digicert®

Certification Practice Statement for PKIoverheid Certificates

Version 2.0, 15 September 2024

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 2020	1.2	CAA Records Update and minor formatting changes.
QuoVadis PMA	6 August 2020	1.3	Improved alignment with RFC3647, updated Certificate profiles, and editorial changes.
QuoVadis PMA	25 August 2020	1.4	Revisions including addition of PKIo Domain Server 2020, removal notices for PKIo EV SSL, change to OU for TLS, clarification of revocation services, alignment with PvE.
QuoVadis PMA	30 September 2020	1.5	Updates to comply with CA/B Forum Ballots SC30, SC31, SC33; edits to Relying Party obligations, reporting for Key Compromise.
QuoVadis PMA	22 March 2021	1.6	Minor updates for clarity. Updates to Issuing CAs.
QuoVadis PMA	28 June 2021	1.7	Clarification on Terms and Conditions, minor editorial changes, and updates to Certificate types.
QuoVadis PMA	3 August 2021	1.8	Update to OCSP Response, note added for the 2022 expiry of public trust TLS.
QuoVadis PMA	24 September 2021	1.9	Minor clarification of revocation service times, TLS validity.
QuoVadis PMA	6 December 2021	1.10	Update for ETSI TS 119 461, Remote Identity Verification (RIV).
QuoVadis PMA	20 December 2021	1.11	Clarification to Section 3.2.3 and minor editorial changes.
QuoVadis PMA	16 March 2022	1.12	Updates for Organisation Person 2022, Organisation Services 2022.
QuoVadis PMA	5 July 2022	1.13	Minor editorial corrections, including CA and profile names, and updated revocation contacts. Discontinuation of OU. Clarification of Certificate Policy OIDs in Appendix A.
QuoVadis PMA	23 September 2022	1.14	Correction to Burger 2021 Certificate Profile.

Author	Date	Version	Comment
QuoVadis PMA	9 June 2023	1.15	Updated domain methods in Section 3.2.3. Clarification in Section 4.9.2 on who may request revocation. Updated CRL information in Section 4.9.7. Updated reference for Section 4.9.9 ArchiveCutoff extension. Discontinuation of Domain CA 2020. Minor corrections and updates.
QuoVadis PMA	22 November 2023	1.16	Updates for new Issuing CAs and realigning description of Certificate types with PKIo hierarchy, updating references for S/MIME BR including new 3.2.2.5, 9.2.1 insurance, minor editorial changes, updated Certificate profiles in Appendix A.
QuoVadis PMA	XX March 2024	1.17	Update PoR references, revocation updates in 1.5.2.1 and 3.4, renewal 4.6.1, assessment 8.1, minor editorial updates.
DCPA	15 September 2024	2.00	Change Quovadis to DigiCert Europe, update revocation timeline to align with PKIo changes, include S/MIME CAA requirements, weak key and firewall logging requirements.

Previous Documents Published in Dutch

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

digicert®

Contents

1. INTRODUCTION 12
1.1. OVERVIEW 12
1.1.1. Intended Audience 12
1.2. DOCUMENT NAME AND IDENTIFICATION 13
1.3. PKI PARTICIPANTS 15
1.3.1. Certification Authorities 16
1.3.2. Registration Authorities 16
1.3.3. Subscribers 16
1.3.4. Relying Parties 17
1.3.5. Other Participants 17
1.4. CERTIFICATE USAGE 17
1.4.1. Appropriate Certificate Uses 17
1.4.2. Prohibited Certificate Usage 18
1.5. POLICY ADMINISTRATION 19
1.5.1. Organisation Administering the Document 19
1.5.2. Contact Person 19
1.5.3. Person Determining The CPS Suitability 19
1.5.4. CPS Approval Procedures 20
1.6. DEFINITIONS AND ACRONYMS 20
1.6.1. Definitions 20
1.6.2. Acronyms 21
1.6.3. Conventions 23
2. PUBLICATION AND REPOSITORY RESPONSIBILITIES 23
2.1. REPOSITORIES 23
2.2. PUBLICATION OF CERTIFICATE INFORMATION 23
2.3. TIME OR FREQUENCY OF PUBLICATION 23
2.4. ACCESS CONTROLS ON REPOSITORIES 24
3. IDENTIFICATION AND AUTHENTICATION 24
3.1. NAMING 24
3.1.1. Types Of Names 24
3.1.2. Need For Names To Be Meaningful 26
3.1.3. Pseudonymous Subscribers 26
3.1.4. Rules For Interpreting Various Name Forms 26
3.1.5. Uniqueness Of Names 26

3.1.6. Recognition, Authentication, And Role Of Trademarks 26
3.2. INITIAL IDENTITY VALIDATION 26
3.2.1. Method To Prove Possession Of Private Key 28
3.2.2. Authentication Of Organisation Identity 28
3.2.3. Authentication Of Individual Identity 32
3.2.4. Non-Verified Subscriber Information 34
3.2.5. Validation Of Authority 35
3.2.6. Criteria for Interoperation 35
3.3. IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS 35
3.3.1. Identification And Authentication For Routine Re-Key 35
3.3.2. Identification and Authentication For Re-Key After Revocation 35
3.4. IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUESTS 36
4. CERTIFICATE LIFE-CYCLE OPERATION REQUIREMENTS 36
4.1. CERTIFICATE APPLICATION 36
4.1.1. Who Can Submit A Certificate Application 36
4.1.2. Enrolment Process And Responsibilities 37
4.2. CERTIFICATE APPLICATION PROCESSING 37
4.2.1. Performing Identification And Authentication Functions 37
4.2.2. Approval Or Rejection Of Certificate Applications 37
4.2.3. Time To Process Certificate Applications 37
4.2.4. CAA Checking 38
4.3. CERTIFICATE ISSUANCE 39
4.3.1. CA Actions During Certificate Issuance 39
4.3.2. Notification To Subscriber By The CA Of Issuance Of Certificate 39
4.4. CERTIFICATE ACCEPTANCE 39
4.4.1. Conduct Constituting Certificate Acceptance 39
4.4.2. Publication Of The Certificate By The CA 39
4.4.3. Notification Of Certificate Issuance By The CA To Other Entities 39
4.5. KEY PAIR AND CERTIFICATE USAGE 40
4.5.1. Subscriber Private Key And Certificate Usage 40
4.5.2. Relying Party Public Key And Certificate Usage 40
4.6. CERTIFICATE RENEWAL 41
4.6.1. Circumstance For Certificate Renewal 41
4.6.2. Who May Request Renewal 41
4.6.3. Processing Certificate Renewal Requests 41

4.6.4. Notification of New Certificate Issuance To Subscriber 41
4.6.5. Conduct Constituting Acceptance Of A Renewal Certificate 41
4.6.6. Publication of the Renewal Certificate By The CA 41
4.6.7. Notification Of Certificate Issuance By The CA To Other Entities 41
4.7. CERTIFICATE RE-KEY 41
4.7.1. Circumstance for Certificate Re-Key 41
4.7.2. Who May Request Re-Key 42
4.7.3. Processing Certificate Re-Key Request 42
4.7.4. Notification of Certificate Re-Key To Subscriber 42
4.7.5. Conduct Constituting Acceptance Of A Re-Key Certificate 42
4.7.6. Publication of The Re-Key Certificate By The CA 42
4.7.7. Notification of Certificate Re-Key By The CA To Other Entities 42
4.8. CERTIFICATE MODIFICATION 42
4.8.1. Circumstances For Certificate Modification 42
4.8.2. Who May Request Certificate Modification 42
4.8.3. Processing Certificate Modification Requests 42
4.8.4. Notification Of Certificate Modification To Subscriber 42
4.8.5. Conduct Constituting Acceptance Of A Modified Certificate 42
4.8.6. Publication Of The Modified Certificate By The CA 42
4.8.7. Notification Of Certificate Modification By The CA To Other Entities 42
4.9. CERTIFICATE REVOCATION AND SUSPENSION 43
4.9.1. Circumstances For Revocation 43
4.9.2. Who Can Request Revocation 44
4.9.3. Procedure For Revocation Request 45
4.9.4. Revocation Request Grace Period 45
4.9.5. Time Within Which The CA Must Process The Revocation Request 45
4.9.6. Revocation Checking Requirement for Relying Parties 45
4.9.7. CRL Issuance Frequency 46
4.9.9. On-Line Revocation/Status Checking Availability 46
4.9.10. OCSP Checking Requirement 46
4.9.11. Other Forms Of Revocation Advertisements Available 47
4.9.12. Special Requirements for Key Compromise 47
4.9.13. Circumstances For Suspension 47
4.9.14. Who Can Request Suspension 47
4.9.15. Procedure For Suspension Request 47

4.9.16. Limits On Suspension Period 48
4.10. CERTIFICATE STATUS SERVICES 48
4.10.1. Operational Characteristics 48
4.10.2. Service Availability 48
4.10.3. Optional Features 48
4.11. END OF SUBSCRIPTION 48
4.12. KEY ESCROW AND RECOVERY 48
4.12.1. Key Archival Escrow And Recovery Policy And Practices 48
4.12.2. Session Key Encapsulation And Recovery Policy And Practices 48
5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS 48
5.1. PHYSICAL CONTROLS 49
5.1.1. Site Location and Construction 49
5.1.2. Physical Access 49
5.1.3. Power And Air-Conditioning 49
5.1.4. Water Exposures 49
5.1.5. Fire Prevention And Protection 49
5.1.6. Media Storage 49
5.1.7. Waste Disposal 50
5.1.8. Off-Site Backup 50
5.2. PROCEDURAL CONTROLS 50
5.2.1. Trusted Roles 50
5.2.2. Number Of Persons Required Per Task 51
5.2.3. Identification And Authentication For Each Role 51
5.2.4. Roles Requiring Separation Of Duties 51
5.3. PERSONNEL CONTROLS 51
5.3.1. Qualifications, Experience, And Clearance Requirements 51
5.3.2. Background Check Procedures 52
5.3.3. Training Requirements 52
5.3.4. Retraining Frequency And Requirements 53
5.3.5. Job Rotation Frequency And Sequence 53
5.3.6. Sanctions For Unauthorised Actions 53
5.3.7. Independent Contractor Requirements 53
5.3.8. Documentation Supplied To Personnel 53
5.4. AUDIT LOGGING PROCEDURES 53
5.4.1. Types Of Events Recorded 53

5.4.2. Frequency Of Processing Log 54
5.4.3. Retention Period For Audit Log 55
5.4.4. Protection Of Audit Log 55
5.4.5. Audit Log Backup Procedures 55
5.4.6. Audit Collection System 55
5.4.7. Notification To Event-Causing Subject 55
5.4.8. Vulnerability Assessment 55
5.5. RECORDS ARCHIVAL 56
5.5.1. Types Of Records Archived 56
5.5.2. Retention Period For Archive 56
5.5.4. Archive Backup Procedures 57
5.5.5. Requirements For Time-Stamping Of Records 57
5.5.7. Procedures To Obtain And Verify Archive Information 57
5.6. KEY CHANGEOVER 57
5.7. COMPROMISE AND DISASTER RECOVERY 57
5.7.1. Incident and Compromise Handling Procedures 57
5.7.2. Computing Resources, Software, and/or Data Are Corrupted 58
5.7.3. Entity Private Key Compromise Procedures 58
5.7.4. Business Continuity Capabilities after a Disaster 58
5.8. CA AND/OR RA TERMINATION 58
6. TECHNICAL SECURITY CONTROLS 59
6.1. KEY PAIR GENERATION AND INSTALLATION 59
6.1.1. Key Pair Generation 59
6.1.1.1. Root CA Key pair generation 59
6.1.2. Private Key Delivery To Subscriber 60
6.1.3. Public Key Delivery To Certificate Issuer 61
6.1.4. CA Public Key To Relying Parties 61
6.1.5. Key Sizes 61
6.1.6. Public Key Parameters Generation And Quality Checking 61
6.1.7. Key Usage Purposes (As Per X.509 V3 Key Usage Field) 61
6.2. PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS 61
6.2.1. Cryptographic Module Standards And Controls 61
6.2.2. Private Key (N of M) Multi-Person Control 62
6.2.3. Private Key Escrow 62
6.2.4. Private Key Backup 62

6.2.5. Private Key Archive 62
6.2.6. Private Key Transfer Into Or From A Cryptographic Module 62
6.2.7. Private Key Storage On Cryptographic Module 62
6.2.8. Method Of Activating Private Key 63
6.2.9. Method Of Deactivating Private Key 63
6.2.10. Method Of Destroying Private Key 63
6.2.11. Cryptographic Module Rating 63
6.3. OTHER ASPECTS OF KEY PAIR MANAGEMENT 63
6.3.1. Public Key Archival 63
6.3.2. Certificate Operational Periods And Key Pair Usage Periods 63
6.4. ACTIVATION DATA 64
6.4.1. Activation Data Generation And Installation 64
6.4.2. Activation Data Protection 64
6.4.3. Other Aspects Of Activation Data 64
6.5. COMPUTER SECURITY CONTROLS 64
6.5.1. Specific Computer Security Technical Requirements 65
6.5.2. Computer Security Rating 65
6.6. LIFE CYCLE TECHNICAL CONTROLS 65
6.6.1. System Development Controls 65
6.6.2. Security Management Controls 66
6.6.3. Life Cycle Security Controls 66
6.7. NETWORK SECURITY CONTROLS 66
6.8. TIME-STAMPING 66
7. CERTIFICATE, CRL, AND OCSP PROFILES 67
7.1. CERTIFICATE PROFILE 67
7.1.1. Version Numbers 67
7.1.2. Serial Number 67
7.1.3. Certificate Extensions 67
7.2. CRL PROFILE 68
7.2.1. Version Number 70
7.2.2. CRL And CRL Entry Extensions 71
7.3. ONLINE CERTIFICATE STATUS PROTOCOL PROFILE 71
7.3.1. OCSP Version Numbers 71
7.3.2. OCSP Extensions 71
8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS 72

8.1. FREQUENCY, CIRCUMSTANCE AND STANDARDS OF ASSESSMENT 72
8.2. IDENTITY AND QUALIFICATIONS OF ASSESSOR 74
8.3. ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY 74
8.4. TOPICS COVERED BY ASSESSMENT 74
8.5. ACTIONS TAKEN AS A RESULT OF DEFICIENCY 74
8.6. PUBLICATION OF AUDIT RESULTS 74
8.7. SELF AUDITS 74
9. OTHER BUSINESS AND LEGAL MATTERS 74
9.1. FEES 74
9.1.1. Certificate Issuance Or Renewal Fees 74
9.1.2. Certificate Access Fees 75
9.1.3. Revocation Or Status Information Access Fees 75
9.1.4. Fees For Other Services 75
9.1.5. Refund Policy 75
9.2. FINANCIAL RESPONSIBILITIES 75
9.2.1. Insurance Coverage 75
9.2.2. Other Assets 75
9.2.3. Insurance Or Warranty Coverage For End-Entities 75
9.3. CONFIDENTIALITY OF BUSINESS-SENSITIVE DATA 76
9.3.1. Scope Of Confidential Information 76
9.3.2. Information Not Within The Scope Of Confidential Information 76
9.3.3. Responsibility To Protect Private Information 76
9.4. PRIVACY OF PERSONAL INFORMATION 76
9.4.1. Privacy Plan 76
9.4.2. Information Treated As Private 76
9.4.3. Information Deemed Not Private 76
9.4.4. Responsibility To Protect Private Information 77
9.4.5. Notice And Consent To Use Private Information 77
9.4.6. Disclosure Pursuant To Judicial Or Administrative Process 77
9.5. INTELLECTUAL PROPERTY RIGHTS 77
9.5.1. Property Rights in Certificates and Revocation Information 77
9.5.2. Property Rights in the CPS 77
9.5.3. Property Rights in Names 77
9.5.4. Property Rights in Keys and Key Material 78
9.5.5. Violation of Property Rights 78

9.6. REPRESENTATIONS AND WARRANTIES 78
9.6.1. Certification Authority Representations 78
9.6.2. RA Representations and Warranties 79
9.6.3. Subscriber Representations And Warranties 79
9.6.4. Relying Parties Representations And Warranties 80
9.6.5. Representations And Warranties Of Other Participants 82
9.7. DISCLAIMERS OF WARRANTIES 82
9.8. LIABILITY AND LIMITATIONS OF LIABILITY 82
9.9. INDEMNITIES 83
9.9.1. Indemnification By DigiCert Europe 83
9.9.2. Indemnification By Subscribers 83
9.9.3. Indemnification By Relying Parties 83
9.10. TERM AND TERMINATION 83
9.10.1. Term 83
9.10.2. Termination 83
9.10.3. Effect Of Termination And Survival 83
9.11. INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS 84
9.12. AMENDMENTS 84
9.12.1. Procedure For Amendment 84
9.12.2. Notification Mechanism And Period 84
9.12.3. Circumstances Under Which OID Must Be Changed 84
9.13. DISPUTE RESOLUTION PROVISIONS 84
9.14. GOVERNING LAW 85
9.15. COMPLIANCE WITH APPLICABLE LAW 85
9.16. MISCELLANEOUS PROVISIONS 85
9.16.1. Entire Agreement 85
9.16.2. Assignment 85
9.16.3. Severability 86
9.16.4. Enforcement (Waiver Of Rights) 86
9.17. OTHER PROVISIONS 86
APPENDIX A – CERTIFICATE PROFILES FOR PKIOVERHEID 86

1. INTRODUCTION

This document is the DigiCert Europe Certification Practice Statement (CPS) for PKIoverheid Certificates. DigiCert Europe Netherlands B.V., previously known as Quovadis Trustlink Netherlands B.V., a subsidiary of DigiCert Inc., is a Company registered in the Netherlands, trading under the names "DigiCert + QuoVadis" and "DigiCert Europe". DigiCert Europe B.V. is certified as a Trust Service Provider ("TSP") for the issuance of Certificates under the Staat der Nederlanden PKIoverheid Roots.

1.1. OVERVIEW

This CPS describes the practices and procedures that are employed in the life-cycle management, including the generation, issuance, and revocation, of PKIoverheid Certificates.

The Dutch Government provides the Policy Authority (PKIo PA) for PKIoverheid Certificates and impose strict requirements on TSPs to issue PKIoverheid Certificates under their hierarchies. The requirements are known as the "Programma van Eisen" (PvE) or "Program of Requirements". These are maintained and managed by Logius. See more at https://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. To preserve the outline specified by RFC 3647, section headings that do not apply are accompanied with the statement "Not applicable" or "No stipulation".

In addition the PKI Disclosure Statement for PKIoverheid which summarises this document is available in the DigiCert Europe Repository.

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 (QCP-n-qscd).

Where relevant, DigiCert Europe conforms to the current version of the Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates and the Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates published at https://www.cabforum.org/. In the event of any inconsistency between this document and the normative provisions of those Applicable Requirements, those Applicable Requirements take precedence over this document.

DigiCert Europe is evaluated against multiple requirements, including PKIoverheid Program of Requirements https://www.quovadisglobal.com/accreditations/ for details.

Trust service components for EU Qualified Certificates shall only be performed by DigiCert Europe-approved entities that have the relevant certifications. See also Section 1.3.2. When trust service components are provided by another party DigiCert Europe maintains overall responsibility and undertakes procedures to ensure that security and functionality of the trust service meet the appropriate requirements.

DigiCert Europe is also assessed against the Root distribution policies of Application Software Suppliers including Apple, Chrome, Mozilla, and Microsoft.

1.1.1. Intended Audience

- Certificate Manager;
- Subscriber;
- Organisations of Registered Professionals;

- Authorities/regulators who are involved in the regulation of PKIo activities (e.g., Logius);
- Application Software Suppliers; and
- Relying Parties or other third parties submitting Certificate Problem Reports informing DigiCert Europe of reasonable cause to revoke the Certificate

1.2. DOCUMENT NAME AND IDENTIFICATION

This document is the DigiCert Europe Netherlands B.V. "Certificate Practice Statement for PKIoverheid Certificates". DigiCert Europe issues Subscriber Certificates in the following PKIoverheid hierarchies:

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	Organisatie Persoon Authentication G3	2.16.528.1.1003.1.2.5.1
QuoVadis PKIoverheid Organisatie Persoon CA - G3	Organisatie Persoon Non-Repudiation G3	2.16.528.1.1003.1.2.5.2
QuoVadis PKIoverheid Organisatie Persoon CA - G3	Organisatie Persoon Encryption G3	2.16.528.1.1003.1.2.5.3
QuoVadis PKIoverheid Organisatie Persoon CA-2022	Organisatie Persoon Authentication	2.16.528.1.1003.1.2.5.1
QuoVadis PKIoverheid Organisatie Persoon CA-2022	Organisatie Persoon Non-Repudiation	2.16.528.1.1003.1.2.5.2
QuoVadis PKIoverheid Organisatie Persoon CA-2022	Organisatie Persoon Encryption	2.16.528.1.1003.1.2.5.3
DigiCert QuoVadis PKIoverheid Organisatie Persoon CA - 2023	PKIOverheid Personal Organisation Authenticity	2.16.528.1.1003.1.2.5.1
DigiCert QuoVadis PKIoverheid Organisatie Persoon CA - 2023	PKIOverheid Personal Organisation NonRepudiation	2.16.528.1.1003.1.2.5.2
DigiCert QuoVadis PKIoverheid Organisatie Persoon CA - 2023	PKIOverheid Personal Organisation Encryption	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 - 2021	Burger Authentication 2021	2.16.528.1.1003.1.2.3.1

QuoVadis PKIoverheid Burger CA - 2021	Burger Non-Repudiation 2021	2.16.528.1.1003.1.2.3.2
QuoVadis PKIoverheid Burger CA - 2021	Burger Encryption 2021	2.16.528.1.1003.1.2.3.3
DigiCert QuoVadis PKIoverheid Burger CA - 2023	PKIOverheid Personal Citizen Authenticity	2.16.528.1.1003.1.2.3.1
DigiCert QuoVadis PKIoverheid Burger CA - 2023	PKIOverheid Personal Citizen NonRepudiation	2.16.528.1.1003.1.2.3.2
DigiCert QuoVadis PKIoverheid Burger CA - 2023	PKIOverheid Personal Citizen Encryption	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 Services CA G3	Organisatie Services Authentication G3	2.16.528.1.1003.1.2.5.4
QuoVadis PKIoverheid Organisatie Services CA G3	Organisatie Services Non-Repudiation G3	2.16.528.1.1003.1.2.5.7
QuoVadis PKIoverheid Organisatie Services CA G3	Organisatie Services Encryption G3	2.16.528.1.1003.1.2.5.5
QuoVadis PKIoverheid Organisatie Services CA-2022	Organisatie Services Authentication	2.16.528.1.1003.1.2.5.4
QuoVadis PKIoverheid Organisatie Services CA-2022	Organisatie Services Non-Repudiation	2.16.528.1.1003.1.2.5.7
QuoVadis PKIoverheid Organisatie Services CA-2022	Organisatie Services Encryption	2.16.528.1.1003.1.2.5.5
DigiCert QuoVadis PKIoverheid Organisatie Services CA - 2023	PKIOverheid Organisation Service Authenticity	2.16.528.1.1003.1.2.5.4
DigiCert QuoVadis PKIoverheid Organisatie Services CA - 2023	PKIOverheid Organisation Service Seal	2.16.528.1.1003.1.2.5.7
DigiCert QuoVadis PKIoverheid Organisatie Services CA - 2023	PKIOverheid Organisation Service Encryption	2.16.528.1.1003.1.2.5.5

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 Personen Authentication	2.16.528.1.1003.1.2.8.1
QuoVadis PKIoverheid Private Personen CA - G1	Private Personen Non-Repudiation	2.16.528.1.1003.1.2.8.2
QuoVadis PKIoverheid Private Personen CA - G1	Private Personen Encryption	2.16.528.1.1003.1.2.8.3
DigiCert QuoVadis PKIoverheid Private Personen CA - 2023	PKIOverheid Private Personal Authenticity	2.16.528.1.1003.1.2.8.1
DigiCert QuoVadis PKIoverheid Private Personen CA - 2023	PKIOverheid Private Personal NonRepudiation	2.16.528.1.1003.1.2.8.2
DigiCert QuoVadis PKIoverheid Private Personen CA - 2023	PKIOverheid 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
QuoVadis PKIoverheid Private Services CA – G1	Private Services – Server	2.16.528.1.1003.1.2.8.6
DigiCert QuoVadis PKIoverheid Private Services CA - 2023	PKIOverheid Private Services – Authenticity	2.16.528.1.1003.1.2.8.4
DigiCert QuoVadis PKIoverheid Private Services CA - 2023	PKIOverheid Private Services – Encryption	2.16.528.1.1003.1.2.8.5
DigiCert QuoVadis PKIoverheid Private Services CA - 2023	PKIOverheid Private Services – Server	2.16.528.1.1003.1.2.8.6

DigiCert Europe may include other OIDs as appropriate. OIDs in this list and in DigiCert Europe Certificates belong to their respective owners.

1.3. PKI PARTICIPANTS

Participants within the DigiCert Europe PKIo include:

- Certification Authorities (CA) and Registration Authorities (RA);
- Subscribers including Applicants for Certificates prior to certificate issuance;
- Relying Parties; and
- Subcontractors.

1.3.1. Certification Authorities

Trusted Root and Intermediate CAs are owned and operated by the Staat der Nederlanden/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. This national PKI hierarchy consists of Root CAs and multiple domain CAs (sub-CAs) that issue Trust Service Providers (TSP) CA Certificates. TSPs like DigiCert Europe are responsible for issuing Certificates to end-user Subscribers.

1.3.1.1. Issuing CAs and Their Obligations

DigiCert Europe operates CAs that issue Digital Certificates. As the operator of CAs, DigiCert Europe performs functions associated with Public Key operations, including receiving Certificate Requests, issuing, revoking, rekeying, and renewing a digital Certificate, and maintaining, issuing, and publishing CRLs and OCSP responses. Issuing CAs are operated by DigiCert Europe as authorised by the PKIo PA to participate within the PKIoverheid. Issuing CAs are required to act in accordance with their respective Issuing CA Agreements and to be bound by the terms of this CPS.

1.3.2. Registration Authorities

A Registration Authority (RA) is an entity that performs Identification and Authentication of Certificate Applicants, and initiates, passes along revocation requests for end user Subscriber Certificates, and approves applications for renewal or re-keying Certificates on behalf of an Issuing CA. DigiCert Europe and Issuing CAs may act as RAs for Certificates they issue.

RAs may be authorised by DigiCert Europe to delegate the performance of certain functions to third party validators if it meets the requirements of this CPS. DigiCert Europe contractually obligates each RA and delegated third party to abide by the policies and industry standards that are applicable to their responsibilities.

DigiCert Europe is required to establish the identity of applicants by physical presence or using methods which provide equivalent assurance to physical presence. For certain Certificate Requests, DigiCert Europe employs the services of organisations to assist in the performance of identity validation:

- AMP Group: provide physical face-to-face check services via an in-person meeting with one of their representatives.
- IDNow: provide remote identity validation services (as opposed to physical meetings) via the use of an app and specialist software. The IDNow service includes ReadID NFC-reading services provided by Innovalor.

DigiCert Europe conducts ongoing supervision of these activities, and these organisations also hold relevant certifications covering the services provided to DigiCert Europe. DigiCert Europe only allows the use of identity validation methods that have been approved by an appropriate Conformity Assessment Body and/or Supervisory Body.

Validation of Domains and IP Addresses for TLS and of email addresses included in Certificate Subject fields cannot be delegated and may only be only validated by the RA of the Issuing CA.

1.3.3. Subscribers

Subscribers are required to act in accordance with this CPS, Subscriber Agreement, and Terms of Use. Subscribers can be a natural person, a natural person in association with a legal person, or a legal person which is represented by a natural person.

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 TLS Server Certificates are legal persons. The Certificate Manager is an Authorised Representative of an Organisation and is also the holder of the Private Key.

1.3.4. Relying Parties

Relying Parties are entities that act in Reasonable Reliance on a Certificate, Electronic Signature and/or e-Seal issued by DigiCert Europe. A Relying Party may, or may not, also be a Subscriber of the DigiCert Europe PKI. Relying parties must check the appropriate CRL or OCSP response prior to relying on information featured in a Certificate. The location of the Certificate Status service is detailed within the Certificate.

Relying Parties are required to act in accordance with this CPS and the Relying Party Agreement. See also Section 9.6.4.

1.3.5. Other Participants

Other Participants in the DigiCert Europe PKIo are required to act in accordance with this CPS and/or applicable agreements. Other participants include Accreditation Authorities such as Policy Management Authorities, Application Software Suppliers, and applicable Community-of-Interest sponsors. Accreditation Authorities are granted an unlimited right to re-distribute DigiCert Europe CA Certificates and related information in connection with the accreditation.

1.4. CERTIFICATE USAGE

At all times, participants in the DigiCert Europe PKIo are required to utilise Certificates in accordance with this CPS and all applicable laws and regulations.

1.4.1. Appropriate Certificate Uses

Certificates issued pursuant to this DigiCert Europe PKIo CPS may be used for all legal authentication, encryption, access control, and digital signature purposes, as designated by the key usage and extended key usage fields found within the Certificate. However, the sensitivity of the information processed or protected by a Certificate varies greatly, and each Relying Party must evaluate the application environment and associated risks before deciding on whether to use a Certificate issued under this CPS. Reference is made below to the relevant PKIoverheid Program of Requirements (PoR) sections (https://cp.pkioverheid.nl/):

Organisatie Persoon (including Certificates for Registered Professionals)

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

Organisatie 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 (i.e, an e-Seal).

Burger

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

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.

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.

Private Persoon

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

DigiCert Europe PKIo Certificates shall be used only to the extent the use is consistent with applicable law or regulation, the PKIoverheid Program of Requirements, and in particular shall be used only to the extent permitted by applicable export or import laws. CA Certificates subject to the Mozilla Root Store Policy will not be used for any functions except CA functions. In addition, end-user Subscriber Certificates cannot be used as CA Certificates.

DigiCert Europe may periodically re-key Intermediate CAs. Third party applications or platforms that have an Intermediate CA embedded as a root certificate may not operate as designed after the Intermediate CA has been rekeyed.

DigiCert Europe strongly discourages key pinning and does not consider it a sufficient reason to delay revocation. Customers should also take care in not mixing Certificates trusted for the web with non-web PKI. Any Certificates trusted by Application Software Suppliers must comply with all requirements of all applicable root distribution policies, including revocation periods described in Section 4.9.

1.5. POLICY ADMINISTRATION

1.5.1. Organisation Administering the Document

This CPS and related agreements and security policy documents referenced within this document are administered by the DigiCert Policy Authority (DCPA).

1.5.2. Contact Person

Enquiries or other communications about this CPS should be addressed to the DCPA.

DigiCert Europe Netherlands B.V. attn. DigiCert Policy Authority
Nevelgaarde 56 Noord
3436 ZZ Nieuwegein
The Netherlands

Tel: +31 30 232 4320 Fax: +31 30 232 4329
Website: http://www.quovadisglobal.com/nl
DCPA e-mail: policy@digicert.com
Support (non revocation) requests: nl.support@digicert.com
Customer complaints: qvcomplaints@digicert.com

1.5.2.1. Certificate Problem Reports and Revocation

Subscribers can revoke their own Certificates 24x7 via the DigiCert Europe Portal at https://tl.quovadisglobal.com/ or https://www.certcentral.digicert.eu/.

For other types of PKIoverheid problem reports and revocation requests, please email revoke@digicert.com. During office hours (CET), problem reports and revocation requests can also be made using the DigiCert Europe RA and support line +31 (0) 30 232 4320. Outside of office hours CET the emergency revocation hotline can be used at +1 651 229 3456. For further information please refer to the practices described in Section 3.4.

In addition, DigiCert Europe provides a website for reporting keyCompromise and other Certificate issues: https://problemreport.digicert.com/

DigiCert Europe or an RA will authenticate and process problem reports and revocation requests according to Section 4.9 of this CPS.

Entities submitting Certificate revocation requests must explain the reason for requesting revocation. DigiCert Europe or an RA will authenticate and log each revocation request according to Section 4.9 of this CP/CPS. DigiCert Europe will always revoke a Certificate if the request is authenticated as originating from the Subscriber or an authorised representative of the Organisation listed in the Certificate. If revocation is requested by someone other than an authorised representative of the Subscriber or Affiliated Organisation, DigiCert Europe or an RA will investigate the alleged basis for the revocation request prior to taking action. See also Section 4.9.1 and 4.9.3.

1.5.3. Person Determining The CPS Suitability

The DCPA determines the suitability and applicability of this CPS based on the results and recommendations received from an independent auditor, (see Section 8). The PMA is also responsible for evaluating and acting upon the results of compliance audits.

1.5.4. CPS Approval Procedures

This CPS is reviewed and approved at least on an annual basis by the DCPA, and if any significant change in the provision of PKIoverheid Certificates occurs. The DCPA, at its sole discretion, determines whether changes to this CPS require notice.

1.6. DEFINITIONS AND ACRONYMS

1.6.1. Definitions

Applicant: The Applicant is an entity applying for a Certificate.

Application Software Supplier: Means a software developer whose software displays or uses DigiCert Europe or PKIoverheid Certificates and distributes Root Certificates.

Authority Letter: The Authority Letter is a signed by a Confirming Person acting for the Applicant for EV Certificates to establish the authority of individuals to act as the Subscriber's agents.

Certificate Approver: A Certificate Approver is a natural person who is employed by the Applicant, or an authorised agent who has express authority to represent the Applicant to: (i) act as a Certificate Requester and to authorise other employees or third parties to act as a Certificate Requesters, and (ii) to approve Certificate Requests submitted by other Certificate Requesters.

Certificate Application: Any of several forms completed by Applicant or DigiCert Europe and used to process the request for an EV Certificate, including but not limited to agreements signed by Contract Signers and online forms submitted by Certificate Requesters.

Certification Authority Authorization or CAA: From RFC 9495: "The Certification Authority Authorization (CAA) DNS resource record (RR) provides a mechanism for domains to express the allowed set of Certification Authorities that are authorized to issue certificates for the domain." CAA Resource Records allow a public CA to implement additional controls to reduce the risk of unintended certificate mis-issue.

Certificate Manager: A Certificate Manager is an authorised representative of an Organisation and is also the holder of the Private Key.

Certificate Requester: A Certificate Requester is a natural person who is employed by the Applicant, or an authorised agent who has express authority to represent the Applicant or a third party (such as an ISP or hosting company), and who completes and submits a Certificate Request on behalf of the Applicant.

Confirming Person: A confirming Person is a natural person who must be a senior officer of the Applicant (e.g., Secretary, President, CEO, CFO, COO, CIO, CSO, Director, etc.) who has express authority to sign the QV Authority Letter on behalf of the Applicant.

Contract Signer: A Contract Signer is a natural person who is employed by the Applicant and who has express authority to sign Subscriber Agreements on behalf of the Applicant.

Internal Server Name: A Server Name (which may or may not include an Unregistered Domain Name) that is not resolvable using the public DNS.

Participants: A Participant is an individual or entity within the DigiCert Europe PKI and may include: CAs and their Subsidiaries and Holding Companies; Subscribers including Applicants; and Relying Parties.

Qualified Certificate for Electronic Signature means a Certificate for Electronic Signatures, that is issued by a QTSP to a Natural Person (an Individual) and meets the requirements laid down in Annex I of the eIDAS Regulation (Regulation (EU) No. 910/2014).

Qualified Certificate for Electronic Seal means a Certificate issued to a Legal Person (company) by a QTSP and is used to secure authenticity, integrity and confidentiality in electronic communication of messages and documents.

Reliable Data Source: An identification document or source of data used to verify Subject Identity Information that is generally recognized among commercial enterprises and governments as reliable, and which was created by a third party for a purpose other than the Applicant obtaining a Certificate.

Relying Party: The Relying Party is an individual or entity that relies upon the information contained within the Certificate.

Relying Party Agreement: The Relying Party Agreement is an agreement which must be read and accepted by a Relying Party prior to validating, relying on or using a Certificate or accessing or using the DigiCert Europe Repository.

Repository: The Repository refers to the CRL, OCSP, and other directory services provided by DigiCert Europe containing issued and revoked Certificates.

Required Website Content: Either a Random Value or a Request Token, together with additional information that uniquely identifies the Subscriber, as specified by the CA. A Random Value is specified by DigiCert Europe and exhibits at least 112 bits of entropy.

Reserved IP Address: An IPv4 or IPv6 address that the IANA has marked as reserved.

Subordinate CA: A Certification Authority whose Certificate is signed by the Root CA or another Subordinate CA. Also known as Issuing CA or sub-CA.

Subscriber: Means either the Individual to whom an end entity Certificate is issued or the Individual responsible for requesting, installing and maintaining the trusted system for which a Certificate has been issued.

Subscriber Agreement: Is the agreement executed between a Subscriber and DigiCert Europe relating to the provision of designated Certificate-related services that governs the Subscriber's rights and obligations related to the Certificate.

Technically Constrained Subordinate CA Certificate: A Sub-CA Certificate which uses a combination of Extended Key Usage and Name Constraint settings to limit the scope within which the Sub-CA Certificate may issue Subscriber or additional Sub-CA Certificates.

Terms and Conditions means the Master Services Agreement, Certificate Terms of Use (or the Qualified Certificate Terms of Use), Privacy Policy, and relevant DigiCert Europe CP/CPS. The Master Services Agreement references and makes the Certificate Terms of Use, Privacy Policy, and relevant DigiCert Europe CP/CPS part of the Terms and Conditions.

1.6.2. Acronyms

ALPN	TLS Application-Layer Protocol Negotiation (ALPN) Extension [RFC7301] as defined in RFC 8737
ADN	Authorisation Domain Name

CA	Certificate Authority or Certification Authority
CAA	Certificate Authority Authorisation
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
CT	Certificate Transparency
DCPA	DigiCert Europe Policy Management Authority
eIDAS	Regulation (EU) No. 910/2014 on electronic identification and trust services for electronic transactions in the internal market
ETSI	European Telecommunications Standards Institute
EV	Extended Validation
FIPS	Federal Information Processing Standard
ICANN	Internet Corporation for Assigned Names and Numbers
IETF	Internet Engineering Task Force
ITU	International Telecommunication Union
ERA	Enterprise Registration Authority
LRA	Local Registration Authority
NCA	National Competent Authority
NCSC	National Cyber Security Centre.
OID	Object Identifier
PKIo PA	PKIoverheid Policy Authority
PKI	Public Key Infrastructure
PKIX	IETF Working Group on Public Key Infrastructure
PKCS	Public Key Cryptography Standard
Portal	DigiCert Europe Certificate Management System
PvE	Program of Requirements / Programma van Eisen
QWAC	Qualified Website Authentication Certificate
QSCD	Qualified Electronic Signature/Seal Creation Device
QTSP	Qualified Trust Service Provider
RA	Registration Authority

SSCD	Signature/Seal Creation Device
SSL	Secure Sockets Layer
TLS	Transport Layer Security
X.509	The ITU-T standard for Certificates and their corresponding authentication framework

1.6.3. Conventions

The key words “MUST”, “MUST NOT”, "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this CPS shall be interpreted in accordance with RFC 2119.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1. REPOSITORIES

DigiCert Europe provides public repositories for its CA Certificates, revocation data for issued Certificates, CPS, Terms and Conditions, Privacy Notice, and other important policy documents. The DigiCert Europe Repository is located at https://www.quovadisglobal.com/repository.

All Repository information is publicly available in read-only format and is available 24 x 7. In the event that the Repository is unavailable then DigiCert Europe aims to restore availability within 24 hours.

DigiCert Europe registers TLS Server Certificates with publicly accessible Certificate Transparency (CT) Logs. CTLog information is publicly accessible. Once submitted, Certificate information cannot be removed from a CT Log.

2.2. PUBLICATION OF CERTIFICATE INFORMATION

The Repository contains:

- DigiCert Europe CPS for PKIoverheid
- DigiCert Europe PKI Disclosure Statement for PKIoverheid
- Master Services Agreement, Terms of Use, Privacy Notice
- Certificates for Subscribers (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

DigiCert Europe publishes CRL and OCSP resources to allow Relying Parties to determine the validity of a DigiCert Europe Certificate. Certificate information is published promptly following generation and issue and immediately following the completion of the revocation process. DigiCert Europe updates this CPS at least annually to describe how DigiCert Europe meets the requirements of PKIoverheid and other applicable standards including the CA/Browser Forum TLS Baseline Requirements and S/MIME Baseline Requirements.

Those updates indicate conformance by incrementing the version number and adding a dated changelog entry even if no other changes are made to the document as specified in section 1.2 of this CPS

New or modified versions of the CPS and other policies are typically published within seven days after their approval. In the event that a new version will be published the PKIo PA will be informed.

DigiCert Europe publishes a list of revoked Certificates. The CRL is updated within 10 minutes of a revocation and automatically updated every 12 hours; each CRL is valid for 72 hours. OCSP is updated immediately when a Certificate is revoked. OCSP responses are valid for a maximum of 48 hours. All OCSP responses conform to RFC 6960.

2.4. ACCESS CONTROLS ON REPOSITORIES

Read-only access to the Repository is unrestricted. Logical and physical controls prevent unauthorised write access to Repositories. In the event that the Repository is unavailable then DigiCert Europe aims to restore availability within 24 hours.

3. IDENTIFICATION AND AUTHENTICATION

The Identification and Authentication procedures used by DigiCert Europe depend on the Class of Certificate being issued. See Appendix A for Certificate Profiles and the relevant verification requirements.

3.1. NAMING

3.1.1. Types Of Names

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 in Association 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

Field	Description	Max. length
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

Organisatie Services

Field	Description	Max. length
CN - Common name	Full name of the Subscriber	64
C - Country	Two-digit country code for the location	2
O - Organisation Name	Full name of the subscriber	64
L - Locality	Place the Organisation is located	128
ST - State	State or province the Organisation is located	128

Private Services Certificates

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

Private Services Server

Field	Description	Max. length
CN - Common name	FQDN to which the Certificate and keypair are assigned	64

Field	Description	Max. length
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

3.1.2. Need For Names To Be Meaningful

DigiCert Europe 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. Pseudonymous 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 and ASN.1 syntax. DigiCert Europe may allow the conversion of Identity information usually rendered in non-ASCII characters (for example é and à may be represented by r or a, and umlauts such as ö or ü may be represented by oe or ue, o or u respectively). DigiCert Europe may use language variants (such as Munich or München) for geographic names.

3.1.5. Uniqueness Of Names

The Subject Name of each Certificate issued by an Issuing CA shall be unique within each class of Certificate issued by that Issuing CA over the lifetime of that Issuing CA and shall conform to applicable X.500 standards for the uniqueness of names.

The Issuing CA will, when necessary, insert additional numbers or letters to the Subscriber's Subject Common Name, or other attribute such as subject serialNumber, in order to distinguish between two Certificates that would otherwise have the same Subject Name. Name uniqueness is not violated when multiple Certificates are issued to the same entity.

3.1.6. Recognition, Authentication, And Role Of Trademarks

Certificate Applicants shall not use names which infringe upon the intellectual property rights of others. DigiCert Europe 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. DigiCert Europe reserves the right, without liability, to reject any application for a Certificate.

3.2. INITIAL IDENTITY VALIDATION

DigiCert Europe may use any legal means of communication or investigation to DigiCert Europe the identity of an organisational or individual Applicant. DigiCert Europe may refuse to issue a Certificate in its sole

discretion. The Applicant begins the application on the DigiCert Europe website: https://www.quovadisglobal.com/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 DigiCert Europe representative is responsible for the processing of applications in accordance with Section 3.2.2. and Section 3.2.3. Identity verification can also be performed by Delegated RAs described in Section 1.3.2.

DigiCert Europe does not provide Certificate Modification. DigiCert Europe 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.

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	Checks and Validations Performed
PKIo Organisatie Persoon Certificates	Individual Identity Checks
Domain CA: Staat der Nederlanden Organisatie Persoon CA - G3	Organisation Checks (when Organisation is included in the Certificate)
Domain CA: Staat der Nederlanden Organisatie Persoon CA-2022	Profession checks (when profession is included in the Certificate)
PKIo Burger Certificates	Individual Identity Checks. This may include information provided by the Gemeentelijk Basis Administratie (GBA).
Staat der Nederlanden Burger CA - G3	
Note: Includes the profession variant (Beroepscertificaat).	
PKIo Private Persoon Certificates	Individual Identity Checks
Staat der Nederlanden Private Personen CA – G1	Organisation Checks (when Organisation is included in the Certificate)
	Profession checks (when profession is included in the Certificate)
PKIo Private Services Certificates	Individual Identity Checks
QuoVadis PKIoverheid Private Services CA – G1	Authorised Person Checks
	FQDN Checks (if applicable)
	CSR
PKIO Organisatie Services Certificates (Seals)	Individual Identity Checks
Domain CA: Staat der Nederlanden Organisatie Services CA-G3	Authorised Person Checks
	FQDN Checks (if applicable)
Domain CA: Staat der Nederlanden Organisatie Services CA-2022	

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

3.2.1. Method To Prove Possession Of Private Key

DigiCert Europe ensures that the Applicant delivers the Certificate Signing Request (CSR) in a secure manner. The delivery must take place securely, as follows:

- Inputting the CSR into the DigiCert Europe Certificate Management System (Portal) or website using an HTTPS connection which uses a PKIoverheid TLS Server Certificate or equivalent;
- 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 Organisation Identity

In issuing Certificates linked to Organisations (legal persons) then DigiCert Europe will verify the Applicant/Subscriber is an existing Organisation. If the Applicant requests a Certificate that will contain Subject identity information then DigiCert Europe will verify this information, including;

- Verification of country;
- Identity of the Applicant; and
- Authenticity and authorisation of the Applicant's representative.

All evidence relied upon during the verification process will be inspected for alteration or falsification.

3.2.2.1. Identity

DigiCert Europe verifies that the Applicant is an existing and legal Organisation. As proof that it is an existing and legal organisation, DigiCert Europe 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 must not be older than 825 days;
- For Organisations outside of the Netherlands the following must be used where the Authorised Representative is shown;

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

Additional information is provided in Acceptable Sources for DigiCert Europe Authentication of Identity in the DigiCert Europe Repository.

DigiCert Europe 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/en/policies/fight-against-terrorism/terrorist-list/#terrorists. DigiCert Europe will not issue a Certificate to an Organisation on this list.

3.2.2.2. DBA/Tradename

If the Certificate is to contain a Subject DBA or tradename then DigiCert Europe will verify the Applicant's right to use the DBA/tradename by using at least one of the following sources;

- For Organisations in the Netherlands a certified extract from the Kamer van Koophandel (KvK) Trader register. Extracts must not be older than 825 days;
- For Organisations outside of the Netherlands the following must be used where the Authorised Representative is shown;
    - Trade Registers or equivalent
    - Article of Association; or
    - Generation Administrative Order.

3.2.2.3. Verification of Country

If the Certificate is to contain the Subject Country information then this will be verified by DigiCert Europe using the information evidence described in Section 3.2.2.1.

3.2.2.4. Validation of Domain and Email Authorisation and Control

For each FQDN listed in a Certificate, DigiCert Europe 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:

1. BR Section 3.2.2.4.1 is no longer used as it is deprecated as of August 1, 2018;
2. 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);
3. BR Section 3.2.2.4.3 is no longer used because it is deprecated as of May 31, 2019;
4. Communicating with the Domain's administrator using a constructed email address created by prepending 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' to the Authorisation Domain Name (ADN). Performed in accordance with BR section 3.2.2.4.4;
5. BR Section 3.2.2.4.5 is no longer used because it is deprecated as of August 1, 2018;
6. BR Section 3.2.2.4.6 is no longer used because it is deprecated as of April 24, 2020;
7. Confirming the Applicant's control over the requested ADN (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
8. 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 Section 3.2.2.4.8;
9. BR Section 3.2.2.4.9 is no longer used because it was deprecated as of March 16, 2019;
10. BR Section 3.2.2.4.10 is no longer used because it was deprecated as of September 22, 2020;
11. BR Section 3.2.2.4.11 is no longer used because it is deprecated as of February 5, 2018;
12. BR Section 3.2.2.4.12 is not used by QuoVadis;

13. 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;

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

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

16. 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 ADN. Each phone call can confirm control of multiple ADN provided that the same DNS TXT Record Phone Contact phone number is listed for each ADN being verified and they provide a confirming response for each ADN, performed in accordance with BR Section 3.2.2.4.16;

17. Confirming the Applicant's control over the FQDN by calling the DNS CAA Phone Contact's phone number and obtain a confirming response. Each phone call can confirm control of multiple domains provided that the same DNS CAA Phone Contact phone number is listed for each domain being verified and a confirming response is provided for each domain. Performed in accordance with BR Section 3.2.2.4.17;

18. Confirming the Applicant's control over the requested FQDN by verifying that the Request Token or Random Value is contained in the contents of a file (such as a Request Token,Random Value that does not appear in the request used to retrieve the file and receipt of a successful HTTP 2xx status code response from the request). Performed in accordance with BR section 3.2.2.4.18;

19. 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 and section 8.3 of RFC 8555 as prescribed; or

20. BR Section 3.2.2.4.20 is not used by QuoVadis.

Wildcard Domain Name validation is completed using the above list as permitted by the CA/B Forum TLS Baseline Requirements along with current best practice of consulting a public suffix list. DigiCert Europe maintains a list of High Risk Domains and has implemented technical controls to prevent the issuance of Certificates to certain domains. DigiCert Europe follows documented procedures that identify and require additional verification activity for High Risk Certificate Requests prior to the Certificate's approval.

3.2.2.5. Verification of Email

DigiCert Europe and its Issuing CAs verify an Applicant's or Organisation's right to use or control of a Mailbox Address to be included in a Certificate that will have the id-kp-emailProtection EKU using one of the following procedures, which may not be delegated:

i. By verifying domain control over the email Domain Name using one of the procedures listed in this Section in accordance with S/MIME BR Section 3.2.2.1; or

ii. By sending an email message containing a unique Random Value to the Mailbox Address to be included in the Certificate and receiving a confirming response within 24 hours that includes the Random Value to indicate that the Applicant controls that same Mailbox Address, in accordance with S/MIME BR Section 3.2.2.2; or

iii. By confirming control of the SMTP FQDN to which a message delivered to the Mailbox Address should be directed, in accordance with S/MIME BR Section 3.2.2.3.

3.2.2.6. Authentication for an IP Address

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

i. 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/pki-validation" directory on the IP Address, performed in accordance with BR Section 3.2.2.5.1;

ii. 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 utilising the Random Value, performed in accordance with BR Section 3.2.2.5.2;

iii. Performing a reverse-IP address lookup and then verifying control over the resulting Domain Name, as set forth above and in accordance with BR Section 3.2.2.5.3;

iv. BR Section 3.2.2.5.3 is no longer used because it was deprecated as of July 31, 2019.

v. Confirming the Applicant's control over the IP Address by calling the IP Address Contact's phone number, as identified by the IP Address RA, 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;

vi. 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-ietf-acme-ip-04#section-4, performed in accordance with BR Section 3.2.2.5.6; or

vii. BR Section 3.2.2.5.7 is not used by DigiCert Europe.

3.2.2.7. Wildcard Domain Names

Wildcard domains are not permitted for use within PKIoverheid.

3.2.2.8. Data Source Accuracy

Prior to using a data source as a Reliable Data Source, DigiCert Europe evaluates it for reliability, accuracy and resistance to falsification. DigiCert Europe will consider:

- The age of the information provided;
- The frequency of updates to the information source;
- The data provider and purpose of the data collected;
- The public accessibility of the data availability; and
- The probability that the data could be falsified or altered.

Databases maintained by the CA, its owner, or its affiliated companies do not qualify as a Reliable Data Source if the primary purpose of the database is to collect information for the purpose of fulfilling the validation requirements under this Section 3.2.

3.2.2.9. CAA Records

DigiCert Europe performs CAA record checks for TLS Certificates which are described further in Section 4.2.4. All potential issuances that were prevented by a CAA record will be recorded in sufficient detail to the CA/Browser Forum and the circumstances, and may dispatch reports of those issuance requests to the contact(s) stipulated in the CAA iodef record(s), if present.

3.2.3. Authentication Of Individual Identity

An Individual's Identity is to be authenticated in accordance with the class/type of Certificate together with the relevant application data and documentation. TLS Server Certificates are only issued to legal persons and not natural persons.

3.2.3.1. Natural Person

The following checks are carried out for a natural person;

i. Personal Details: The personal details are verified using the details on a Legal Identity Document. This includes full legal name(s), date of birth, place of birth, or other attributes which can be used to, as far as possible, distinguish the person from others with the same name.

ii. 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 a DigiCert Europe Portal.

iii. Legal Identity Document: Verification of the Applicant is done by verifying the Legal Identity Document (LID). DigiCert Europe 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.

iv. Face-to-face check or Remote Identity Validation: Part of the registration process is a Face-to-Face (physical identification of the natural person applying for the Certificate) or by Remote Identity Validation (identity verification performed via an app, which provides equivalent assurance as physical presence). Face-to-Face identity vetting or Remote Identity Validation is performed for all the individuals who are listed on the applicable PKIoverheid application forms. During the Face-toFace vetting process the Applicant must place their signature on a copy of the LID as provided by DigiCert Europe or a third party acting on behalf of DigiCert Europe.

v. Extract from the Gemeentelijke Basis Administratie (GBA): Part of the registration process for a DigiCert Europe PKIo Burger Certificate or a DigiCert Europe PKIo Private Person Certificate is for the applicant to obtain an extract from the GBA, that is not older than 6 months, and shows the name and address of the subject to be contained in the certificate.

By requesting a DigiCert Europe Certificate, an Applicant accepts to undertake one of the following identity proofing methods and the related terms and conditions. Where applicable, an Applicant may choose from the alternative methods available to the relevant Certificate Class.

For PKIoverheid, DigiCert Europe authenticates an Individual's Identity and, if applicable, any specific attributes using the following methods:

- Physical presence;

- Remote identity verification means which provide equivalent assurance in terms of reliability to the physical presence; and/or
- Reliance on a Qualified Electronic Signature.

Evidence is verified that the Subject is affiliated with the organisational entity which may include reference to an attestation or a trusted register. Attestations can be made by directors, executives, board members, or a natural person with authorisation duly delegated from another natural person in an authorised role. The current validity must be established of any attestation or document regarding a natural person's relationship to a legal person. The role and authorisation of the natural person providing such attestation or document shall be recorded. At least one digital or physical identity document shall be used as authoritative evidence. Identity documents must be valid at the time of proofing. Acceptable identity documents must contain a face photo and/or other information that can be compared with the Applicant's physical appearance. If physical identity documents are used as evidence, the documents shall be presented in their original form by the Subject of the identity proofing. If digital identity documents are used as evidence, only eMRTD (Electronic Machine Readable Travel Documents) according to ICAO 9303 part 10 and other digital documents that offer comparable reliability of the identity shall be accepted.

The Trusted Registers and identity documents accepted in DigiCert Europe verification procedures are identified in *Acceptable Sources for DigiCert Europe Authentication of Identity* in the DigiCert Europe Repository.

Identity proofing may use additional digital or physical identity documents, trusted registers, proof of access, or other documents and attestations as supplementary evidence. Only official national or nationally approved registers are accepted as trusted registers.

By loading or using identity proofing software provided by DigiCert Europe, Applicants agree that such use will be subject to the terms and conditions of the Master Services Agreement. Use of the software may also be subject to additional terms between the Applicant and the identity proofing software provider.

3.2.3.2. Physical Presence

In-person (manual) verification requires the physical presence of the Applicant in order to conduct the identity proofing, to validate the identity document, and to bind the identity to the Applicant. The Applicant is not required to be present for all steps of the verification, which may include manual procedures or a hybrid approach using manual and automated procedures.

Entities that can perform this verification include the CA or RA, a Public Official or third-party validator approved by DigiCert Europe, or a registered Notary/Lawyer. In some cases, a Delegated RA such as an Enterprise RA may confirm attributes where Certificates may assert the Individual's affiliation with an Organisation.

3.2.3.3. Remote Identity Verification

Remote Identity Verification (RIV) allows the Applicant to use identity proofing software to assist in automating the proofing and validation of either physical or digital identity documents and the binding to the Applicant. For PKIoverheid, DigiCert Europe uses a hybrid approach using manual and automated procedures.

DigiCert Europe only accepts Remote Identity Verification following review and acceptance of the method by the relevant Conformity Assessment Body and/or Supervisory Body.

For PKIoverheid Certificates, DigiCert Europe shall use its RIV4 method which includes Base RIV plus NFC Authentication with manual review in all cases. The RIV4 method has an assurance level of 'High' as set out in Article 8 of the eIDAS Regulation.

Base RIV includes OCR reading of identity documents, video capture, biometric comparison, liveness checks, and other document security checks. NFC options include read of eMRTD data, Passive Authentication, and Active Authentication. Information collected and verified includes:

First name	ID number	ID issuance date
Last name	ID valid until	Issuing authority
Phone number	Scan of ID Document	Image of face
Email	Place of birth	Street
Date of birth	Nationality	Zipcode
ID type	Issuing country	City
Title (optional)		

Entities that can perform this verification include the CA, RA, or third-party validators approved by DigiCert Europe.

3.2.3.4. Reliance On Electronic Signature

DigiCert Europe may rely upon an existing Electronic Signature with a supporting Certificate as evidence. The Electronic Signature can be applied by a natural person (electronic signature as defined by eIDAS), a legal person (electronic seal as defined by eIDAS), or a natural person representing a legal person.

For PKIoverheid Certificates, DigiCert Europe shall rely upon a Qualified Electronic Signature created as part of the identity proofing process in order to verify an Applicant's identity and additional attributes if the currently valid Certificate was issued by DigiCert Europe, or by another Issuing CA, following validation of the Certificate using the relevant Trusted List.

Entities that can perform this verification include the CA or RA.

PROFESSION CHECK Verification of the natural person in the applicable professional registrar is done when applicable for the specific Certificate that is applied for. DigiCert Europe currently issue Certificates for professions that appear on the EU Regulated Professions Database: https://ec.europa.eu/growth/toolsdatabases/regprof/index.cfm?action=regprofs

NOTE: Dutch Driving Licenses are considered acceptable legal identity documents but do not contain all names in full. The use of full and complete names are mandatory for the issuance of Certificates within PKIoverheid and eIDAS, therefore DigiCert Europe cannot accept driving licenses from Applicants.

NOTE: Certificates issued to natural persons are not interpreted as a means of identification defined in the Dutch Compulsory Identification act (WID), and therefore cannot be used for identification purposes.

3.2.4. Non-Verified Subscriber Information

No stipulation.

3.2.5. Validation Of Authority

Where an Applicant's Name is to be associated with an Organisational Name to indicate his or her status as a Counterparty, Employee or specifies an authorisation level to act on behalf of an Organisation, the RA will validate the Applicant's Authority by reference to business records maintained by the RA, its Subsidiaries, Holding Companies or Affiliates. Validation of authority is conducted in compliance with this CPS and the Certificate Profiles detailed in Appendix A. Validity of authority of Applicant Representatives and Agents is verified against contractual documentation and Reliable Data Sources.

In addition, DigiCert Europe will allow an Applicant to specify the individuals who may request Certificates. If an Applicant specifies, in writing, the individuals who may request a Certificate, then Certificate Requests that are outside this specification will not be accepted. DigiCert Europe will provide an Applicant with a list of its authorised Certificate Requesters upon the Applicant's verified written request

3.2.6. Criteria for Interoperation

No stipulation.

3.3. IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1. Identification And Authentication For Routine Re-Key

Subscribers may request re-key of a Certificate prior to a Certificate's expiration.

When replacing a personal certificate at the end of its lifetime the Qualified Electronic Signature of the nonrepudiation Certificate can be used during registration and identification, instead of the physical presence of the certificate holder. This is subject to conditions of PKIoverheid:

- The non-repudiation Certificate must be valid at the time of renewal;
- The file must be current and complete, including a copy of a valid ID document;
- Subject details in the valid non-repudiation Certificate, e.g., Subject:Organisation field;
- Unlimited renewals of the Certificate within 72 months, without physical appearance, is only possible if DigiCert Europe issued the previous non-repudiation Certificate based on physical appearance.

After receiving a request for re-key, DigiCert Europe creates a new Certificate with the same Certificate contents except for a new Public Key and, optionally, an extended validity period. If the Certificate has an extended validity period, DigiCert Europe may perform some revalidation of the Applicant but may also rely on information previously provided or obtained. DigiCert Europe does not re-key a Certificate without additional Identification and Authentication if doing so would allow the Subscriber to use the Certificate beyond the limits specified for the applicable Certificate Profile.

3.3.2. Identification and Authentication For Re-Key After Revocation

After revocation of the Certificate the relevant keys cannot be recertified. Applicants will be required to apply for a new Certificates using new keys.

3.4. IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUESTS

All revocation requests are authenticated by DigiCert Europe or the RA responsible for issuing the Certificate. DigiCert Europe authenticate revocation requests by referencing the Certificate's Public Key, regardless of whether the associated Private Key is compromised.

All revocation requests are authenticated by DigiCert Europe or the RA responsible for issuing the Certificate. DigiCert Europe 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 a DigiCert Europe Portal and requesting revocation via that system;
- Applying in person to the RA, Issuing CA or DigiCert Europe supplying either original proof of identification in the form of a valid Passport or National ID; or
- Telephonic communication using a pre-existing shared secret, password or other information associated with Subscriber's account with the CA following appropriate verification.
- Applying by writing in an email, or letter, to a DigiCert Europe or DigiCert office in Europe, with details of the Certificate and identifiable information that can be checked against the Subscriber account.

See Section 4.9 for information about Certificate Revocation procedures

4. CERTIFICATE LIFE-CYCLE OPERATION REQUIREMENTS

4.1. CERTIFICATE APPLICATION

4.1.1. Who Can Submit A Certificate Application

Either the Applicant or an individual authorised to request Certificates on behalf of the Applicant may submit Certificate Requests. Applicants are responsible for any data that the Applicant or an agent of the Applicant supplies to DigiCert Europe. DigiCert Europe 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 U.S. prohibit doing business.

DigiCert Europe 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/en/policies/fight-against-terrorism/terrorist-list/#terrorists. DigiCert Europe will not issue a Certificate to an Organisation on this list.

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 Master Service Agreement and Terms of Use of both DigiCert Europe and the PKIoverheid framework, and the Privacy Notice 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, DigiCert Europe will reject the application for a Certificate.

DigiCert Europe maintain an internal database of all previously revoked Certificates and previously rejected Certificate Requests due to suspected phishing or other fraudulent usage or concerns. This information is used to identify any subsequent suspicious Certificate Requests. Subscribers have obligations regarding usage of DigiCert Europe PKIo Certificates, which are set out in the Terms of Use documentation and the other agreements to be found in the Repository.

4.1.2. Enrolment Process And Responsibilities

Certificate Requests must be in a form prescribed by the Issuing CA and typically include i) an application form including all registration information as described by this CPS, ii) secure generation of Key Pair and delivery of the Public Key to DigiCert Europe, (a CSR may not be required), iii) acceptance of the relevant Subscriber Agreement or other Terms of Use upon which the Certificate is to be issued, and iv) payment of fees. All applications are subject to review, approval, and acceptance by the Issuing CA in its discretion.

All agreements concerning the use of, or reliance upon, Certificates issued within the DigiCert Europe PKIo must incorporate by reference the requirements of this DigiCert Europe CPS as it may be amended from time to time.

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. DigiCert Europe can only make approval assessments based on the information provided by the Applicant and information retrieved from Trusted Registers and Attestations as defined in the Acceptable Sources for DigiCert Europe Authentication of Identity in the DigiCert Europe Repository.

The Applicant has the obligation to ensure all information provided is accurate and complete at the time of application, DigiCert Europe provides no guarantees to the issuance of Certificates.

DigiCert Europe considers a data source's availability, purpose, and reputation when determining whether a thirdparty source is reasonably reliable. For TLS DigiCert Europe does not consider a database, source, or form of identification reasonably reliable if DigiCert Europe or the RA is the sole source of the information

4.2.2. Approval Or Rejection Of Certificate Applications

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

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

4.2.3. Time To Process Certificate Applications

DigiCert Europe makes reasonable efforts to confirm Certificate Application information and issue a Certificate within a reasonable time frame, which is dependent on the Applicant providing the requested necessary details and documentation in a timely manner, as well as the availability of Trusted Registers and Attestations where applicable. Events outside of the control of DigiCert Europe may delay the issuance process.

4.2.4. CAA Checking

Prior to issuing a TLS certificate, Issuer CAs check the DNS for the existence of a CAA record for each DNSName in the subjectAltName extension of the certificate to be issued. DigiCert Europe processes the "issue" and "issuewild" property tags.

Prior to issuing an S/MIME certificate on or after March 15, 2025, Issuer CAs check the DNS for the existence of a CAA record in accordance with RFC 9495 for each Mailbox Address in the subjectAltName extension of the S/MIME certificate to be issued. DigiCert Europe processes the "issuemail" property tag.

Certificates passing the CAA check are issued within the Time to Live (TTL) of the CAA record, or 8 hours, whichever is greater. DigiCert Europe logs actions taken based on CAA records, and documents issuance prevented by CAA for feedback to the CA/B Forum. DigiCert Europe may not dispatch reports of issuance requests to the contact(s) listed in an "iodef" property tag. CAA checking is optional for certificates issued by a Technically Constrained Subordinate CA Certificate.

DigiCert Europe may treat a record lookup failure as permission to issue if:

- The failure is outside the DigiCert's infrastructure; and
- The lookup has been retried at least once; and
- The domain's zone does not have a DNSSEC validation chain to the ICANN root.

The CA identifiers that DigiCert Europe recognizes are:

- digicert.com
- digicert.ne.jp
- cybertrust.ne.jp
- symantec.com
- thawte.com
- geotrust.com
- quovadisglobal.com
- rapidssl.com
- digitalcertvalidation.com
- volusion.digitalcertvalidation.com
- stratossl.digitalcertvalidation.com
- intermediatecertificate.digitalcertvalidation.com
- 1and1.digitalcertvalidation.com
- amazon.com
- amazontrust.com
- awstrust.com

- amazonaws.com
- www.digicert.com
- pkioverheid.nl

4.3. CERTIFICATE ISSUANCE

4.3.1. CA Actions During Certificate Issuance

DigiCert Europe 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 DigiCert Europe issued Certificate. Acceptance of Certificates is deemed to have taken place after completion of the Certificate issue via the Certificate Management Portal.

4.3.2. Notification To Subscriber By The CA Of Issuance Of Certificate

DigiCert Europe may deliver Certificates in any secure manner within a reasonable time after issuance. Generally, DigiCert Europe delivers instructions via email to the email address designated by the Certificate Requester during the application process.

4.4. CERTIFICATE ACCEPTANCE

4.4.1. Conduct Constituting Certificate Acceptance

The Certificate Requester is responsible for installing the issued Certificate on the Subscriber's computer or cryptographic module according to the Subscriber's system specifications. A Subscriber is deemed to have accepted a Certificate when:

- The Subscriber downloads, installs, or otherwise takes delivery of the Certificate; or
- 30 days pass since issuance of the Certificate.

BY ACCEPTING A CERTIFICATE, THE SUBSCRIBER ACKNOWLEDGES THAT THEY AGREE TO THE TERMS AND CONDITIONS CONTAINED IN THIS CPS AND THE APPLICABLE SUBSCRIBER AGREEMENT. BY ACCEPTING A CERTIFICATE, THE SUBSCRIBER ASSUMES A DUTY TO RETAIN CONTROL OF THE CERTIFICATE'S PRIVATE KEY, TO USE A TRUSTWORTHY SYSTEM AND TO TAKE REASONABLE PRECAUTIONS TO PREVENT ITS LOSS, EXCLUSION, MODIFICATION OR UNAUTHORISED USE.

4.4.2. Publication Of The Certificate By The CA

DigiCert Europe publishes all CA Certificates in its Repository. DigiCert Europe publishes end-entity Certificates by delivering them to the Subscriber.

4.4.3. Notification Of Certificate Issuance By The CA To Other Entities

DigiCert Europe TLS Server Certificates may include Signed Certificate Timestamps (SCT) from independent CT Logs in accordance with IETF RFC 6962 (see also 4.4.3-pkio154 of the PvE Additional Requirements).

4.5. KEY PAIR AND CERTIFICATE USAGE

4.5.1. Subscriber Private Key And Certificate Usage

Subscribers are obligated to protect their Private Keys from unauthorised use or disclosure, discontinue using a Private Key after expiration or revocation of the associated Certificate, and use Certificates in accordance with their intended purpose.

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 to ensure that each Certificate in the Certificate Chain is valid, unexpired, and non-revoked.

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.

4.5.2. Relying Party Public Key And Certificate Usage

Relying Parties may only use software that is compliant with X.509, IETF RFCs, and other applicable standards. DigiCert Europe 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 DigiCert Europe 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 DigiCert Europe Repository. A Relying Party should rely on a Electronic Signature or TLS handshake only if:

i. the Electronic Signature or TLS session was created during the operational period of a valid Certificate and can be verified by referencing a valid Certificate;

ii. 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

iii. the Certificate is being used for its intended purpose and in accordance with this CPS.

4.6. CERTIFICATE RENEWAL

4.6.1. Circumstance For Certificate Renewal

Renewal means the issuance of a new Certificate to the Subscriber without changing the Subscriber or other participant's Public Key or any other information in the Certificate. DigiCert Europe may renew a Certificate if:

i. the associated Public Key has not reached the end of its validity period;

ii. the Subscriber and attributes are consistent; and

iii. the associated Private Key remains uncompromised.

DigiCert Europe may also renew a Certificate if a CA Certificate is re-keyed or as otherwise necessary to provide services to a customer. DigiCert Europe may notify Subscribers prior to a Certificate's expiration date. DigiCert Europe renewal requires payment of additional fees.

4.6.2. Who May Request Renewal

Only the Certificate Subject or an authorised representative of the Certificate Subject may request renewal of the Subscriber's Certificates.

4.6.3. Processing Certificate Renewal Requests

Renewal application requirements and procedures are generally the same as those used during the Certificate's original issuance. DigiCert Europe will revalidate any information that is older than the periods specified in applicable standards for the Certificate Profile.

4.6.4. Notification of New Certificate Issuance To Subscriber

DigiCert Europe may deliver the Certificate in any secure fashion, such as using a DigiCert Europe Portal.

4.6.5. Conduct Constituting Acceptance Of A Renewal Certificate

Conduct constituting acceptance of a renewed Certificate is in accordance with section 4.4.1. Issued Certificates are considered accepted 30 days after the Certificate is renewed, or earlier upon use of the Certificate when evidence exists that the Subscriber used the Certificate.

4.6.6. Publication of the Renewal Certificate By The CA

DigiCert Europe publishes a renewed Certificate by delivering it to the Subscriber. All renewed CA Certificates are published in DigiCert Europe's Repository.

4.6.7. Notification Of Certificate Issuance By The CA To Other Entities

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

4.7. CERTIFICATE RE-KEY

Re-keying a Certificate means creating a new Certificate with a new Public Key and serial number while keeping the Subject information the same.

4.7.1. Circumstance for Certificate Re-Key

No stipulation.

4.7.2. Who May Request Re-Key

No stipulation.

4.7.3. Processing Certificate Re-Key Request

No stipulation.

4.7.4. Notification of Certificate Re-Key To Subscriber

No stipulation.

4.7.5. Conduct Constituting Acceptance Of A Re-Key Certificate

No stipulation.

4.7.6. Publication of The Re-Key Certificate By The CA

No stipulation.

4.7.7. Notification of Certificate Re-Key By The CA To Other Entities

No stipulation.

4.8. CERTIFICATE MODIFICATION

4.8.1. Circumstances For Certificate Modification

DigiCert Europe does not provide Certificate Modification. DigiCert Europe 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.

4.8.2. Who May Request Certificate Modification

No stipulation.

4.8.3. Processing Certificate Modification Requests

No stipulation.

4.8.4. Notification Of Certificate Modification To Subscriber

No stipulation.

4.8.5. Conduct Constituting Acceptance Of A Modified Certificate

No stipulation.

4.8.6. Publication Of The Modified Certificate By The CA

No stipulation.

4.8.7. Notification Of Certificate Modification By The CA To Other Entities

No stipulation.

4.9. CERTIFICATE REVOCATION AND SUSPENSION

Revocation of a Certificate permanently ends the operational period of the Certificate prior to the Certificate reaching the end of its stated validity period. Prior to revoking a Certificate, DigiCert Europe and Issuing CAs verify that a revocation request was initiated by Subscribers, an RA, an Issuing CA, and other entities listed in section 4.9.2 of this CPS. Issuing CAs are required to provide evidence of the revocation authorisation to DigiCert Europe upon request.

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

4.9.1. Circumstances For Revocation

Certificates will be revoked within 24 hours of the receipt and use the corresponding CRLReason in accordance with Section 7.2, confirming one or more of the following occurred:

i. Subscriber requests in writing that DigiCert Europe can revoke the Certificate;

ii. Subscriber notifies DigiCert Europe that the original Certificate Request was not authorised and does not retroactively grant authorisation;

iii. DigiCert Europe 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;

iv. DigiCert Europe obtains reasonable evidence that the Certificate has been used for a purpose outside of that indicated in the Certificate or in DigiCert Europe's Subscriber Agreements, the Certificate Policy of the PKIo PA or this CPS;

v. DigiCert Europe receives notice or otherwise becomes aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement;

vi. DigiCert Europe receives notice or otherwise becomes aware of any circumstance indicating that the use of the email address in the Certificate in no longer legally permitted;

vii. DigiCert Europe receives notice or otherwise becomes aware of a substantial change in the information that is provided in the Certificate rending such information inaccurate;

viii. DigiCert Europe determines that the Certificate has not been issued in line with (or in violation of) the Certificate Policy of the PKIo PA, Subscriber Agreements, applicable requirements, Root policies of Microsoft or Mozilla, CA/Browser Forum TLS and/or S/MIME Baseline requirements (as relevant), or this CPS;

ix. DigiCert Europe determines that any of the information appearing in the Certificate is inaccurate or misleading;

x. If DigiCert Europe ceases its activities and the CRL and OCSP services are not undertaken by another TSP.

xi. The PKIo PA determines that the technical content of the Certificate entails an irresponsible risk to Subscriber, relying parties and third parties (e.g., browser parties);

xii. The Certificate revocation is required as a measure to combat an emergency e.g., Private Key compromise or suspected Private Key compromise of DigiCert Europe;

xiii. DigiCert Europe obtains evidence that the validation of domain authorisation or control for any FDQN or IP address in the Certificate should not be relied upon.

xiv. That the Certificate no longer complies with the Sections 6.1.5 or 6.1.6 of this CPS;

xv. DigiCert Europe obtains evidence that the Certificate was misused;

xvi. DigiCert Europe receives notice or otherwise becomes aware of any circumstance indicating that the use of the email address in the Certificate is no longer legally permitted;

xvii. DigiCert Europe is made aware of any circumstance indicating that use of a FQDN or IP address in the Certificate is no longer legally permitted (e.g., a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a licensing or services agreement between the Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name);

xviii. DigiCert Europe is made aware of a material change in the information contained in the Certificate;

xix. Revocation is required by the Certificate Policy of PKIoverheid and/or this CPS;

xx. 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;

xxi. 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 including but not limited to those identified in Section 6.1.1.3, or if there is clear evidence that the specific method used to generate the Private Key was flawed;

xxii. If the technical content or format of the Certificate presents an unacceptable risk;

Certificates can be withdrawn if DigiCert Europe becomes aware that a QSCD used for QCP-n-qscd or QCP-l-qscd loses its certification status.

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 DigiCert Europe with which Certificates are signed.

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

4.9.2. Who Can Request Revocation

DigiCert Europe will revoke a Certificate following a valid request to do so from the Subscriber or the Certificate Manager (including the party that purchased the Certificate on behalf of a Subscriber and the party that manages the Portal account to which the Certificate is tied), the PKIo PA, organisations of Registered Professionals (where professional status may be reflected in the Certificate), Application Software Suppliers, or other third parties at the discretion of DigiCert Europe. DigiCert Europe itself may also initiate revocation requests.

A Relying Party may not request a revocation, but may provide certificate problem reports with evidence that may give grounds for revocation of a Certificate. DigiCert Europe will investigate such reports and, if there is reason to do so, will revoke the Certificate. See also https://problemreport.digicert.com and other resources listed in Section 1.5.2.1.

4.9.3. Procedure For Revocation Request

Subscribers may also revoke their Certificates directly via the DigiCert Europe Portal. DigiCert Europe maintains a continuous 24x7 ability to internally respond to high priority revocation requests (see Section 1.5.2 for contact details).

DigiCert Europe processes a revocation request as follows:

i. DigiCert Europe logs the request or problem report and the reason for requesting revocation based on the list in section 4.9.1, including contact information for the requestor. DigiCert Europe may also include its own reasons for revocation in the log.

ii. DigiCert Europe may request confirmation of the revocation from a known administrator, where applicable, via out-of-band communication (e.g., telephone, fax, etc.).

iii. If the request is authenticated as originating from the Subscriber or an authorized party, DigiCert Europe revokes the Certificate.

iv. For requests from third parties, DigiCert Europe personnel begin investigating the request within 24 hours after receipt and decide whether revocation is appropriate.

v. If DigiCert Europe determines that revocation is appropriate, DigiCert Europe personnel revoke the Certificate and update the Certificate Status including the RFC 5280 Revocation reason. If DigiCert Europe deems appropriate, DigiCert Europe may forward the revocation reports to law enforcement.

In the case of system defects, service activities, or other factors that are beyond the scope of DigiCert Europe, DigiCert Europe will do everything possible to ensure that the unavailability of the revocation facility will not last longer than twenty-four (24) hours. In the case of unavailability, the RA has the option of having a Certificate revoked directly via an emergency procedure on the DigiCert Europe PKIoverheid CA environments.

4.9.4. Revocation Request Grace Period

DigiCert Europe will revoke Certificates as soon as reasonably practical following verification of a revocation request.

4.9.5. Time Within Which The CA Must Process The Revocation Request

The maximum delay between receiving a valid revocation request and the amendment of revocation status information available to all Relying Parties is 4 hours.

Within 24 hours after receiving a certificate problem report, DigiCert Europe investigates the facts and circumstances involved with the report and will provide a preliminary report on its findings to both the Subscriber and the entity who filed the certificate problem report. The time used for the provision of revocation services is synchronised with UTC at least every 24 hours.

4.9.6. Revocation Checking Requirement for Relying Parties

Prior to relying on information listed in a Certificate, a Relying Party must confirm the validity of each Certificate in the certificate path in accordance with IETF PKIX standards, including checking for certificate validity, issuer-to-subject name chaining, policy and key use constraints, and revocation status through CRLs or OCSP responders identified in each Certificate in the chain.

DigiCert Europe uses an OCSP and a CRL to make the certificate status information available 24x7. In the event the revocation status information becomes unavailable, DigiCert Europe aims to restore this information availability within 4 hours.

4.9.7. CRL Issuance Frequency

DigiCert Europe uses its offline Root CAs to publish CRLs for its Issuing CAs at least every 6 months and within 18 hours after revoking an Issuing CA Certificate. DigiCert Europe updates the CRL for end-user Certificates at least every 12.5 hours and the date of the nextUpdate field will not be more than 72.5 hours after the date in the field thisUpdate field.

Before revoking an Issuing CA Certificate a last CRL is generated with a nextUpdate field value of "99991231235959Z". The last CRL is available in accordance with Section 5.5.2. DigiCert Europe does not issue a last CRL until all Certificates in the scope of the CRL are either expired or revoked.

After the expiry date of an Issuing CA the most recent CRL will be published for at least 24 hours. DigiCert Europe does not use the ExpiredCertsOnCRL extension.

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. Regularly scheduled CRLs are posted prior to the nextUpdate field in the previously issued CRL of the same scope.

4.9.9. On-Line Revocation/Status Checking Availability

In addition to CRLs, DigiCert Europe also provides certificate status information via OCSP in accordance with RFC 6960. The OCSP service is updated immediately when a Certificate is revoked. OCSP responses are valid for a maximum of 48.5 hours. Where applicable, the URL for the OCSP responder may be found within the Authority Information Access (AIA) extension of the Certificate.

Upon expiry of the Issuing CA, the associated OCSP Responder service is discontinued. For Qualified and PKIoverheid Certificates, DigiCert Europe uses the OCSP ArchiveCutoff extension. DigiCert Europe does not compute a last OCSP answer for issued Certificates with the nextUpdate field set to "99991231235959Z".

OCSP responses of DigiCert Europe are signed by either:

- the Private Key for the CA which issued the Certificate for which the status is requested; or
- the Private Key of an OCSP Signing Certificate for an OCSP responder designated by DigiCert Europe;

In the latter case, 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" (see RFC6960).

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. The validity interval of an OCSP response is the difference in time between the thisUpdate and nextUpdate field, inclusive. For purposes of computing differences, a difference of 3,600 seconds shall be equal to one hour, and a difference of 86,400 seconds shall be equal to one day, ignoring leap-seconds.

DigiCert Europe supports an OCSP capability using the GET method for Certificates. OCSP responders under DigiCert Europe's direct control respond with an "unauthorised" status for Certificates that have not been issued. DigiCert Europe may monitor its OCSP responders for requests for non-issued Certificates as part of its security response procedures.

4.9.11. Other Forms Of Revocation Advertisements Available

No stipulation.

4.9.12. Special Requirements for Key Compromise

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

Reports to DigiCert Europe of key compromise must include:

- Proof of key compromise in either of the following formats:
    - A CSR signed by the compromised private key with the Common Name "Proof of Key Compromise for DigiCert"; or
    - The private key itself
- If a CSR is provided, DigiCert Europe will only accept proof of key compromise, if one of the following algorithms are used to sign the CSR:
    - SHA256WithRSA
    - SHA384WithRSA
    - SHA512WithRSA
    - ECDSAWithSHA256
    - ECDSAWithSHA384
    - ECDSAWithSHA512
    - SHA256WithRSAPSS
    - SHA384WithRSAPSS
    - SHA512WithRSAPSS
    - PureEd25519
- A valid email address so that you can receive confirmation of your problem report and associated certificate revocations.

4.9.13. Circumstances For Suspension

No suspension of Certificates is permissible within the DigiCert Europe PKIo.

4.9.14. Who Can Request Suspension

No suspension of Certificates is permissible within the DigiCert Europe PKIo.

4.9.15. Procedure For Suspension Request

No suspension of Certificates is permissible within the DigiCert Europe PKIo.

4.9.16. Limits On Suspension Period

No suspension of Certificates is permissible within the DigiCert Europe PKIo.

4.10. CERTIFICATE STATUS SERVICES

4.10.1. Operational Characteristics

Certificate status information is available via CRL and OCSP responder. Certificates, revocation entries on a CRL or OCSP Response are not removed until after the expiration of the revoked Certificate. The serial number of a revoked Certificate remains on the CRL until one additional CRL is published after the end of the Certificate's validity period.

4.10.2. Service Availability

Certificate status services are available 24x7. DigiCert Europe 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.

DigiCert Europe also maintains a 24x7 ability to respond internally to a high-priority certificate problem report, and where appropriate, forward such a complaint to law enforcement authorities, and/or revoke a Certificate that is the subject of such a complaint.

In the event the revocation status service becomes unavailable, DigiCert Europe aim to restore this availability within 4 hours.

4.10.3. Optional Features

No stipulation.

4.11. END OF SUBSCRIPTION

A Subscriber's subscription service ends if its Certificate expires or is revoked or if the applicable Subscriber Agreement expires without renewal.

4.12. KEY ESCROW AND RECOVERY

Within PKIoverheid, DigiCert Europe does not support key escrow.

4.12.1. Key Archival Escrow And Recovery Policy And Practices

No stipulation.

4.12.2. Session Key Encapsulation And Recovery Policy And Practices

No stipulation.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

The section of the CPS provides a high level description of the security policy, physical and logical access control mechanisms, service levels, and personnel policies used by DigiCert Europe to provide trustworthy

and reliable CA operations. DigiCert Europe maintains a security program to: i) Protect the confidentiality, integrity, and availability of data and business process; ii) Protect against anticipated threats or hazards to the confidentiality, integrity, and availability of data and business process; iii) Protect against unauthorised or unlawful access, use, disclosure, alteration, or destruction of data and business process; iv) Protect against accidental loss or destruction of, or damage to data and business processes; and v) Comply with all other security requirements applicable to the CA by law and industry best practices. DigiCert Europe performs an annual risk assessment to identify internal and external threats and assess likelihood and potential impact of these threats to data and business processes.

5.1. PHYSICAL CONTROLS

DigiCert Europe manages and implements appropriate physical security controls to restrict access to the hardware and software used in connection with CA operations.

5.1.1. Site Location and Construction

DigiCert Europe operations facilities are especially designed for computer operations and as such have been built to meet the security requirements that apply to QTSPs. The datacentres are equipped with logical and physical controls that make DigiCert Europe's CA and TSA operations inaccessible to non-trusted personnel. DigiCert Europe operates under a security policy designed to detect, deter, and prevent unauthorised access to DigiCert Europe's operations.

5.1.2. Physical Access

DigiCert Europe 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 DigiCert Europe Netherlands 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 DigiCert Europe staff.

5.1.3. Power And Air-Conditioning

Datacentres have primary and secondary power supplies that ensure continuous and uninterrupted access to electric power. Uninterrupted power supplies (UPS) and generators provide redundant backup power.

5.1.4. Water Exposures

The cabinets housing DigiCert Europe's CA systems are designed to prevent and protect against water exposure.

5.1.5. Fire Prevention And Protection

DigiCert Europe datacentres are equipped with fire suppression mechanisms.

5.1.6. Media Storage

DigiCert Europe protects its media from accidental damage, environmental hazards, unauthorised physical access, and from obsolescence/deterioration during the period that records are required to be retained. Backup files are created on a daily basis. DigiCert Europe backup files are maintained at either within the DigiCert Europe service operations area or in a secure off-site storage area.

5.1.7. Waste Disposal

All unnecessary copies of printed sensitive information are shredded on-site before disposal. All electronic media are physically destroyed or are overwritten multiple times to prevent the recovery of the data.

5.1.8. Off-Site Backup

An offsite location is used for the storage and retention of backup software and data. The off site storage is available to authorised personnel 24x7 for the purpose of retrieving software and data; and has appropriate levels of physical security in place (i.e., software and data are stored in fire-rated safes and containers which are located behind access-controlled doors in areas accessible only by authorised personnel).

5.2. PROCEDURAL CONTROLS

DigiCert Europe implements physical and technical security procedures in accordance with this CPS and other relevant internal operational documents. DigiCert Europe does not delegate PKI operations to other organisations, other than RA operations described in Section 1.3.2.

DigiCert Europe performs a risk analysis at least every year, and more frequently if instructed by the PKIo PA and/or NCSC. The risk analysis will cover all PKIoverheid processes that are under the responsibility of DigiCert Europe.

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. 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 – Portal, RA, Validation and Vetting Personnel

The Registration Officer role is responsible for issuing and revoking Certificates.

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 critical systems updated with software patches and other maintenance needed for system stability and recoverability.

5.2.1.4. Internal Auditors

Internal Auditors are responsible for reviewing, maintaining, and archiving audit logs and performing or overseeing internal compliance audits to determine if DigiCert Europe, an Issuing CA, or RA is operating in accordance with this CPS or approved registration procedures.

5.2.1.5. RA Administrators

RA Administrators are responsible for the RA certificate management systems.

5.2.1.6. Security Officers

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

5.2.2. Number Of Persons Required Per Task

DigiCert Europe ensures that the number of staff available for tasks is adequate to ensure that all security, risk, and compliance regulations are met.

DigiCert Europe 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 Each 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. Access privileges are configured using the "least privileges" principle for the role.

Employees in Trusted Roles use a Certificate issued by DigiCert Europe, 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 Requiring 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, DigiCert Europe specifically designates individuals to the trusted roles defined in Section 5.2.1 above. Individuals designated as Registration Officer or Administrator may perform Operator duties, but an Internal Auditor may not assume any other role. DigiCert Europe systems identify and authenticate individuals acting in trusted roles, and restrict an individual from assuming multiple roles at the same time.

5.3. PERSONNEL CONTROLS

5.3.1. Qualifications, Experience, And Clearance Requirements

Before issuing services Server Certificates, DigiCert Europe 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. A Verklaring Omtrent Gedrag (VOG or Declaration of Conduct) is required for all Netherlands employees.

DigiCert Europe is not liable for the conduct of employees who are outside the performance of their duties and over which DigiCert Europe 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 DigiCert Europe based on a valid Passport or National ID card.

For determining the reliability of the employee, DigiCert Europe 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 VOG from the employee.

5.3.3. Training Requirements

DigiCert Europe provides relevant skills training to all employees involved in PKI and TSA operations for the personnel performing information verification duties including:

- basic PKI knowledge;
- software versions used by DigiCert Europe;
- authentication and verification policies and procedures;
- DigiCert Europe security principles and mechanisms;
- disaster recovery and business continuity procedures;
- common threats to the validation process, including phishing and other social engineering tactics; and
- CA/Browser Forum guidelines and other applicable industry and government guidelines.

DigiCert Europe maintains records of who received training. 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 TLS and/or S/MIME Baseline Requirements (as relevant) prior to validating and approving the issuance of such Certificates.

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 as necessary for them to perform their role. DigiCert Europe makes all employees acting in trusted roles aware of any changes to DigiCert Europe's operations. If DigiCert Europe's operations change, DigiCert Europe will provide documented training, in accordance with an executed training plan, to all employees acting in relevant trusted roles to those changes.

5.3.5. Job Rotation Frequency And Sequence

No stipulation.

5.3.6. Sanctions For Unauthorised Actions

DigiCert Europe DigiCert employees and agents failing to comply with this CPS, whether through negligence or malicious intent, are subject to internally maintained processes specifying guidance on administrative or disciplinary actions, up to and including termination of employment or agency and criminal sanctions.

5.3.7. 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.

5.3.8. Documentation Supplied To Personnel

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

5.4. AUDIT LOGGING PROCEDURES

DigiCert Europe 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 DigiCert Europe 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 DigiCert Europe include, but are not limited to:

- CA Certificate and key lifecycle management events;
    - Certificate Requests, renewal, and re-key requests, and revocation;
    - Approval and rejection of Certificate Requests;
    - Cryptographic device lifecycle management events;
    - Generation of CRLs and OCSP entries; and
    - Certificate Profiles management.

- Subscriber Certificate lifecycle management events, including:
    - Certificate Requests, renewal, and re-key requests, and revocation;
    - Verification activities;
    - Approval and rejection of Certificate Requests;
    - Issuance of Certificates; and
    - Generation of CRLs and OCSP entries.
- Security events, including
    - Successful and unsuccessful PKI system access attempts;
    - PKI and security system actions performed;
    - Security profile changes;
    - Installation, update and removal of software on a PKI System;
    - System crashes, hardware failures, and other anomalies;
    - Relevant firewall and router activities; and
    - Entries to and exits from the CA facility.

All log entries provide at least the following:

- Date and time of the record;
- Identity of the entity making the journal record (when applicable); and
- Details of the of record.

5.4.1.1 Router and Firewall Activities Logs

Logging of router and firewall activities necessary to meet the requirements of Section 5.4.1, must at a minimum include:

1. Successful and unsuccessful login attempts to routers and firewalls; and
2. Logging of all administrative actions performed on routers and firewalls, including configuration changes, firmware updates, and access control modifications; and
3. Logging of all changes made to firewall rules, including additions, modifications, and deletions; and
4. Logging of all system events and errors, including hardware failures, software crashes, and system restarts.

5.4.2. Frequency Of Processing Log

As required, generally within at least once every two months, a DigiCert Europe administrator reviews the logs generated by DigiCert Europe's systems, makes system and file integrity checks, and conducts a vulnerability assessment. The administrator may perform the checks using automated tools. During these checks, the administrator (i) checks whether anyone has tampered with the log, (ii) scans for anomalies or specific conditions, including any evidence of malicious activity, and (iii) if necessary, prepares a written summary of

the review. Any anomalies or irregularities found in the logs are investigated. The summaries may include recommendations to DigiCert's operations management committee and are made available to auditors upon request. DigiCert Europe documents any actions taken as a result of a review.

5.4.3. Retention Period For Audit Log

DigiCert Europe log files for events related to Lifecycle events and certificate lifecycle events are retained for a period of 7 years before deletion starting from the destruction of the CA Private Key or revocation or expiration of the Certificate. Log files for incidents relating to threats and risks will be retained for 24 months and then deleted.

All logfiles are backed up daily. The logfiles are stored in such a way that the integrity and accessibility of the data is guaranteed. DigiCert Europe makes the audit logs available to auditors, as defined in Section 8, available upon request.

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 DigiCert Europe PKI. Only certain DigiCert Europe Trusted Roles and auditors may view audit logs in whole. DigiCert Europe 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 premises and storage at a secure, offsite 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

Where an event is logged, no notice is required to be given to the individual, organisation, device, or application that caused the event.

5.4.8. Vulnerability Assessment

DigiCert Europe performs annual risk assessments that identify and assess reasonably foreseeable internal and external threats that could result in unauthorised access, disclosure, misuse, alteration, or destruction of any certificate data or certificate issuance process. DigiCert Europe also routinely assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that DigiCert Europe has in place to control risks identified in risk assessments. DigiCert Europe's Internal Auditors review the security audit data checks for continuity. DigiCert Europe's 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.

DigiCert Europe performs monthly vulnerability scans on its available PKI systems and infrastructure. Identified vulnerabilities are rated on the basis of Common Vulnerability Scoring System (CVSS), and addressed based on the designation of Critical, High, Medium and Low.

Based on the risk assessment, DigiCert Europe develops, implements, and maintains a security plan consisting of security procedures, measures, and products designed to achieve the objectives set forth above and to manage and control the risks identified during the risk assessment, commensurate with the sensitivity of the certificate data and management processes.

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 DigiCert Europe 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. Types Of Records Archived

DigiCert Europe 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; and
- Audit findings as discussed within this CPS.

5.5.1.1. Storage of information

DigiCert Europe 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

DigiCert Europe 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 DigiCert Europe.

5.5.2. Retention Period For Archive

DigiCert Europe 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 or revocation date of the Certificate.

5.5.3. Protection Of Archive

Archive records are stored at a secure location and are maintained in a manner that prevents unauthorised modification, substitution, or destruction. Archives are not released except as allowed by the PMA or as

required by law. DigiCert Europe maintains any software application required to process the archive data until the data is either destroyed or transferred to a newer medium.

If DigiCert Europe 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. Archive Backup Procedures

DigiCert Europe maintains and implements backup procedures so that in the event of the loss or destruction of the primary archives a complete set of backup copies will be readily available.

5.5.5. Requirements For Time-Stamping Of Records

DigiCert Europe supports time stamping of all of its records. All events that are recorded within the DigiCert Europe service include the date and time of when the event took place. This date and time are based on the system time on which the CA program is operating. DigiCert Europe uses procedures to review and ensure that all systems operating within the DigiCert Europe PKIo rely on a trusted time source.

5.5.6. Archive Collection System

The DigiCert Europe Archive Collection System is internal.

5.5.7. Procedures To Obtain And Verify Archive Information

Access to archives is granted only to persons in Trusted Roles and based on least privilege. 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. DigiCert Europe 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, DigiCert Europe stops using this Private Key for signing public keys and only uses the expiring Private Key to sign CRLs and OCSP 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

DigiCert Europe has implemented procedures to minimise the consequence of disasters as much as possible. These measures include a Disaster Recovery Program and a CA Key Compromise Plan (see also Section 5.7.3).

- Incident investigation and reporting is the responsibility of the DigiCert Europe PMA.
- If an incident is verified the PKIo PA, the Supervisory Authority, the Conformity Assessment Body (CAB), the NCSC, and Subscribers are notified.

- In the case of loss of privacy sensitive information, incidents will be handled by the DigiCert Europe Data Protection Officer (DPO), and the Autoriteit Persoonsgevents (Dutch Data Protection Agency) will be informed.
- Noncompliance with Application Software Supplier policies are classified as an incident and will be reported in the appropriate forum.

DigiCert Europe will inform the PKIo PA immediately about the risks, dangers, or events that can directly or indirectly threaten or influence the security of the services and/or the image of the PKIoverheid.

5.7.2. Computing Resources, Software, and/or Data Are Corrupted

DigiCert Europe makes regular system backups on a weekly basis and maintains backup copies of its CA Private Keys, which are stored in a secure, separate location. If DigiCert Europe discovers that any of its computing resources, software, or data operations have been compromised, DigiCert Europe assesses the threats and risks that the compromise presents to the integrity or security of its operations or those of affected parties. If DigiCert Europe determines that a continued operation could pose a significant risk to Relying Parties or Subscribers, DigiCert Europe suspends such operation until it determines that the risk is mitigated.

5.7.3. Entity Private Key Compromise Procedures

In event of a compromise of a CA Private Key:

- The affected CA Certificate as well as its valid end entity Certificates are revoked;
- Subscribers are informed about the incident and its effects;
- The PKIo PA, the Supervisory Authority, the CAB, and the NCSC are notified; and
- A notice is provided on the DigiCert Europe website and Portal, including a statement that Certificates issued by the affected CA are no longer valid. See also Section 5.7.1.

Taking into account the reason for compromise, a new CA Key Pair will be generated to replace end entity Certificates.

5.7.4. Business Continuity Capabilities after a Disaster

DigiCert Europe 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 TLS Baseline Requirements and PKIoverheid Program of Requirements. The BCP is a confidential document and has been audited and approved by external auditors.

5.8. CA AND/OR RA TERMINATION

Unless otherwise addressed in an applicable agreement between DigiCert Europe and a counterparty, before terminating its CA or RA activities, DigiCert Europe may:

i. Notify relevant Government and Certification bodies under applicable laws and related regulations;

ii. Provide notice and information about the termination by sending notice by email to its Subscribers, Relying Parties and other relevant parties within PKIoverheid; and

iii. Transfer all responsibilities to a qualified successor entity.

Unless otherwise addressed in an applicable agreement between DigiCert Europe and a counterparty, if a qualified successor entity does not exist, DigiCert Europe will:

i. transfer those functions capable of being transferred to a reliable third party and arrange to preserve all relevant records with a reliable third party or a government, regulatory, or legal body with appropriate authority;

ii. revoke all Certificates that are still un-revoked or un-expired on a date as specified in the notice and publish final CRLs;

iii. destroy all Private Keys; and

iv. make other necessary arrangements that are in accordance with this CPS.

For EU Qualified Certificates, DigiCert Europe procedures provide for the transfer of relevant records to a regulatory body and the continuation of revocation status in the event of termination.

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 DigiCert Europe within PKIoverheid. This requires that Subjects and 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

DigiCert Europe 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. In the case that a QSCD used by DigiCert Europe for QCPn-qscd or QCP-l-qscd loses its certification status, non-expired Certificates using the affected QCSD will be revoked.

The DigiCert Europe shall reject a certificate request if one or more of the following conditions are met:

1. The Key Pair does not meet the requirements set forth in Section 6.1.5 and/or Section 6.1.6;

2. There is clear evidence that the specific method used to generate the Private Key was flawed;
3. DigiCert Europe is aware of a demonstrated or proven method that exposes the Applicant's Private Key to compromise;
4. DigiCert Europe has previously been notified that the applicant's Private Key has suffered a Key Compromise using DigiCert Europe's procedure for revocation request as described in Section 4.9.3 and Section 4.9.12;
5. The Public Key corresponds to an industry-demonstrated weak Private Key. For requests submitted on or after November 15, 2024, at least the following precautions shall be implemented:
    1. In the case of Debian weak keys vulnerability (https://wiki.debian.org/SSLkeys), DigiCert Europe shall reject all keys found at https://github.com/cabforum/Debian-weak-keys/ for each key type (e.g. RSA, ECDSA) and size listed in the repository. For all other keys meeting the requirements of Section 6.1.5, with the exception of RSA key sizes greater than 8192 bits, the Issuer CA shall reject Debian weak keys.
    2. In the case of ROCA vulnerability, the Issuer CA shall reject keys identified by the tools available at https://github.com/crocs-muni/roca or equivalent.
    3. In the case of Close Primes vulnerability (https://fermatattack.secvuln.info/), DigiCert Europe shall reject weak keys which can be factored within 100 rounds using Fermat's factorization method.

6.1.1.4. Algorithm of key pairs of the Subscribers

With exception of the Certificate policy Private Service Server DigiCert Europe 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 DigiCert Europe manages the keys on behalf of the Subscriber, DigiCert Europe 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. Private Key Delivery To Subscriber

Subscribers can choose to have their Key Pair generated by DigiCert Europe, or to generate it themselves.

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

For some Qualified Certificates DigiCert Europe may generate the Private Keys on behalf of the Subscriber; they are delivered in a secure manner via the DigiCert Europe Portal.

For some EU Qualified Certificates, DigiCert Europe may generate and manage 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. Public Key Delivery To Certificate Issuer

Except as noted in Section 6.1.2, 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 the DigiCert Europe Portal.

6.1.4. CA Public Key To Relying Parties

DigiCert Europe's Public Keys are provided to Relying Parties as specified in a certificate validation or path discovery policy file, as trust anchors in root stores or an EU Trusted List, and/or as roots signed by PKIoverheid. All accreditation authorities supporting DigiCert Europe Certificates and all Application Software Providers are permitted to redistribute DigiCert Europe root anchors.

DigiCert Europe may also distribute Public Keys that are part of an updated signature Key Pair as a self-signed Certificate, as a new CA Certificate, or in a key roll-over Certificate. Relying Parties may also obtain DigiCert Europe CA Certificates from DigiCert Europe's web site or by email.

6.1.5. Key Sizes

The minimal key length for the DigiCert Europe PKIoverheid CAs is 2048-bits. DigiCert Europe supports higher-bits keys for certain Certificates as determined by customer request. The keys are based on sha256WithRSAEncryption. The length of the Subscriber's cryptographic keys must fulfill the requirements defined in ETSI TS 119 312.

Signatures on CRLs, OCSP responses, and OCSP responder Certificates that provide status information forCertificates that were generated using SHA-1 may continue to be generated using the SHA-1 algorithm if it is compliant with all applicable programs listed in Section 1.1. All other signatures on CRLs, OCSP responses, and OCSP responder Certificates must use the SHA-256 hash algorithm or one that is equally or more resistant to collision attack.

6.1.6. Public Key Parameters Generation And Quality Checking

DigiCert Europe uses cryptographic modules that conform to FIPS 186-2 and provide 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. Key Usage Purposes (As Per X.509 V3 Key Usage Field)

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

6.2. PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1. Cryptographic Module Standards And Controls

The Private Keys of DigiCert Europe 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 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 of M) Multi-Person Control

DigiCert Europe's authentication mechanisms are protected securely when not in use and may only be accessed by actions of multiple trusted persons. Backups of CA Private Keys are securely stored and require two-person access. Re-activation of a backed-up CA Private Key (unwrapping) requires the same security and multiperson control as when performing other sensitive CA Private Key operations.

6.2.3. Private Key Escrow

DigiCert Europe does not support Private Key Escrow for PKIoverheid Certificates.

6.2.4. Private Key Backup

DigiCert Europe's CA Private Keys are generated and operated inside cryptographic modules which have been evaluated to at least FIPS 140-2 Level 3. When keys are transferred to other media for backup and disaster recovery purposes, the keys are transferred and stored in an encrypted form. DigiCert Europe's CA Key Pairs are backed up by multiple trusted individuals using a cryptographic hardware device as part of scripted key backup process.

DigiCert Europe does not backup Subscriber Private Keys.

6.2.5. Private Key Archive

DigiCert Europe does not archive CA Certificate Private Keys or Subscriber Private Keys.

6.2.6. Private Key Transfer Into Or From A Cryptographic Module

All CA keys must be generated by and in a cryptographic module. Private Keys are exported from the cryptographic module into backup tokens only for HSM transfer, offline storage, and backup purposes. The Private Keys are encrypted when transferred out of the module and never exist in plaintext form. When transported between cryptographic modules, DigiCert Europe encrypts the Private Key and protects the keys used for encryption from disclosure. Private Keys used to encrypt backups are securely stored and require twoperson access. If DigiCert Europe becomes aware that an Issuing CA's Private Key has been communicated to an unauthorized person or an organization not affiliated with the Issuing CA, then DigiCert Europe will revoke all Certificates that include the Public Key corresponding to the communicated Private Key.

6.2.7. Private Key Storage On Cryptographic Module

CA Private Keys are generated and stored in a physically secure environment within cryptographic modules that are validated to FIPS 140-2 Level-3. Root CA Private Keys are stored offline in cryptographic modules or backup tokens as described above in Sections 6.2.2, 6.2.4, and 6.2.6.

6.2.8. Method Of Activating Private Key

DigiCert Europe's Private Keys are activated according to the specifications of the HSM manufacturer. Activation data entry is protected from disclosure.

6.2.9. Method Of Deactivating Private Key

The Private Key of operational DigiCert Europe PKIoverheid CAs are not normally deactivated but remain 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 Of Destroying Private Key

DigiCert Europe personnel, acting in trusted roles, destroy CA, RA, and status server Private Keys when no longer needed. DigiCert Europe may destroy a Private Key by deleting it from all known storage partitions. DigiCert Europe also zeroizes the HSM device and associated backup tokens according to the specifications of the hardware manufacturer. This reinitializes the device and overwrites the data with binary zeros. If the zeroization or reinitialization procedure fails, DigiCert Europe will crush, shred, and/or incinerate the device in a manner that destroys the ability to extract any Private Key. Such destruction shall be 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 QSCD. Where DigiCert Europe manages the QSCD on behalf of the Subscriber, DigiCert Europe operates the QSCD in accordance with Annex II of the eIDAS Regulation.

DigiCert Europe verifies that QSCDs are certified as a QSCD in accordance requirements laid down in Annex II of the eIDAS Regulation. DigiCert Europe 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 DigiCert Europe monitoring are in scope of the external eIDAS/ ETSI conformity assessments.

6.3. OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1. Public Key Archival

Public Keys will be recorded in Certificates that will be archived in the Repository. No separate archive of Public Keys will be maintained. Archived information is retained for at least 7 years after the expiry of the Certificate.

6.3.2. Certificate Operational Periods And Key Pair Usage Periods

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 DigiCert Europe CA used is always longer than the specified validity of the Certificate for the Subscriber. The maximum validity of end-user Certificates is 3 years, and for TLS Server Certificates 398 days. An overview of the current validity of the different DigiCert Europe CAs is as follows:

Issuing CA	Valid to	Version
QuoVadis PKIoverheid Burger CA - 2021	12-Nov-28	-
QuoVadis PKIoverheid Organisatie Persoon CA - G3	11-Nov-28	G3

Issuing CA	Valid to	Version
QuoVadis PKIoverheid Organisatie Persoon CA-2022	11-Nov-28	G3
QuoVadis PKIoverheid Organisatie Services CA - G3	11-Nov-28	G3
QuoVadis PKIoverheid Organisatie Services CA-2022	11-Nov-28	G3
QuoVadis PKIoverheid Private Personen CA - G1	11-Nov-28	G1
QuoVadis PKIoverheid Private Services CA - G1	11-Nov-28	G1

For the purpose of calculations, a day is measured as 86,400 seconds. Any amount of time greater than this, including fractional seconds and/or leap seconds, represents an additional day. For the purposes of calculating time periods in this document, increments are rounded down subject to the imposed maximums of the requirements listed in Section 1.1 as applicable.

6.4. ACTIVATION DATA

6.4.1. Activation Data Generation And Installation

DigiCert Europe 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 as explained in Section 5.2.2 and elsewhere in this CPS. DigiCert Europe will only transmit activation data via an appropriately protected channel and at a time and place that is distinct from the delivery of the associated cryptographic module.

DigiCert Europe 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 and other relevant standards.

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

DigiCert Europe has a formal Information Security Policy that documents the DigiCert Europe policies, standards and guidelines relating to information security. This Information Security Policy has been approved by management and is communicated to all employees.

6.5.1. Specific Computer Security Technical Requirements

DigiCert Europe secures its CA systems and authenticates and protects communications between its systems and trusted roles. DigiCert Europe's 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. Inactivity log out timeframes are set and enforced through internal information security policies and procedures to ensure security.

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

i. authenticate the identity of users before permitting access to the system or applications;

ii. manage privileges to limit users to their assigned roles;

iii. enforce domain integrity boundaries for security critical processes; and

iv. support recovery from key or system failure.

DigiCert Europe enforces multi-factor authentication on any Portal account capable of directly causing certificate issuance.

6.5.2. Computer Security Rating

A version of the core CA software used by DigiCert Europe has obtained the Common Criteria EAL 4+ certification.

6.6. LIFE CYCLE TECHNICAL CONTROLS

6.6.1. System Development Controls

DigiCert Europe uses standard products from accredited suppliers who fulfil the security classifications required by the PKIoverheid PvE (see 6.1 and 6.2). DigiCert Europe 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 DigiCert Europe and used for use in services within PKIoverheid is developed in a controlled environment which fulfils strict safety requirements. The software developed within DigiCert Europe 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

DigiCert Europe has mechanisms in place to control and continuously monitor the security-related configurations of its CA systems. When loading software onto a CA system, DigiCert Europe 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

DigiCert Europe conforms to the CA/Browser Forum Network Security Controls as well as network security requirements from PKIoverheid. DigiCert Europe ensures that all PKIoverheid systems relating to the registration service, certificate generation service, subject device provision service, dissemination service, revocation management service and revocation status service:

- Are equipped with the latest updates;
- The web application controls and filters all input by users;
- The web application codes the dynamic output;
- The web application maintains a secure session with the user; and
- The web application uses a secured database.

DigiCert Europe use the NCSC's "Security of Web Applications Checklist" as guidance.

DigiCert Europe carry out monthly security scans on all PKI infrastructure and documents the results of these security scans and any measures taken.

DigiCert Europe arranges a yearly penetration test to be performed on the PKIoverheid infrastructure. In the event of any significant change to the PKIoverheid infrastructure then DigiCert Europe will arrange additional penetration testing. Significant changes include:

- New software;
- New versions of existing software (excluding patches); and
- Significant changes in infrastructure.

DigiCert Europe is obliged to comply with instructions from the PKIo PA to carry out additional penetration tests when requested.

6.8. TIME-STAMPING

DigiCert Europe does not provide time stamps within the PKIoverheid framework. A separate DigiCert Europe TimeStamp Policy/Practice Statement, structured in accordance with ETSI EN 319 421, describes DigiCert Europe's commercial service.

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1. CERTIFICATE PROFILE

DigiCert Europe only uses approved Certificate Profiles for the issuance of PKIoverheid Certificates. See Appendix A.

7.1.1. Version Numbers

Information for interpreting Certificate and CRL Profiles may be found in IETF RFC 5280. DigiCert Europe Certificates for PKIoverheid follow the ITU X.509v3 standard and the PKIoverheid PvE.

For publicly-trusted Certificates, DigiCert Europe meets the technical requirements set forth in Sections 2.2, 6.1.5, and 6.1.6 of the CA/Browser Forum TLS and/or S/MIME Baseline Requirements (as relevant) and this CPS.

7.1.2. Serial Number

The serial number is no longer than 160 bits (20 octets) ECC Certificates. DigiCert Europe may 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

DigiCert Europe generates non-sequential certificate serial numbers (positive numbers greater than zero) that contain at least 64 bits of output from a CSPRNG.

7.1.3. Certificate Extensions

See Appendix A.

7.1.4. Algorithm Object Identifiers

See Appendix A.

7.1.5. Name Forms

Each Certificate includes a serial number that is unique to the Issuing CA. TLS Server Certificates cannot contain metadata and/or any other indication that the value is absent, incomplete, or not applicable. Certificates are populated with the Issuer Name and Subject Distinguished Name required under Section 3.1.1.

7.1.6. Name Constraints

All Certificates are configured to meet the applicable requirements, including Regulation (EU) No. 910/2014, TLS and/or S/MIME Baseline Requirements (as relevant), ETSI EN 319 411-1, ETSI EN 319 411-2 and PvE (Logius, PKIoverheid).

7.1.7. Certificate Policy Object Identifier

Certificate Policy object identifiers (OIDs) are described in Section 1.2.

7.1.8. Usage Of Policy Constraints Extension

No stipulation.

7.1.9. Policy Qualifiers Syntax And Semantics

DigiCert Europe Certificates include a brief statement in the Policy Qualifier field of the Certificate Policy extension to inform potential Relying Parties on notice of the limitations of liability and other terms and conditions on the use of the Certificate, including those contained in this CPS, which are incorporated by reference into the Certificate.

7.1.10. Processing Semantics For The Critical Certificate Policies Extension

No stipulation.

7.2. CRL PROFILE

If present, this extension cannot be marked critical. This extension must be present for a Root CA or Issuing CA Certificate, including Cross Certificates. This extension may be present for Certificates not technically capable of causing issuance, subject to the requirement that the CRLReason cannot be certificateHold (6).

If a reasonCode CRL entry extension is present, the CRLReason must indicate the most appropriate reason for revocation of the Certificate unless the reason is unspecified. DigiCert Europe may use the following reasonCode values from RFC 5280:

- keyCompromise (1)
- affiliationChanged (3)
- superseded (4)
- cessationOfOperation (5)

In addition, DigiCert Europe administrators may assign the reasonCode for cACompromise (2) or privilegeWithdrawn (9).

For TLS Server Certificates issued on or after October 1, 2022 DigiCert Europe or a Subscriber are obligated to use the following CRLReasons appropriate for their revocation circumstances:

keyCompromise

The CRLReason keyCompromise will be used when one or more of the following occurs:

- DigiCert Europe obtains verifiable evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a key compromise; or
- DigiCert Europe is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise; or
- There is clear evidence that the specific method used to generate the Private Key was flawed; or
- DigiCert Europe is made aware of a demonstrated or proven method that can easily compute the Subscriber's Private Key based on the Public Key in the Certificate (such as a Debian weak key, see https://wiki.debian.org/TLSkeys); or
- the Subscriber requests that DigiCert Europe revoke the Certificate for this reason, with the scope of revocation being described below.

If anyone requesting revocation for keyCompromise has previously demonstrated or can currently demonstrate possession of the Private Key of the Certificate, then DigiCert Europe will revoke all instances of that key across all Subscribers.

If the Subscriber requests that DigiCert Europe revoke the Certificate for keyCompromise, and has not previously demonstrated and cannot currently demonstrate possession of the associated Private Key of that Certificate, DigiCert Europe may revoke all Certificates associated with that Subscriber that contain that public key.

When DigiCert Europe obtains verifiable evidence of Private Key compromise for a Certificate whose CRL entry does not contain a reasonCode extension or has a reasonCode extension with a non-keyCompromise reason, DigiCert Europe may update the CRL entry to enter keyCompromise as the CRLReason in the reasonCode extension. Additionally, DigiCert Europe may update the revocation date in a CRL entry when it is determined that the Private Key of the Certificate was compromised prior to the revocation date that is indicated in the CRL entry for that Certificate.

privilegeWithdrawn

The CRLReason privilegeWithdrawn is intended to be used when there has been a Subscriber-side infraction that has not resulted in keyCompromise, such as the Subscriber provided misleading information in their Certificate request or has not upheld their material obligations under the Subscriber agreement or terms of use. Unless keyCompromise is being used, privilegeWithdrawn must be used when:

- DigiCert Europe obtains evidence that the Certificate was misused; or
- DigiCert Europe is made aware that the Subscriber has violated one or more of its material obligations under the Subscriber agreement or terms of use; or
- DigiCert Europe is made aware that a wildcard Certificate has been used to authenticate a fraudulently misleading subordinate fully-qualified domain name; or
- DigiCert Europe is made aware of a material change in the information contained in the Certificate; or
- DigiCert Europe determines or is made aware that any of the information appearing in the Certificate is inaccurate; or
- DigiCert Europe is made aware that the original Certificate request was not authorized and that the Subscriber does not retroactively grant authorization.

Otherwise, privilegeWithdrawn must not be used.

cessationOfOperation

The CRLReason cessationOfOperation is intended to be used when the website with the Certificate is shut down prior to the expiration of the Certificate, or if the Subscriber no longer owns or controls the domain name in the Certificate. This revocation reason is intended to be used in the following circumstances:

- the Subscriber no longer controls, or is no longer authorized to use, all of the domain names in the Certificate; or
- the Subscriber will no longer be using the Certificate because they are discontinuing their website; or
- DigiCert Europe is made aware of any circumstance indicating that use of a fully-qualified domain name or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has

revoked a domain name registrant's right to use the domain name, a relevant licensing or services agreement between the domain name registrant and the Applicant has terminated, or the domain name registrant has failed to renew the domain name).

Unless keyCompromise is being used, cessationOfOperation must be used when:

- the Subscriber has requested that their Certificate be revoked for this reason; or
- DigiCert Europe received verifiable evidence that the Subscriber no longer controls, or is no longer authorized to use, all of the domain names in the Certificate.

Otherwise, cessationOfOperation must not be used.

affiliationChanged

The CRLReason affiliationChanged is intended to be used to indicate that the Subject's name or other subject identity information in the Certificate has changed, but there is no cause to suspect that the Certificate's Private Key has been compromised.

Unless CRLReason is being used, affiliationChanged will be used when:

- the Subscriber has requested that their Certificate be revoked for this reason; or
- DigiCert Europe replaced the Certificate due to changes in the Certificate's subject information and the CA has not replaced the Certificate for the other reasons: keyCompromise, superseded, cessationOfOperation, or privilegeWithdrawn.

Otherwise, affiliationChanged must not be used.

superseded The CRLReason superseded is intended to be used to indicate when: * the Subscriber has requested a new Certificate to replace an existing Certificate; or * DigiCert Europe obtains reasonable evidence that the validation of domain authorization or control for any fully-qualified domain name or IP address in the Certificate should not be relied upon; or * DigiCert Europe revoked the Certificate for compliance reasons such as the Certificate does not comply with the DigiCert Europe CP/CPS, this CPS, the CA/Browser Forum's TLS and/or SMIME Baseline Requirements (as relevant), or the Mozilla Root Store Policy.

Unless the keyCompromise is being used, superseded must be used when:

- the Subscriber has requested that their Certificate be revoked for this reason; or
- DigiCert Europe revoked the Certificate due to domain authorization or compliance issues other than those related to keyCompromise or privilegeWithdrawn.

Otherwise, superseded must not be used.

7.2.1. Version Number

DigiCert Europe issues X.509 version 2 CRLs that may contain the following fields per requirements:

Basic Contents	Value	Demarcation
Issuer.CountryName	NL	Fixed
Issuer.OrganisationName	QuoVadis Trustlink BV	Fixed
Issuer.OrgIdentifier	NTRNL-30237459	Fixed

Basic Contents	Value	Demarcation
Issuer.CommonName	Common name of the relevant issuer	Fixed
Effective date	Date	Required
Next update	Date	Required
SignatureAlgorithm	sha256RSA	Fixed
Revoked Certificates	List of revoked Certificates: - Serial Number - Revocation Date and Time - Revocation Reason	Required

7.2.2. CRL And CRL Entry Extensions

DigiCert Europe CRLs may have the following extensions per RFC 5280 and other requirements:

Extension	Value
CRL Number	Never repeated monotonically increasing integer
Authority Key Identifier	Subject Key Identifier of the CRL issuer Certificate
Invalidity Date	[Optional date in UTC format]
Reason Code	Reason for revocation as described in Section 7.2
Issuing Distribution Point	Configured per RFC 5280 requirements, if included.

7.3. ONLINE CERTIFICATE STATUS PROTOCOL PROFILE

7.3.1. OCSP Version Numbers

OCSP Version 1, as defined by RFC 6960, is supported. OCSP Responder Certificates have a maximum validity of 12 months.

7.3.2. OCSP Extensions

The OCSP Certificate profile below provides an overview of the Certificate profile as issued in accordance with the PKIoverheid Program of Requirements

Basic Contents	Value	Demarcation
SignatureAlgorithm	sha256RSA	Fixed
Issuer.CountryName	NL	Fixed
Issuer.OrganisationName	QuoVadis Trustlink BV	Fixed
Issuer.OrganisationIdentifier	NTRNL-30237459	Fixed

Basic Contents	Value	Demarcation
Issuer.CommonName	Common name of the relevant issuer	Fixed
Validity.NotBefore	Date and Time	Required
Validity.NotAfter	Date and Time	Required
Subject.CommonName	QuoVadis OCSP Authority Signature	Required
Subject.OrganisationName	QuoVadis Limited or DigiCert Bermuda Limited	Required
Subject.CountryName	NL	Required
Subject.PublicKeyInfo	RSA (2048 bit) / System Generated	Required
Extensions		**Fixed**
KeyUsage (CRITICAL)	Digital Signature	Fixed
CertificatePolicies	G3: - Organisation Person: 2.16.528.1.1003.1.2.5.1 - Organisation Services: 2.16.528.1.1003.1.2.5.4 - Citizen: 2.16.528.1.1003.1.2.3.1 Private Root: - 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	OCSP Signing	Fixed
ocspNoCheck	Null	Fixed

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1. FREQUENCY, CIRCUMSTANCE AND STANDARDS OF ASSESSMENT

DigiCert Europe is a TSP as referred to in Regulation (EU) No. 910/2014 (the eIDAS framework) and DigiCert Europe operations under this CPS comply with the applicable requirements of the following standards and regulations:

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

- Regulation (EU) No. 910/2014
- CA/Browser Forum Network and Certificate System Security Requirements
- CA/Browser Forum TLS Baseline Requirements and S/MIME Baseline Requirements
- GDPR – EU 2016/679
- PKIoverheid Programma van Eisen (PvE) or Program of Requirements (PoR)

Rijksinspectie Digitale Infrastructuur supervises DigiCert Europe for compliance with eIDAS (Regulation (EU) No. 910/2014). DigiCert Europe undergoes conformity assessment for compliance with ETSI EN 319 411-1, 319 411-2, and other relevant standards on an annual basis.

External auditors are independent and have no business interests or business affiliation with DigiCert Europe, DigiCert or affiliated companies. Audits are carried out by external auditors at least annually. 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
- Cryptographic Controls
- Operation Security
- Network Security
- Logical and Physical Access
- Logging and Monitoring
- Human Resource Security
- Business Continuity Management
- Compliance
- Asset Management
- Termination Plans

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

DigiCert Europe 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.

8.2. IDENTITY AND QUALIFICATIONS OF ASSESSOR

ETSI Conformity Assessment Bodies must meet the requirements of the relevant national accrediting authority. Auditors shall be experienced in performing information security audits, specifically having significant experience with PKI and cryptographic technologies.

8.3. ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

DigiCert Europe and the assessors do not have any other relationship that would impair their independence and objectivity under Generally Accepted Auditing Standards. These relationships include financial, legal, social or other relationships that could result in a conflict of interest.

8.4. TOPICS COVERED BY ASSESSMENT

Audits as applicable cover DigiCert Europe's business practices disclosure, the integrity of DigiCert Europe's PKIo operations, and an Issuing CAs' compliance with this CPS and referenced requirements. Audits verify that DigiCert Europe is compliant with the CPS and applicable standards and regulatory requirements.

8.5. ACTIONS TAKEN AS A RESULT OF DEFICIENCY

If an audit reports a material noncompliance with applicable law, this CPS, or any other contractual obligations related to DigiCert Europe's services, then (i) the auditor will document the discrepancy, (ii) the auditor will promptly notify DigiCert Europe, and (iii) DigiCert Europe will develop a Corrective Action Plan (CAP) to cure the noncompliance. DigiCert Europe will submit the plan to the PMA for approval and to any third party that DigiCert Europe is legally obligated to satisfy. The PMA may require additional action if necessary to rectify any significant issues created by the non-compliance, including requiring revocation of affected Certificates. DigiCert Europe is entitled to suspend and/or terminate of services through revocation or other actions as deemed by the PMA to address the noncompliant Issuing CA

8.6. PUBLICATION OF AUDIT RESULTS

The results of each audit are reported to the PMA and to any third-party entities which are entitled by law, regulation, or agreement to receive a copy of the audit results. The results of the most recent audits of DigiCert Europe are posted at https://www.quovadisglobal.com/accreditations/.

8.7. SELF AUDITS

DigiCert Europe controls service quality by performing quarterly self-audits against a randomly selected sample of TLS Server Certificates being no less than three percent of the Certificates issued. Audits of other Certificate types will be at the discretion of DigiCert Europe to gain reasonable assurance of compliance to applicable requirements.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1. FEES

9.1.1. Certificate Issuance Or Renewal Fees

DigiCert Europe charges fees for verification, certificate issuance and renewal. DigiCert Europe may change its fees at any time in accordance with the applicable customer agreement.

9.1.2. Certificate Access Fees

DigiCert Europe may charge a reasonable fee for access to its certificate databases.

9.1.3. Revocation Or Status Information Access Fees

DigiCert Europe does not charge a certificate revocation fee or a fee for checking the validity status of an issued Certificate using a CRL. DigiCert Europe may charge a fee for providing customised CRLs, OCSP services, or other value-added revocation and status information services. DigiCert Europe does not permit access to revocation information, certificate status information, or time stamping in their Repositories by third parties that provide products or services that utilise such certificate status information without DigiCert Europe's prior express written consent.

9.1.4. Fees For Other Services

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

9.1.5. Refund Policy

DigiCert Europe may establish a refund policy, details of which may be contained in relevant contractual agreements.

9.2. FINANCIAL RESPONSIBILITIES

9.2.1. Insurance Coverage

DigiCert Europe maintains Commercial General Liability insurance with a policy limit of at least $2 million in coverage and Professional Liability/Errors & Omissions insurance with a policy limit of at least $5 million in coverage. Insurance is carried through companies rated no less than A- as to Policy Holder's Rating in the current edition of Best's Insurance Guide (or with an association of companies, each of the members of which are so rated).

More details about liability and insurance are in the Terms and Conditions and the contractual agreements between the Subscriber, Relying Parties and DigiCert Europe. DigiCert Europe does not provide for any other undertakings, guarantees and/or commitments than those explicitly provided for in the Terms of Use and the contractual agreements.

9.2.2. Other Assets

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

9.2.3. Insurance Or Warranty Coverage For End-Entities

No stipulation.

9.3. CONFIDENTIALITY OF BUSINESS-SENSITIVE DATA

9.3.1. Scope Of Confidential Information

DigiCert Europe keeps the following types of information confidential and maintains reasonable controls to prevent the exposure of such records to non-trusted personnel.

i. Private Keys;

ii. Activation data used to access Private Keys or to gain access to the CA system;

iii. Business continuity, incident response, contingency, and disaster recovery plans;

iv. Other security practices used to protect the confidentiality, integrity, or availability of information;

v. Information held by DigiCert Europe as private information in accordance with Section 9.4;

vi. Audit logs and archive records; and

vii. Transaction records, financial audit records, and external or internal audit trail records and any audit reports (with the exception of an auditor's letter confirming the effectiveness of the controls set forth in this CPS).

9.3.2. Information Not Within The Scope Of Confidential Information

Information appearing in Certificates or stored in the Repository is considered public and not within the scope of confidential information, unless statutes or special agreements so dictate.

9.3.3. Responsibility To Protect Private Information

DigiCert Europe employees, agents, and contractors are responsible for protecting confidential information and are contractually obligated to do so. Employees receive training on how to handle confidential information.

9.4. PRIVACY OF PERSONAL INFORMATION

9.4.1. Privacy Plan

DigiCert Europe follows the Privacy Notices posted on its website when handling personal information. See https://www.quovadisglobal.com/privacy-policy/ which includes privacy information for Remote Identity Verification. Personal information is only disclosed when the disclosure is required by law or when requested by the subject of the personal information. Such privacy policies shall conform to applicable local privacy laws and regulations including the Council Directive 95/46/EC of the European Parliament and the Swiss Federal Act on Data Protection of June 19, 1992 (SR 235.1).

9.4.2. Information Treated As Private

Personal information about an individual that is not publicly available in the contents of a Certificate or CRL is considered private. DigiCert Europe protects private information using appropriate safeguards and a reasonable degree of care.

9.4.3. Information Deemed Not Private

Certificates, CRLs, and personal or corporate information appearing in them are not considered private. This DigiCert Europe CPS is a public document and is not confidential information and is not treated as private.

9.4.4. Responsibility To Protect Private Information

DigiCert Europe employees and contractors are expected to handle personal information in strict confidence and meet the requirements of US and European law concerning the protection of personal data. DigiCert Europe will not divulge any private Subscriber information to any third party for any reason, unless compelled to do so by law or competent regulatory authority. All sensitive information is securely stored and protected against accidental disclosure.

9.4.5. Notice And Consent To Use Private Information

In the course of accepting a Certificate, individuals have agreed to allow their personal data submitted in the course of registration to be processed by and on behalf of the DigiCert Europe CA, and used as explained in the registration process. They have also been given an opportunity to decline from having their personal data used for particular purposes. They have also agreed to let certain personal data to appear in publicly accessible directories and be communicated to others.

9.4.6. Disclosure Pursuant To Judicial Or Administrative Process

If required by a legitimate and lawful judicial order or regulation that complies with requirements of this CPS, DigiCert Europe may disclose private information without notice.

9.5. INTELLECTUAL PROPERTY RIGHTS

DigiCert Europe owns the intellectual property rights in DigiCert Europe's services, including the Certificates, trademarks and the Proprietary Marks used in providing the services, and this CPS.

For the avoidance of doubt, external documents or electronic records signed or protected using DigiCert Europe Certificates are not considered to be DigiCert Europe documents for the purposes of this section, nor is DigiCert Europe responsible for the content of those documents or records.

Intellectual property rights and restrictions thereof are described in the Subscriber Agreements. DigiCert Europe indemnifies the Subscriber in respect of claims by third parties due to violations of intellectual property rights by DigiCert Europe.

9.5.1. Property Rights in Certificates and Revocation Information

DigiCert Europe retains all intellectual property rights in and to the Certificates and revocation information that it issues. DigiCert Europe and customers shall grant permission to reproduce and distribute Certificates on a nonexclusive royalty-free basis, provided that they are reproduced in full and that use of Certificates is subject to the Relying Party Agreement referenced in the Certificate. DigiCert Europe, and customers shall grant permission to use revocation information to perform Relying Party functions subject to the applicable CRL usage agreement, Relying Party Agreement, or any other applicable agreements.

9.5.2. Property Rights in the CPS

Issuing CAs acknowledge that DigiCert Europe retains all intellectual property rights in and to this CPS.

9.5.3. Property Rights in Names

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

9.5.4. Property Rights in Keys and Key Material

Key Pairs corresponding to Certificates of CAs and end-user Subscribers are the property of DigiCert Europe and end-user Subscribers that are the respective subjects of the Certificates, regardless of the physical medium within which they are stored and protected, and such persons retain all intellectual property rights in and to these Key Pairs. Without limiting the generality of the foregoing, DigiCert Europe Root Public Keys and the Root CA Certificates containing them, including all Public Keys and self-signed Certificates, are the property of DigiCert Europe. DigiCert Europe licenses software and hardware manufacturers to reproduce such Root and CA Certificates to place copies in trustworthy hardware devices or software

9.5.5. Violation of Property Rights

Issuing CAs shall not knowingly violate the intellectual property rights of any third party.

9.6. REPRESENTATIONS AND WARRANTIES

9.6.1. Certification Authority Representations

DigiCert Europe 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 DigiCert Europe 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.

DigiCert Europe is only liable in respect to Certificate Subscribers or Relying Parties for immediate loss resulting from the violation by DigiCert Europe 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).

DigiCert Europe 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.

- DigiCert Europe can, at the direction of the PKIo PA, include restrictions on its use in the signature Certificate, provided the relevant restrictions are clear to third parties. DigiCert Europe is not liable for damage resulting from the use of a signature/non-repudiation Certificate in violation of such an included restriction. DigiCert Europe does not accept any form of liability for damage suffered by Relying Parties, with the following exceptions:
- DigiCert Europe is, in principle, liable in accordance with Article 6.19b, first to third paragraphs, of the Dutch Civil Code, on the understanding that:
    - “a Qualified Certificate as referred to in Article 1.1. section ss Telecommunications Act” is read as follows: "an Authentication Certificate"
    - "Signatory": is read as: “Subscriber”;
    - "Electronic Signatures" is read as: "Authentication characteristics".
    - DigiCert Europe is, in principle, liable in accordance with Article 6.19b, first to third paragraphs, of the Dutch Civil Code, on the understanding that:

- “a Qualified Certificate as referred to in Article 1.1. section ss Telecommunications Act” is read as follows: "an EV TLS Server Certificate";
- "Signatory": is read as: “Subscriber”;
- "creating Electronic Signatures" is read as: "creating Encrypted Data";
- "verifying Electronic Signatures" is read as: "decrypting Encrypted Data".
- “a Qualified Certificate as referred to in Article 1.1. section ss Telecommunications Act” is read as follows: "a Server Certificate";
- "Signatory": is read as: “Subscriber”;
- "creating Electronic Signatures" is read as: "verifying Authentication characteristics and creating Encrypted Data";
- "verifying Electronic Signatures" is read as: "decrypting Authentication characteristics and Encrypted Data".

DigiCert Europe provides test certificates for all types of certificates.

9.6.2. RA Representations and Warranties

RAs represent and warrant that:

i. The RA’s certificate issuance and management services conform to the DigiCert Europe CPS and applicable CA or RA Agreements;

ii. Information provided by the RA does not contain any false or misleading information;

iii. Reasonable steps are taken to verify that the information contained in any Certificate is accurate at the time of issue;

iv. Translations performed by the RA are an accurate translation of the original information;

v. All Certificates requested by the RA meet the requirements of this CPS and RA Agreement; and

vi. The RA will request that Certificates be revoked by DigiCert Europe if they believe or are notified that the contents of the Certificate are no longer accurate, or that the key associated with a Certificate has been compromised in any way.

DigiCert Europe’a RA Agreement may contain additional representations. Subscriber Agreements may include additional representations and warranties.

9.6.3. Subscriber Representations And Warranties

Prior to being issued and receiving a Certificate, Subscribers are solely responsible for any misrepresentations they make to third parties and for all transactions that use Subscriber’s Private Key, regardless of whether such use was authorised. Subscribers are required to notify DigiCert Europe and any applicable RA if a change occurs that could affect the status of the Certificate.

DigiCert Europe requires, as part of the Subscriber Agreement or Terms of Use, that the Applicant make the commitments and warranties in this section for the benefit of DigiCert Europe and all Relying Parties and Application Software Suppliers. This make take the form of either:

1. The Applicant’s agreement to the Subscriber Agreement with DigiCert Europe; or

2. The Applicant's acknowledgement of the Terms of Use.

Subscribers represent to DigiCert Europe, Application Software Suppliers, and Relying Parties that, for each Certificate, the Subscriber will:

1. Securely generate its Private Keys and protect its Private Keys from compromise, and exercise sole and complete control and use of its Private Keys;
2. Provide accurate and complete information when communicating with DigiCert Europe, and to respond to DigiCert Europe's instructions concerning Key Compromise or Certificate misuse;
3. Confirm the accuracy of the certificate data prior to installing or using the Certificate;
4. For Qualified Certificates
    a. if the policy requires the use of a QSCD, Electronic Signatures must only be created by a QSCD,
    b. in the case of natural persons, the Private Key should only be used for Electronic Signatures, and
    c. in the case of legal persons, the Private Key must be maintained and used under the control of the Subscriber and it should only be used for Electronic Seals.
5. Promptly
    a. request revocation of a Certificate, cease using it and its associated Private Key, and notify DigiCert Europe if there is any actual or suspected misuse or compromise of the Private Key associated with the Public Key included in the Certificate, and
    b. request revocation of the Certificate, and cease using it, if any information in the Certificate is or becomes incorrect or inaccurate;
6. For Remote Identity Verification, use the identity proofing software distributed by DigiCert Europe. The Subscriber is obliged to agree with the processing of biometric data for identity verification purposes during Remote Identity Verification;
7. Ensure that individuals using Certificates on behalf of an Organisation have received security training appropriate to the Certificate;
8. Use the Certificate only for authorised and legal purposes, consistent with the Certificate purpose, this CPS, and the relevant Subscriber Agreement, including only installing TLS Server Certificates on servers accessible at the Domain listed in the Certificate and not using code signing Certificates to sign malicious code or any code that is downloaded without a user's consent; and
9. Promptly cease using the Certificate and related Private Key after the Certificate's expiration or revocation, or in the event that DigiCert Europe notifies the Subscriber that the DigiCert Europe PKIo has been compromised.

Subscriber Agreements may include additional representations and warranties.

9.6.4. Relying Parties Representations And Warranties

Each Relying Party represents that it:

i. Prior to relying on the Certificate or other authentication product or service, Relying Parties are obliged to check all status information provided by DigiCert Europe related to the Certificate or other authentication product or service to confirm that the information was still valid and that the product or service had not expired or been revoked. For Certificates, this includes checking to ensure that each Certificate in the Certificate Chain is valid, unexpired, and non-revoked (by using any CRL or OCSP information available).

   - to be relied upon as an EU Qualified Certificate, the CA/trust anchor for the validation of the Certificate shall be as identified in a service digital identifier of an EU Trusted List entry with service type identifier "http://uri.etsi.org/TrstSvc/Svctype/CA/QC" for a Qualified Trust Service Provider. ETSI TS 119 615 provides guidance on how to validate a Certificate against the EU Trusted Lists. ETSI TS 119 172-4 describes how to validate an Electronic Signature to determine whether it can be considered as an EU Qualified electronic signature or seal.

ii. Prior to relying on an authentication product or service, Relying Parties must gather sufficient information to make an informed decision about the proper use of the authentication product or service and whether intended reliance on the authentication product or service was reasonable in light of the circumstances. This includes evaluating the risks associated with their intended use and the limitations associated with the authentication product or service provided by DigiCert Europe.

iii. Relying Parties' reliance on the authentication product or service is reasonable based on the circumstances. Relying Parties reliance will be deemed reasonable if:

   - the attributes of the Certificate relied upon and the level of assurance in the Identification and Authentication provided by the Certificate are appropriate in all respects to the level of risk and the reliance placed upon that Certificate by the Relying Party;
   - the Relying Party has, at the time of that reliance, used the Certificate for purposes appropriate and permitted by the CPS and under the laws and regulations of the jurisdiction in which the Relying Party is located;
   - the Relying Party has, at the time of that reliance, acted in good faith and in a manner appropriate to all the circumstances known, or circumstances that ought reasonably to have been known, to the Relying Party;
   - the Relying Party has, at the time of that reliance, verified the Electronic Signature, if any;
   - the Relying Party has, at the time of that reliance, verified that the Electronic Signature, if any, was created during the Operational Term of the Certificate being relied upon;
   - the Relying Party ensures that the data signed has not been altered following signature by utilising trusted application software,
   - the signature is trusted and the results of the signature are displayed correctly by utilising trusted application software;
   - the identity of the Subscriber is displayed correctly by utilising trusted application software; and
   - any alterations arising from security changes are identified by utilising trusted application software.

If the circumstances indicate a need for additional assurances, it is Relying Parties' responsibility to obtain such assurances. A Relying Party shall make no assumptions about information that does not appear in a

Certificate. All obligations and warranties within this Section relate to Reasonable Reliance on the validity of a Electronic Signature, not the accuracy of the underlying electronic record.

Any unauthorised reliance on a Certificate is at a party's own risk. Relying Party Agreements may include additional representations and warranties.

9.6.5. Representations And Warranties Of Other Participants

Participants within the DigiCert Europe PKIo represent and warrant that they accept and will perform any and all duties and obligations as specified by this CPS.

9.7. DISCLAIMERS OF WARRANTIES

OTHER THAN AS PROVIDED IN SECTION 9.6.1, THE CERTIFICATES ARE PROVIDED "AS IS" AND "AS AVAILABLE" AND TO THE MAXIMUM EXTENT PERMITTED BY LAW, DIGICERT EUROPE DISCLAIMS ALL EXPRESS AND IMPLIED WARRANTIES, INCLUDING WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. DIGICERT EUROPE DOES NOT WARRANT THAT ANY CERTIFICATE WILL MEET SUBSCRIBER'S OR ANY OTHER PARTY'S EXPECTATIONS OR THAT ACCESS TO THE CERTIFICATES WILL BE TIMELY OR ERROR-FREE. DIGICERT EUROPE does not guarantee the accessibility of any Certificates and may modify or discontinue offering any Certificates at any time. Subscriber's sole remedy for a defect in the Certificates is for DIGICERT EUROPE to use commercially reasonable efforts, upon notice of such defect from Subscriber, to correct the defect, except that DIGICERT EUROPE has no obligation to correct defects that arise from (i) misuse, damage, modification or damage of the Certificates or combination of the Certificates with other products and services by parties other than DIGICERT EUROPE, or (ii) Subscriber's breach of any provision of the Subscriber Agreement.

9.8. LIABILITY AND LIMITATIONS OF LIABILITY

This Section 9.8 does not limit a party's liability for: (i) death or personal injury resulting from the negligence of a party; (ii) gross negligence, willful misconduct or violations of applicable law, or (iii) fraud or fraudulent statements made by a party to the other party in connection with this CPS. TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW AND NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY OR LIMITATION OF LIABILITY: (A) DIGICERT EUROPE AND ITS AFFILIATES, SUBSIDIARIES, OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, PARTNERS AND LICENSORS (THE "DIGICERT EUROPE ENTITIES") WILL NOT BE LIABLE FOR ANY SPECIAL, INDIRECT, INCIDENTAL, CONSEQUENTIAL, OR PUNITIVE DAMAGES (INCLUDING ANY DAMAGES ARISING FROM LOSS OF USE, LOSS OF DATA, LOST PROFITS, BUSINESS INTERRUPTION, OR COSTS OF PROCURING SUBSTITUTE SOFTWARE OR SERVICES) ARISING OUT OF OR RELATING TO THIS CPS OR THE SUBJECT MATTER HEREOF; AND (B) THE 'DIGICERT EUROPE ENTITIES' TOTAL CUMULATIVE LIABILITY ARISING OUT OF OR RELATING TO THIS CPS OR THE SUBJECT MATTER HEREOF WILL NOT EXCEED THE AMOUNTS PAID BY OR ON BEHALF OF SUBSCRIBER TO DIGICERT EUROPE IN THE TWELVE MONTHS PRIOR TO THE EVENT GIVING RISE TO SUCH LIABILITY, REGARDLESS OF WHETHER SUCH LIABILITY ARISES FROM CONTRACT, INDEMNIFICATION, WARRANTY, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY OR OTHERWISE, AND REGARDLESS OF WHETHER DIGICERT EUROPE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE. NO CLAIM, REGARDLESS OF FORM, WHICH IN ANY WAY ARISES OUT OF THIS CPS, MAY BE MADE OR BROUGHT BY SUBSCRIBER OR SUBSCRIBER'S REPRESENTATIVES MORE THAN ONE (1) YEAR AFTER THE BASIS FOR THE CLAIM BECOMES KNOWN TO SUBSCRIBER. For EU Qualified Certificates, DigiCert Europe liability is in accordance with Extract 37 and Article 13 of the eIDAS Regulation.

9.9. INDEMNITIES

9.9.1. Indemnification By DigiCert Europe

To the extent permitted by applicable law, DigiCert Europe shall indemnify each Application Software Supplier against any claim, damage, or loss suffered by an Application Software Supplier related to an Certificate issued by DigiCert Europe, regardless of the cause of action or legal theory involved, except where the claim, damage, or loss suffered by the Application Software Supplier was directly caused by the Application Software Supplier's software displaying either (i) a valid and trustworthy Certificate as not valid or trustworthy or (ii) displaying as trustworthy (a) an Certificate that has expired or (b) a revoked Certificate where the revocation status is available online but the Application Software Supplier's software failed to check or ignored the status.

9.9.2. Indemnification By Subscribers

Customer will indemnify, defend and hold harmless DigiCert Europe and DigiCert Europe's employees, officers, directors, shareholders, Affiliates, and assigns (each an "Indemnified Party") against all third party claims and all related liabilities, damages, and costs, including reasonable attorneys' fees, arising from (i) Customer's breach of this Agreement; (ii) Customer's online properties for which DigiCert Europe provides Services hereunder, or the technology or content embodied therein or made available through such properties; (iii) DigiCert Europe's access or use in compliance with this Agreement of any information, systems, data or materials provided by or on behalf of Customer to DigiCert Europe hereunder, (iv) Customer's failure to protect the authentication mechanisms used to secure the Portal or a Portal Account; (v) Customer's modification of a DigiCert Europe product or service or combination of a DigiCert Europe product or service with any product or service not provided by DigiCert Europe; (vi) an allegation that personal injury or property damage was caused by the fault or negligence of Customer; (vii) Customer's failure to disclose a material fact related to the use or issuance of the Services; or (viii) an allegation that the Customer, or an agent of Customer, used DigiCert Europe's Services to infringe on the rights of a third party.

9.9.3. Indemnification By Relying Parties

To the extent permitted by law, each Relying Party shall indemnify DigiCert Europe, its partners, and their respective directors, officers, employees, agents, and contractors against any loss, damage, or expense, including reasonable attorney's fees, related to the Relying Party's (i) breach of the Relying Party Agreement, an End-User License Agreement, this CPS, or applicable law; (ii) unreasonable reliance on a Certificate; or (iii) failure to check the Certificate's status prior to use.

9.10. TERM AND TERMINATION

9.10.1. Term

This CPS and any amendments to this CPS are effective when published in the DigiCert Europe Repository and remain in effect until replaced with a newer version.

9.10.2. Termination

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

9.10.3. 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.

9.11. INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

DigiCert Europe accepts notices related to this CPS at the locations specified in Section 2.2. Notices are deemed effective after the sender receives a valid and digitally signed acknowledgment of receipt from DigiCert Europe. If an acknowledgement of receipt is not received within five days, the sender must resend the notice in paper form to the street address specified in Section 2.2 using either a courier service that confirms delivery or via certified or registered mail with postage prepaid and return receipt requested. DigiCert Europe may allow other forms of notice in its Subscriber Agreements. Notices to Application Software Suppliers are sent out in accordance with the respective requirements.

9.12. AMENDMENTS

9.12.1. Procedure For Amendment

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

There are two possible types of policy change: * the issue of a new CPS; or * a change or adjustment of a policy in the existing CPS.

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

9.12.2. Notification Mechanism And Period

The new or modified CPS is published in the Repository at https://www.quovadisglobal.com/repository/. The DCPA is responsible for determining what constitutes a material change of the CPS. For routine modifications, DigiCert Europe does not guarantee or set a notice-and-comment period and may make changes to this CPS without notice and without changing the version number.

When the DCPA determines a CPS change may have a significant impact on Subscribers or Relying Parties, due notice of seven (7) days will be provided in the Repository. Subscribers whose Certificates remain valid at the effective date of the CPS change shall be deemed to have accepted the modification. If there is an intention to change the CA structure, DigiCert Europe submits this information to the PKIo PA. In the event of any change to this CPS then PKIoverheid (Logius) will be notified of such change.

9.12.3. Circumstances Under Which OID Must Be Changed

OIDs used within PKIoverheid Certificates are determined by the PKIo PA; DigiCert Europe does not control the circumstances for those changes.

9.13. DISPUTE RESOLUTION PROVISIONS

For general complaints subscribers and subjects can send an email to qv.complaints@digicert.com. For dispute resolution, to the extent permitted by law, before a Participant files suit or initiates an arbitration claim with respect to a dispute involving any aspect of this Agreement, Participant shall notify DigiCert Europe, and any other party to the dispute for the purpose of seeking business resolution. Both Participant

and DigiCert Europe shall make good faith efforts to resolve such dispute via business discussions. If the dispute is not resolved within sixty (60) days after the initial notice, then a party may proceed as permitted under applicable law and as specified under this CPS and other relevant agreements.

i. Arbitration: In the event a dispute is allowed or required to be resolved through arbitration, the parties will maintain the confidential nature of the existence, content, or results of any arbitration hereunder, except as may be necessary to prepare for or conduct the arbitration hearing on the merits, or except as may be necessary in connection with a court application for a preliminary remedy, a judicial confirmation or challenge to an arbitration award or its enforcement, or unless otherwise required by law or judicial decision.

ii. Class Action and Jury Trial Waiver: THE PARTIES EXPRESSLY WAIVE THEIR RESPECTIVE RIGHTS TO A JURY TRIAL FOR THE PURPOSES OF LITIGATING DISPUTES HEREUNDER. Each party agrees that any dispute must be brought in the respective party's individual capacity, and not as a plaintiff or class member in any purported class, collective, representative, multiple plaintiff, or similar proceeding ("Class Action"). The parties expressly waive any ability to maintain any Class Action in any forum in connection with any dispute. If the dispute is subject to arbitration, the arbitrator will not have authority to combine or aggregate similar claims or conduct any Class Action nor make an award to any person or entity not a party to the arbitration. Any claim that all or part of this Class Action waiver is unenforceable, unconscionable, void, or voidable may be determined only by a court of competent jurisdiction and not by an arbitrator.

9.14. GOVERNING LAW

All agreements entered into by DigiCert Europe under this CPS are governed by Dutch law, unless otherwise specified.

9.15. COMPLIANCE WITH APPLICABLE LAW

This CPS is subject to all applicable laws and regulations, including United States restrictions on the export of software and cryptography products. Subject to section 9.4.5, DigiCert Europe meets the requirements of the European data protection laws and has established appropriate technical and organisation measures against unauthorised or unlawful processing of personal data and against the loss, damage, or destruction of personal data.

9.16. MISCELLANEOUS PROVISIONS

9.16.1. Entire Agreement

DigiCert Europe contractually obligates each RA to comply with this CPS and applicable industry guidelines. DigiCert Europe also requires each party using its products and services to enter into an agreement that delineates the terms associated with the product or service. If an agreement has provisions that differ from this CPS, then the agreement with that party controls, but solely with respect to that party. Third parties may not rely on or bring action to enforce such agreement.

9.16.2. Assignment

Any entities operating under this CPS may not assign their rights or obligations without the prior written consent of DigiCert Europe. Unless specified otherwise in a contact with a party, DigiCert Europe does not provide notice of assignment.

9.16.3. Severability

If any provision of this CPS is held invalid or unenforceable by a competent court or tribunal, the remainder of the CPS will remain valid and enforceable. Each provision of this CPS that provides for a limitation of liability, disclaimer of a warranty, or an exclusion of damages is severable and independent of any other provision.

9.16.4. Enforcement (Waiver Of Rights)

DigiCert Europe may seek indemnification and attorneys' fees from a party for damages, losses, and expenses related to that party's conduct. DigiCert Europe's failure to enforce a provision of this CPS does not waive DigiCert Europe's right to enforce the same provision later or right to enforce any other provision of this CPS. To be effective, waivers must be in writing and signed by DigiCert Europe.

9.16.5. Force Majeure

Except for Customer's payment obligations, neither party is liable for any failure or delay in performing its obligations under this Agreement to the extent that the circumstances causing such failure or delay are beyond a party's reasonable control. Customer acknowledges that the Services (including the Portal and Certificates) are subject to the operation and telecommunication infrastructures of the Internet and the operation of Customer's Internet connection services, all of which are beyond DigiCert Europe's control.

9.17. OTHER PROVISIONS

DigiCert Europe ensures that it is capable of issuing all types of Certificate listed in this CPS per the PvE requirements.

APPENDIX A – CERTIFICATE PROFILES FOR PKIOVERHEID

Domain CA: Staat der Nederlanden Organisatie Persoon CA - G3

Authentication

- QuoVadis PKIoverheid Organisatie Persoon CA - G3
    - Profile: Organisatie Persoon Authentication G3
- QuoVadis PKIoverheid Organisatie Persoon CA-2022
    - Profile: Organisatie Persoon Authentication
- DigiCert QuoVadis PKIoverheid Organisatie Persoon CA – 2023
    - Profile: PKIOverheid Personal Organisation Authenticity

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

Basic Contents	Value	Demarcation
Subject.SerialNumber	SerialNumber	Required
Subject.OrganisationName	OrganisationName	Required
Subject.organisationalUnitName	OrganisationalUnitName	Disallowed for Certificates issued after June 27, 2022.
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 0.4.0.2042.1.2 (ETSI NCP+), 2.23.140.1.5.3.1 (S/MIME BR, optional)	Fixed
subjectAltName.Rfc822Name	Rfc822 email address	Optional - for e-mail signing
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 or http://crl.quovadisglobal.com/quovadispkioverheidorganisatiepersoonca2022.crl or http://crl.digicert.eu/DigiCertQuoVadisPKIoverheidOrganisatiePersoonCA-2023.crl	Fixed
AuthorityInfoAccess	http://uw.ocsp.quovadisglobal.com or http://ocsp.digicert.eu or http://trust.quovadisglobal.com/pkiopersong3.crt or http://trust.quovadisglobal.com/quovadispkioverheidorganisatiepersoonca2022.crt or	Fixed

Basic Contents	Value	Demarcation
	http://cacerts.digicert.eu/DigiCertQuoVadisPKIoverheidOrganisatiePersoonCA-2023.crt	

Non-Repudiation

- QuoVadis PKIoverheid Organisatie Persoon CA - G3
    - Profile: Organisatie Persoon Non-Repudiation G3
- QuoVadis PKIoverheid Organisatie Persoon CA-2022
    - Profile: Organisatie Persoon Non-Repudiation
- DigiCert QuoVadis PKIoverheid Organisatie Persoon CA – 2023
    - Profile: PKIOverheid Personal Organisation 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	Disallowed for Certificates issued after June 27, 2022.
Subject.title	Title	Optional
Subject.CountryName	Country	Required
Subject.PublicKeyInfo	RSA (2048 bit)	Required
Extensions	Fixed	KeyUsage (CRITICAL)
Non-Repudiation	Fixed	extKeyUsage

Basic Contents	Value	Demarcation
	E-Mail Protection	Optional
CertPolicyID	2.16.528.1.1003.1.2.5.2 0.4.0.2042.1.2 (ETSI NCP+), 0.4.0.194112.1.2 (ETSI QCP-n-qscd), 2.23.140.1.5.3.1 (S/MIME BR, optional) 0.4.0.19431.1.1.3 'eu-remote-	Fixed Only included when DigiCert Europe generates & manages Private Keys on behalf of Subscriber on a QSCD.

Basic Contents	Value	Demarcation
	qscd' EUSCP: EU SSASC Policy (ETSI TS 119 431-1)	
subjectAltName.Rfc822Name	Rfc822 email address	Optional - for e-mail signing
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 or http://crl.quovadisglobal.com/quovadispkioverheidorganisatiepersoonca2022.crl or http://crl.digicert.eu/DigiCertQuoVadisPKIoverheidOrganisatiePersoonCA-2023.crl	Fixed
AuthorityInfoAccess	http://uw.ocsp.quovadisglobal.com or http://ocsp.digicert.eu or http://trust.quovadisglobal.com/pkiopersong3.crt or http://trust.quovadisglobal.com/quovadispkioverheidorganisatiepersoonca2022.crt or http://cacerts.digicert.eu/DigiCertQuoVadisPKIoverheidOrganisatiePersoonCA-2023.crt	Fixed
QC Statements	Id-etsi-qcs-QcCompliance { id-etsi-qcs 1 } 0.4.0.1862.1.1 Id-etsi-qct-esign { 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

Encryption

- QuoVadis PKIoverheid Organisatie Persoon CA - G3
    - Profile: Organisatie Persoon Encryption G3
- QuoVadis PKIoverheid Organisatie Persoon CA-2022
    - Profile: Organisatie Persoon Encryption

- DigiCert QuoVadis PKIoverheid Organisatie Persoon CA – 2023
    - Profile: PKIOverheid Personal Organisation Encryption

Basic Contents	Value	Demarcation
Subject.Common Name	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, 0.4.0.2042.1.1 (ETSI NCP), 2.23.140.1.5.3.1 (S/MIME BR, optional)	Fixed
subjectAltName.Rfc822Name	Rfc822 email address	Optional - for e-mail signing
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/pkiope rsong3.crl or http://crl.quovadisglobal.com/quovadis pkioverheidorganisatiepersoonca2022.crl or http://crl.digicert.eu/DigiCertQuoVadisPKIoverheid OrganisatiePersoonCA-2023.crl	Fixed

Basic Contents	Value	Demarcation
AuthorityInfoAccess	http://uw.ocsp.quovadisglobal.com or http://ocsp.digicert.eu or http://trust.quovadisglobal.com/pkiopersong3.crt or http://trust.quovadisglobal.com/quovadispkioverheidorganisatiepersoonca2022.crt or http://cacerts.digicert.eu/DigiCertQuoVadisPKIoverheidOrganisatiePersoonCA-2023.crt	Fixed

Domain CA: QuoVadis PKIoverheid Private Services CA – G1

Authentication

- QuoVadis PKIoverheid Private Services CA – G1
    - Profile: Private Services – Authentication
- DigiCert QuoVadis PKIoverheid Private Services CA – 2023
    - Profile: PKIOverheid Private Services – Authenticity

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, 0.4.0.2042.1.1 (ETSI NCP), 2.23.140.1.5.2.1 (S/MIME BR, optional)	Fixed
subjectAltName.Rfc822Name	Rfc822 email address	Optional - for e-mail signing
subjectAltName.User Principle Name (MS UPN)	user@domain (used for Single Sign On)	Optional

Basic Contents	Value	Demarcation
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 or http://crl.digicert.eu/DigiCertQuoVadisPKIoverheidPrivateServicesCA2023.crl	Fixed
AuthorityInfoAccess	http://sl.ocsp.quovadisglobal.com or http://ocsp.digicert.eu or http://trust.quovadisglobal.com/pkio privserv.crt or http://cacerts.digicert.eu/DigiCertQuoVadisPKIoverheidPrivateServicesCA2023.crt	Fixed

Encryption

- QuoVadis PKIoverheid Private Services CA – G1
    - Profile: Private Services – Encryption
- DigiCert QuoVadis PKIoverheid Private Services CA – 2023
    - Profile: PKIOverheid Private Services – Encryption

Basic Contents	Value	Demarcation
Subject.Common Name	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

Basic Contents	Value	Demarcation
extKeyUsage	Encrypting File System, E-Mail Protection	Required
CertificatePolicies	2.16.528.1.1003.1.2.8.5, 0.4.0.2042.1.1 (ETSI NCP), 2.23.140.1.5.2.1 (S/MIME BR, optional)	Fixed
subjectAltName.Rfc822Name	Rfc822 email address	Optional - for e-mail signing
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 or http://crl.digicert.eu/DigiCertQuoVadisPKIoverheidPrivateServicesCA2023.crl	Fixed
AuthorityInfoAccess	http://sl.ocsp.quovadisglobal.com or http://ocsp.digicert.eu or http://trust.quovadisglobal.com/pkio privserv.crt or http://cacerts.digicert.eu/DigiCertQuoVadisPKIoverheidPrivateServicesCA2023.crt	Fixed

Server

- QuoVadis PKIoverheid Private Services CA – G1
    - Profile: Private Services – Server
- DigiCert QuoVadis PKIoverheid Private Services CA – 2023
    - Profile: PKIOverheid Private Services – Server

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

Basic Contents	Value	Demarcation
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 - for e-mail signing
subjectAltName.dNSname	If FQDN is used it must be in the first SAN DNS field. Otherwise usage of this field is prohibited	Required/Prohibited
subjectAltName.ip address	Only public IP addresses	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 or http://crl.digicert.eu/DigiCertQuoVadisPKIoverheidPrivateServicesCA2023.crl	Fixed
AuthorityInfoAccess	http://sl.ocsp.quovadisglobal.com or http://ocsp.digicert.eu or http://trust.quovadisglobal.com/pkio privserv.crt or http://cacerts.digicert.eu/DigiCertQuoVadisPKIoverheidPrivateServicesCA2023.crt	Fixed

Domain CA: Staat der Nederlanden Private Personen CA – G1

Authentication

- QuoVadis PKIoverheid Private Personen CA - G1
    - Profile: Private Personen Authentication
- DigiCert QuoVadis PKIoverheid Private Personen CA – 2023
    - Profile: PKIOverheid Private Personal Authenticity

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

Basic Contents	Value	Demarcation
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, 0.4.0.2042.1.1 (ETSI NCP), 2.23.140.1.5.3.1 (S/MIME BR, optional)	Fixed
subjectAltName.Rfc822Name	Rfc822 email address	Optional - for e-mail signing
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 or http://crl.digicert.eu/DigiCertQuoVadisPKIoverheidPrivatePersonenCA2023.crl	Fixed
AuthorityInfoAccess	http://uw.ocsp.quovadisglobal.com or http://ocsp.digicert.eu or http://trust.quovadisglobal.com/pkio privpersg1.crt or http://cacerts.digicert.eu/DigiCertQuoVadisPKIoverheidPrivatePersonenCA-2023.crt	Fixed

Non-Repudiation

- QuoVadis PKIoverheid Private Personen CA - G1
    - Profile: Private Personen Non-Repudiation
- DigiCert QuoVadis PKIoverheid Private Personen CA – 2023
    - Profile: PKIOverheid 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, 0.4.0.2042.1.2 (ETSI NCP+), 0.4.0.194112.1.2 (ETSI QCP-n-qscd), 2.23.140.1.5.3.1 (S/MIME BR, optional)	Fixed
subjectAltName.Rfc822Name	Rfc822 email address	Optional - for e-mail signing
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 or http://crl.digicert.eu/DigiCertQuoVadisPKIoverheidPrivatePersonenCA2023.crl	Fixed

Basic Contents	Value	Demarcation
AuthorityInfoAccess	http://uw.ocsp.quovadisglobal.com or http://ocsp.digicert.eu or http://trust.quovadisglobal.com/pkioprivpersg1.crt or http://cacerts.digicert.eu/DigiCertQuoVadisPKIoverheidPrivatePersonenCA-2023.crt	Fixed
QC Statements	Id-etsi-qcs-QcCompliance { id-etsi-qcs 1 } 0.4.0.1862.1.1, Id-etsi-qct-esign { 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

Encryption

- QuoVadis PKIoverheid Private Personen CA - G1
    - Profile: Private Personen Encryption
- DigiCert QuoVadis PKIoverheid Private Personen CA – 2023
    - Profile: PKIOverheid 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

Basic Contents	Value	Demarcation
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, 2.23.140.1.5.3.1 (S/MIME BR, optional)	Fixed
subjectAltName.Rfc822Name	Rfc822 email address	Optional - for e-mail signing
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 or http://crl.digicert.eu/DigiCertQuoVadisPKIoverheidPrivatePersonenCA2023.crl	Required
AuthorityInfoAccess	http://uw.ocsp.quovadisglobal.com or http://ocsp.digicert.eu or http://trust.quovadisglobal.com/pkio privpersg1.crt or http://cacerts.digicert.eu/DigiCertQuoVadisPKIoverheidPrivatePersonenCA-2023.crt	Fixed