable standards. QuoVadis does not warrant that any third party software will support or enforce the controls and requirements found herein.

A Relying Party should use discretion when relying on a Certificate and should consider the totality of the circumstances and risk of loss prior to relying on a Certificate. If the circumstances indicate that additional assurances are required, the Relying Party must obtain such assurances before using the Certificate. Any warranties provided by QuoVadis are only valid if a Relying Party's reliance was

reasonable and if the Relying Party adhered to the Relying Party Agreement set forth in the QuoVadis Repository.

- A Relying Party should rely on a digital signature or TLS/SSL handshake only if:
- the Digital Signature or TLS/SSL session was created during the operational period of a valid Certificate and can be verified by referencing a valid Certificate,
- the Certificate is not revoked and the Relying Party checked the revocation status of the Certificate prior to the Certificate's use by referring to the relevant CRLs or OCSP responses, and
- the Certificate is being used for its intended purpose and in accordance with this CP/CPS

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 Subscribers of the imminent expiration of a Certificate.

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 Subscriber'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 CERTIFICATE REVOCATION & SUSPENSION

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.

For PKIoverheid, Certificates will be revoked within 4 hours of receipt of the revocation request

4.9.1 Circumstances for Revocation

Certificates will be revoked when:

1. Subscriber requests in writing that QuoVadis can revoke the Certificate;
2. Subscriber notifies QuoVadis that the original Certificate request was not authorised and does not retroactively grant authorisation;
3. QuoVadis obtains evidence that the Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with applicable requirements. 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;

4. QuoVadis obtains evidence that the validation of domain authorisation or control for any FDQN or IP address in the Certificate should not be relied upon.
5. That the Certificate no longer complies with the Sections 6.1.5 or 6.1.6 of this CPS document;
6. QuoVadis obtains evidence that the Certificate was misused;
7. QuoVadis is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms & Conditions;
8. QuoVadis is made aware of any circumstance indicating that use of a FQDN in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a licensing or services agreement between the Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name);
9. QuoVadis is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name
10. QuoVadis is made aware of a material change in the information contained in the Certificate;
11. QuoVadis is made aware that the Certificate was not issued in accordance with the requirements or QuoVadis' Certificate Policy or Certification Practice Statement;
12. QuoVadis determines that any of the information appearing in the Certificate is inaccurate or misleading;
13. Revocation is required by the QuoVadis' Certificate Policy and/or Certification Practice Statement;
14. The CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP Repository;
15. The CA is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise, methods have been developed that can easily calculate it based on the Public Key (such as a Debian weak key, see http://wiki.debian.org/SSLkeys), or if there is clear evidence that the specific method used to generate the Private Key was flawed;
16. If the technical content or format of the Certificate presents an unacceptable risk;
17. If QuoVadis ceases its activities and the CRL and OCSP services are not undertaken by another TSP.

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 Revocation

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

- The Certificate Manager

- The Subscriber
- QuoVadis as a TSP
- Organisations of Registered Professionals
- Authorities/regulators who are involved in the regulation of PKIo activities e.g. Logius.
- Application Software Suppliers.

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.

4.9.3.1 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.

4.9.4 Revocation Grace Period

Requests for revocation are processed immediately for PKIo Certificates. There is no grace period.

4.9.5 Time Within Which the CA Must Process the Revocation Request

Revocation will be processed and completed within 4 hours of receipt of a legitimate revocation request.

4.9.6 Certificate Status Information

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

4.9.6.1 Validity of CRL

A CRL is valid for a maximum of 72 hours and is generated at least every 12 hours.

4.9.7 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”.

4.9.7.1 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 PvE 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"

4.9.8 Maximum Latency For CRL

CRLs for Certificates issued to end entity Subscribers are posted automatically to the online Repository within a commercially reasonable time after generation, usually within 10 minutes of generation.

4.9.9 On-Line Revocation/Status Checking Availability

QuoVadis provides OCSP checking. Where applicable, the URL for the OCSP responder may be found within the Authority Information Access (AIA) extension of the Certificate.

4.9.9.1 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.

4.9.10 OCSP Checking Requirement

A Relying Party must confirm the validity of a Certificate in accordance with section 4.9.6 prior to relying on the Certificate.
QuoVadis supports an OCSP capability using the GET method for Certificates. OCSP Responders under QuoVadis’ direct control will not respond with a "good" status for a certificate that has not been issued, in accordance with the Baseline Requirements. The CRLReason for non-issued Certificates is “certificateHold” (value 6).

4.9.11 Other Forms Of Revocation Advertisements Available

Not applicable.

4.9.12 Special Requirements in Relation to Key Compromise

QuoVadis uses commercially reasonable efforts to notify potential Relying Parties if it discovers or suspects the compromise of a Private Key. QuoVadis will select the CRLReason code "keyCompromise" (value 1) upon discovery of such reason or as required by an applicable CP/CPS. Should a CA Private Key become compromised, all Certificates issued by that CA shall be revoked.

4.9.13 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.

4.9.14 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.
QuoVadis does not provide Certificate Modification. QuoVadis may reissue or replace a valid Certificate when the Subscriber'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.

4.10 CERTIFICATE STATUS

4.10.1 Operational Characteristics

The status of Certificates issued within the QuoVadis PKI is published in a CRL (http://crl.quovadisglobal.com/<caname>.crl) or OCSP (http://ocsp.quovadisglobal.com) where available.
Revocation entries on a CRL or OCSP response are not removed until after the expiry date of the revoked Certificate, except for revoked Code Signing Certificates which remain on the CRL for at least 10 years following the Certificate's validity period.

4.10.2 Service Availability

Certificate status services are available 24x7. QuoVadis operates and maintains its CRL and OCSP capability with resources sufficient to provide a response time of ten seconds or less under normal operating conditions.

4.10.3 Optional Features

No stipulation.

4.11 END OF SUBSCRIPTION

No stipulation.

4.12 KEY ESCROW AND RECOVERY

Within PKIoverheid, QuoVadis does not support key escrow.

4.13 SUSPENSION OF CERTIFICATES

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

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 Trusted Roles

Personnel acting in trusted roles include CA, TSA, and RA system administration personnel, and personnel involved with identity vetting and the issuance and revocation of Certificates. The functions and duties performed by persons in trusted roles are distributed so that one person alone cannot circumvent security measures or subvert the security and trustworthiness of the PKI or TSA operations. Trusted roles are appointed by senior management. A list of personnel appointed to trusted roles is maintained and reviewed annually.

-

5.2.1.1 CA Administrators

The CA Administrator installs and configures the CA software, including key generation, key backup, and key management. The CA Administrator performs and securely stores regular system backups of the CA system. Administrators do not issue Certificates to Subscribers.

5.2.1.2 Registration Officers – CMS, RA, Validation and Vetting Personnel

The Registration Officer role is responsible for issuing and revoking Certificates, including enrolment, identity verification, and compliance with required issuance and revocation steps such as managing the certificate request queue and completing certificate approval checklists as identity vetting tasks are successfully completed.

5.2.1.3 System Administrators/System Engineers (Operator)

The System Administrator / System Engineer installs and configures system hardware, including servers, routers, firewalls, and network configurations. The System Administrator/System Engineer also keeps CA, CMS and RA systems updated with software patches and other maintenance needed for system stability and recoverability.

5.2.1.4 Internal Auditor

Internal Auditors are responsible for reviewing, maintaining, and archiving audit logs and performing or overseeing internal compliance audits to determine if DigiCert, an Issuer CA, or RA is operating in accordance with this CPS or an RA's Registration Practices Statement.

5.2.1.5 RA Administrators

RA Administrators install, configure and manage the RA software, including the assignment of Issuing CAs and certificate profiles to customer accounts.

5.2.1.6 Security Officer

The Security Officer is responsible for administering and implementing security practices..

5.2.2 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.

5.2.3 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.

5.2.4 Roles that require a separation of duties

Trusted roles requiring a separation of duties include those performing:

- authorisation functions such as the verification of information in Certificate Requests and certain approvals of Certificate applications and revocation requests,
- backups, recording, and record keeping functions;
- audit, review, oversight, or reconciliation functions; and
- duties related to CA/TSA key management or CA/TSA administration.

To accomplish this separation of duties, QuoVadis specifically designates individuals to the trusted roles defined in Section 5.2.1 above. QuoVadis appoints individuals to only one of the Registration Officer, Administrator, Operator, or Internal Auditor roles. Individuals designated as Registration Officer or Administrator may perform Operator duties, but an Internal Auditor may not assume any other role.

5.3 PERSONNEL CONTROLS

5.3.1 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.

5.3.2 Background Check Procedures

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.
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.

5.3.3 Training Requirements

QuoVadis provides relevant skills training to all employees involved in QuoVadis' PKI and TSA operations. The training relates to the person's job functions and covers:

1. basic PKI knowledge,
2. software versions used by QuoVadis,
3. authentication and verification policies and procedures,
4. QuoVadis security principles and mechanisms,
5. disaster recovery and business continuity procedures,
6. common threats to the validation process, including phishing and other social engineering tactics, and
7. CA/Browser Forum Guidelines and other applicable industry and government guidelines.

QuoVadis maintains records of who received training and what level of training was completed. Registration Officers must have the minimum skills necessary to satisfactorily perform validation duties before being granted validation privileges. All Registration Officers are required to pass an internal examination on the EV Guidelines and the Baseline Requirements prior to validating and approving the issuance of Certificates. Where competence is demonstrated in lieu of training, QuoVadis maintains supporting documentation.

5.3.4 Retraining Frequency and Requirements

Employees must maintain skill levels that are consistent with industry-relevant training and performance programs in order to continue acting in trusted roles. QuoVadis makes all employees acting in trusted roles aware of any changes to QuoVadis' operations. If QuoVadis' operations change, QuoVadis will provide documented training, in accordance with an executed training plan, to all employees acting in trusted roles.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorised Actions

QuoVadis DigiCert employees and agents failing to comply with this CPS, whether through negligence or malicious intent, are subject to administrative or disciplinary actions, including termination of employment or agency and criminal sanctions. If a person in a trusted role is cited by management for unauthorized or inappropriate actions, the person will be immediately removed from the trusted role pending management review. After management has reviewed and discussed the incident with the employee involved, management may reassign that employee to a non-trusted role or dismiss the individual from employment as appropriate.

5.3.7 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.

5.3.8 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.

5.3.9 Independent Contractor Requirements

Independent contractors who are assigned to perform trusted roles are subject to the duties and requirements specified for such roles in this Section 5.3 and are subject to sanctions stated above in Section 5.3.6

5.4 AUDIT 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 Period for Audit Log

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 backed up daily. The logfiles are stored in such a way that the integrity and accessibility of the data is guaranteed.

5.4.3 Protection of Audit Log

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 Protection of Audit Log

The relevant audit data collected is regularly analysed for any attempts to violate the integrity of any element of the QuoVadis PKI. Only certain QuoVadis Trusted Roles and auditors may view audit logs in whole. QuoVadis decides whether particular audit records need to be viewed by others in specific instances and makes those records available. Consolidated logs are protected from modification and destruction. All audit logs are protected in an encrypted format via a Key and/or Certificate generated especially for the purpose of protecting the logs.

5.4.5 Audit Log Backup Procedures

Each Issuing CA performs an onsite backup of the audit log daily. The backup process includes weekly physical removal of the audit log copy from the Issuing CA's premises and storage at a secure, off-site location.

5.4.6 Audit Collection System

The security audit process of each Issuing CA runs independently of the Issuing CA software. Security audit processes are invoked at system start up and cease only at system shutdown.

5.4.7 Notification To Event-Causing Subject

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

5.4.8 Vulnerability Assessments

QuoVadis performs annual risk assessments that identify and assess reasonably foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any certificate data or certificate issuance process. QuoVadis also routinely assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that QuoVadis has in place to control such risks. QuoVadis' Internal Auditors review the security audit data checks for continuity. QuoVadis' audit log monitoring tools alert the appropriate personnel of any events, such as repeated failed actions, requests for privileged information, attempted access of system files, and unauthenticated responses.

Penetration tests are also 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 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.

5.5 RECORDS ARCHIVAL

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.

5.5.2 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.

5.5.3 Protection of the archive

Archive records are stored at a secure location and are maintained in a manner that prevents unauthorized modification, substitution, or destruction. Archives are not released except as allowed by the PMA or as required by law. QuoVadis maintains any software application required to process the archive data until the data is either destroyed or transferred to a newer medium.

If QuoVadis needs to transfer any media to a different archive site or equipment, DigiCert will maintain both archived locations and/or pieces of equipment until the transfer are complete. All transfers to new archives will occur in a secure manner.

5.5.4 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.

5.5.5 Requirements for Time-Stamping of Records

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.

5.5.6 Archiving System

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

5.5.7 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 Incident and Compromise Handling Procedures

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 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. In the event of any termination QuoVadis will take steps to inform the Supervisory Body Agentschap Telecom (AT), as well as other stakeholders, such as Government and Certification bodies where appropriate.

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, Subscribers, 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 Subscribers whose Certificates have been withdrawn. This requires that Subscriber and the Subscribers 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 CONTROLS

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 Key Pair Generation

6.1.1.1 Root CA Key pair generation

QuoVadis does not perform the key pair generation for PKIoverheid Root Certificates, and certain PKIoverheid intermediate Certificates.

6.1.1.2 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.

6.1.1.3 Generation of key pairs of the Subscribers

The keys of Subscribers (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.

6.1.1.4 Algorithm of key pairs of the Subscribers

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

6.1.1.5 Key pairs managed on behalf of the Subscribers

In the case of Qualified Certificates, where QuoVadis manages the keys on behalf of the Subscriber, 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 Subscribers' 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 sole control.

6.1.2 Delivery of the Private Key to the Subscriber

Subscribes can choose to have their Key Pair generated by QuoVadis, or to generate it themselves.

Subscribers must generate their Key Pair in a manner that is appropriate for the certificate type. Subscribers for TLS/SSL Certificates are solely responsible for the generation of the Private Keys used in their Certificate Requests. QuoVadis does not provide TLS/SSL key generation, escrow, recovery or backup facilities.

For Qualified Certificates QuoVadis generates the Private Keys on behalf of the Subscriber, they are provided in a secure manner via the QuoVadis CMS.

For some EU Qualified Certificates, QuoVadis may generate and manages Private Keys on behalf of the Subscriber. Where the policy requires the use of a QSCD then the signatures shall only be created by the QSCD.

6.1.3 Delivery of a public key

For all other Certificates e.g. EV, SSL, Subscribers generate Key Pairs and deliver Public Keys to the Issuing CA in a secure and trustworthy manner, such as submitting a Certificate Signing Request (CSR) message to a QuoVadis CMS.

6.1.4 CA Public Key distribution to Relying 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 Sizes

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 Public Key Parameters Generations and Quality Checking

QuoVadis uses cryptographic modules that conform to FIPS 186-2 and provides random number generation and on-board generation of Public Keys and a wide range of ECC curves. The value of this public exponent equates to an odd number equal to three or more.

6.1.7 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 AND CRYPTOGRAPHIC CONTROLS

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 Subscriber 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.

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 Subscribers 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 Subscribers under this CPS.

6.2.6 Private Key Storage 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 Module Rating

For relevant Qualified Certificates, in accordance with the eIDAS Regulation, the Subscriber 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 Subscriber, 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.

6.3 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 Subscriber. 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 Subscriber. 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

6.3.2 Certificate operational periods and key pair usage periods

Private keys that are used by a Subscriber 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

6.4.1 Activation Data Generation and Installation

QuoVadis activates the cryptographic module containing its CA Private Keys according to the specifications of the hardware manufacturer, meeting the requirements of FIPS 140-2 Level-3 and/or Common Criteria EAL 4. The cryptographic hardware is held under two-person control. QuoVadis personnel and Subscribers are instructed to use strong passwords and to protect PINs and passwords that meet the requirements specified by the CA/B Forum's Network Security Requirements.

6.4.2 Activation Data Protection

If activation data must be transmitted, it shall be via a channel of appropriate protection, and distinct in time and place from the associated Cryptographic Module. PINs may be supplied to Users in two portions using different delivery methods, for example by e-mail and by standard post, to provide increased security against third-party interception of the PIN. Activation Data should be memorised, not written down. Activation Data

must never be shared. Activation data must not consist solely of information that could be easily guessed, e.g., a Subscriber's personal information.

6.4.3 Other Aspects of Activation Data

Where a PIN is used, the User is required to enter the PIN and identification details such as their Distinguished Name before they are able to access and install their Keys and Certificates.

6.5 COMPUTER SECURITY CONTROLS

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

QuoVadis secures its CA systems and authenticates and protects communications between its systems and trusted roles. QuoVadis' CA servers and support-and-vetting workstations run on trustworthy systems that are configured and hardened using industry best practices. All CA systems are scanned for malicious code and protected against spyware and viruses.

RAs must ensure that the systems maintaining RA software and data files are trustworthy systems secure from unauthorized access, which can be demonstrated by compliance with audit criteria applicable under Section 5.4.1.

QuoVadis' CA systems are configured to:

I. authenticate the identity of users before permitting access to the system or applications;
II. manage the privileges of users and limit users to their assigned roles;
III. generate and archive audit records for all transactions;
IV. enforce domain integrity boundaries for security critical processes; and
V. support recovery from key or system failure.

All Certificate Status Servers:

VI. authenticate the identity of users before permitting access to the system or applications;
VII. manage privileges to limit users to their assigned roles;
VIII. enforce domain integrity boundaries for security critical processes; and
IX. support recovery from key or system failure.

QuoVadis enforces multi-factor authentication on any CMS account capable of directly causing Certificate issuance.

6.6 LIFECYCLE TECHNICAL CONTROLS

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 Security Management Controls

QuoVadis has mechanisms in place to control and continuously monitor the security-related configurations of its CA systems. When loading software onto a CA system, QuoVadis verifies that the software is the correct version and is supplied by the vendor free of any modifications.

6.6.3 Life cycle Security Controls

No stipulation.

6.7 NETWORK SECURITY CONTROLS

QuoVadis CA and RA functions are performed using networks secured in accordance to prevent unauthorised access, tampering, and denial-of-service attacks. Communications of sensitive information shall be protected using point-to-point encryption for confidentiality and digital signatures for non-repudiation and authentication.

QuoVadis documents and controls the configuration of its systems, including any upgrades or modifications made. Root Keys are kept offline and brought online only when necessary to sign Issuing CA Certificates, OCSP Responder Certificates, or periodic CRLs. Firewalls and boundary control devices are configured to allow access only by the addresses, ports, protocols and commands required for the trustworthy provision of PKI services by such systems.

The QuoVadis security policy is to block all ports and protocols and open only ports necessary to enable CA functions. All CA equipment is configured with a minimum number of services and all unused network ports and services are disabled.

6.8 TIME STAMPING

QuoVadis does not provide time stamps within the PKIoverheid framework.

7 CERTIFICATE PROFILES

7.1 CERTIFICATE PROFILE

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.

7.1.1 Version Number

Certificates MUST be of type X.509 v3.

7.1.1.1 Serial Number

The serial number is no longer than 160 bits (20 octets)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

7.1.2 Certificate Extensions

7.1.2.1 Root CA Certificates

Defined and managed by PKIoverheid.

7.1.2.2 Subordinate CA Certificates

Defined and managed by PKIoverheid.

7.1.2.3 Subscriber Certificates

All subscriber Certificates are configured to meet the applicable requirements, including eIDAS Reg No 910/2014 (EU), Baseline Requirements, ETSI EN 319 411-1, ETSI EN 319 411-2 and Programma van Eisen (Logius, PKIoveheid).

7.1.2.4 All Certificates

All other fields and extensions are set in accordance with RFC 5280.

7.1.3 Algorithm Object Identifiers

QuoVadis Certificates use SHA-2 algorithm.

7.1.4 Name Forms

Each Certificate includes a unique serial number that is never reused. SSL/TLS Server Certificates cannot contain metadata such as '.', '-' and ' ' characters or and/or any other indication that the value/field is absent, incomplete, or not applicable. Certificates are populated with the Issuer Name and Subject Distinguished Name required under Section 3.1.1.

7.1.5 Name Constraints

All Certificates are configured to meet the applicable requirements, including eIDAS Reg No 910/2014 (EU), Baseline Requirements, ETSI EN 319 411-1, ETSI EN 319 411-2 and Programma van Eisen (Logius, PKIoveheid).

7.1.6 Certificate Policy Object Identifier

All Certificate Policy object identifiers are described in Section 1.2.

7.2 CRL PROFILE

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

7.3 OCSP PROFILE

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

7.4 CERTIFICATES FOR PKIOVERHEID

7.4.1 QuoVadis PKIoverheid Organisatie Persoon CA - G3

7.4.1.1 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

7.4.1.2 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

7.4.1.3 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

7.5 QUOVADIS CSP - PKIOVERHEID CA - G2

7.5.1.1 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

7.5.1.2 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 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

7.5.1.3 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

7.5.1.4 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

7.5.1.5 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

7.5.1.6 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	Fixed

	Key Encipherment	
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

7.5.2 QuoVadis PKIoverheid Organisatie Services CA - G3

7.5.2.1 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). 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)	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	

7.5.2.2 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

7.5.2.3 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 Policy Identifier=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.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	Fixed

	{ 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	

7.5.3 QuoVadis PKIoverheid Burger CA - G3

7.5.3.1 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

7.5.3.2 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	Required

	E-Mail Protection	
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

7.5.3.3 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:	Required

	<unique identifier>@2.16.528.1.1003.1.3.3.3.1	
CRLDistributionPoints	http://crl.quovadisglobal.com/pkioburgerg3.crl	Fixed
AuthorityInfoAccess	http://ocsp.quovadisglobal.com http://trust.quovadisglobal.com/pkioburgerg3.crt	Fixed

7.5.4 QuoVadis PKIoverheid Organisatie Server CA – G3

7.5.4.1 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

7.5.5 QuoVadis PKIoverheid EV CA

7.5.5.1 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

7.5.5.2 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	Required

	Entity", or "Non-Commercial Entity"	
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 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	Fixed

7.5.6 QuoVadis PKIOverheid Private services CA - G1

7.5.6.1 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

7.5.6.2 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

7.5.6.3 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 Server Authentication	Required
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

7.5.7 QuoVadis PKIOverheid Private Personen CA - G1

7.5.7.1 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

7.5.7.2 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

7.5.7.3 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

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

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 CertificateSubcriber 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, CertificateSubcribers, 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 CertificateSubcribers 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.
CertificateSubcribers 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 CertificateSubcriber.
QuoVadis guarantees to its Subscribers and CertificateSubcribers 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 REPRESENTATIONS AND WARRANTIES

9.6.1 CA Representations and Warranties

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 CertificateSubcribers 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: “Subscriber”;
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: “Subscriber”;
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: “Subscriber”;
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 Subscribers

Subscribers guarantee that:

- the Private Key is protected and there has never been access for another person
- all representations made by the Subscriber 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 Subscriber 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, Subscriber 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 CertificateSubcriber 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 *TERMINATION*

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

9.10.1 Effect of termination and survival

The provisions within this CPS survive the termination or revocation of a Subscriber 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.

9.10.2 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).

9.11 CHANGES

9.11.1 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.

9.11.2 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 CertificateSubcribers, QuoVadis will make the change known to its registered Subscribers and/or CertificateSubcribers 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.
In the event of any change to this CPS then PKIoverheid (Logius) will be notified of such change.

9.12 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.

9.13 APPLICABLE LEGISLATION

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

9.14 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.

9.15 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 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