Digidentity

Certificate Practice Statement

PKIoverheid Certificates

Title	Certificate Practice Statement - PKIoverheid Certificates
Date	3 November 2026
Valid from	10 November 2026
Version	2026-v2
Location	https://www.digidentity.eu/en/documentation/
Classification	Public

© Digidentity

Revisions

Version	Date	Description
2019-v1	25 February 2019	Initial publication
2019-v2	6 December 2019	Digidentity address modified, removed URL to test certificates G2, aligned CPS with CPS for Digidentity Certificates, added missing sections and removed empty sections to comply to RFC3647 and Mozilla Root Store Policy, updated to Baseline requirements 1.6.6
2020-v1	16 March 2020	Updated to BR 1.6.8, updated to Mozilla Root Store Policy 2.7, updated to PKIoverheid PvE 4.8, removed G2 certificates and references (CA expired), updated section on linters (6.1.6), minor text updates, updated Appendix A
2020-v2	9 September 2020	Updated to BR 1.7.1, updated certificates profiles, changed extensions in authorityInfoAccess and cRLDistributionPoints, removed PKIoverheid Burger G3 -CA, added Remote Identification and updated face-2-face identification, added clarifications
2020-v3	1 December 2020	Added PKIo SSL G3, adjusted expiry Registered Profession certificate
2021-v1	1 June 2021	Updated to BR 1.7.4, add PKIoverheid Issuing CA's, removed PKIoverheid Server G3 CA, aligned Section 9 with General Terms & Conditions, processed comments Bugzilla review, add PKIoverheid Burger 2021 CA and Organisatie Services 2021 CA
2022-v1	31 January 2022	Updated to BR 1.8.0, updated 6.2.1 with actions in case of revocation HSM certification (ETSI), removed PKIoverheid Server 2020 CA, updated remote identification, added handling of attributes, added new ISO certifications
2022-v2	7 October 2022	Updated to BR 1.8.4, added obligations for Seal, updated F2F process, minor corrections, added revocation notification for issuing CA Digidentity PKIoverheid Server CA 2020
2023-v1	8 August 2023	Removed issuing CA Digidentity PKIoverheid Server CA 2020, updated profiles, removed references to Baseline Requirements, notification to stop issuing encryption certificates
2024-v1	18 March 2024	Updated address Digidentity, updated ISO27001 certification to 2022 version, added S/MIME requirements, minor corrections
2024-v2	8 October 2024	Added PKIoverheid G4 Issuing CA and certificate profiles, updated to eIDAS 2024/1183, removed encryption certificate profiles
2024-v3	20 November 2024	Updated PKIoverheid certificate profiles, reverted reference to eIDAS
2025-v1	7 October 2025	Added sponsored certificate profiles, added certificate profile G1 Digipoort Server, added updated G4 Issuing CA, added FQDN validation, minor updates and corrections
2026-v1	24 February 2026	Added vulnerability remediation timelines, updated use cases (461)
2026-v2	3 November 2026	Remove G3 Hierarchy and references, added eIDAS Implementing Acts and NIS2 and NIS2 Implementing act, updated Section 5

(*) All changes are marked in grey highlight.

Digidentity B.V.

Den Haag, 03 November 2026
eIDAS Qualified Electronic Seal

Digidentity

Contents

1 Introduction 6

1.1 Overview 6
1.2 Document Name & Identification 10
1.3 PKI Participants 11
1.4 Certificate usage 12
1.5 Policy Administration 13
1.6 Definitions & Abbreviations 14

2 Publication & Repository Responsibilities 15

2.1 Repositories 15
2.2 Publication of Information 15
2.3 Time or Frequency of Publication 15
2.4 Access Control & Repositories 15

3 Identification & Authentication 16

3.1 Naming 16
3.2 Initial Identity Validation 18
3.3 Identification & Authentication for Re-Key Requests 26
3.4 Identification & Authentication for Revocation Request 26

4 Certificate Life-Cycle Operation Requirements 29

4.1 Certificate Application 29
4.2 Certification Application Processing 29
4.3 Certificate Issuance 30
4.4 Certificate Acceptance 30
4.5 Key Pair & Certificate Usage 31
4.6 Certificate Renewal 31
4.7 Certificate Re-Key 31
4.8 Certificate Modification 31
4.9 Certificate Revocation & Suspension 31
4.10 Certificate Status Services 35
4.11 End of Subscription 35
4.12 Key Escrow & Recovery 35

CPS PKIoverheid @ Digidentity

5 Facility, Management & Operational Controls 36
5.1 Physical Security Controls 36
5.2 Procedural Controls 37
5.3 Personnel Controls 38
5.4 Audit Logging Procedures 39
5.5 Records Archival 41
5.6 Key Changeover 41
5.7 Compromise & Disaster Recovery 42
5.8 CA or RA Termination 42

6 Technical Controls 43
6.1 Key Pair Generation & Installation 43
6.2 Private Key Protection & Cryptographic Module Engineering Controls 45
6.3 Other Aspects of Key Pair Management 46
6.4 Activation Data 46
6.5 Computer Security Controls 47
6.6 Life Cycle Technical Controls 47
6.7 Network Security Controls 48
6.8 Time Stamping 48

7 Certificate, CRL & OCSP Profiles 49
7.1 Certificate Profiles 49
7.2 CRL Profile 50
7.3 OCSP Profile 50

8 Compliance Audit & Other Assessments 51
8.1 Frequency or Circumstances of Assessment 52
8.2 Identity/Qualifications of Assessor 53
8.3 Assessor's Relationship to Assessed Entity 53
8.4 Topics Covered by Assessment 54
8.5 Actions Taken as a Result of Deficiency 54
8.6 Communication of Results 54
8.7 Self-Audits 54

CPS PKIoverheid @ Digidentity

9 Other Business & Legal Matters 55
9.1 Fees 55
9.2 Financial Responsibility 55
9.3 Confidentiality of Business Information 56
9.4 Protection of Personal Data 56
9.5 Intellectual Property Rights 57
9.6 Representation & Warranties 57
9.7 Disclaimers of Warranties 59
9.8 Limitations of Liability 59
9.9 Indemnities 60
9.10 Term & Termination 60
9.11 Individual Notices & Communications with Participants 60
9.12 Amendments 61
9.13 Dispute Resolution Provisions 61
9.14 Governing Law 61
9.15 Compliance with Applicable Law 62
9.16 Miscellaneous Provisions 62
9.17 Other Provisions 62

Appendix A – Definitions & Abbreviations 63

Appendix B – Certificate Profiles 65
PKIoverheid G1 Certificates Profiles 65
PKIoverheid G4 Subscriber Certificates Profiles 67
CRL Certificate Profiles 73
OCSP Signing Certificate Profiles 74

CPS PKIoverheid @ Digidentity

1 Introduction

Digidentity B.V. (Digidentity) is a Certificate Authority (CA) and a Qualified Trust Service Provider (QTSP) in the issuance, management, and revocation of Public Key Infrastructure (PKI) certificates. These certificates offer the highest level of reliability.

This Certificate Practice Statement (CPS) is also known as Trust Service Practice Statement (TSPS) and Identity Proofing Service Practice Statement (IPSPS). When referred to the CPS, the TSPS and IPSPS are included.

1.1 Overview

This Certificate Practice Statement (CPS) – describes the practices and procedures that Digidentity Certificate Authority (CA) employs in the life-cycle management containing generation, issuance and revocation of PKIoverheid certificates.

This Certificate Practice Statement is structured per RFC 3647 and is divided into nine parts that cover the security controls, practices, certificate profiles and procedures for certificate issuance.

Personal qualified certificates and electronic seal may be used as a signature to legally sign documents.

The Dutch Government are the Policy Authority (PA) and has strict requirements for TSPs and for the issuance of publicly trusted certificates and qualified certificates. This is managed and controlled by the Dutch government organisation Logius with the mandatory requirement for Digidentity CAs to implement the Program of Requirements.

Personal QES certificates and Professional QES certificates are also EU Qualified Certificates issued to natural persons and Business Seals are also EU Qualified Certificates issued to legal persons according to Regulation (EU) No 910.2014.

Digidentity is evaluated against the requirements of ETSI EN 319 401, ETSI EN 319 411-1, ETSI EN 319 411-2 (including CA/Browser Forum Network Security requirements), PKIoverheid Program of Requirements, ISO27001:2022, ISO27701:2019, ISO27017:2015, ISO27018:2019, ISO9001:2015 and ISO22301:2019.

Digidentity is certified against the ETSI EN 319 411-1, ETSI EN 319 411-2, ISO27001:2022, ISO27701:2019, ISO27017:2015, ISO27018:2025, ISO22301:2019 and ISO9001:2015 standards, eIDAS (Regulation (EU) No 910.2014) including Implementation Acts 2024.2160 (artcle 19a.2 – Risks of non-qualified TSP), 2025.1566 (article 24.1c – Identity Verification), 2025.1943 (article 28.6 & 38.6 – Qualified Signatures & Seal) and 2025.2530 (article 24.5 – Requirements for QTSP) and NIS2 (EU Directive 2022.2555 including Implementation Act 2024.2690 – Technical requirement).

Uso PKIoverheid @ Digidentity

This CPS covers the following Certificate Authorities of Digidentity:

- Digidentity BV PKIoverheid Private Services CA – G1
- Digidentity - G4 PKIo EUTL G-Sigs NP - 2025
- Digidentity - G4 PKIo EUTL G-Sigs LP - 2025
- Digidentity - G4 PKIo Priv G-Other NP - 2025
- Digidentity - G4 PKIo Priv G-Other LP - 2025
- Digidentity - G4 PKIo Priv G-TLS - 2025

As of 31 October 2026, Digidentity no longer issues certificates from the PKIoverheid G3 hierarchy and does have any active certificates from the PKIoverheid G3 hierarchy.

1.1.1 Intended audience

This document is intended for:

- Applicants
- Subscribers
- Certificate Holders
- Company Administrators
- Relying parties
- Registration Authorities
- Resellers of Digidentity Products

1.1.2 CA Hierarchy

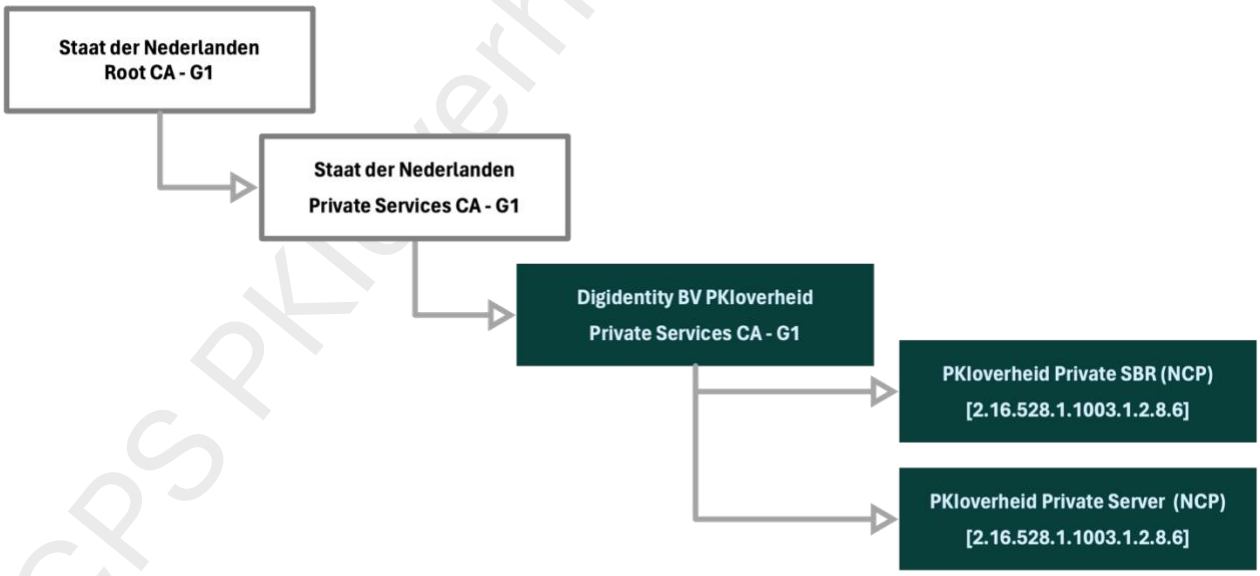


Figure 1 - PKIoverheid G1 Hierarchy

CPS PKIoverheid @ Digidentity

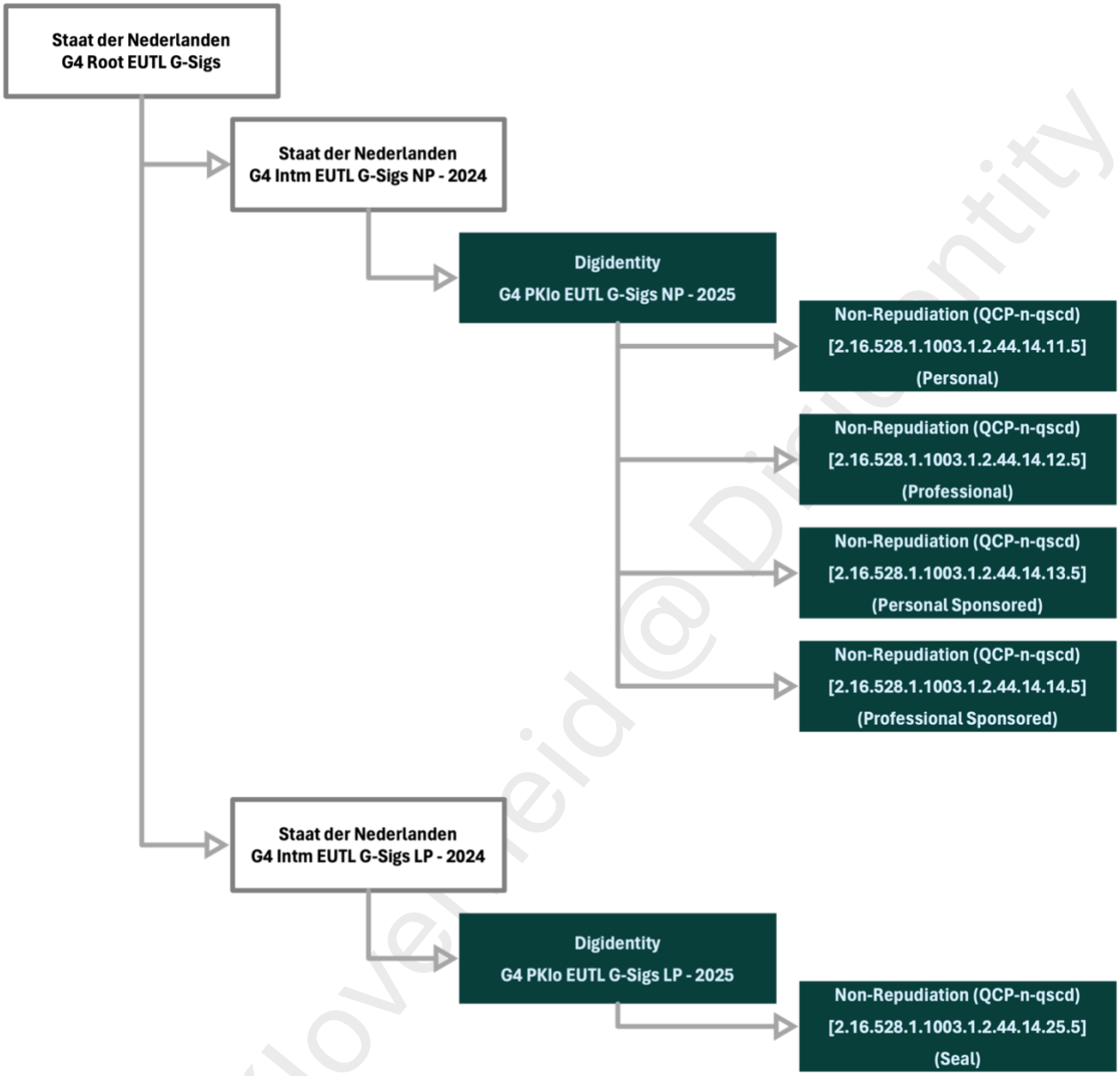


Figure 2 - PKIoverheid G4 EU Trust List Hierarchy

CPS PKIoverheid @ Digidentity

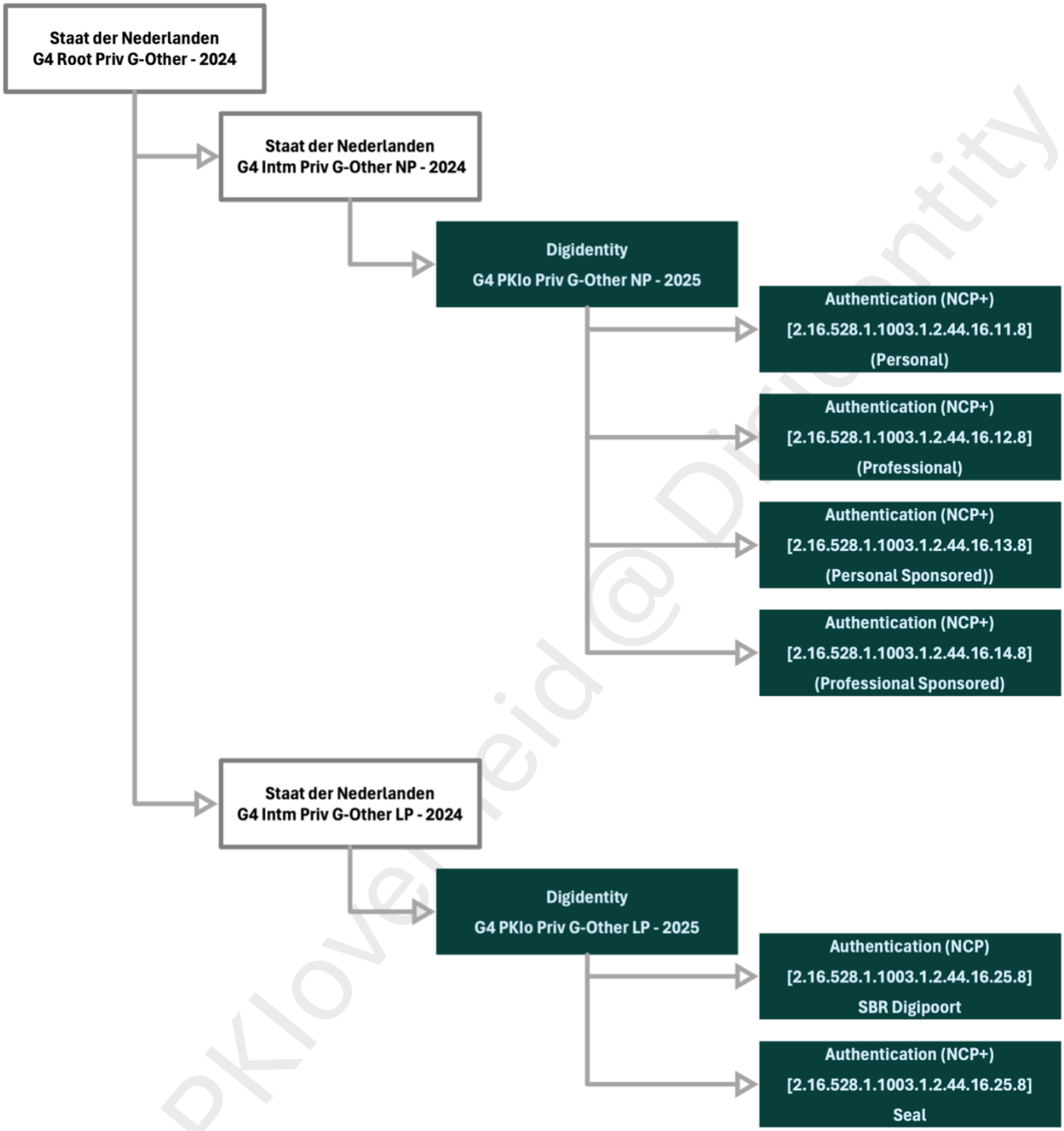


Figure 3 - PKIoverheid G4 Other Hierarchy

CPS PKIoverheid @ Digidentity

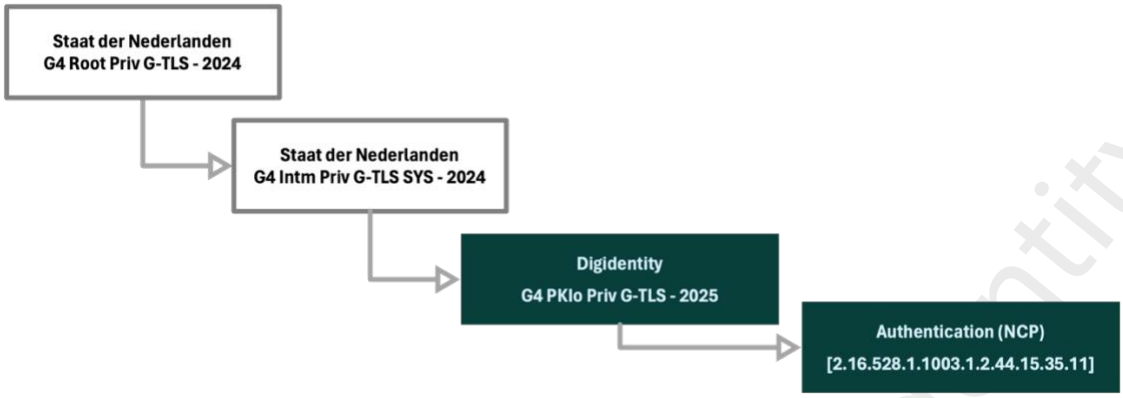


Figure 4 PKIoverheid G4 Private TLS Hierarchy

1.2 Document Name & Identification

This document is identified as Certificate Practice Statement for PKIoverheid Certificates. The Certificate Policies adopted by Digidentity are found in the list within brackets and are equal to the same certificate policies defined in ETSI EN 319 411-1 and ETSI EN 319 411-2.

Digidentity issues subscriber certificates from PKIoverheid G1 hierarchy for:

- Server certificates for Digipoort (Digidentity BV PKIoverheid Private Services CA - G1)
  - PKIoverheid Private SBR (NCP) – OID 2.16.528.1.1003.1.2.8.6
  - PKIoverheid Private Server (NCP) – OID 2.16.528.1.1003.1.2.8.6

Digidentity issues subscriber certificates from PKIoverheid G4 hierarchy for:

- PKIoverheid Private SBR (Digidentity - G4 PKIo Priv G-Other LP - 2025
  - Authentication (NCP) – OID 2.16.528.1.1003.1.2.44.16.25.8
- QES - Personal qualified signing certificates (Digidentity - G4 PKIo EUTL G-Sigs NP - 2025)
  - Personal non-repudiation (QCP-n-qscd) – 2.16.528.1.1003.1.2.44.14.11.5
  - Professional non-repudiation (QCP-n-qscd) – OID 2.16.528.1.1003.1.2.44.14.12.5
  - Personal Organisation non-repudiation (QCP-n-qscd) – OID 2.16.528.1.1003.1.2.44.14.13.5
  - Professional Organisation non-repudiation (QCP-n-qscd) – OID 2.16.528.1.1003.1.2.44.14.14.5
- Personal authentication certificates (G4 PKIo Priv G-Other NP - 2025)
  - Authentication (NCP+) – OID 2.16.528.1.1003.1.2.44.16.11.8
  - Professional authentication (NCP+) – OID 2.16.528.1.1003.1.2.44.16.12.8
  - Personal Organisation authentication (NCP+) – OID 2.16.528.1.1003.1.2.44.16.13.8
  - Professional Organisation authentication (NCP+) – OID 2.16.528.1.1003.1.2.44.16.14.8
- Seal - Qualified signing certificates for organisations (Digidentity - G4 PKIo EUTL G-Sigs LP - 2025)
  - Non-Repudiation (QCP-l-qscd) – OID 2.16.528.1.1003.1.44.14.25.5
- Authentication certificates for organisations (G4 PKIo Priv G-Other LP - 2025)
  - Organisation authentication (NCP+) – OID 2.16.528.1.1003.1.2.44.16.25.8
- Server certificates for organisations (G4 PKIo Priv G-TLS - 2025)
  - Private Server (NCP) – OID 2.16.528.1.1003.1.2.44.15.35.11

CPS PKIoverheid @ Digidentity

Qualified certificates for electronic signatures issued to natural persons and Qualified certificates for electronic seals issued to legal persons are also EU Qualified certificates according to Regulation (EU) No 910.2014.

Relying Parties shall recognise a certificate by inspecting the Certificate Policies extension field of the certificate, which shall hold one of the policy OIDs above.

1.3 PKI Participants

This document is intended for Registration Authorities, Applicants, Subscribers, Relying Parties, Subcontractors, and Resellers of Digidentity Products.

1.3.1 Certificate Authorities

Digidentity is the Certificate Authority for PKIoverheid Certificates listed in section 1.2.

1.3.2 Registration Authorities

A Registration Authority (RA) is an entity that performs the validation and verification the identity of the applicant when requesting a certificate. Once the Registration Authority has provided approval, then the CA can issue the certificate to the applicant. Once the certificate is issued, the applicant becomes the Subscriber.

The Registration Authority (RA) is Digidentity. Digidentity may authorise a delegate RA to perform functions of the registration process. Any delegated RA must comply to the requirements of this document. Digidentity will contractually require each RA or delegated third party to comply the policies and applicable standards and regulations.

1.3.3 Subscribers, Certificate Holder, Company Administrator

Subscribers can be a;

[1] natural person
[2] natural person with a professional title
[3] natural person representing a legal person
[4] legal person represented by natural person(s)

Subscribers use our Products. Subscribers are not always the party identified in a certificate, e.g. when a certificate is issued to a device. The Subscriber must accept the General Terms & Conditions regarding the use of the certificate.

The subject of a certificate is the party named in the certificate as the holder of the Private Key associated with the Public Key given in the certificate. The subject can be a;

[1] natural person
[2] legal person (e.g. Organisation)
[3] device or system operated, represented by a natural or legal person

CPS PKIoverheid © Digidentity

A subscriber may refer to the subject of the certificate and the entity that contracted Digidentity for the certificate's issuance. Before the identity of the Subscriber is verified, a Subscriber is an Applicant.

The Certificate Holder is the entity stated in the subject field of the certificate, and the holder of the private key. Holders of personal certificates are natural persons. Holders of server certificates or Seal are organisations. The Company Administrator is the representative of an organisation and holder of the private key.

1.3.4 Relying Parties

Relying parties are parties who rely upon the trusted status of the certificate. Relying parties will assess the status of the issued certificate before continuing communication with the subscriber. The status of the certificate can be valid, revoked or expired.

1.3.5 Other Participants

In the provision of Products related to digital certificates, Digidentity has the following participants;

[1] Identity verification services
[2] Identity document validation services
[3] Professional Bodies (e.g. Royal Netherlands Institute of Chartered Accountants)
[4] Resellers of Digidentity Products
[5] Organisation verification services (e.g. Chamber of Commerce)
[6] Conformity Assessment Bodies (SERMI)

1.4 Certificate usage

1.4.1 Appropriate certificate usage

Within PKIoverheid Digidentity CAs issues certificates which may be used for the purposes explained in this document, in the Terms & Conditions and as identified in the Key Usage field of the certificate.

Personal Certificates (Qualified) – Personal, Registered Profession/Professional or Sponsored

- Authentication Certificate: can be used to reliably authenticate a natural person.
- Non-repudiation Certificate: can be used to digitally sign documents. These certificates are issued as Qualified certificates and are issued and stored on a Qualified Secure Signature Creation Device (QSCD). Digidentity complies to the EU regulations for electronic signatures No. 910.2014 (eIDAS).

Seals (Qualified)

- Authentication Certificate: can be used to reliably authenticate a legal person.
- Non-repudiation Certificate: can be used to digitally sign documents on behalf of an organisation. These certificates are issued as qualified certificates for electronic seals. The certificates are issued and stored on a Qualified Secure Signature Creation Device (QSCD). Digidentity complies to the EU regulations for electronic signatures No. 910.2014 (eIDAS).

CPS PKIoverheid @ Digidentity

Authentication or Server Certificates

Authentication certificates can be used for authenticating an application or device which are related to an organisation. Server certificates can be used to identify and secure servers in the PKIoverheid Private Root infrastructure. A server certificate supports one (1) domain name (FQDN) and ten (10) server names.

1.4.2 Prohibited certificate usage

Certificates issued under this CPS are prohibited from being used for any other purpose than described. Certificates do not guarantee that the subject is trustworthy, honest, reputable, safe to do business with, or compliant with any laws. A certificate only establishes that the information in the certificate was verified in accordance with this CPS when the certificate issued.

1.5 Policy Administration

1.5.1 Organisation Administration

Digidentity B.V.
Schenkkade 50
2595 AR The Hague
The Netherlands

1.5.2 Contact Person

For questions about this document please contact;

Digidentity B.V.
Security, Risk & Compliance (SRC)
Schenkkade 50
2595 AR The Hague

Tel: +31 (0)88 778 78 78
E-mail: security@digidentity.com

In case of suspected Private Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates or this document, Relying Parties, Application Software Suppliers, and other third parties can contact Digidentity at security@digidentity.com.

The process for revocation of certificates, including contact details, is described in paragraph 4.9.3.

1.5.3 Person determining CPS suitability for the Policy

No stipulation

1.5.4 CPS Approval Procedures

This document is subject to a review at least once a year and is included in the internal audit schedule. The version of this document and the changelog will be updated even if no changes are made. Compliance of this document with RFC 3647, ETSI EN 319 401, ETSI EN 319 411-1, ETSI EN 319 411-2, PKIoverheid Program of Requirements and eIDAS will be assessed, and any inconsistency remedied. Before publishing, this document is approved by Digidentity Management with a digital signature.

CPS PKIoverheid @ Digidentity

This document will be published signed with a Digidentity Seal and thus made available after approval from Digidentity Management.

1.6 Definitions & Abbreviations

See Appendix A – Definitions & Abbreviations for the table with abbreviations and definitions.

CPS PKIoverheid @ Digidentity

2 Publication & Repository Responsibilities

2.1 Repositories

Digidentity maintains an online repository, containing:

[a] Certificate Practice Statement, PKI Disclosure Statement

[b] General Terms & Conditions, Privacy Statement, Product Specific Terms & Conditions

[c] Certificates of Digidentity TSP CAs and issuing CAs for PKIoverheid

All information is available in a read-only format and can be accessed via: https://cps.digidentity-pki.com/.

2.2 Publication of Information

Digidentity maintains a repository and is responsible for the repository functions for the issuing CAs under its control. The Certificate Practice Statement for PKIoverheid Certificates is available 24 x 7 in a read-only format on the Digidentity website (https://cps.digidentity-pki.com/).

The Certificate Practice Statement is structured in accordance with RFC 3647 and includes all material required by RFC 3647.

All PKIoverheid certificates issued by Digidentity have a CRL distribution point extension that contains an URL for CRL retrieval. All PKIoverheid Server certificates also have an Authority Information Access extension that contains an URL for the OCSP service.

Subscribers can download their certificates in their Digidentity account.

2.3 Time or Frequency of Publication

Digidentity publishes updates of this document and other documents in the repository at least once per year or when significant changes are implemented. Changes are documented in the revisions table and incrementing the version number of this document.

2.4 Access Control & Repositories

The repository is protected against unauthorised changes. All publications in the repository are available 24 hours a day, 7 days a week. Digidentity aims to restore the website and/or repository within four (4) hours in the event the website becomes unavailable.

CPS PKIoverheid @ Digidentity

3 Identification & Authentication

3.1 Naming

Digidentity recognises and interpret names per x.500 name standard to define the assignment of certificates, where a distinguished name (DN) is specified in each certificate issued.

3.1.1 Types of Names

The types of names used by Digidentity are shown in the tables below. The "Max. Length" refers to the maximum number of characters which may be used for each field.

Personal Certificates

Field	Description	Max. Length
CommonName (CN)	Given Names and Surname as extracted from identity evidence	64
serialNumber (SN)	Unique number to identify subject	64
Country (C)	Two-digit country code (nationality or ID issuing country)	2
givenName (GN)	Given Names as extracted from identity evidence	64
surname (S)	Surname as extracted from identity evidence	64

Personal Certificates for Registered Professions/Professionals or Sponsored

Field	Description	Max. Length
CommonName (CN)	Given Names and Surname as extracted from identity evidence	64
givenName (GN)	Given Names as extracted from identity evidence	64
surname (S)	Surname as extracted from identity evidence	64
Title (T) (*)	Professional title of the Subject	64
serialNumber (SN)	Unique number to identify subject	64
organizationName (O) (*)	Name of the Organisation as registered in Trade Register	64
organizationIdentifier (*)	Organisation Trade Register number	64
Country (C)	Two-digit country code (nationality or ID issuing country)	2

(*) Optional fields

Organisation Certificates (Seal)

Field	Description	Max. Length
CommonName (CN)	Name of the Organisation as registered in Trade Register	64
Country (C)	Two-digit country code (nationality or ID issuing country)	2
organizationName (O)	Name of the Organisation as registered in Trade Register	64
organizationIdentifier	Organisation Trade Register number	64

PKIoverheid Private TLS Server certificates (G1 & G4)

Field	Description	Max. Length
CommonName (CN)	Server name (contains Fully Qualified Domain Name (FQDN))	64
organizationName (O)	Name of the Organisation as registered in Trade Register	64
Country (C)	Two-digit country code (as registered in Trade Register)	2
Organisation Identifier	Organisation Identifier Number (OIN)	64
serialNumber (SN)	Organisation Identifier Number (OIN)	64

PKIoverheid Private SBR certificates (G1 & G4)

Field	Description	Max. Length
CommonName (CN)	SBR Digipoort	64
organizationName (O)	Name of the Organisation as registered in Trade Register	64
Country (C)	Two-digit country code (nationality or ID issuing country)	2
organizationIdentifier	Organisation Identifier Number (OIN)	64
serialNumber (SN)	Organisation Identifier Number (OIN)	64

3.1.2 Need for Names to be Meaningful

The naming of the Distinguished Name in the certificates based on the tables above, should result in names to be meaningful, unambiguous, and unique and allows any relying party to identify the subscriber.

3.1.3 Anonymity or Pseudonymity of Subscribers

No stipulation.

3.1.4 Rules for Interpreting Various Name Forms

No stipulation.

3.1.5 Uniqueness of Names

No stipulation.

3.1.6 Recognition, Authentication and Role of Trademarks

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

Digidentity is not required and do not determine whether a certificate applicant has intellectual property rights, and therefore do not mediate, arbitrate or try to resolve any dispute regarding the ownership of any intellectual property or trademarks.

Digidentity reserves the right, without liability, to reject any application for a certificate.

CPS PKIoverheid @ Digidentity

3.2 Initial Identity Validation

All applicants start the registration by creating a personal account on the Digidentity website (https://auth.digidentity.eu/accounts/new). Depending on the products, additional identity validation of an individual (see 3.2.4) or organisation (see 3.2.2) is performed.

In the Digidentity Self-Service Portal (https://selfservice.digidentity.eu), server certificates can be revoked. A Digidentity account is required to access the Self-Service Portal. An applicant can register for an account on the My Digidentity website (my.digidentity.eu).

3.2.1 Method to prove possession of Private Key

For Personal Qualified certificates, Personal Qualified certificates for Registered Profession, and Seals, Digidentity generates and stores private keys within Hardware Security Modules (HSMs). The HSM is controlled by Digidentity within the CA operations facilities. During the process of registration, the subscriber will create a PIN code on their mobile device to link the private keys on the HSM to the mobile device (e.g. mobile phone or tablet) and the verified identity of the subscriber to guarantee the private key is under the subscriber's sole control.

The PIN code protecting the private keys is only known to the subscriber. The private keys remain encrypted in the HSM, until a service is accessed by the subscriber, and the correct PIN code is provided via their mobile device. The subscriber will receive a push notification on their mobile phone upon successful instigation of a signing request e.g. using their login details.

For server certificates, Applicants or Subscriber generate their own private key and send a signed Certificate Signing Request (CSR) to prove possession of the private key, which corresponds to the public key in the certificate request. For server certificates the private key is in control of the Company Administrator of the subscribing organisation.

3.2.2 Authentication of Organisation & Domain Identity

Digidentity verifies certificate requests for FQDN used in PKIoverheid Private infrastructure. We do not issue certificates with FQDN as Publicly Trusted Certificates (PTC).

Server certificates containing a FQDN are organisation validated certificates where the Applicant first must register as a Company Administration with Certificate Manager authorisation to request, manage and revoke server certificates on behalf of an organisation.

The Company Administrator and if applicable legal representatives, are identified on eIDAS Level High (LoA4). During the registration for Company Administrator, the organisation is identified, and the Applicant is identified, and the authorisation is verified.

The Company Administrator can request server certificates containing FQDN. Domain validation is performed as described in section 3.2.2.4.4 and 3.2.2.4.14.

CPS PKIoverheid @ Digidentity

3.2.2.1 Identity

Digidentity verifies organisational identities with an authentic source (National Trade Register) using the registration number of the organisation. After the trade register number is entered, the details are retrieved automatically via a secure connection either directly from the trade register or via our supplier Kyckr, who provides data from international trade registers. The address, name, legal representatives and country details are taken directly from the trade register.

For PKIoverheid server certificates, an OIN (Organisation Identification Number) and trade register are used to verify the identity of the organisation. The OIN is issued by the Dutch government.

The identity of foreign organisations and legal representatives can be verified by local authoritative source or a notary.

Identification of natural person legally representing an organisation or authorised to act on behalf of an organisation, is described in section 3.2.3.

3.2.2.2 DBA/Tradename

The organisation tradename is checked via the trade register details. The tradename must match the one on the registry document. The company must be fully operational, with no limitations recorded e.g. bankruptcy, limitations on trading/operation. If there is a limitation appearing on the registry, Digidentity will reject the application for a certificate.

3.2.2.3 Verification of Country

Digidentity uses the method in section 3.2.2.1.

3.2.2.4 Validation of Domain Authorisation or Control

Digidentity issues certificates with FQDN for PKIoverheid G1 and G4 Private Root only. Digidentity does not issue Publicly Trusted Certificates (PTC).

Digidentity uses the method described in 3.2.2.4.4.

3.2.2.4.1 Validating the Applicant as a Domain Contact

This method is retired.

3.2.2.4.2 E-mail, Fax, SMS or Postal Mail to Domain Contact

Digidentity does not use this method.

3.2.2.4.3 Phone Contact with Domain Contact

This method is retired.

CPS PKIoverheid @ Digidentity

3.2.2.4.4 Constructed E-mail to Domain Contact

Digidentity confirms the Applicant's control over the domain name or Fully Qualified Domain Name (FQDN) by:

[a] sending an e-mail to one or more addresses created by using 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' as the local part, followed by the at- sign ("@"), followed by a Domain Name,

[b] including a random confirmation code in the e-mail, and

[c] receiving a confirming response utilising the random confirmation code.

Once Digidentity receives a response from one of these e-mail addresses, with a matching random value (confirmation code), then control over the domain name is confirmed. The confirmation code is valid for seven (7) days. When used, this validation method is recorded during the application for a certificate.

Digidentity checks whether the domain name is registered on a phishing list. If so, the certificate request of the applicant or for the domain name will be rejected.

3.2.2.4.5 Domain Authorisation Document

This method is retired.

3.2.2.4.6 Agreed-Upon Change to Website

This method is retired.

3.2.2.4.7 DNS Change

Digidentity does not use this method.

3.2.2.4.8 IP Address

Digidentity does not use this method.

3.2.2.4.9 Test Certificate

This method is retired.

3.2.2.4.10 TLS Using a Random Number

This method is retired.

3.2.2.4.11 Any Other Method

This method is retired.

3.2.2.4.12 Validating Applicant as a Domain Contact

Digidentity does not use this method.

3.2.2.4.13 E-mail to DNS CAA Contact

Digidentity does not use this method.

CPS PKIoverheid @ Digidentity

3.2.2.4.14 E-mail to DNS TXT Contact

Digidentity can verify control over the domain by asking the Applicant to add a validation e-mail address to the Domain Name Server (DNS). Digidentity uses the e-mail address entry in the DNS to send a random verification token to that e-mail address. The Applicant must enter the verification token on the Digidentity website to confirm receiving the token

The record added to the DNS is:

Type:	TXT
Host name:	validation_email
Value:	<e-mail address to receive validation e-mail>

3.2.2.4.15 Phone Contact with Domain Contact

Digidentity does not use this method.

3.2.2.4.16 Phone Contact with DNS TXT Record Phone Contact

Digidentity does not use this method.

3.2.2.4.17 Phone Contact with DNS CAA Phone Contact

Digidentity does not use this method.

3.2.2.4.18 Agreed-Upon Change to Website v2

Digidentity does not use this method.

3.2.2.4.19 Agreed-Upon Change to Website - ACME

Digidentity does not use this method.

3.2.2.4.20 TLS using ALPN

Digidentity does not use this method.

3.2.2.4.21 DNS Labeled with Account ID - ACME

Digidentity does not use this method.

3.2.2.5 Authentication for an IP Address

Digidentity does not use this method.

3.2.2.6 Wildcard Domain Validation

Digidentity does not issue wildcard domain certificates.

3.2.2.7 Data Source Accuracy

Documents relied upon by Digidentity for the verification may not be expired at the time of certificate issuance. This includes:

- Authentic source for legal person data – not older than fifteen (15) days
- Domain name check and validation – always performed on issuance
- Digidentity may request updated documents from the applicant. Digidentity impose these time limits to ensure the accuracy and reliability of data.
- Upon request for a new certificate, it may be necessary to request a new identity document to reverify information included in the certificate.

CPS PKIoverheid @ Digidentity

3.2.2.8 CAA Records

Digidentity issues server certificates from the PKIoverheid G1 Private Root which are not Publicly Trusted Certificates (PTC). A check of the CAA records is not required or applicable to private root certificates.

3.2.2.9 Multi-Perspective Issuance Corroboration

Digidentity does not use this method. The Policy Authority has allowed Digidentity not to use Multi-Perspective Issuance Corroboration to validate the DNS record. The certificates containing domain name are used in private root system and cannot be used as publicly trusted certificates.

3.2.3 Authentication of Individual Identity

Digidentity verifies the identity of natural persons for qualified certificates or the legal representative/ delegated authorised person (see below) of an organisation with the data described the next sections.

For detailed description of identity proofing for each context, we refer to the document "Identity Proofing @ Digidentity" on our website (https://www.digidentity.eu/en/documentation).

3.2.3.1 Personal Details

Full legal name as shown on a copy of a valid government issued identity document (passport or national ID card), date of birth, place of birth, document expiry date, document number and gender.

Digidentity uses the records of professional bodies to verify the natural person is allowed to use the title of the profession. The professional title must be independently confirmed by a Professional Body.

3.2.3.2 E-mail address

Applicants are required to enter an e-mail address during account creation process or when requesting a certificate containing an e-mail address. Digidentity verifies the e-mail address by sending a confirmation code to the entered e-mail address. The Applicant enters the confirmation code to confirm control over the e-mail address. If this confirmation code is not entered, or entered incorrectly, registration will not proceed. The confirmation code is a generated as Random Value. The confirmation code is valid for seven (7) days.

3.2.3.3 Country

The country field in the certificate will be field with the nationality of the Applicant if present on the identity document or the issuing country of the identity document.

For certificates where the subject is an organisation, the country code is the country where the organisation is registered based on data from company registers (e.g. national trade registers).

For certificates where the country of the subject is unknown, the country code of Digidentity (NL) is used.

CPS PKIoverheid @ Digidentity

3.2.3.4 Remote identification

Digidentity has developed and implemented a Remote Identification process as an alternative to face-to-face verification to verify the identity of the natural person, validation of the identity document and linking natural person to the identity document.

Our remote identification process uses the NFC capabilities of the mobile phone to read the NFC chip in the ID or take video and photos from the ID.

Digidentity conforms to the applicable requirements of ETSI TS 119 461 for the use cases:

- 9.2 Use cases for identity proofing of natural person
- 9.2.3 Use cases for unattended remote identity proofing
- 9.2.3.3 Use case for hybrid manual and automated operation
- 9.2.3.4 Use case for automated operation
- 9.2.4 Use case for identity proofing by authentication using eID means
- 9.3 Use case for identity proofing of legal person
- 9.4 Use case for identity proofing of natural person representing legal person
- C.3.2 Use case for identity proofing by authentication using eID means
- C.3.4 Use case for identity proofing by other identification means
- C.3.5 Use case for identity proofing of legal person
- C.3.6 Use case for identity proofing of natural person representing legal person

Digidentity uses remote identification to perform identity proofing for all identity proofing contexts. The remote identification method is determined by the level of assurance of the Product selected:

- Level of Assurance 4, EU Qualified or eIDAS High - remote identification using NFC, biometric verification
- Level of Assurance 3, EU Advanced or eIDAS Substantial - remote identification using NFC or video of ID, biometric verification
- Level of Assurance 2 or eIDAS Low - remote identification using NFC or video of ID, biometric verification

For eID on eIDAS High, all remote identity proofing must be verified manually (Registration Officer checks the identity proofing and approves registration).

The Digidentity Remote Identification process has been confirmed by an external auditor as equal assurance to physical presence.

3.2.3.4.1 Cryptographic Validation of Digital Identity Documents

Digidentity supports the use of Near Field Communication (NFC) to read the NFC chip in modern identity documents (e.g. passports, identity cards and driving licenses). This chip is standardised as part of Doc 9303, Machine Readable Travel Documents (MRTD), by the International Civil Aviation Organization (ICAO). Digidentity performs an automated cryptographic validation of the identity document and verification of the data.

CPS PKIoverheid @ Digidentity

The Applicant uses the Digidentity Wallet (mobile app for iOS and Android) to read the data from the chip in the identity document using passive authentication and if available clone detection. The data uploaded to Digidentity includes the high-resolution photo of the document holder.

This method is used for all Products but is mandatory for Qualified certificates, Seals and eIDAS High or other Level of Assurance level 4 Products.

3.2.3.4.2 Optical Validation of Physical Identity Documents

Digidentity supports the validation of identity documents optical validation checks using photos of the physical identity document. The Applicant uses the Digidentity Wallet (iOS and Android) to record a video of the front and back of the identity document. The video is uploaded to Digidentity. Two images (one of the front and one of the back of the identity document) are extracted from the video.

An automated check of the security features of the document is performed to detect manipulation. The validity of the document is inspected, as well as the date issuance. The data on the document from the Visual Inspection Zone (VIZ) and the Machine-Readable Zone (MRZ) is extracted. The data is compared, analysed, and verified to determine the correctness and plausibility of the data.

The validation process uses a combination of technologies to validate the genuineness of the identity document. This includes sophisticated artificial intelligence analytics (computer vision, machine learning and deep learning) to analyse video of IDs, collecting evidence for identity verification. A higher level of machine learning weighs the results from hundreds of these algorithms, making an intelligent decision about the relative importance of each piece of evidence, then predicts whether the ID is genuine. The analysis will detect if a photo is real and not a photo of a screen or copy of an identity document.

This method is used for Products with a Level of Assurance 3 or eIDAS Substantial and lower.

A detailed description of identity document validation is documented in "Identity Proofing @ Digidentity" available on our website at https://www.digidentity.eu/documentation.

3.2.3.4.3 Verification of natural person using Liveness Detection

Digidentity performs liveness detection using artificial intelligence to verify an actual 'live' person is performing the registration process. Liveness detection of the Applicant is performed during the selfie taking process.

The Digidentity Wallet starts a video stream of the Applicant where the Applicant must move their head in a randomly selected direction. The Wallet extracts to images from the video stream which are used for the liveness detection. The artificial intelligence system detects natural movement of the head and verifies that the photos are not taken from a screen, video or the Applicant is wearing a mask. The registration process continues when liveness detection was successful. The Applicant is allowed to perform five liveness detection attempts. The registration process stops when liveness is not detected after five attempts.

A detailed description of liveness detection is documented in "Identity Proofing @ Digidentity" available on our website at https://www.digidentity.eu/documentation.

CPS Rijkoverheid @ Digidentity

3.2.3.4.4 Binding a natural person to an Identity Document using Face Comparison

Digidentity uses face comparison to link or bind the natural person to the identity document provided as evidence. We use the high-resolution image from the NFC chip or the image extracted from the photo of the ID to compare to the selfies taken by the Applicant.

The comparison is performed on our servers. No user profiles are created. Using a combination of sophisticated artificial intelligence analytics (computer vision, machine learning and deep learning) to analyse photos from the IDs and end-users' face selfies, collecting evidence for identity verification. A higher level of machine learning weighs the results from hundreds of these algorithms, making an intelligent decision about the relative importance of each piece of evidence, then predicts whether the ID photo is genuine and belongs to the Applicant. The analysis will detect if a photo is real and not a photo of a screen or copy of an ID and if the live person matches the person on the ID.

A detailed description of liveness detection is documented in "Identity Proofing @ Digidentity" available on our website at https://www.digidentity.eu/documentation.

3.2.3.5 Terms & Conditions and Privacy Statement

During registration, it is required to agree with the General Terms & Conditions and Privacy Statement available on our website at https://www.digidentity.eu/documentation.

3.2.3.6 General verifications

For all applications, Digidentity verifies:

- Organisational information where applicable
- All representatives must be identified on the level of assurance of the Product
- FQDN status and Applicant details where applicable

If the legal representative of an organisation approves, it is possible to authorise another person to handle the application and management of certificates as a Company Administrator. The delegated person will be verified via the process described above, including remote identification. The delegated person also needs to submit a signed authorisation letter from the legal representative, stating the authorisation for the delegated person. Digidentity verifies the authorisation letter by name and signature match of the legal representative.

If the legal representative of an organisation approves, it is possible to authorise another person to handle the authorisations of the organisation as the Company Administrator. The delegated person will be verified via the process described above, including remote identification. The delegated person also needs to submit a signed authorisation letter from the legal representative, stating the authorisation for the delegated person. Digidentity verifies the authorisation letter by name and signature match of the legal representative.

A detailed description of verifying the legal person identity is documented in "Identity Proofing @ Digidentity" available on our website at https://www.digidentity.eu/documentation.

CPS PKIoverheid @ Digidentity

3.2.4 Non-Verified Subscribers Information

Digidentity does not verify any IP addresses, or intellectual property rights of applicants.

3.2.5 Validation of Authority

Digidentity validates the applicant's legal status (described in section 3.2.2) by:

- Checking the company registration with an authentic source (e.g. national trade registers, PROBAS, OIN register, other register or notary) for organisational applicants
- Checking the identity of the applicant with remote identification
- Where the applicant has been authorised by the legal representative of an organisation, authorisation must be completed, or there must be a completed authorisation available.

3.2.6 Criteria for Interoperation or Certification

Digidentity has no interoperation or cross-certification.

3.3 Identification & Authentication for Re-Key Requests

Digidentity does not perform re-key of certificates.

3.4 Identification & Authentication for Revocation Request

If the subscriber wishes to make an application for revocation (deletion and deactivation included), then the following is applicable;

3.4.1 Website

Subscribers can log into their account and revoke personal certificate(s). If a Subscriber can log into their account, the identity is verified. After selecting 'delete smart card and revoke certificates', the subscriber must confirm revocation on the mobile device by entering the Virtual Smart Card's PIN code. After confirmation on the mobile device, the certificates are revoked and the link between mobile device and certificates is deleted.

To revoke server certificates, the Subscriber or Company Administrator must log into their account to access the Self-Service Portal (SSP). In the SSP, the Subscriber or Company Administrator can select the certificate to be revoked. A confirmation of the revocation is sent via e-mail.

3.4.2 Account recovery

Digidentity asks Subscribers to revoke their certificates themselves. If a Subscriber is not able to access the account and is unable to revoke the certificate(s), an account recovery process should be started. For personal certificates, the account recovery process verifies possession of the e-mail address in the account by sending a confirmation code to the Subscriber. After the confirmation code is entered, the Subscriber can enter a new password to access the account.

CPS PKIoverheid @ Digidentity

3.4.3 Recover authenticator

In case the Subscriber has lost the device, forgotten the five-digit pin code or has deleted the mobile app, the Subscriber has to create a new authenticator to recover the 'lost' certificates. The Subscriber can log in to the account and click on "I lost access to these authenticators", when asked for a two-factor authenticator. The account recovery process is started where, for additional verification, the date of birth is requested. After providing the correct confirmation code and date of birth, the Subscriber has access to the account.

The Subscriber can request a new authenticator with certificates by clicking "recover". In the account, the evidence collected from the identity document during registration is deleted, the product status is moved to 'pending' and the authenticator is deactivated. The Subscriber can now start the process to create a new authenticator and certificates by scanning a QR-code and uploading an identity document. After verification, a QR code can be scanned to create the authenticator with Certificates as well as a new five-digit pin code. The authenticator with new certificates is then activated.

3.4.4 Phone

If the Subscribers or Company Administrators cannot login to the account, it is possible to receive support to access the account by calling Digidentity. The Service Desk is available during office hours. Outside office hours, you can call the emergency revocation line (see Section 4.9.3).

Digidentity will always support the subscriber to revoke the certificates themselves on the website. In case, access to the account is lost or access to the smart card on the mobile device is lost, we support the subscriber with the recovery process as described in 3.4.1.

Digidentity recognises that it is not always possible for Company Administrators to revoke certificates. In these instances, Company Administrators may call Digidentity (see Section 4.9.3 for the revocation procedure).

Company Administrators are required to answer questions to confirm their identity, and the certificate that requires revocation:

- Official Name
- Company registration number
- Organisation name
- E-mail address
- Certificate to be revoked

If answered correctly, Digidentity will send an e-mail, requesting confirmation for the revocation, to the Company Administrators' e-mail address, as shown in the account. The Company Administrator must reply to this for the revocation to take place. If the Company Administrators no longer has the e-mail address in the account, we request a copy of their identity document to verify their identity.

CPS PKIoverheid © Digidentity

3.4.5 E-mail

Digidentity does not accept revocation requests via e-mail or other means. We are required to revoke certificates within four (4) hours after the request is made which we cannot guarantee if the revocation request is not performed according to the three procedures described.

If the subscriber has lost access to the e-mail address in the account, the account cannot be recovered.

3.4.6 Professional Bodies

Professional Bodies can request revocation of certificates for Professional QES issued to a natural person. Digidentity and the Professional Body agreed on a procedure for revocation requests to revoke these certificates in case a professional is no longer entitled to the title of the profession.

CPS PKIoverheid @ Digidentity

4 Certificate Life-Cycle Operation Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

A certificate application can be submitted by a:

[1] Natural person applying for a personal qualified certificate

[2] Natural person applying for a Professional QES

[3] Natural person legally representing an Organisation (legal entity) and applying for a business qualified certificate for electronic seals or Professional QES

[4] Natural person legally representing an Organisation (legal entity) and applying for a server certificate for that Organisation.

Before applying for a certificate, an Applicant must register via the Digidentity website or the Digidentity Wallet.

4.1.2 Enrolment Process and Responsibilities

The Applicant is responsible for providing Digidentity with correct and up-to-date data required for the generation and issuance of certificates and for the correct use of the certificates. The Applicant warrants to Digidentity and Relying Parties that they will abide by the General Terms & Conditions, Product Terms & Conditions, and the CPS.

The Applicant is required to accept the General Terms & Conditions, Product Terms & Conditions and Privacy Statement. If any of the information required to issue a certificate is missing, incomplete or produces a negative outcome e.g. the organisation is in bankruptcy, or the identification document is indicated not to be genuine, then Digidentity will reject the application for a certificate. Certificates linked to an organisation require an authorisation process during registration, to determine the legal status of the applicant as an organisational representative and a verification of the organisation details.

For certificates for Registered Professions, a Dutch trade register registration is required.

Subscribers have obligations for the use of the certificate, which are set out in General Terms & Conditions, Product Terms & Conditions, the CPS and a contract where applicable. Prior to any certificate issuance the subscriber will be required to accept the applicable Terms & Conditions.

4.2 Certification Application Processing

Digidentity carries out verification procedures during the registration process (see Section 3.2).

4.2.1 Performing Identification and Authentication Functions

See section 3.2.

CPS PKIoverheid © Digidentity

4.2.2 Approval or Rejection of Certificate Applications

Digidentity rejects any certificate application that cannot be verified. Digidentity does not issue certificates containing Internal Names.

If any steps in the registration process fail, Digidentity will reject the certificate request.

4.2.3 Time to Process Certificate Applications

Digidentity can process certificate application information during Service Desk opening hours. Completion of the certification issuing process is dependent on type of certificate and the availability of both parties (Digidentity and applicant) to make an appointment for the face-to-face identity check if applicable. The total processing time from application to issuance of a certificate is approximately fifteen (15) minutes to five (5) working days.

4.3 Certificate Issuance

The issuance of any certificate by Digidentity is carried out per the information in this CPS, per the requirements (legal and regulatory) described in Section 1.1.

For Qualified Certificates, and Seals, once the authenticator creation is completed, the Subscriber has possession. The authenticator is used/activated by entering the pin code upon receiving a push notification on their mobile phone. The Subscriber can download the certificates from their Digidentity account. Company Administrators are able to download server certificates by signing into Self Service Portal using their account credentials.

4.3.1 CA Actions During Certificate Issuance

Certificate issuance by the Root CA's is only performed by the Policy Authority operations facility.

4.3.2 Notification of Certificate Issuance

Upon successful application and issuance of a certificate, the applicant will receive a notification via e-mail.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

Upon successful issuance of the certificate, the Applicant is known as the Subscriber. The certificate is deemed to have been accepted by the subscriber once:

- The authenticator is linked with a pin code to the Subscriber
- The certificate has been downloaded, used and/or installed.
- A period of more than one (1) calendar month has passed and no communication has been received from the Subscriber.

CPS PKIoverheid @ Digidentity

4.4.2 Publication of the Certificate by the CA

Digidentity has published all CA certificates of the Digidentity CA hierarchy as described in section 1.1.2 in the repository on the Digidentity website (https://cps.digidentity-pki.com/).

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

Digidentity only notifies the Subscriber of a certificate. Other relying parties are able to enquire certificate statuses via the CRL and possibly the OCSP.

4.5 Key Pair & Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

The Subscriber has the obligation to use the certificate in accordance with this CPS, the General Terms & Conditions, Product Terms & Conditions and the Key Usage field on the certificate itself. Relying parties may only use the public key of the certificate for the purposes described in the relying party agreements with Digidentity, and as described in this document. The appropriate certificate usage is denoted by the Key Usage field provided in the certificate.

4.5.2 Relying Party Public Key and Certificate Usage

Relying parties are responsible for verifying:

[a] certificate validity.
[b] validity of the complete chain of certificates, up to the root certificate.
[c] revocation status of the certificate.
[d] limitations on any use of the certificate
[e] authenticity of all Certificate Status information is verified by the electronic signature by which the information has been signed

4.6 Certificate Renewal

Digidentity does not perform renewal of issued certificates. Digidentity renews a certificate by issuing new certificate.

4.7 Certificate Re-Key

Digidentity does not perform re-key of certificates.

4.8 Certificate Modification

Digidentity does not perform modification of certificates.

4.9 Certificate Revocation & Suspension

4.9.1 Circumstances for Revocation

Revocation occurs when the certificate is permanently revoked before the natural expiration time of the certificate. Digidentity reserves the right to revoke certificates at its own discretion and/or based on information received.

CPS PKIoverheid @ Digidentity

4.9.1.1 Reasons for Revoking a Subscriber Certificate

Digidentity will revoke a certificate when:

[1] Subscriber notifies the CA that the original certificate request was not authorised and does not retroactively grant authorisation;

[2] CA obtains evidence that the Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of Section 6.1.5 and 6.1.6;

[3] CA obtains evidence that the certificate was misused;

[4] CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement, General Terms & Conditions or Product Terms & Conditions;

[5] CA is made aware of a material change in the information contained in the certificate;

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

[7] CA is made aware that the certificate was not issued in accordance with the requirements or the CAs Certificate Policy or Certification Practice Statement;

[8] CA determines that any of the information appearing in the certificate is inaccurate or misleading;

[9] CA ceases operation for any reason and has not made arrangements for another CA to provide support for revocation of the Certificate;

[10] Revocation is required by the CA's Certificate Policy and/or Certification Practice Statement; or

[11] Technical content or format of the certificate presents an unacceptable risk to Subscribers, Relying Parties and third parties;

[12] The Subscriber ceases operation;

[13] The Subscriber is deceased.

4.9.1.2 Reasons for Revoking a Subordinate CA Certificate

Revocation of Subordinate CA Certificate is performed by the Policy Authority PKIoverheid.

4.9.2 Who can request Revocation?

Revocation can be requested by:

[a] Subscriber (or Certificate Holder)

[b] Legal representative or authorised person of the organisation (Company Administrator)

[c] Digidentity

[d] Professional Bodies

[e] Authorities/regulators who are involved in the regulation of PKIoverheid activities, e.g. Logius

Digidentity has the requirement to revoke certificates if there is notification that the Subscriber/or legal representative in the certificate is deceased.

CPS PKIoverheid © Digidentity

4.9.3 Procedure for Revocation Request

Revocation of certificates can be performed:

[1] By the Subscriber themselves, by logging into their account and requesting the revocation of issued certificates. The Subscriber is able to click “Change two-factor authentication”, “Revoke Certificates”.

[2] During office hours (9.00 – 17.00 hours) by calling the Service Desk at +31 (0)88 778 78 78

[3] Outside of office hours by calling the emergency revocation line at +31 (0)88 778 78 00

Revocation must be performed by the Subscriber. If you call Digidentity for revocation, we will support you in accessing your account and enable you to revoke your certificates yourself. Digidentity will not revoke the certificate on your behalf.

Subscriber is able to log into their account and click “Revoke certificates”. The Subscriber is able view their authenticator which contains their certificates. By deleting a specific authenticator, all associated certificates (authentication, encryption and non-repudiation) will be revoked. Revocation occurs immediately.

To revoke server certificates, the Subscriber or Company Administrator must log into their account in the Self-Service Portal (SSP) using two factor authentication. In the SSP, the certificate to be revoked.

Third parties can request revocation of a Subscriber certificate by contacting Digidentity to request revocation and provide evidence to support the revocation request.

The Subscriber or Company Administrator will receive confirmation of the revocation of the certificates. The procedure for identity validation for revocation is described in section 3.4.

4.9.4 Revocation Request Grace Period

For certificates the revocation is immediate. There is no grace period.

4.9.5 Time within which Certificate Authority must process the Revocation Request

Digidentity processes and completes the revocation of certificates within four (4) hours of receiving the request to revoke from the Subscriber.

4.9.6 Revocation Checking Requirement for Relying Parties

Relying Parties are responsible for checking the certificate status and CRL. Relying Parties that fail to check the status of the certificate cannot legitimately rely on the certificate.

4.9.7 CRL Issuance Frequency

Digidentity publishes the CRL for the issuing CA every four (4) hours, whereby the CRL is valid for 24 hours.

All Digidentity certificates issued by Digidentity have a CRL distribution point extension that contains an URL for CRL retrieval.

CPS PKIoverheid @ Digidentity

4.9.8 Maximum Latency for CRLs

The maximum latency for the CRL is ten (10) seconds.

4.9.9 Online Revocation/Status checking Availability

All Digidentity server certificates have an Authority Information Access extension that contains an URL for the OCSP service. OCSP is updated within 4 hours when a certificate is revoked. OCSP responses are valid for 24 hours. All OCSP responses conform to RFC6960.

All responses are digitally signed by the private key of Digidentity TSP CA, or by a Digidentity issuing CA which issued the related certificate.

4.9.10 Online Revocation checking Requirements

Relying parties are responsible for checking the certificate status and CRL. Relying parties that fail to check the status of the certificate cannot legitimately rely on the certificate.

Digidentity supports an OCSP capability using the HTTP GET method for certificates as described in RFC6960 and RFC5019. OCSP Responders under Digidentity's control will respond to a request for the status of a certificate serial number that is "unused" with an "unknown" status.

4.9.11 Other Forms of Revocation Advertisements available

No stipulation

4.9.12 Special Requirements related to Key Compromise

Digidentity has implemented measures to notify relying parties if there is discovery or suspicion that a CA's private key has been compromised. For more information refer to section 4.9.1.

Revocation of a domain or a TSP certificate (or distrust in case of a root certificate) will be considered if the signing key belonging to the certificate is compromised or suspected to be compromised. Indicators of private key compromise may include:

[a] Theft or loss of device holding a private key;
[b] Audit findings indicating private key compromise;
[c] Incidents reported by third parties which may indicate key compromise.

All indicators are registered, analysed, and followed up accordingly.

4.9.13 Circumstances for Suspension

Digidentity does not perform suspension of certificates.

4.9.14 Who Can Request Suspension

Digidentity does not perform suspension of certificates.

CPS PKIoverheid © Digidentity

4.9.15 Procedure for Suspension Request

Digidentity does not perform suspension of certificates.

4.9.16 Limits on Suspension Period

Digidentity does not perform suspension of certificates.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

Digidentity makes certificate status information available on the CRL and via an OCSP responder. The serial number of a revoked certificate remains on the CRL until one additional CRL is published after the expiration date of the certificate. For Qualified certificates, the serial number of a revoked certificate remain on the CRL permanently.

4.10.2 Service Availability

Digidentity operates and maintains a CRL and OCSP with sufficient resources to provide a response time of ten seconds or less under normal operating conditions. Digidentity maintains an online 24 x 7 repository that application software can use to automatically check the current status of all unexpired certificates issued by the CA. Digidentity maintain a continuous 24x7 ability to respond internally to a high-priority Certificate Problem Report.

Digidentity aims to restore the service within four (4) hours in the event the service becomes unavailable.

4.10.3 Optional Features

No stipulation.

4.11 End of Subscription

See General Terms & Conditions for information on ending a Subscription.

4.12 Key Escrow & Recovery

Digidentity does not use key escrow and key recovery.

CPS PKIoverheid © Digidentity

5 Facility, Management & Operational Controls

5.1 Physical Security Controls

5.1.1 Site Location & Construction

All Digidentity's operations facilities are specifically designed for computer operations and have been customised to meet the security requirements that apply to Digidentity as a Certificate Authority. Relevant prevention and detection mechanisms are to address environmental incidents, such as power loss, loss of communication, water exposure, fire and temperature changes.

Digidentity uses two data centres from North-C (https://www.northcdatacenters.com/en/) in The Netherlands for Trustworthy systems such as HSM which are not allowed in the cloud. These data centres are secured, and only authorised employees have access to the data centres. The data centres provide fail over mechanisms in case of disruption of service in one of the data centres.

The data centres have redundant power connection to the utility grid, redundant Uninterruptable Power Supply (UPS), emergency power redundancy, direct adiabatic cooling, redundant cooling, fire detection system, HI-FOG water mist system fire extinguishing.

The data centres are secured using layered physical security, fences and gated areas, CCTV surveillance inside and outside the data centres, professional security personnel 24×7, biometric access controls.

All other services are provided from AWS from the Amazon data centre in Dublin (Ireland) and fail over site in Frankfurt (Germany).

Digidentity requires that data centres are ISO27001 certified and review annually the scope, Statement of Applicability and validity of the certification. Digidentity tests and reviews the physical security controls and updates the controls if applicable.

5.1.2 Physical Access

Access to Digidentity's facilities is restricted to authorised personnel only. Non-authorised personnel, including visitors, are only allowed to access the facilities under escort and continuous surveillance by authorised personnel. Controls have been implemented for physical access to the CA operations facilities.

Access to the Digidentity offices is controlled. Access is permitted to employees with an electronic key system. Visitors receive access on appointment only.

Physical access to the data centre is limited to specific employees in specific roles. All access to the data centre is logged. Employees accessing the data centre are subjected to multi-factor authentication using ID card and a biometric authentication. Digidentity reviews and if applicable update the physical access controls.

CPS PKIoverheid @ Digidentity

5.1.3 Power and Air Conditions

See section 5.1.1.

5.1.4 Water Exposures

See section 5.1.1.

5.1.5 Fire Prevention and Protection

See section 5.1.1.

5.1.6 Media Storage

See section 5.1.1.

5.1.7 Waste Disposal

See section 5.1.1.

5.1.8 Off-Site Backup

See section 5.1.1.

5.2 Procedural Controls

5.2.1 Trusted Roles

Digidentity has safeguards to ensure that operations are as secure as they can be. All employees at Digidentity are required to register for their own administrative account, details of accounts are never shared. The types of accounts assigned to users is dependent on their role.

The Trusted Roles within Digidentity are:

- Registration Authority Officers (RA): responsible for verifying information that is necessary for certificate issuance and approval of certification requests.
- Revocation Officers (RO): Responsible for operating certificate status changes.
- System Administrators (SA): Authorised to install, configure and maintain systems
- System Operators (SO): responsible for the day-to-day operation of systems. Authorised to perform backup and restore procedures.
- System Auditors (SAU): Authorised to view archives and audit logs of Digidentity systems for the purposes of auditing.
- Chief Security Officer (CSO): overall responsibility for maintenance and implementation of the security policies and practices.
- Data Protection Officer (DPO) - Responsible for the handling of all security incidents involving Person Data Breach/Leakage.

5.2.2 Number of Individuals required per task

Digidentity ensures that the number of staff available for tasks is adequate to meet demand, but also adequate to ensure that all security, risk and compliance regulation requirements are met.

Issuance of intermediate CA certificates by the Digidentity root CAs and maintenance operations involving CA private keys is under dual control by authorised, trusted personnel.

CPS PKIoverheid @ Digidentity

5.2.3 Identification & Authentication for Trusted Roles

Employees in Trusted Roles at Digidentity undergo background screening, and all employees are verified and authenticated, including face-to-face checks and identification checks based on government issued identity documents.

5.2.4 Roles requiring Separation of Duties

Digidentity has a comprehensive list of roles (see 5.2.1) and associated access rights. Privileges are assigned based on the tasks for the role, and a "need-to-know" and "least privilege" principle for access, rather than a default permission. Digidentity keeps a record of all access rights held by employees. Digidentity performs regular reviews on issued authorisations and privileges.

Personnel who have a specific trusted role will, in some circumstances, be unable to participate as a second trusted role e.g. System Auditors cannot have the joint role of System Operators.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

For every role in Digidentity there is a written set of requirements. Any employee at Digidentity must meet the qualifications and experience requirements to fulfil the role. The background check results are stating that there are no objections to perform the role in the category/categories it was requested for.

5.3.2 Background Check Procedures

Digidentity carries out background check procedure for all employees. These checks will consist of;

- Previous employment and references
- Qualifications
- Good conduct (requested by the individual for the purpose of employment at Digidentity and performed by a Dutch Government Judicial Service. Result is communicated to the individual).

5.3.3 Training Requirements and Procedures

Digidentity provides all personnel performing information verification duties with skills-training that covers basic Public Key Infrastructure knowledge, authentication and vetting policies and procedures (including the CA's Certificate Policy and/or Certification Practice Statement), common threats to the information verification process (including phishing and other social engineering tactics), and the relevant Trust Service Provider and CA requirements.

Digidentity maintains records of such training and ensure that personnel entrusted with Validation Specialist duties maintain a skill level that enables them to perform such duties satisfactorily. Digidentity document that each Validation Specialist possesses the skills required by a task before allowing the Validation Specialist to perform that task. Digidentity requires all Validation Specialists to pass an examination provided by Digidentity on the information verification requirements outlined in this document.

CPS PKIoverheid © Digidentity

Upon employment, all new employees follow a training plan. The training includes security awareness and other training related training associated with their specific function, which includes (where applicable) software, hardware, office procedures and security awareness.

5.3.4 Retraining Frequency and Requirements

All employees are required to take regular security awareness training. Service Desk employees are required to participate in the annual validation specialist training.

5.3.5 Job Rotation Frequency and Sequence

Digidentity does not use this method.

5.3.6 Sanctions for Unauthorized Actions

Digidentity has a disciplinary procedure. In the event of unauthorised employee actions, the procedure will be followed. Disciplinary action can result in termination of employment and/or legal action where applicable.

5.3.7 Independent Contractor Controls

Digidentity employs contractors. Contractors employed in roles at Digidentity are background checked per the procedures used for direct personnel.

5.3.8 Documentation Supplied to Personnel

All employees are provided with a contract of employment, a defined job role, and a personnel handbook. Collectively these documents provide necessary information regarding role, rights, laws and procedures pertaining to employment at Digidentity.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

The logging system records the following types of events;

[1] Key Lifecycle Events;
- **[a]** Key generation, backup, storage, recovery, archival and destruction
- **[b]** Cryptographic device lifecycle management events

[2] Certificate Lifecycle Events;
- **[a]** Certificate requests and revocation
- **[b]** Verification activities
- **[c]** Date, time, phone numbers, contact persons, and verification of those
- **[d]** Acceptance and rejection of certificate requests
- **[e]** Issuance of certificates
- **[f]** Generation of CRLs and OCSPs

[3] Security Events;
- **[a]** Access attempts
- **[b]** System actions performed
- **[c]** Profile changes

CPS PKIoverheid @ Digidentity

[d] System activity
[e] Firewall and router activity
[f] Entries to and from Digidentity controlled areas

All log entries provide the date and time, the identity of the person and a description of the event.

5.4.2 Frequency of Processing Audit Log

Daily backups are made of all data resulting from CA key lifecycle and certificate lifecycle management, including systems thereof.

5.4.3 Retention Period for Audit Logs

Logs associated with CA key lifecycle and certificate lifecycle management events are kept for seven (7) years, per the regulatory and legal requirements.

5.4.4 Protection of Audit Logs

All audit events recorded are digitally signed to ensure logs have not been tampered. The audit log data is available in a read-only format and subject to access restrictions.

5.4.5 Audit Log Backup Procedures

Digidentity performs daily backups.

5.4.6 Audit Log Collection System (Internal vs. External)

The internal Audit Logger records events as they pass through the system. Upon unavailability of the Audit Logger, dependent services stop functioning.

5.4.7 Notifications to Event-Causing Subject

Digidentity does not notify people of their actions creating an event.

5.4.8 Vulnerability Assessments

Digidentity performs an annual risk assessment to maintain the risk register. In case of significant changes, a risk assessment for the significant change must be performed.

Digidentity's systems are assessed via internal and external vulnerability scans and penetration tests. The tests are carried out per the schedule. Penetration tests are carried out by external contractors at least once per year. All foreseeable internal and external threats are assessed with the risk analysis of Digidentity at least once per year or in case of significant changes to the infrastructure or applications.

CPS PKIoverheid @ Digidentity

5.5 Records Archival

5.5.1 Types of Records Archived

Digidentity archives the following types of records:

- identity proofing data,
- certificate life cycle events,
- authorisations,
- configurations,
- authentications,
- revocation,
- face-to-face checks,
- name,

5.5.2 Retention Period for Archive

All records are kept for a maximum of seven (7) years and then destroyed, as per regulatory and legal requirements.

5.5.3 Protection of Archive

Archive data associated with the key lifecycle management and certificate lifecycle processes are subject to access restrictions and controls. Data is only available in a read-only format. The archive data is encrypted and subject to access restrictions. Paper-based archives are subject to access restrictions and controls. Only authorised personnel have access to those areas.

5.5.4 Archive Backup Procedures

Digital archive data is automatically generated via the internal systems processes. Backups of systems are made daily and in accordance with the backup procedures and policies at Digidentity.

5.5.5 Requirement for Time-Stamping of Records

Digidentity CA time-stamps all records related to CA activities.

5.5.6 Archive Collection System (Internal or External)

The archive collection systems are in the data centres. The data centres are described in Section 5.1.1.

5.5.7 Procedures to Obtain & Verify Archive Information

Archive data access is strictly limited. Only very specific authorised employees may access this system. Digidentity will further only release information from the archive upon a legal court order to do so.

5.6 Key Changeover

Digidentity do not do key changeover for any of its issuing CA. Digidentity's PKIoverheid issuing CA expire on the same date as their respective root CA.

CPS PKIoverheid @ Digidentity

5.7 Compromise & Disaster Recovery

Digidentity has a business continuity plan 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, and continuity of Products for the Subscriber affected. The business continuity plan is a confidential document and has been audited and approved by external auditors.

5.7.1 Incident and Compromise Handling Procedures

Digidentity has an Incident Response Plan and a Disaster Recovery Plan. Digidentity documents a business continuity and disaster recovery procedure designed to notify and reasonably protect Application Software Suppliers, Subscribers, and Relying Parties in the event of a disaster, security compromise, or business failure. Digidentity makes its business continuity plan and security plans available to auditors upon request. Digidentity annually tests, reviews, and updates these procedures.

5.7.2 Recovery Procedures if Computing Resources, Software, and/or Data Are Corrupted

No Stipulation

5.7.3 Recovery Procedures After Key Compromise

No Stipulation

5.7.4 Business Continuity Capabilities after a Disaster

Digidentity is certified against the requirements of ISO22301:2019 Business Continuity Management System.

5.8 CA or RA Termination

Digidentity has a CA Termination plan in the event of a CA operation ends. This termination plan aims to manage the termination, while carrying out actions per regulatory and legal requirements. Digidentity has the necessary arrangements and agreements with third parties for continued operations and fulfilment of obligations in case of CA termination. Digidentity's CA Termination plan is confidential and has been audited by external auditors.

CPS PKIoverheid @ Digidentity

6 Technical Controls

6.1 Key Pair Generation & Installation

6.1.1 Key Pair Generation

6.1.1.1 CA Key Pair Generation

Digidentity has a procedure key pair generation. Digidentity maintains a record of all key ceremony performed. All key ceremonies are audited by qualified external auditors conform the requirements. All attendees who have roles in the key ceremony are recorded. In addition, a sign-off is required for the documented key ceremony.

Digidentity does not perform key pair generation for the PKIoverheid root CA.

All key generation takes place in a physically secured environment, using personnel in trusted roles, and within cryptographic modules in accordance with this CPS as described in chapter 5. All keys are generated conform the specified key lengths and algorithms as per ETSI TS 119 312.

6.1.1.2 RA Key Pair Generation

No stipulation.

6.1.1.3 Subscriber Key Pair Generation

Digidentity generates and stores the key pair for qualified, advanced and seals in the HSM. For server certificates, the Subscriber generates a new key pair for each certificate and is required to keep the private key secret as defined in the applicable Terms & Conditions.

Digidentity reject a certificate request if the requested Public Key does not meet the requirements set forth in Sections 6.1.5 and 6.1.6 or if it has a known weak Private Key (such as a Debian weak key, see http://wiki.debian.org/SSLkeys) or the Key Pair was previously generated by Digidentity.

6.1.2 Private Key Delivery to Subscriber

See section 3.2.1.

6.1.3 Public Key Delivery to Certificate Issuer

Public Keys for SSL/SBR certificates are delivered to Digidentity via the CSR, since they are generated by the applicant during the registration process and submitted via the online secure interface.

6.1.4 CA Public Key Delivery to Relying Parties

The root CA's of Digidentity for this CPS is Staat der Nederlanden, which means that the public key does not require delivery by Digidentity. Digidentity CA public keys of can be downloaded from the repository online: https://cps.digidentity-pki.com/.

CPS PKIoverheid @ Digidentity

6.1.5 Key sizes

All PKIoverheid CAs makes use of 4.096 bits RSA keys. All PKIoverheid Root Certificates and Subordinate CA are defined and configured by PKIoverheid.

The length of the Subscriber's cryptographic keys must fulfil the requirements defined in ETSI TS 119 312. All Digidentity Subscriber Certificates make use of 2.048 bits, 3.072 bits or 4.096 bits RSA keys.

Since 1 October 2026, Digidentity keys will have length of 3.072 bits.

6.1.6 Public Key Parameters Generation & Quality Checking

Digidentity employs several certificate validators (linters) where applicable. The (pre-)certificate issuance process will abort if a linter detects any non-conformities to the requirements.

ZLint

The ZLint linter verify compliance to X.509 RFCs and ETSI standards. Digidentity has implemented these linters for distinct issuance phases: pre-issuance and post-issuance of final certificates.

RSA Key Validator

The RSA Key Validator checks if the public key of the certificate has:

- Modulus is 3.072 or 4.096 bits,
- the value of the public exponent is an odd number equal to 3 or more;
- the public exponent is in the range between 2^{16+1} and 2^{256-1}
- the modulus is an odd number, not the power of a prime, and have no factors smaller than 752
- Key passes a ROCA vulnerability test (recovery of Private Key from the Public Key)
- Key is not a Debian Weak Key (entropy check)

Digidentity has implemented the RSA Key Validator on issuance of all certificates.

Digidentity Linters

Digidentity has developed and implemented own linters to verify compliance to CPS. These linters are available for:

- Generation of PKIoverheid SBR & Server certificates
- Generation of PKIoverheid Qualified certificates
- Generation of PKIoverheid authentication certificates

Digidentity has implemented these linters for pre-issuance of all Subscriber certificates, post-issuance of pre-certificates (if applicable) (server) and post-issuance of all final certificates.

6.1.7 Key Usage Purposes

Keys may be used in accordance with the certificate uses described in this CPS, for the signing of public keys and signing of the CRLs and OCSPs.

CPS PKIoverheid @ Digidentity

6.2 Private Key Protection & Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

Digidentity uses certified Hardware Security Modules to store private keys for subscribers. Digidentity actively monitors the QSCD certification of the HSM to verify compliance and update systems in case certification will expire. The CA Private Keys are stored and protected by an HSM.

If the QSCD certification of the HSM is revoked before expiration, Digidentity will contact the manufacturer, the external auditor and supervisory body to determine the course of actions to resolve the issue.

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

All physical access to the CA Private Key requires dual control.

6.2.3 Private Key Escrow

Digidentity do not use escrow.

6.2.4 Private Key Backup

Digidentity CAs' private keys are encrypted backed up by authorised personnel in trusted roles and under dual control. The backup of the CA Private Key is only activated and used within the CA operations facility.

6.2.5 Private Key Archival

Digidentity archives CA private keys for a period of seven (7) years.

6.2.6 Private Key Transfer into or from a Cryptographic Module

Digidentity does not do key transfer.

6.2.7 Private Key Storage on Cryptographic Module

The CA Private Keys are stored and protected by an HSM where access control mechanisms ensure that the Private Key is not accessible outside the module. Our HSM are compliant to FIPS 140-2 level 3 and accepted under eIDAS article 51. Digidentity verifies that the secure cryptographic modules are functioning correctly at startup. Dual control is required for all physical access to cryptographic devices containing a copy of the CA Private Key.

Digidentity uses the Entrust nShield 5c HSM appliance containing the nShield 5s HSM PCI cards. The nShield 5s HSM v13.5.1 has been certified as a Qualified Signature Creation Device (QSCD). The certificate is available at: https://www.commoncriteriaportal.org/nfs/ccpfiles/files/epfiles/NSCIB-CC-2200057-01-Cert.pdf

6.2.8 Activating Private Keys

Digidentity Private Keys are protected by and used within an HSM. The CA Private Key is only activated and used within the CA operations facility.

CIS Rijverheid @ Digidentity

6.2.9 Deactivating Private Keys

Digidentity do not deactivate private keys.

6.2.10 Destroying Private Keys

Private keys are destroyed when they are no longer required, or when the corresponding certificate expired or is revoked. On retirement of an HSM, all keys necessary to decrypt CA private signing keys are destroyed.

6.2.11 Cryptographic Module Rating

Digidentity maintains procedure that cover the secure lifecycle management (generation, backup, archival, destruction) of all cryptographic modules containing the CA Private Key. All cryptographic modules containing copies of the CA Private Key is physically protected under dual control.

All signing operations with the CA Private Key is performed in Digidentity's secure operations facility.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

Public keys are registered and archived digitally. All public key material is archived for a mandatory requirement of seven (7) years once the key is expired. These archives are encrypted.

6.3.2 Certificate Operational Periods & Key Pair Usage Periods

Certificates are issued for a specific period, where the associated keys will only be valid for the same length of time. Once a certificate is revoked, the associated key pair is also deemed revoked.

- Digidentity BV PKIoverheid Private Services CA – G1 is valid until 12 November 2028
  - Certificates are valid for one (1), two (2) or three (3) years
- Digidentity - G4 PKIo EUTL G-Sigs NP - 2025 is valid until 18 May 2039
  - Certificates are valid for 365 days
- Digidentity - G4 PKIo EUTL G-Sigs LP – 2025 is valid until 18 May 2039
  - Certificates are valid for 365 days
- Digidentity - G4 PKIo Priv G-Other NP - 2025 is valid until 18 May 2039
  - Certificates are valid for 365 days
- Digidentity - G4 PKIo Priv G-Other LP - 2025 is valid until 18 May 2039
  - PKIoverheid Private SBR certificates are valid for one (1), two (2) or three (3) years
  - Other certificates are valid for 365 days
- Digidentity - G4 PKIo Priv G-TLS - 2025 is valid until 18 May 2039
  - Certificates are valid for one (1), two (2) or three (3) years

6.4 Activation Data

See section 3.2.

CPS PKIoverheid @ Digidentity

6.4.1 Activation data generation and installation

No stipulation.

6.4.2 Activation data protection

No stipulation.

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

All computer equipment and systems are under strict security measures:

- Dual Control on all CA systems
- All systems that are capable of causing certificate issuance are adequately protected with multi-factor authentication or other technical controls
- Multifactor authentication for online portals/interfaces
- The use of encryption certificates (SSL/TLS) on all systems
- Separation of duties and use of trusted roles
- Use of x.509 certificates for all administrators

6.5.2 Computer Security Rating

All environments, including staging, pre-production and production are “live” under these security controls. Digidentity has a policy that only authorised personnel have access to systems under its control. Digidentity will never permit visitors to access its systems.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

All software development is carried out by Digidentity, by approved and screened Digidentity employees. The measures are strict so that Digidentity can meet the stringent legal and regulatory requirements.

Access to code and systems related to development is strictly limited to personnel approved to carry out their roles.

6.6.2 Security Management Controls

All operational systems and networks of Digidentity are monitored, managed and controlled to ensure their integrity and correct operation.

Digidentity has procedures and schedules for the systems and the related maintenance of them. The team responsible are required to carry out regular systems monitoring and checks. Additional to manual monitoring, it is also an automated process, where the relevant trusted personnel are alerted upon any activity which is out of the expected behaviour.

CPS PKIoverheid @ Digidentity

6.6.3 Life Cycle Security Controls

Digidentity ensures that all systems with respect to the registration service, certificate generation service, subject device provision service, dissemination service, revocation management service and revocation status service:

- have the latest security updates and;
- web application controls and filters all input from users;
- web application encodes the dynamic output and;
- web application maintains a safe session with the user and;
- web application uses a database in a secure manner.

6.7 Network Security Controls

Digidentity performs all technical actions, described in this document, using secure networking measures to prevent unauthorised and malicious activity. All access to systems is under the conditions of strict access controls. Digidentity protects data by using encryption and digital signatures.

The controls are preventive, detective, repressive and corrective in nature. Controls include regular (at least monthly) vulnerability scans and (at least annually) a penetration test.

Digidentity shall adhere to the following timeframes for responding to and remediating vulnerabilities:

Upon identification or notification of a vulnerability, the issue shall be assessed and addressed within 24 hours, based on its severity level.

Remediation timelines are determined by severity as follows: critical vulnerabilities shall be remediated within 72 hours; non-critical vulnerabilities within 7 days; and medium- to low-severity vulnerabilities within 30 to 90 days.

If immediate remediation is not feasible, temporary mitigation measures shall be implemented to reduce risk until a permanent corrective action is deployed. Any exceptions shall be documented by Digidentity.

6.8 Time Stamping

Digidentity performs time-stamping using an external supplier.

CPS PKIoverheid @ Digidentity

7 Certificate, CRL & OCSP Profiles

Digidentity use only approved Certificate Profiles for the issuance of PKI certificates. This document describes the approved certificate profiles for all certificates issued from PKIoverheid (PKIo) issuing CA. CA Hierarchy is documented in Section 1.1.2.

7.1 Certificate Profiles

Digidentity generates non-sequential certificate serial number using 128 bits resulting in serial numbers that have at least 64 bits of output.

7.1.1 Version Number(s)

All certificates are of type X.509 v3.

7.1.2 Certificate Content & Extensions

All Root Certificates and Subordinate Certificates are defined and configured by PKIoverheid.

All Subscriber Certificates are configured per eIDAS and/or ETSI EN 319 411-1/ 411-2.

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

7.1.3 Algorithm Object Identifiers

Digidentity uses RSA encryption with SHA-2 algorithm or RSA-PSS Signature Scheme. All Certificates are configured per eIDAS and/or ETSI EN 319 411-1/411-2.

7.1.4 Name Forms

See Certificates Profiles in section 7.1.10.

7.1.5 Name Constraints

Deleted

7.1.6 Certificate Policy Object Identifier

All policy object identifiers are described in section 1.2. Root certificates are defined and configured by Policy Authority PKIoverheid.

7.1.7 Usage of Policy Constraints Extension

No stipulation.

7.1.8 Policy Qualifiers Syntax and Semantics

No stipulation.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

CPS PKIoverheid © Digidentity

7.1.10 Certificate Tables

See Appendix B – Certificate Profiles for all certificates profiles

7.2 CRL Profile

7.2.1 Version Number(s)

All CRL certificates are of type X.509 v2.

7.2.2 CRL & CRL entry extensions

Any revocation of a CRL entry for a Root CA and Subordinate CA Certificate, is performed by Policy Authority PKIoverheid.

See Appendix B – Certificate Profiles for all CRL certificate profiles.

7.3 OCSP Profile

The OCSP responses and OCSP signing certificates fulfil the requirements laid down in IETF RFC 6960. OCSP signing certificates are compliant with the X.509v3 standard for public key certificates. Any OCSP responses for a Root CA and Subordinate CA Certificate, is performed by Policy Authority PKIoverheid.

7.3.1 Version number(s)

All certificates are of type X.509 v3.

7.3.2 OCSP extensions

Any OCSP responses for a Root CA and Subordinate CA Certificate, is performed by Policy Authority PKIoverheid.

See Appendix B – Certificate Profiles for all OCSP Signing certificate profiles.

CPS PKIoverheid © Digidentity

8 Compliance Audit & Other Assessments

Digidentity is a Qualified Trust Service Provider (QTSP) as defined in EU Regulation 910/2014 also known as eIDAS. As a QTSP within PKIoverheid, Digidentity must comply to the applicable requirements from Dutch government defined in the Program of Requirements (PoR). Digidentity is compliant to the applicable requirements of the following standards, requirements and regulations:

Regulation or Standard	Description
ISO27001:2022	Information Security Management System (ISMS)
ISO27701:2025	Privacy Information Management System (PIMS)
ISO27017:2015	Information Security in the Cloud
ISO27018:2025	Securing Personal Data in the Cloud
ISO9001:2015	Quality Management System (QMS)
ISO22301:2019	Business Continuity Management System (BCMS)
ETSI EN 319 401	General Policy Requirements for Trust Service Providers
ETSI EN 319 411-1	Electronic Signatures and Infrastructures (ESI) - Policy and security requirements for Trust Service Providers issuing certificates – Part 1: General requirements
ETSI EN 319 411-2	Electronic Signatures and Infrastructures (ESI) - Policy and security requirements for Trust Service Providers issuing certificates – Part 2: Requirements for trust service providers issuing EU qualified certificates
ETSI TS 119 461	Electronic Signatures and Infrastructures (ESI) - Policy and security requirements for trust service components providing identity proofing of trust service subjects
eIDAS	Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, Chapter III – Trust Services
CIR 2024.2160	eIDAS Implementing Act – Article 19a.2 – Risks of non-qualified TSP
CIR 2025.1566	eIDAS Implementing Act – Article 24.1c – Identity Verification
CIR 2025.1943	eIDAS Implementing Act – Article 28.6 & 38.6 – Qualified Signatures & Seal
CIR 2025.2530	eIDAS Implementing Act – Article 24.5 – Requirements for QTSP
GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
NIS2	Directive (EU) 2022/2555 – measures for a high common level of cybersecurity across the Union
CIR 2024.2690	NIS2 Implementing Regulation – Technical and methodological requirements of cybersecurity risk-management measures

Regulation or Standard	Description
Cybersecuritywet (Cbw)	Dutch National Legislation for NIS2
Cybersecuritywet Implemetatie	Dutch National Legislation for NIS2 (Implementation)
Critical Entities Resilience Act (CER)	Directive (EU) 2022.2557 – Critical Entities Resilience Act
CA/Browser Forum	Network and Certificate System Security Requirements
UK Trust Framework	UK Digital Identity and Attributes Trust Framework

8.1 Frequency or Circumstances of Assessment

Digidentity is under supervision and inspected by the Dutch Authority for Digital Infrastructure (RDI) for compliance with the EU Regulation on electronic signatures No. 910/2014 eIDAS.

Digidentity is certified against the ETSI EN 319 401, ETSI EN 319 411-1, ETSI EN 319 411-2, eIDAS, ISO27001:2022, ISO27701:2025, ISO27017:2015 ISO27018:2025, ISO9001:2015 and ISO22301:2019 standards and audited annually by an independent auditor.

CPS PKI overheid © Digidentity

8.2 Identity/Qualifications of Assessor

Digidentity is audited annually by Attestic B.V. for the ETSI certifications to assess compliance with national laws, regulations and standards mentioned. Attestic B.V. is accredited by RvA (Dutch Accreditation Body) for assessments under ISO17065 and the requirements defined in ETSI EN 319 403. Attestic B.V. is bound by law, government regulation, or professional code of ethics.

Digidentity is audited annually by DNV on compliance ISO27001, ISO27017, ISO27018, ISO27701, ISO9001 and ISO22301. DNV is accredited by RvA (Dutch Accreditation Body) for assessment under ISO17021.

8.3 Assessor's Relationship to Assessed Entity

External auditors are independent and have no business interests in Digidentity. No external auditor has any business affiliation with Digidentity.

CPS PKIoverheid @ Digidentity

8.4 Topics Covered by Assessment

The scope of the audit covers all requirements from the standards with subjects;

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

8.5 Actions Taken as a Result of Deficiency

In case the auditor registers a nonconformity during the audit, Digidentity addresses the nonconformity in a Corrective Action Plan (CAP). In the CAP the actions and planning are documented to resolve the nonconformity within 90 days.

8.6 Communication of Results

All Conformity Assessment Reports are available in the repository https://cps.digidentity-pki.com/.

8.7 Self-Audits

Digidentity carries out regular internal audits to continuously assess compliance with the laws, regulations, internal policies, and requirements mentioned in this document.

All other internal audits are carried out at least once a year for high-risk processes and at least once every two years for low-risk processes and per an approved and externally audited schedule.

CPS PKIoverheid @ Digidentity

9 Other Business & Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

All fees are published on the Digidentity website (https://www.digidentity.eu), on pages for the relevant Products.

9.1.2 Certificate Access Fees

There are no certificate access fees.

9.1.3 Revocation or Status Information Access Fees

There are no revocation or status information access fees.

9.1.4 Fees for Other Services

Products (certificates) described in the CPS that are subject to face-to-face checks, during which a person's identity is verified along with their identity document. Digidentity charges a fee for this service. Fees related to the face-to-face checks are available online.

Once the certificate has been issued the Subscriber will receive a request for payment.

Digidentity can provide additional Products to Subscribers for a consultancy fee. Digidentity will provide a quote for any Products requested by Subscribers before any consultancy is carried out.

If certificates must be repeatedly replaced due to the Subscriber's fault, Digidentity reserves the right to charge an administration fee at its discretion. This fee will be proportionate to the work and costs involved in issuing the replacement certificates.

9.1.5 Refund Policy

Digidentity does not refund paid invoices.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

Digidentity maintains appropriate liability insurance policy which provides coverage of at least €1.000.000. Provisions concerning liability can be found in the General Terms & Conditions (also: "Terms") of Digidentity, which form an integral part of any contractual agreement between the Subscriber and Digidentity.

9.2.2 Other Assets

No Stipulation

9.2.3 Insurance or Warranty Coverage for End-Entities

No Stipulation

CPS PKIoverheid © Digidentity

9.3 Confidentiality of Business Information

9.3.1 Scope of confidential information

All business data that is not intended for public disclosure is considered confidential. This applies to all information which is exchanged and communicated in procedures and processes involving participants.

9.3.2 Information Not within the scope of confidential information

Information that is publicly available, including information on the Digidentity website, documentation and materials in the online repository, and any other publicly accessible information, does not constitute confidential information.

9.3.3 Responsibility to protect confidential information

Digidentity and all participants described in this CPS have a responsibility to protect confidential information.

9.4 Protection of Personal Data

9.4.1 Privacy Plan

Digidentity is fully compliant with all EU laws and Regulations currently in force for the protection of personal data. Digidentity undergoes regular internal and external audits to verify and maintain its compliance with privacy requirements.

More information about the processing, and protection of personal data by Digidentity can be found in our Privacy Statement (https://www.digidentity.eu/en/documentation/)

9.4.2 Information Treated as Private

Digidentity treats all personal data as private, meaning that Digidentity only processes personal data in accordance with applicable privacy law and its Privacy Statement.

9.4.3 Information Not Deemed Private

Information which is not confidential information (as defined in section 9.3.1 above) and not personal data (as defined in accordance with the Privacy Statement and applicable law) is not deemed private. All personal data will be handled in accordance with applicable data protection laws.

9.4.4 Responsibility to protect private information

Digidentity will not publish, disclose or otherwise make personal data available for unauthorised view or use. Digidentity has implemented appropriate technical and organisational security measures to protect personal data.

9.4.5 Notice and consent to use private information

During the registration process all applicants are provided with the applicable Terms, the Privacy Statement, and any contractual terms associated with products provided by Digidentity. The processing of personal data is

CPS PKIoverheid @ Digidentity

based on the execution of a contract or another valid legal basis, in accordance with the Privacy Statement and applicable law.

9.4.6 Disclosure pursuant to judicial or administrative process

Digidentity will comply with legal requirements to provide data for forensic purposes as requested by law enforcement or in connection with judicial proceedings, in accordance with applicable legal and administrative procedures. Digidentity also reserves the right to report fraudulent or other criminal activity to the relevant authorities, in line with its Terms.

9.4.7 Other information disclosure circumstances

There is no other information disclosure circumstances.

9.5 Intellectual Property Rights

Any intellectual property rights related to the products, services, and associated materials provided by Digidentity remain the property of Digidentity, its licensors, or suppliers. All information regarding conditions pertaining to intellectual property rights can be found in the associated terms and conditions and any contractual agreements with Digidentity.

9.6 Representation & Warranties

9.6.1 CA Representations & Warranties

Upon the issuance of a certificate, Digidentity makes the following warranties;

[a] At the time of issuance, Digidentity has followed the procedures set forth in this CPS and has verified that the subject authorised the issuance of the certificate, and that the applicant, acting on behalf of the subject, was authorised to request the certificate.

[b] At the time of issuance Digidentity has followed the procedures in this CPS to verify the accuracy of the information provided by the applicant.

[c] At the time of issuance Digidentity has followed the procedures in this CPS to reduce the likelihood that the information contained in the certificate is misleading.

[d] Digidentity has followed the procedures in this CPS to verify the identity of any applicant for a certificate.

[e] Digidentity and the Subscriber have a legally enforceable Subscriber agreement. The Subscriber has been provided with Digidentity's Terms & Conditions, which are incorporated into the agreement.

[f] Digidentity maintains a 24 x 7 publicly accessible repository available for checking certificate status.

[g] Digidentity will revoke a certificate for reasons already described in this CPS.

[h] Digidentity, as the issuing CA for Root Staat der Nederlanden certificates takes no other responsibilities which are for the Root CA's or Intermediate CA's.

Digidentity shall only be liable for actions or omissions that are contrary to the provisions of this CPS, applicable law, regulations, requirements or contractual obligations. Such liability, including liability arising from negligence shall in all cases be limited to the maximum amount specified in Section 9.2 per event or series of related events occurring within a period of twelve (12) months.

CPS Rijksoverheid @ Digidentity

9.6.2 RA Representations & Warranties

Digidentity operates with the RA functions or uses delegates RA functions. Please refer to 9.6.1.

9.6.3 Subscriber Representations & Warranties

Subscriber represents and warrants:

[a] that all information and documents provided by the subscriber are accurate and authentic to the best of the subscriber's knowledge;

[b] That any certificates issued to the subscriber will be used solely in accordance with this CPS and applicable laws. And the certificate will not be used to violate appliable law or the rights of any other party;

[c] to take all reasonable measures to assure control of, keep confidential, and protect the private key which corresponds to the public key of the issued certificate. As a personal subscriber, you ensure the private key is under your sole control. As an organisational subscriber (legal subscriber) you ensure the private key is under the control of the respective organisation.

Additionally, in case of application and use of a Qualified Certificate for a Legal Person (Seal), the Subscriber represents and warrants that:

[a] All Subscribers and Company Administrators must be identified according to the requirements applicable for qualified certificates.

[b] The Subscriber acknowledges that its Users and Company Administrators have the authority to use and apply EU Qualified Electronic Seals to documents on behalf of the Subscribers.

[c] The Subscriber acknowledges full responsibility for use and control of the Seal during the subscription period. This includes ensuring authorised use and management of the Seal by (appointed) authorised representatives, control of documents.

[d] Where applicable, the Subscriber accepts full responsibility for corresponding document hashes submitted to Digidentity, and implementation and maintenance of any necessary security measures, and any delegated usage or management of the Seal by third parties.

[e] Subscriber implements internal control mechanisms to ensure that only their authorised Users and Company Administrators can use the Seal.

[f] The Subscriber shall maintain up-to-date internal access control systems throughout the entire subscription period and must be able to demonstrate their effectiveness upon request. This also applies to third parties that manage and/or use the Seal on behalf of Subscriber.

[g] The Subscriber shall provide and maintain fair, current, accurate and complete information on authorised representatives and/or Users who have the authority to manage and apply EU Qualified Electronic Seals to documents on behalf of their Subscriber. This also applies to authorised representative(s) and/or Users belonging to a third party.

[h] The Subscriber shall ensure that all persons authorised to manage and apply EU Qualified Electronic Seals on behalf of the Subscriber are and will remain fully aware of their role as well as their corresponding responsibilities. They can perform their role in line with any obligations stipulated in this CPS.

[i] The Subscriber expressly acknowledges and agrees that it shall bear full liability for any loss or damage resulting from: (i) the provision of outdated, incomplete, incorrect, misleading, or deceptive information and/or documents to Digidentity; (ii) the appointment of representatives to manage or use the Seal without the necessary authority, capacity, or formal authorization; or (iii) any breach of other obligations under this

CPS PKIoverheid © Digidentity

CPS relating to the Seal. This includes any acts or omissions by appointed authorised representatives or third parties who manage or use the Seal on behalf of the Subscriber.

Additionally, in case of application and use of a Qualified Certificate for a Legal Person (Seal) in automatic signing configuration, the Subscriber represents and warrants:

[j] The Subscriber acknowledges that it may only provide hashes of documents to Digidentity. This also applies to any transactions facilitated by third parties.

[k] The Subscriber must inform Digidentity if a third-party service provider is involved in the management or usage of the Seal.

[l] The Subscriber must formally authorise any third parties acting on behalf of the Subscriber in matters related to management or usage of the Seal.

[m] Upon request by Digidentity, the Subscriber must be able to provide clear demonstrable evidence of formal authorisation(s) provided to third parties.

9.6.4 Relying Party Representations & Warranties

Relying Party represents and warrants that:

[a] the relying party will verify if the electronic signature is from an authorised signatory. Digidentity did not verify if the Subscriber of a personal certificate for qualified electronic signatures is an authorised signatory and is allowed to sign on behalf of an organisation.

9.6.5 Representations and Warranties of Other Participants

No stipulation

9.7 Disclaimers of Warranties

Digidentity provides no warranties concerning certificates other than the warranties which have been explicitly provided under 9.6.1 above. Any implied warranties, including merchantability and fitness for a particular purpose, are explicitly disclaimed to the extent permitted under applicable law.

9.8 Limitations of Liability

Digidentity's liability is limited as set forth in Digidentity's Terms.

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

- If the Certificate, held by the claimant, has not been used in accordance with the certificate usage described in section 1.4;
- If the Certificate, held by the claimant or otherwise subject of any claim, has expired or been revoked before the date of the claim;
- If the private key, which corresponds to the Certificate, held by the claimant or otherwise subject to any claim, is compromised;

CPS PKIoverheid © Digidentity

- Novel computer hardware or software, or mathematical algorithms can be used to break or circumvent the encryption or other safety measures used to ensure the validity of certificates insofar as such encryption and measures are commonly deemed appropriate in accordance with industry practices.

9.9 Indemnities

9.9.1 Indemnification by CAs

No stipulation.

9.9.2 Indemnification by Subscribers

The subscriber shall indemnify and hold harmless Digidentity from and against any damages, claims or other negative consequences which may arise as a result of a breach of the subscriber's warranties in accordance with 9.6.3 above.

9.9.3 Indemnification by Relying Parties

No stipulation

9.10 Term & Termination

9.10.1 Term

This CPS applies for as long as any certificate issued by Digidentity under this CPS remains valid.

9.10.2 Termination

This CPS remains effective until a new version is published in the Digidentity repository. It continues to apply to Digidentity's services as long as those services are offered. If Digidentity ceases to issue certificates and revokes all outstanding certificates from the Digidentity CA, this CPS shall no longer be applicable.

9.10.3 Effect of termination and survival

The provisions of this CPS shall terminate upon Digidentity's cessation of its issuance of Digidentity certificates.

9.11 Individual Notices & Communications with Participants

Digidentity provides notifications to participants in the following ways;

- Website: Notifications and announcements.
- E-mails: Sent to the Subscriber's confirmed e-mail address.
- Telephone calls: Made to the Subscriber's confirmed telephone number.
- Self Service Portal: notifications and announcements
- Account page: notifications and announcements

CPS PKIoverheid @ Digidentity

9.12 Amendments

9.12.1 Procedure for Amendment

Digidentity has the right to amend or supplement this document. Digidentity will review and update this document when;

[a] The scheduled yearly review is performed;
[b] There are changes to the process, procedures or policy described in this document;
[c] There are changes to the law, regulations or requirements;
[d] There are changes to the business interests of Digidentity and changes are required.
[e] Any changes which are not noted in the document history are grammatical, typographical or format changes which do not impact the underlying information pertaining to processes, procedures and policy.

9.12.2 Notification Mechanism and Period

When this CPS is modified, the new version will be published on Digidentity's website (https://www.digidentity.eu/en/documentation/).

The Subscribers can comment on the content of this CPS, however, Digidentity reserves the right to decide whether to implement any changes in response to such comments. All changes will be carried out per the change release management process, where final approval is provided by management.

Digidentity has an obligation to inform the PA if there are any changes to be made to the hierarchal structure of Digidentity CAs.

Digidentity will announce any changes to this document. The CPS is published at least seven (7) days prior to the date of validity.

9.12.3 Circumstances under which OID must be changed

No stipulation.

9.13 Dispute Resolution Provisions

Digidentity has a complaint procedure published on the website, which is available via: https://www.digidentity.eu/en/documentation/

Complaints will be handled with by Digidentity per the described procedure. Complaints can be handled via e-mail: info@digidentity.com, via the website chat facility and via telephone. All contact details are available on the website.

9.14 Governing Law

The Agreement is governed by the laws of the Netherlands. Any provisions within these laws that may lead to the applicability of any other legal system or laws will not be applied.

CPS PKIoverheid © Digidentity

9.15 Compliance with Applicable Law

Digidentity complies with all applicable laws, regulations and requirements for the provision of products and services described in this document. Compliance includes, but is not limited to, hardware, software, systems, business information, data processes and all related undertakings during the daily operations of business practices.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

No stipulation.

9.16.4 Enforcement

No stipulation.

9.16.5 Force Majeure

No stipulation

9.17 Other Provisions

No stipulation

CPS PKIoverheid @ Digidentity

Appendix A – Definitions & Abbreviations

Term	Description
Applicant	New customer that applies for a certificate.
CA	Certificate Authority - within a PKI area the delivery and control of certificates.
CC	Common Criteria
Certificate Holder	the entity stated in the subject field of the certificate, and the holder of the private key. Holders of personal certificates are natural persons. Holders of server certificates are organisations or natural persons.
CP	Certificate Policy
CRL	Certificate Revocation List
Cryptographic Key	A string of bits used by a cryptographic algorithm to transform plain text into cipher text or vice versa. This key remains private and ensures secure communication. A cryptographic key is the core part of cryptographic operations.
CSP	Certificate Service Provider
CSR	Certificate Signing Request - a request by a PKI user for their certificate to be signed by the CA. This signing means that the CA confirms the identity of the requester according to the PKI regulations.
ETSI	European Telecommunications Standards Institute
FIPS	Federal Information Processing Standards
FQDN	Fully Qualified Domain Name
GDPR	General Data Protection Regulation
HSM	Hardware Security Module - special equipment which generates and stores digital keys securely.
NCP	Normalized Certificate Policy
OCSP	Online Certificate Status Protocol
Phishing	The fraudulent practice of sending e-mails purporting to be from reputable companies to induce individuals to reveal personal information, such as passwords and credit card numbers.
PKI	Public Key Infrastructure - a combination of processes and systems for the allocation and management of digital certificates.
Private Key	The private key of the asymmetric key pair that is used to digitally sign or decrypt data. The private key may not be distributed.
Professional Body	an organisation with individual members practicing a profession or occupation in which the organisation maintains an oversight of the knowledge, skills, conduct and practice of that profession or occupation.
Pseudonym	The use of a unique string of characters (numbers and letters) to identify a specific user. A name substitute.

Term	Description
Public Key	The public key of an asymmetric key pair used to digitally sign or decrypt data. The public key can be distributed.
PTC	Publicly Trusted Certificates
QCP	Qualified Certificate Policy
QCP-l-qscd	Qualified Certificate Policy for legal persons stored on qualified signature creation device
QCP-n-qscd	Qualified Certificate Policy for natural persons stored on qualified signature creation device
RA	Registration Authority - within PKI secure environment the control of client's personal details via the CA.
RDI	Rijkinspectie Digitale Infrastructuur (Dutch Authority for Digital Infrastructure)
Registration	The process of a user signing up and the subsequent verification of their identity and/or entity (organisation).
SSCD	Secure Signature Creation Device.
SSL	Secure Sockets Layer
Subject	The subject of a certificate is the party named in the certificate as the holder of the Private Key associated with the Public Key given in the certificate. The subject can be a; ▪ natural person ▪ legal person (e.g. Organisation) ▪ device or system operated represented by a natural or legal person
Subscriber	An Applicant who has been verified and been issued a certificate. Subscribers use our Products. Subscribers are not always the party identified in a certificate, e.g. when a certificate is issued to an organisation. Before the identity of the Subscriber is verified, a Subscriber is an applicant.
TLS	Transport Layer Security
TSP	Trust Service Provider
Validation	The process of checking the validity of information e.g. validation of passport details.
Verification	The process of verifying the user's identity in order to complete registration for a product - to the required Level of Assurance (LoA).
VSC	Virtual Smart Card
WID	Wet op Identificatieplicht. Law regarding mandatory provision of identification.

Appendix B – Certificate Profiles

PKIoverheid G1 Certificates Profiles

PKIoverheid Private SBR – PKIoverheid Private Services CA – G1 (Subscriber Certificate)

Field	OID	Value	Critical	Type
Version		x.509 version 3		Required
SerialNumber	2.5.4.5	Automatically created unique number		Required
SignatureAlgorithm	1.2.840.113549.1.1.11	sha256WithRSAEncryption		Required
Validity				
NotValidBefore		<date of issuance>		Required
NotValidAfter		<+1, +2, +3 years>		Required
Issuer DN				
commonName	(2.5.4.3) {id-at-3}	CN=Digidentity BV PKIoverheid Private Services CA – G1		Required
organizationName	(2.5.4.10)	O=Digidentity B.V.		Required
countryName	(2.5.4.6) {id-at-6}	C=NL		Required
organizationIdentifier	(2.5.4.97)	NTRNL-27322631		Required
Subject DN				
commonName	(2.5.4.3) {id-at-3}	CN=SBR Digipoort		Required
organizationName	(2.5.4.10)	O=<Organisation Name>		Required
organizationIdentifier	(2.5.4.97)	<Organisation Identification Number (OIN)>		Required
serialNumber	(2.5.4.5)	<Organisation Identification Number (OIN)>		Optional
countryName	(2.5.4.6) {id-at-6}	C=<Two letter Country Code e.g. NL>		Required
Public Key				
algorithm	(1.2.840.113549.1.1.1)	sha256WithRSAEncryption		Required
keySize		2.048 or 3.072 or 4.096 bits		Required
signature		512 bits		Required
Extensions				
keyUsage	(2.5.29.15) {id-ce 15}	digitalSignature, keyEncipherment	Yes	Required
extKeyUsage	(2.5.29.37) {id-ce 37}	id-kp-serverAuth (1.3.6.1.5.5.7.3.1) id-kp-clientAuth (1.3.6.1.5.5.7.3.2)	No	Required
certificatePolicies	(2.5.29.32) {id-ce 32}	PolicyID1=2.16.528.1.1003.1.2.8.6 (server) QualifierID1=1.3.6.1.5.5.7.2.2 (id-qt-unotice) UserNotice=For the use of this certificate the associated CPS applies. QualifierID2: 1.3.6.1.5.5.7.2.1 (id-qt-cps) URl=https://cps.digidentity-pki.com	No	Required
subjectKeyIdentifier	(2.5.29.14) {id-ce 14}	160-bit SHA-1 hash	No	Required
authorityKeyIdentifier	(2.5.29.35) {id-ce 35}	160-bit SHA-1 hash	No	Required
authorityInfoAccess	{id-pe 1}	Method#1: 1.3.6.1.5.5.7.48.2 (caIssuers) Method#2: 1.3.6.1.5.5.7.48.1 (ocsp) Contains CA Issuers URL and OCSP URL. URLs vary based on Issuing CA.	No	Optional
subjectAltName	(2.5.29.17) {id-ce 17}	<Permanent Identifier: UUID, TSP-OID>	No	Required
cRLDistributionPoints	(2.5.29.31) {id-ce 31}	Contains a CRL URL. URL varies based on Issuing CA.	No	Required

CPS

PKIoverheid Private TLS Server – PKIoverheid Private Services CA – G1 (Subscriber Certificate)

Field	OID	Value	Critical	Type
Version		x.509 version 3		Required
SerialNumber	2.5.4.5	Automatically created unique number		Required
SignatureAlgorithm	1.2.840.113549.1.1.11	sha256WithRSAEncryption		Required
Validity				
NotValidBefore		<date of issuance>		Required
NotValidAfter		<+1, +2, +3 years>		Required
Issuer DN				
commonName	(2.5.4.3) {id-at-3}	CN=Digidentity BV PKIoverheid Private Services CA – G1		Required
organizationName	(2.5.4.10)	O=Digidentity B.V.		Required
organizationIdentifier	(2.5.4.97)	NTRNL-27322631		Required
countryName	(2.5.4.6) {id-at-6}	C=NL		Required
Subject DN				
commonName	(2.5.4.3) {id-at-3}	CN=server name		Required
organizationName	(2.5.4.10)	O=<Organisation Name>		Required
organizationIdentifier	(2.5.4.97)	<Organisation Identification Number (OIN)>		Required
serialNumber	(2.5.4.5)	<Organisation Identification Number (OIN)>		Optional
countryName	(2.5.4.6) {id-at-6}	C=<Two letter Country Code e.g. NL>		Required
Public Key				
algorithm	(1.2.840.113549.1.1.1)	sha256WithRSAEncryption		Required
keySize		2.048 or 3.072 or 4.096 bits		Required
signature		512 bits		Required
Extensions				
keyUsage	(2.5.29.15) {id-ce 15}	digitalSignature, keyEncipherment	Yes	Required
extKeyUsage	(2.5.29.37) {id-ce 37}	id-kp-serverAuth (1.3.6.1.5.5.7.3.1) id-kp-clientAuth (1.3.6.1.5.5.7.3.2)	No	Required
certificatePolicies	(2.5.29.32) {id-ce 32}	PolicyID1=2.16.528.1.1003.1.2.8.6 (server) QualifierID1=1.3.6.1.5.5.7.2.2 (id-qt-unotice) UserNotice=For the use of this certificate the associated CPS applies. QualifierID2: 1.3.6.1.5.5.7.2.1 (id-qt-cps) URl=https://cps.digidentity-pki.com	No	Required
subjectKeyIdentifier	(2.5.29.14) {id-ce 14}	160-bit SHA-1 hash	No	Required
authorityKeyIdentifier	(2.5.29.35) {id-ce 35}	160-bit SHA-1 hash	No	Required
authorityInfoAccess	{id-pe 1}	Method#1: 1.3.6.1.5.5.7.48.2 (caIssuers) Method#2: 1.3.6.1.5.5.7.48.1 (ocsp) Contains CA Issuers URL and OCSP URL. URLs vary based on Issuing CA.	No	Optional
subjectAltName	(2.5.29.17) {id-ce 17}	Multiple server names	No	Required
cRLDistributionPoints	(2.5.29.31) {id-ce 31}	Contains a CRL URL. URL varies based on Issuing CA.	No	Required

PKIoverheid G4 Subscriber Certificates Profiles

Standard Business Reporting (SBR) - Subscriber certificate (G4)

Field	OID	Value	Critical	Type
Version		x.509 version 3		Required
SerialNumber	2.5.4.5	Automatically created unique number		Required
SignatureAlgorithm	1.2.840.113549.1.1.10	RSA-PSS Signature Scheme		Required
Validity				
NotValidBefore		<date of issuance>		Required
NotValidAfter		<+1, +2, +3 years>		Required
Issuer DN				
commonName	(2.5.4.3) {id-at-3}	CN=Digidentity - G4 PKIo Priv G-Other LP - 2025		Required
organizationName	(2.5.4.10)	O=Digidentity B.V.		Required
organizationIdentifier	(2.5.4.97)	NTRNL-27322631		Required
countryName	(2.5.4.6) {id-at-6}	C=NL		Required
Subject DN				
commonName	(2.5.4.3) {id-at-3}	CN=SBR Digipoort		Required
organizationName	(2.5.4.10)	O=<full registered name of the legal person>		Required
organizationIdentifier	(2.5.4.97)	<Organisation Identification Number (OIN)>		Required
serialNumber	(2.5.4.5)	<Organisation Identification Number (OIN)>		Optional
countryName	(2.5.4.6) {id-at-6}	C=<Two letter Country Code e.g. NL>		Required
Public Key				
algorithm	(1.2.840.113549.1.1.1)	RSAEncryption		Required
keySize		2.048 or 3.072 or 4.096 bits		Required
signature		512 bits		Required
Extensions				
keyUsage	(2.5.29.15) {id-ce 15}	digitalSignature	Yes	Required
extKeyUsage	(2.5.29.37) {id-ce 37}	id-kp-clientAuth (1.3.6.1.5.5.7.3.2)	No	Required
certificatePolicies	(2.5.29.32) {id-ce 32}	PolicyID1=0.4.0.2042.1.1 (ETSI/NCP) PolicyID2=2.16.528.1.1003.1.2.44.16.25.8 (Authentication) QualifierID1: 1.3.6.1.5.5.7.2.1 (id-qt-cps) URl=https://cps.digidentity-pki.com	No	Required
subjectKeyIdentifier	(2.5.29.14) {id-ce 14}	160-bit SHA-1 hash	No	Required
authorityKeyIdentifier	(2.5.29.35) {id-ce 35}	160-bit SHA-1 hash	No	Required
authorityInfoAccess	{id-pe 1}	Method#1:1.3.6.1.5.5.7.48.2 (caIssuers) Method#2:1.3.6.1.5.5.7.48.1 (ocsp) Contains CA Issuers URL and OCSP URL. URLs vary based on Issuing CA.	No	Optional
cRLDistributionPoints	(2.5.29.31) {id-ce 31}	Contains a CRL URL. URL varies based on Issuing CA.	No	Required

PKIoverheid Private TLS Server Legal Person - G4 (Subscriber certificate)

Field	OID	Value	Critical	Type
Version		x.509 version 3		Required
SerialNumber	2.5.4.5	Automatically created unique number		Required
SignatureAlgorithm	1.2.840.113549.1.1.10	RSA-PSS Signature Scheme		Required
Validity				
NotValidBefore		<date of issuance>		Required
NotValidAfter		<+1, +2, +3 years>		Required
Issuer DN				
commonName	(2.5.4.3) {id-at-3}	CN=Digidentity - G4 PKIo Priv G-TLS SYS - 2025		Required
organizationName	(2.5.4.10)	O=Digidentity B.V.		Required
organizationIdentifier	(2.5.4.97)	NTRNL-27322631		Required
countryName	(2.5.4.6) {id-at-6}	C=NL		Required
Subject DN				
commonName	(2.5.4.3) {id-at-3}	CN=<server name>		Required
organizationName	(2.5.4.10)	O=<full registered name of the legal person>		Required
organizationIdentifier	(2.5.4.97)	<Organisation Identification Number (OIN)>		Required
serialNumber	(2.5.4.5)	<Organisation Identification Number (OIN)>		Optional
countryName	(2.5.4.6) {id-at-6}	C=<Two letter Country Code e.g. NL>		Required
Public Key				
algorithm	(1.2.840.113549.1.1.1)	RSAEncryption		Required
keySize		2.048 or 3.072 or 4.096 bits		Required
signature		512 bits		Required
Extensions				
keyUsage	(2.5.29.15) {id-ce 15}	digitalSignature, keyEncipherment	Yes	Required
extKeyUsage	(2.5.29.37) {id-ce 37}	id-kp-serverAuth (1.3.6.1.5.5.7.3.1) id-kp-clientAuth (1.3.6.1.5.5.7.3.2)	No	Required
certificatePolicies	(2.5.29.32) {id-ce 32}	PolicyID1=0.4.0.2042.1.1 (ETSI/NCP) PolicyID2=2.16.528.1.1003.1.2.44.15.35.11 (Authentication)	No	Required
subjectKeyIdentifier	(2.5.29.14) {id-ce 14}	160-bit SHA-1 hash	No	Required
authorityKeyIdentifier	(2.5.29.35) {id-ce 35}	160-bit SHA-1 hash	No	Required
authorityInfoAccess	{id-pe 1}	Method#1:1.3.6.1.5.5.7.48.2 (caIssuers) Method#2:1.3.6.1.5.5.7.48.1 (ocsp) Contains CA Issuers URL and OCSP URL. URLs vary based on Issuing CA.	No	Required
subjectAltName	(2.5.29.17) {id-ce 17}	Multiple server names	No	Required
cRLDistributionPoints	(2.5.29.31){id-ce 31}	Contains a CRL URL. URL varies based on Issuing CA.	No	Required

Qualified - QES (Non-Repudiation Natural Person G4) - Subscriber Certificates

Field	OID	Value	Critical	Type
Version		x.509 version 3		Required
SerialNumber	2.5.4.5	Automatically created unique number		Required
SignatureAlgorithm	1.2.840.113549.1.1.10	RSA-PSS Signature Scheme		Required
Validity				
NotValidBefore		<date of issuance>		Required
NotValidAfter		<+365 days>		Required
Issuer DN				
commonName	(2.5.4.3) {id-at-3}	CN=Digidentity - G4 PKIo EUTL G-Sigs NP - 2025		Required
organisationName	(2.5.4.10)	O=Digidentity B.V.		Required
countryName	(2.5.4.6) {id-at-6}	C=NL		Required
Subject DN				
commonName	(2.5.4.3) {id-at-3}	CN=<Given Names and Surname as extracted from identity evidence>		Required
countryName	(2.5.4.6) {id-at-6}	C=<Two letter Country Code e.g. NL>		Required
givenName	(2.5.4.42)	GN=<Given names as extracted from the identity evidence>		Required
surname	(2.5.4.4)	SN=<Surname as extracted from the identity evidence>		Required
serialNumber	(2.5.4.5)	SERIALNUMBER=<authenticator Identifier>		Required
organizationName	(2.5.4.10)	O=<Name of the Organisation as registered in Trade Register>		Optional
title	(2.5.4.12)	TITLE=<Professional Title>		Optional
Public Key				
algorithm	(1.2.840.113549.1.1.1)	RSAEncryption		Required
keySize		2.048 bits or 3.072 bits		Required
signature		512 bits		Required
Extensions				
keyUsage	(2.5.29.15) {id-ce 15}	nonRepudiation	Yes	Required
extKeyUsage	(2.5.29.37) {id-ce 37}	id-kp-documentSigning (1.3.6.1.5.5.7.3.36) szOID_KP_DOCUMENT_SIGNING (1.3.6.1.4.1.311.10.3.12)	No	Required
certificatePolicies	(2.5.29.32) {id-ce 32}	PolicyID1=0.4.0.2042.1.2 (ETSI/NCP+) PolicyID2=0.4.0.194112.1.2 (ETSI/QCP-n-qscd) PolicyID3=2.16.528.1.1003.1.2.44.14.11.5 (non-repudiation) or PolicyID3=2.16.528.1.1003.1.2.44.14.12.5 (non-repudiation Professional) or PolicyID3=2.16.528.1.1003.1.2.44.14.13.5 (non-repudiation Sponsored) or PolicyID3=2.16.528.1.1003.1.2.44.14.14.5 (non-repudiation Professional Sponsored) QualifierID1: 1.3.6.1.5.5.7.2.1 (id-qt-cps) URl=https://cps.digidentity-pki.com	No	Required
subjectKeyIdentifier	(2.5.29.14) {id-ce 14}	160-bit SHA-1 hash	No	Required
authorityKeyIdentifier	(2.5.29.35) {id-ce 35}	160-bit SHA-1 hash	No	Required
authorityInfoAccess	{id-pe 1}	Method#1:1.3.6.1.5.5.7.48.2 (caIssuers) Method#2:1.3.6.1.5.5.7.48.1 (ocsp) Contains CA Issuers URL and OCSP URL. URLs vary based on Issuing CA.	No	Required
cRLDistributionPoints	(2.5.29.31) {id-ce 31}	Contains a CRL URL. URL varies based on Issuing CA.	No	Required
qcStatements				
esi4-qcStatement-1	id-etsi-qcs-1	id-etsi-qcs-QcCompliance (0.4.0.1862.1.1)		Required
esi4-qcStatement-4	id-etsi-qcs-4	id-etsi-qcs-QcSSCD (0.4.0.1862.1.4)		Required
esi4-qcStatement-5	id-etsi-qcs-5	id-etsi-qcs-QcPDS (0.4.0.1862.1.5) URL= https://cps.digidentity-pki.com Language = EN		Required
esi4-qcStatement-6	id-etsi-qcs-6	id-etsi-qct-esign {id-etsi-qcs-QcType 1} (0.4.0.1862.1.6)		Required

Authentication (Natural Person G4) - Subscriber Certificates

Field	OID	Value	Critical	Type
Version		x.509 version 3		Required
SerialNumber	2.5.4.5	Automatically created unique number		Required
SignatureAlgorithm	1.2.840.113549.1.1.10	RSA-PSS Signature Scheme		Required
Validity				
NotValidBefore		<date of issuance>		Required
NotValidAfter		<+365 days>		Required
Issuer DN				
commonName	(2.5.4.3) {id-at-3}	CN=Digidentity - G4 PKIo Priv G-Other NP - 2025		Required
organisationName	(2.5.4.10)	O=Digidentity B.V.		Required
countryName	(2.5.4.6) {id-at-6}	C=NL		Required
Subject DN				
commonName	(2.5.4.3) {id-at-3}	CN=<Given Names and Surname as extracted from identity evidence>		Required
countryName	(2.5.4.6) {id-at-6}	C=<Two letter Country Code e.g. NL>		Required
givenName	(2.5.4.42)	GN=<Given names as extracted from the identity evidence>		Required
surname	(2.5.4.4)	SN=<Surname as extracted from the identity evidence>		Required
serialNumber	(2.5.4.5)	SERIALNUMBER=<authenticator Identifier>		Required
organizationName	(2.5.4.10)	O=<Name of the Organisation as registered in Trade Register>		Optional
title	(2.5.4.12)	TITLE=<Professional Title>		Optional
Public Key				
algorithm	(1.2.840.113549.1.1.1)	RSAEncryption		Required
keySize		2.048 bits or 3.072 bits		Required
signature		512 bits		Required
Extensions				
keyUsage	(2.5.29.15) {id-ce 15}	digitalSignature	Yes	Required
extKeyUsage	(2.5.29.37) {id-ce 37}	id-kp-clientAuth (1.3.6.1.5.5.7.3.2)	No	Required
certificatePolicies	(2.5.29.32) {id-ce 32}	PolicyID1=0.4.0.2042.1.2 (ETSI/NCP+) PolicyID2=2.16.528.1.1003.1.2.44.16.11.8 (Authentication) or PolicyID2=2.16.528.1.1003.1.2.44.16.12.8 (Authentication Professional) or PolicyID2=2.16.528.1.1003.1.2.44.16.13.8 (Authentication Sponsored) or PolicyID2=2.16.528.1.1003.1.2.44.16.14.8 (Authentication Professional Sponsored) QualifierID1: 1.3.6.1.5.5.7.2.1 (id-qt-cps) URl=https://cps.digidentity-pki.com	No	Required
subjectKeyIdentifier	(2.5.29.14) {id-ce 14}	160-bit SHA-1 hash	No	Required
authorityKeyIdentifier	(2.5.29.35) {id-ce 35}	160-bit SHA-1 hash	No	Required
authorityInfoAccess	{id-pe 1}	Method#1:1.3.6.1.5.5.7.48.2 (caIssuers) Method#2:1.3.6.1.5.5.7.48.1 (ocsp) Contains CA Issuers URL and OCSP URL. URLs vary based on Issuing CA.	No	Required
cRLDistributionPoints	(2.5.29.31) {id-ce 31}	Contains a CRL URL. URL varies based on Issuing CA.	No	Required

Seal (Non-Repudiation Legal Person G4) - Subscriber certificate

Field	OID	Value	Critical	Type
Version		x.509 version 3		Required
SerialNumber	2.5.4.5	Automatically created unique number		Required
SignatureAlgorithm	1.2.840.113549.1.1.10	RSA-PSS Signature Scheme		Required
Validity				
NotValidBefore		<date of issuance>		Required
NotValidAfter		<+365 days>		Required
Issuer DN				
commonName	(2.5.4.3) {id-at-3}	CN= Digidentity - G4 PKIo EUTL G-Sigs LP - 2025		Required
organizationName	(2.5.4.10)	O=Digidentity B.V.		Required
countryName	(2.5.4.6) {id-at-6}	C=NL		Required
Subject DN				
commonName	(2.5.4.3) {id-at-3}	CN=<name commonly used by subject to represent itself>		Required
countryName	(2.5.4.6) {id-at-6}	C=<Two letter Country Code e.g. NL>		Required
organizationIdentifier	(2.5.4.97)	<Trade Register Number>		Required
organizationName	(2.5.4.10)	O=<full registered name of the legal person>		Required
Public Key				
algorithm	(1.2.840.113549.1.1.1)	RSAEncryption		Required
keySize		2.048 bits or 3.072 bits		Required
signature		512 bits		Required
Extensions				
keyUsage	(2.5.29.15) {id-ce 15}	nonRepudiation	Yes	Required
extKeyUsage	(2.5.29.37) {id-ce 37}	id-kp-documentSigning (1.3.6.1.5.5.7.3.36) szOID_KP_DOCUMENT_SIGNING (1.3.6.1.4.1.311.10.3.12)	No	Required
certificatePolicies	(2.5.29.32) {id-ce 32}	PolicyID1=0.4.0.2042.1.2 (ETSI/NCP+) PolicyID2=0.4.0.194112.1.3 (ETSI/QCP-l-qscd) PolicyID3=2.16.528.1.1003.1.2.44.14.25.5 (non-repudiation) QualifierID1:1.3.6.1.5.5.7.2.1 (id-qt-cps) URl=https://cps.digidentity-pki.com	No	Required
subjectKeyIdentifier	(2.5.29.14) {id-ce 14}	160-bit SHA-1 hash	No	Required
authorityKeyIdentifier	(2.5.29.35) {id-ce 35}	160-bit SHA-1 hash	No	Required
authorityInfoAccess	{id-pe 1}	Method#1:1.3.6.1.5.5.7.48.2 (caIssuers) Method#2:1.3.6.1.5.5.7.48.1 (ocsp) Contains CA Issuers URL and OCSP URL. URLs vary based on Issuing CA.	No	Required
cRLDistributionPoints	(2.5.29.31) {id-ce 31}	Contains a CRL URL. URL varies based on Issuing CA.	No	Required
qcStatement				
esi4-qcStatement-1	id-etsi-qcs-1	id-etsi-qcs-QcCompliance (0.4.0.1862.1.1)		Required
esi4-qcStatement-4	id-etsi-qcs-4	id-etsi-qcs-QcSSCD (0.4.0.1862.1.4)		Required
esi4-qcStatement-5	id-etsi-qcs-5	id-etsi-qcs-QcPDS (0.4.0.1862.1.5) URL= URl=https://cps.digidentity-pki.com Language = EN		Required
esi4-qcStatement-6	id-etsi-qcs-6	id-etsi-qct-eseal {id-etsi-qcs-QcType 2} (0.4.0.1862.1.6.2)		Required
qcStatement-2		id-etsi-qcs-semantics-identifiers 2 (0.4.0.194121.1.2)		Required

CPS PKI

Authentication Legal Person - Subscriber certificate

Field	OID	Value	Critical	Type
Version		x.509 version 3		Required
SerialNumber	2.5.4.5	Automatically created unique number		Required
SignatureAlgorithm	1.2.840.113549.1.1.10	RSA-PSS Signature Scheme		Required
Validity				
NotValidBefore		<date of issuance>		Required
NotValidAfter		<+365 days>		Required
Issuer DN				
commonName	(2.5.4.3) {id-at-3}	CN=Digidentity - G4 PKIo Priv G-Other LP - 2025		Required
organisationName	(2.5.4.10)	O=Digidentity B.V.		Required
countryName	(2.5.4.6) {id-at-6}	C=NL		Required
Subject DN				
commonName	(2.5.4.3) {id-at-3}	CN=<name commonly used by subject to represent itself>		Required
countryName	(2.5.4.6) {id-at-6}	C=<Two letter Country Code e.g. NL>		Required
organizationIdentifier	(2.5.4.97)	<Trade Register Number>		Required
organizationName	(2.5.4.10)	O=<full registered name of the legal person>		Required
Public Key				
algorithm	(1.2.840.113549.1.1.1)	RSAEncryption		Required
keySize		2.048 bits or 3.072 bits		Required
signature		512 bits		Required
Extensions				
keyUsage	(2.5.29.15) {id-ce 15}	digitalSignature	Yes	Required
extKeyUsage	(2.5.29.37) {id-ce 37}	id-kp-clientAuth (1.3.6.1.5.5.7.3.2)	No	Required
certificatePolicies	(2.5.29.32) {id-ce 32}	PolicyID1=0.4.0.2042.1.2 (ETSI/NCP+) PolicyID2=2.16.528.1.1003.1.2.44.16.25.8 (Authentication) QualifierID1: 1.3.6.1.5.5.7.2.1 (id-qt-cps) URl=https://cps.digidentity-pki.com	No	Required
subjectKeyIdentifier	(2.5.29.14) {id-ce 14}	160-bit SHA-1 hash	No	Required
authorityKeyIdentifier	(2.5.29.35) {id-ce 35}	160-bit SHA-1 hash	No	Required
authorityInfoAccess	{id-pe 1}	Method#1:1.3.6.1.5.5.7.48.2 (caIssuers) Method#2:1.3.6.1.5.5.7.48.1 (ocsp) Contains CA Issuers URL and OCSP URL. URLs vary based on Issuing CA.	No	Required
cRLDistributionPoints	(2.5.29.31) {id-ce 31}	Contains a CRL URL. URL varies based on Issuing CA.	No	Required

CPS

CRL Certificate Profiles

G4 CRL Profiles

Field	OID	Value	Critical	Type
Version		x.509 version 2		Required
SignatureAlgorithm	1.2.840.113549.1.1.10	RSA-PSS Signature Scheme		Required
Issuer DN				
commonName	(2.5.4.3) {id-at-3}	CN=<Issuer CA Name>		Required
organizationName	(2.5.4.10)	O=Digidentity B.V.		Required
countryName	(2.5.4.6) {id-at-6}	C=NL		Required
Extensions				
ThisUpdate		Issue date and time of this CRL		Required
NextUpdate		< +24 hours >		Required
revokedCertificates		Provides the status e.g. revoked		Required
CRlNumber		Provides the sequential order of the published CRLs		Required
reasonCode	(2.5.29.21) {id-ce 21}	Provides a reason for revocation		Optional

CPS PKIoverheid @ Digidentity

OCSP Signing Certificate Profiles

PKIoverheid Private Services CA – G1 (OCSP Signing certificate)

Field	OID	Value	Critical	Type
Version		x.509 version 3		Required
SerialNumber	2.5.4.5	Automatically created unique number		Required
SignatureAlgorithm	1.2.840.113549.1.1.11	sha256WithRSAEncryption		Required
Validity				
NotValidBefore		<date of issuance>		Required
NotValidAfter		<+1 years>		Required
Issuer DN				
commonName	(2.5.4.3) {id-at-3}	CN=Digidentity BV PKIoverheid Private Services CA - G1		Required
organizationName	(2.5.4.10)	O=Digidentity B.V.		Required
countryName	(2.5.4.6) {id-at-6}	C=NL		Required
organizationIdentifier	(2.5.4.97)	NTRNL-27322631		Required
Subject DN				
commonName	(2.5.4.3) {id-at-3}	CN=Digidentity BV PKIoverheid Private Services CA - G1 OCSP		Required
organizationName	(2.5.4.10)	O=Digidentity B.V.		Required
organizationIdentifier	(2.5.4.97)	NTRNL-27322631		Required
countryName	(2.5.4.6) {id-at-6}	C=NL		Required
Public Key				
algorithm	(1.2.840.113549.1.1.1)	sha256WithRSAEncryption		Required
keySize		2.048 bits, 3.072 bits or 4.096 bits		Required
signature		512 bits		Required
Extensions				
keyUsage	(2.5.29.15) {id-ce 15}	digitalSignature	Yes	Required
extKeyUsage	(2.5.29.37) {id-ce 37}	id-kp-OCSP-signing (1.3.6.1.5.5.7.3.9)	Yes	Required
certificatePolicies	(2.5.29.32) {id-ce 32}	PolicyID1=2.16.528.1.1003.1.2.8.6 (server) PolicyID2= 0.4.0.2042.1.2 (NCP+)	No	Required
subjectKeyIdentifier	(2.5.29.14) {id-ce 14}	160-bit SHA-1 hash	No	Required
authorityKeyIdentifier	(2.5.29.35) {id-ce 35}	160-bit SHA-1 hash	No	Required
ocspNoRevocationCheck		1.3.6.1.5.5.7.48.1.5 (id-pkix-ocsp-nocheck)	No	Required

CPS

Digidentity - G4 PKIo EUTL G-Sigs NP - 2025 (OCSP Signing certificate)

Field	OID	Value	Critical	Type
Version		x.509 version 3		Required
SerialNumber	2.5.4.5	Automatically created unique number		Required
SignatureAlgorithm	1.2.840.113549.1.1.10	RSA-PSS Signature Scheme		Required
Validity				
NotValidBefore		<date of issuance>		Required
NotValidAfter		<+1 year>		Required
Issuer DN				
commonName	(2.5.4.3) {id-at-3}	CN=Digidentity - G4 PKIo EUTL G-Sigs NP – 2025		Required
organisationName	(2.5.4.10)	O=Digidentity B.V.		Required
organizationIdentifier	(2.5.4.97)	NTRNL-27322631		Required
countryName	(2.5.4.6) {id-at-6}	C=NL		Required
Subject DN				
commonName	(2.5.4.3) {id-at-3}	CN=Digidentity - G4 PKIo EUTL G-Sigs NP - 2025 OCSP		Required
organizationName	(2.5.4.10)	O=Digidentity B.V.		Required
organizationIdentifier	(2.5.4.97)	NTRNL-27322631		Required
countryName	(2.5.4.6) {id-at-6}	C=NL		Required
Public Key				
algorithm	(1.2.840.113549.1.1.1)	RSAEncryption		Required
keySize		2.048 bits, 3.072 bits or 4.096 bits		Required
signature		512 bits		Required
Extensions				
keyUsage	(2.5.29.15) {id-ce 15}	digitalSignature	Yes	Required
extKeyUsage	(2.5.29.37) {id-ce 37}	id-kp-OCSP-signing (1.3.6.1.5.5.7.3.9)	Yes	Required
certificatePolicies	(2.5.29.32) {id-ce 32}	PolicyID1=2.16.528.1.1003.1.2.44.14.19.10 (OCSP) PolicyID2= 0.4.0.2042.1.2 (NCP+)	No	Required
subjectKeyIdentifier	(2.5.29.14) {id-ce 14}	160-bit SHA-1 hash	No	Required
authorityKeyIdentifier	(2.5.29.35) {id-ce 35}	160-bit SHA-1 hash	No	Required
ocspNoRevocationCheck		1.3.6.1.5.5.7.48.1.5 (id-pkix-ocsp-nocheck)	No	Required

CPS PKI

Digidentity - G4 PKIo EUTL G-Sigs LP - 2025 (OCSP Signing certificate)

Field	OID	Value	Critical	Type
Version		x.509 version 3		Required
SerialNumber	2.5.4.5	Automatically created unique number		Required
SignatureAlgorithm	1.2.840.113549.1.1.10	RSA-PSS Signature Scheme		Required
Validity				
NotValidBefore		<date of issuance>		Required
NotValidAfter		<+1 year>		Required
Issuer DN				
commonName	(2.5.4.3) {id-at-3}	CN=Digidentity - G4 PKIo EUTL G-Sigs LP – 2025		Required
organisationName	(2.5.4.10)	O=Digidentity B.V.		Required
organizationIdentifier	(2.5.4.97)	NTRNL-27322631		Required
countryName	(2.5.4.6) {id-at-6}	C=NL		Required
Subject DN				
commonName	(2.5.4.3) {id-at-3}	CN=Digidentity - G4 PKIo EUTL G-Sigs LP - 2025 OCSP		Required
organisationName	(2.5.4.10)	O=Digidentity B.V.		Required
organizationIdentifier	(2.5.4.97)	NTRNL-27322631		Required
countryName	(2.5.4.6) {id-at-6}	C=NL		Required
Public Key				
algorithm	(1.2.840.113549.1.1.1)	RSAEncryption		Required
keySize		2.048 bits, 3.072 bits or 4.096 bits		Required
signature		512 bits		Required
Extensions				
keyUsage	(2.5.29.15) {id-ce 15}	digitalSignature	Yes	Required
extKeyUsage	(2.5.29.37) {id-ce 37}	id-kp-OCSP-signing (1.3.6.1.5.5.7.3.9)	Yes	Required
certificatePolicies	(2.5.29.32) {id-ce 32}	PolicyID1=2.16.528.1.1003.1.2.44.14.29.10 (OCSP) PolicyID2= 0.4.0.2042.1.2 (NCP+)	No	Required
subjectKeyIdentifier	(2.5.29.14) {id-ce 14}	160-bit SHA-1 hash	No	Required
authorityKeyIdentifier	(2.5.29.35) {id-ce 35}	160-bit SHA-1 hash	No	Required
ocspNoRevocationCheck		1.3.6.1.5.5.7.48.1.5 (id-pkix-ocsp-nocheck)	No	Required

CPS PUBLIC

Digidentity - G4 PKIo Priv G-Other NP - 2025 (OCSP Signing certificate)

Field	OID	Value	Critical	Type
Version		x.509 version 3		Required
SerialNumber	2.5.4.5	Automatically created unique number		Required
SignatureAlgorithm	1.2.840.113549.1.1.10	RSA-PSS Signature Scheme		Required
Validity				
NotValidBefore		<date of issuance>		Required
NotValidAfter		<+1 year>		Required
Issuer DN				
commonName	(2.5.4.3) {id-at-3}	CN=Digidentity - G4 PKIo Priv G-Other NP – 2025		Required
organizationName	(2.5.4.10)	O=Digidentity B.V.		Required
organizationIdentifier	(2.5.4.97)	NTRNL-27322631		Required
countryName	(2.5.4.6) {id-at-6}	C=NL		Required
Subject DN				
commonName	(2.5.4.3) {id-at-3}	CN= Digidentity - G4 PKIo Priv G-Other NP - 2025 OCSP		Required
organizationName	(2.5.4.10)	O=Digidentity B.V.		Required
organizationIdentifier	(2.5.4.97)	NTRNL-27322631		Required
countryName	(2.5.4.6) {id-at-6}	C=NL		Required
Public Key				
algorithm	(1.2.840.113549.1.1.1)	RSAEncryption		Required
keySize		2.048 bits, 3.072 bits or 4.096 bits		Required
signature		512 bits		Required
Extensions				
keyUsage	(2.5.29.15) {id-ce 15}	digitalSignature	Yes	Required
extKeyUsage	(2.5.29.37) {id-ce 37}	id-kp-OCSP-signing (1.3.6.1.5.5.7.3.9)	Yes	Required
certificatePolicies	(2.5.29.32) {id-ce 32}	PolicyID1=2.16.528.1.1003.1.2.44.16.19.10 (OCSP) PolicyID2= 0.4.0.2042.1.2 (NCP+)	No	Required
subjectKeyIdentifier	(2.5.29.14) {id-ce 14}	160-bit SHA-1 hash	No	Required
authorityKeyIdentifier	(2.5.29.35) {id-ce 35}	160-bit SHA-1 hash	No	Required
ocspNoRevocationCheck		1.3.6.1.5.5.7.48.1.5 (id-pkix-ocsp-nocheck)	No	Required

CPS PKI

Digidentity - G4 PKIo Priv G-Other LP - 2025 (OCSP Signing certificate)

Field	OID	Value	Critical	Type
Version		x.509 version 3		Required
SerialNumber	2.5.4.5	Automatically created unique number		Required
SignatureAlgorithm	1.2.840.113549.1.1.10	RSA-PSS Signature Scheme		Required
Validity				
NotValidBefore		<date of issuance>		Required
NotValidAfter		<+1 year>		Required
Issuer DN				
commonName	(2.5.4.3) {id-at-3}	CN=Digidentity - G4 PKIo Priv G-Other LP – 2025		Required
organisationName	(2.5.4.10)	O=Digidentity B.V.		Required
organizationIdentifier	(2.5.4.97)	NTRNL-27322631		Required
countryName	(2.5.4.6) {id-at-6}	C=NL		Required
Subject DN				
commonName	(2.5.4.3) {id-at-3}	CN= Digidentity - G4 PKIo Priv G-Other LP - 2025 OCSP		Required
organisationName	(2.5.4.10)	O=Digidentity B.V.		Required
organizationIdentifier	(2.5.4.97)	NTRNL-27322631		Required
countryName	(2.5.4.6) {id-at-6}	C=NL		Required
Public Key				
algorithm	(1.2.840.113549.1.1.1)	RSAEncryption		Required
keySize		2.048 bits, 3.072 bits or 4.096 bits		Required
signature		512 bits		Required
Extensions				
keyUsage	(2.5.29.15) {id-ce 15}	digitalSignature	Yes	Required
extKeyUsage	(2.5.29.37) {id-ce 37}	id-kp-OCSP-signing (1.3.6.1.5.5.7.3.9)	Yes	Required
certificatePolicies	(2.5.29.32) {id-ce 32}	PolicyID1=2.16.528.1.1003.1.2.44.16.29.10 (OCSP) PolicyID2= 0.4.0.2042.1.2 (NCP+)	No	Required
subjectKeyIdentifier	(2.5.29.14) {id-ce 14}	160-bit SHA-1 hash	No	Required
authorityKeyIdentifier	(2.5.29.35) {id-ce 35}	160-bit SHA-1 hash	No	Required
ocspNoRevocationCheck		1.3.6.1.5.5.7.48.1.5 (id-pkix-ocsp-nocheck)	No	Required

CPS PUBLIC

Digidentity - Digidentity - G4 PKIo Priv G-TLS - 2025 (OCSP Signing certificate)

Field	OID	Value	Critical	Type
Version		x.509 version 3		Required
SerialNumber	2.5.4.5	Automatically created unique number		Required
SignatureAlgorithm	1.2.840.113549.1.1.10	RSA-PSS Signature Scheme		Required
Validity				
NotValidBefore		<date of issuance>		Required
NotValidAfter		<+1 year>		Required
Issuer DN				
commonName	(2.5.4.3) {id-at-3}	CN= Digidentity - G4 PKIo Priv G-TLS - 2025		Required
organizationName	(2.5.4.10)	O=Digidentity B.V.		Required
organizationIdentifier	(2.5.4.97)	NTRNL-27322631		Required
countryName	(2.5.4.6) {id-at-6}	C=NL		Required
Subject DN				
commonName	(2.5.4.3) {id-at-3}	CN=Digidentity - 4 PKIo Priv G-TLS - 2025 OCSP		Required
organizationName	(2.5.4.10)	O=Digidentity B.V.		Required
organizationIdentifier	(2.5.4.97)	NTRNL-27322631		Required
countryName	(2.5.4.6) {id-at-6}	C=NL		Required
Public Key				
algorithm	(1.2.840.113549.1.1.1)	RSAEncryption		Required
keySize		2.048 bits, 3.072 bits or 4.096 bits		Required
signature		512 bits		Required
Extensions				
keyUsage	(2.5.29.15) {id-ce 15}	digitalSignature	Yes	Required
extKeyUsage	(2.5.29.37) {id-ce 37}	id-kp-OCSP-signing (1.3.6.1.5.5.7.3.9)	Yes	Required
certificatePolicies	(2.5.29.32) {id-ce 32}	PolicyID1= 2.16.528.1.1003.1.2.44.15.39.10 (OCSP) PolicyID2= 0.4.0.2042.1.2 (NCP+)	No	Required
subjectKeyIdentifier	(2.5.29.14) {id-ce 14}	160-bit SHA-1 hash	No	Required
authorityKeyIdentifier	(2.5.29.35) {id-ce 35}	160-bit SHA-1 hash	No	Required
ocspNoRevocationCheck		1.3.6.1.5.5.7.48.1.5 (id-pkix-ocsp-nocheck)	No	Required

CPS PKIo