Digidentity

Certificate Policy & Certificate Practice Statement

Digidentity Certificates

Title	Certificate Practice Statement - Digidentity Certificates
Date	31 January 2022
Valid from	7 February 2022
Version	2022-v1
Classification	Public

Digidentity

Revisions

Version	Date	Description
2019-v1	22 March 2019	Initial document
2019-v2	7 June 2019	Update address Digidentity, update URL test certificates, removed blank sections, removed methods not used, added detail on confirmation code, add CRL for qualified and advanced certificates, set Subject organizationIdentifier to "Unique number identifying Organisation"
2019-v3	12 September 2019	Aligned CPS with CPS for PKIoverheid Certificates, added missing sections and removed empty sections to comply to RFC3647 and Mozilla Root Store Policy, added missing OCSP profile for Digidentity Secure Email CA OSCP, added Digidentity Assurance Root Hierarchy and certificates (data verification, certificate profiles)
2019-v4	6 December 2019	Updated to Baseline requirements 1.6.6, updated Digital Passport certificate profile, added Self Service Portal
2020-v1	16 March 2020	Updated to BR 1.6.7, updated to Mozilla Root Store Policy 2.7, Organisation SSL and Domain SSL validity set to 395 days, Digital Passport validity set to 2 years, 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 issuing CA of Digidentity Services Root CA, changed extensions in authorityInfoAccess and cRLDistributionPoints, added Remote Identification and updated face-2-face identification, added clarifications
2021-v1	1 June 2021	Updated to BR 1.7.4, removed DDY Services Root CA, aligned Section 9 with General Terms & Conditions, processed comments Bugzilla review
2022-v1	31 January 2022	Updated to BR 1.8.0, updated 6.2.1 with actions in case of revocation HSM certification (ETSI), added Digidentity G2 CA and Automotive and eDelivery certificates, removed Digital Passport and ABC, updated remote identification, added handling of attributes, added new ISO certifications

(*) All changes are marked in grey highlight.

30 Jan 2022 12:55 +0100
Den Haag

Digidentity B.V.
QUALIFIED BUSINESS SEAL

Digidentity

Contents

Digidentity

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.

All certificate policy applicable to this CPS is contained within the bordered text boxes in the appropriate clause spaces. Text inside the boxes is the CP. Text outside of the boxes is the detailed response of Digidentity, as the CPS.

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

The Certification Practice Statement MUST be structured in accordance with RFC 3647. The Certification Practice Statement MUST include all material required by RFC 3647.

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 Digidentity 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 advanced certificates may be used as an advanced electronic signature and personal qualified certificates and electronic seal may be used as a signature to legally sign documents.

Personal 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. The Certificate Policy for Qualified Certificates is aligned with the Qualified Certificate Policy for natural persons (QCP-n-qscd) and the Qualified Certificate Policy for legal persons (QCP-l-qscd) as defined in ETSI 319 411-1 and ETSI 319 411-2.

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 Baseline requirements, CA/Browser Forum Network Security requirements), ISO27001:2013, ISO27701:2019, ISO27017:2015, ISO27018:2019, Adobe Approved Trust List (AATL).

Digidentity is certified against the ETSI EN 319 411-1, ETSI EN 319 411-2, ISO27001:2013, ISO27701:2019, ISO27017:2015 and ISO27018:2019 standards and eIDAS (Regulation (EU) No 910/2014).

This CP/CPS covers the following Certificate Authorities of Digidentity:

CA	OID
Digidentity SSCD Root CA	1.3.6.1.4.1.34471.3
Digidentity Personal Qualified CA	1.3.6.1.4.1.34471.3.1
Digidentity Business Qualified CA	1.3.6.1.4.1.34471.3.2
Digidentity Personal Advanced CA	1.3.6.1.4.1.34471.3.3
Digidentity Assurance Root CA	1.3.6.1.4.1.34471.4
Digidentity G2 CA	1.3.6.1.4.1.34471.4.1

1.1.1 Intended audience

This document is intended for:

- Subscribers
- Certificate Holders
- Company Managers
- Relying parties
- Registration Authorities

1.1.2 CA Hierarchy

The CPS shall include the complete CA hierarchy, including root and subordinate CA's.

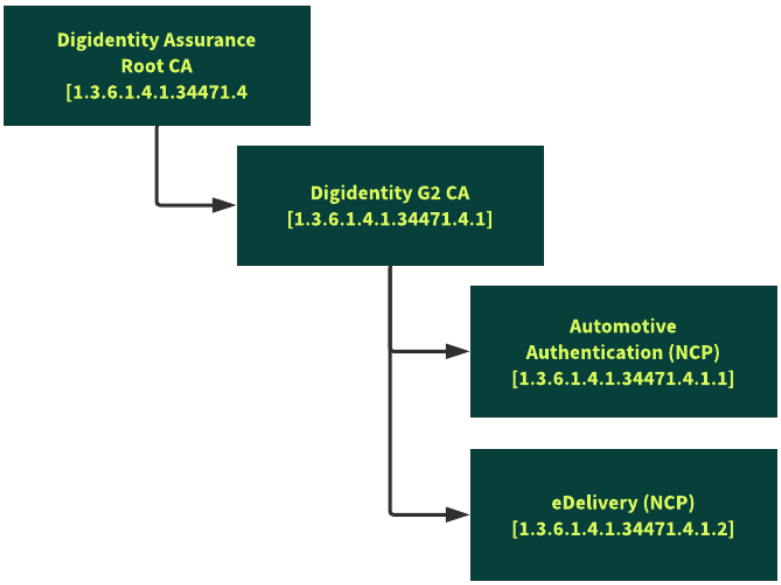


Figure 1 - Digidentity Assurance Root CA hierarchy

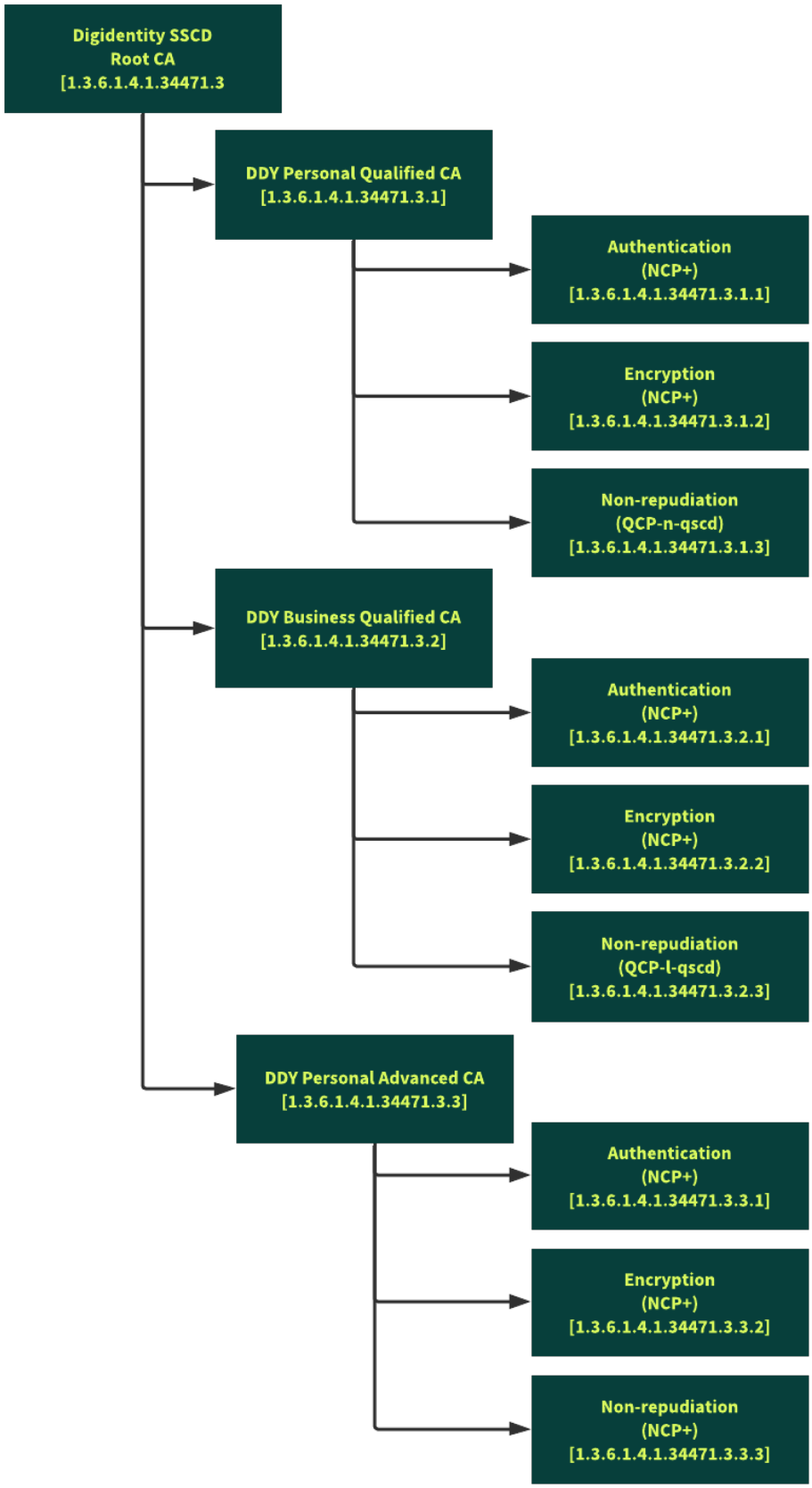


Figure 2 – Digidentity SSCD Root CA hierarchy

1.2 Document Name & Identification

The CA has identified which of the certificate policies defined in the present document it adopts as the basis, plus any variances it chooses to apply. The CA makes available the CPs supported by the TSP to its user community. A unique object identifier shall be obtained for the CP of the form required in Recommendation ITU-T X.509.

This document is identified as: Certificate Policy & Certificate Practice Statement for Digidentity 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 for:

- Qualified certificates for natural persons (Personal Qualified CA) – OID 1.3.6.1.4.1.34471.3.1
  - Personal Authentication (NCP+) – OID 1.3.6.1.4.1.34471.3.1.1
  - Personal Encryption (NCP+) – OID 1.3.6.1.4.1.34471.3.1.2
  - Personal Non-Repudiation (QCP-n-qscd) – OID 1.3.6.1.4.1.34471.3.1.3
- Qualified certificates for legal persons – Seals (Business Qualified CA) – OID 1.3.6.1.4.1.34471.3.2
  - Business Authentication (NCP+) – OID 1.3.6.1.4.1.34471.3.2.1
  - Business Encryption (NCP+) – OID 1.3.6.1.4.1.34471.3.2.2
  - Business Non-Repudiation (QCP-l-qscd) – OID 1.3.6.1.4.1.34471.3.2.3
- Advanced certificates for natural persons (Personal Advanced CA) – OID 1.3.6.1.4.1.34471.3.3
  - Personal Authentication (NCP+) – OID 1.3.6.1.4.1.34471.3.3.1
  - Personal Encryption (NCP+) – OID 1.3.6.1.4.1.34471.3.3.2
  - Personal Non-Repudiation (NCP+) – OID 1.3.6.1.4.1.34471.3.3.3
- Authentication certificates (Digidentity G2 CA) – OID 1.3.6.1.4.1.34471.4.1
  - Automotive Authentication (NCP) – OID 1.3.6.1.4.1.34471.3.4.1.1
  - eDelivery (NCP) – OID 1.3.6.1.4.1.34471.3.4.1.2

Qualified certificates for electronic signatures issued to natural persons (Personal Qualified) and Qualified certificates for electronic seals issued to legal persons are also EU Qualified Certificates according to Regulation (EU) No 910/2014. The Certificate Policy for Qualified Certificates is in this case aligned with the Qualified Certificate Policy for natural persons (QCP-n-qscd as defined in ETSI EN 319 411-2) and Qualified Certificates Policy for electronic seals (QCP-l-qscd as defined in ETSI EN 319 411-2). Advanced certificates for natural persons (Personal Advanced) are issued to natural persons according to Regulation (EU) No 910/2014.

The Certificate Policy for authentication, encryption and non-repudiation (non-qualified) certificates are aligned with the Normalised Certificate Policy (NCP) and Normalised Certificate Policy Plus (NCP+) as defined in ETSI EN 319 411-1.

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, Subscribers, Relying Parties and Subcontractors.

1.3.1 Certificate Authorities

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

1.3.2 Registration Authorities

A Registration Authority (RA) is a function 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 performed by 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 Manager

Subscribers can be a;

[1] natural person
[2] natural person in association with a legal person – a legal representative of an organisation
[3] legal person represented by natural person(s)

Subscribers use our services. Subscribers are not always the party identified in a certificate, e.g. when a certificate is issued to an organisation. 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

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 are organisations or natural persons. The Company Manager 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 services related to digital certificates, Digidentity has the following participants;

[1] Kamer van Koophandel (Dutch Chamber of Commerce)
[2] Identity verification services
[3] Identity document verification services

1.4 Certificate Usage

1.4.1 Appropriate certificate usage

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

Personal Certificates (Advanced & Qualified)

- Authentication Certificate: can be used to reliably authenticate a Subscriber.
- Encryption Certificate: can be used for the securing of trusted information/details which are exchanged in electronic form. This includes exchanges between people as well as people and automated systems.
- Non-repudiation Certificate: can be used to digitally sign documents. These certificates are issued as Advanced or 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 an organisation.
- Encryption Certificate: can be used for the securing of trusted information/details which are exchanged in electronic form.
- 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).

Automotive Authentication Certificates

- Authentication Certificate: can be used to reliably authenticate a Subscriber linked to an organisation.

eDelivery Certificates

- Authentication Certificate: can be used to reliably authenticate an organisation.

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.
Waldorpstraat 13-F
2521 CA The Hague
The Netherlands

1.5.2 Contact Person

For questions about this document please contact;

Digidentity B.V.
Security, Risk & Compliance (SRC)
Waldorpstraat 13-F
2521 CA The Hague
Tel: +31 (0)88 78 78 78
Email: 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 by Subscribers, including contact details, is described in paragraph 4.9.3.

1.5.3 CPS & CP Approval

The CA have a defined review process to ensure that the CP is supported by the CA's CPS. There is a body with final authority and responsibility for specifying and approving the CP. CPs are approved and modified in accordance with a defined review process, including responsibilities for maintaining the CP. Revisions to CPs supported by the CA are made available to subscribers and relying parties.

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, and eIDAS will be assessed, and any inconsistency remedied. Before publishing, this document is approved by Digidentity Management with digital signatures.

This document will be published signed with a Digidentity Seal, and thus made available to subscribers and relying parties after approval from Digidentity Management.

1.6 Definitions & Acronyms

See Appendix A for a table of acronyms and definitions.

Digidentity

2 Publication & Repository Responsibilities

2.1 Repositories

The CA SHALL make revocation information for Subordinate Certificates and Subscriber Certificates available in accordance with this Policy. The CA SHALL make revocation information for Subordinate Certificates and Subscriber Certificates available in accordance with this Policy.

Digidentity maintains an online repository, containing:

[a] Certificate Policy & 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 Digidentity

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

2.2 Publication of Information

The CA SHALL publicly disclose its Certificate Policy and/or Certification Practice Statement through an appropriate and readily accessible online means that is available on a 24x7 basis.

The Certificate Policy and/or Certification Practice Statement MUST be structured in accordance with RFC 3647 and MUST include all material required by RFC 3647.

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

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

Subscribers can download their certificates in their Digidentity account.

2.3 Time or Frequency of Publication

The CA develops, implements, enforces, and annually updates a Certification Practice Statement that describes in detail how the Certificate Policy is implemented.

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 CA provides all repository information and documentation in a read-only format.

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.

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
CN - Common Name	Given Names and Surname as registered on ID	64
Serial Number	Unique number to identify subject	64
C - Country	Two-digit country code (nationality or ID issuing country)	2
GN - Given Name	Given Names as registered on ID	64
S - Surname	Surname as registered on ID	64

Organisation Certificates (Seal)

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

Automotive Authentication certificates

Field	Description	Max. Length
CN - Common Name	Email address of Subscriber	64
eMailAddress	Email address of Subscriber	64
organizationName	Name of the Organisation as registered in Trade Register	64
organizationIdentifier	Organisation Trade Register number	64
Pseudonym	Unique number to identify subject	64
C - Country	Two-digit country code (nationality or ID issuing country)	2

eDelivery certificates

Field	Description	Max. Length
CN - Common Name	Name of the Organisation as registered in Trade Register	64
organizationName	Name of the Organisation as registered in Trade Register	64
organizationIdentifier	Organisation Trade Register number or Legal Entity Identifier	64
eMailAddress	Email address assigned to Subject	64
C - Country	Two-digit country code (nationality or ID issuing country)	2

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 to 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.

3.2 Initial Identity Validation

An Issuer CA may use any legal means of investigation to determine the identity of an organisational or individual Applicant. The Issuer CA may refuse to issue a certificate in its sole discretion.

With the exception of sections 3.2.2.4 and 3.2.2.5, the CA MAY delegate the performance of all, or any part, of Section 3.2 requirements to a Delegated Third Party, provided that the process as a whole fulfils all of the requirements of Section 3.2.

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, Automotive Authentication certificates can be requested. 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). For Automotive Authentication and eDelivery certificates, a Company Administrator role is required.

3.2.1 Method to prove possession of Private Key

The CA SHALL warrant that the Subject named in a Certificate is in possession of the Private Key that corresponds to the Public Key in that Certificate.

If the CA generates the Subject's key:

- *the procedure of issuing the Certificate SHALL be securely linked to the generation of the key pair by the CA*
- *the Private Key SHALL be securely made available to the registered Subject*

For Personal Qualified and Personal Advanced certificates, 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 subscribers' sole control.

The PIN code protecting the private keys is only known to the Subscriber. The private keys remain encrypted in the HSM at all times and may be accessed by the Subscriber after providing the correct PIN code 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.

If the Subject's key pair is generated by the Subject/Subscriber, the certificate request process SHALL ensure that the Subscriber has possession of the Private Key associated with the Public Key presented.

For Seals, Digidentity also allows the Subscriber to generate their own private key on the HSM of the Subscriber and send signed Certificate Signing Request (CSR) to prove possession of the private key, which corresponds to the public key in the certificate request.

For Automotive Authentication certificates, the Company Administrator generates the 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 using the Self-Service Portal.

For eDelivery certificates, the Company Administrator generates the 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 using the ABC Tool.

For Automotive Authentication and eDelivery certificates the private key is in control of the subscribing organisation.

3.2.2 Authentication of Organisation & Domain Identity

This section is relevant only when the Subscriber is different from the Subject. The following Subscriber data SHALL be obtained prior to any Subject initial registration:

- *full name and legal status of the Subscriber as defined in the Central Coordinating Register for Legal Entities*
- *the Subscriber's Organisation Number as defined in the Central Coordinating Register for Legal Entities*
- *name and contact information of Subscriber Representatives authorised to operate as Contract Signer or Certificate Manager*

Digidentity does not issue certificates containing a domain name.

3.2.2.1 Identity

If the Subject Identity Information is to include the name or address of an organisation, the CA SHALL verify the identity and address of the organisation and that the address is the Applicant's address of existence or operation.

Digidentity verifies organisational identities with the Dutch Chamber of Commerce using the Chamber of Commerce registration number (KvK number) of the organisation. After the KvK number is entered, the details are retrieved automatically via a secure connection with KvK. The address, name and country details are taken directly from the KvK register.

For Dutch governmental agencies, an OIN (Organisation Identification Number) is used to verify the identity of the organisation. The OIN is issued by the Dutch government and the organisation details are verified by Digidentity at Logius (Dutch government).

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

If the Subject Identity Information is to include a DBA or tradename, the CA SHALL verify the Applicant's right to use the DBA/tradename.

The organisation tradename is checked via the details on the Chamber of Commerce Registry. 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

If the subject:countryName field is present, then the CA SHALL verify the country associated with the Subject using one of the following: (a) the IP Address range assignment by country for either (i) the web site's IP address, as indicated by the DNS record for the web site or (ii) the Applicant's IP address; (b) the ccTLD of the requested Domain Name; (c) information provided by the Domain Name Registrar; or (d) a method identified in Section 3.2.2.1.

Digidentity uses the method in section 3.2.2.1.

3.2.2.4 Validation of Domain Authorisation or Control

Digidentity does not use these methods. Digidentity does issue certificates containing FQDN.

3.2.2.4.1 Validating the Applicant as a Domain Contact

Digidentity does not use this method.

3.2.2.4.2 Email, Fax, SMS or Postal Mail to Domain Contact

Digidentity does not use this method.

3.2.2.4.3 Phone Contact with Domain Contact

Digidentity does not use this method.

3.2.2.4.4 Constructed Email to Domain Contact

Digidentity does not use this method.

3.2.2.4.5 Domain Authorisation Document

Digidentity does not use this method.

3.2.2.4.6 Agreed-Upon Change to Website

Digidentity does not use this method.

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

Digidentity does not use this method.

3.2.2.4.10 TLS Using a Random Number

Digidentity does not use this method.

3.2.2.4.11 Any Other Method

Digidentity does not use this method.

3.2.2.4.12 Validating Applicant as a Domain Contact

Digidentity does not use this method.

3.2.2.4.13 Email to DNS CAA Contact

Digidentity does not use this method.

3.2.2.4.14 Email to DNS TXT Contact

Digidentity does not use this method.

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.

3.2.2.5 Authentication for an IP Address

Digidentity does not use these methods.

3.2.2.5.1 Agreed-Upon Change to Website

Digidentity does not use this method.

3.2.2.5.2 Email, Fax, SMS, or Postal Mail to IP Address Contact

Digidentity does not use this method.

3.2.2.5.3 Reverse Address Lookup

Digidentity does not use this method.

3.2.2.5.4 Any Other Method

Digidentity does not use this method.

3.2.2.5.5 Phone Contact with IP Address Contact

Digidentity does not use this method.

3.2.2.5.6 ACME "http-01" method for IP Addresses

Digidentity does not use this method.

3.2.2.5.7 ACME "tls-alpn-01" method for IP Addresses

Digidentity does not use this method.

3.2.2.6 Wildcard Domain Validation

Digidentity does not use this method.

3.2.2.7 Data Source Accuracy

Prior to using any data source as a Reliable Data Source, Digidentity will evaluate the source for its reliability, accuracy, and resistance to alteration or falsification.

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

- Chamber of Commerce data - not older than fifteen (15) days

If the document is older, 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 in order to reverify information included in the certificate.

3.2.2.8 CAA Records

Digidentity does not use this method.

3.2.3 Authentication of Individual Identity

If an Applicant subject to this Section 3.2.3 is a natural person, then Digidentity will verify the Applicant's name and the authenticity of the certificate request.

Digidentity will verify the Applicant's name using a legible copy, which discernibly shows the Applicant's face, of at least one currently valid government-issued photo ID (passport, driver's license, military ID, national ID, or equivalent document type).

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 @ DDY" on our website (https://www.digidentity.eu/en/documentation).

3.2.3.1 Personal Details

The CA will verify the Applicant's name using a legible copy, which discernibly shows the Applicant's face, of at least one currently valid government-issued photo ID (passport, driver's license, military ID, national ID, or equivalent document type).

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.

3.2.3.2 Email address

An CA must take reasonable measures to verify that the entity submitting the request for a certificate to be used to sign or encrypt email controls the email account associated with the email address referenced in the certificate or has been authorised by the email account holder to act on the account holder's behalf.

Applicants are required to enter an email address during the initial registration process or when requesting a certificate containing an email address. Digidentity verifies the email address by sending a confirmation code to the entered email address. The Applicant enters the confirmation code to confirm control over the email 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.

For eDelivery, the email address of the Company Manager is verified as written above. The email address in the eDelivery certificate is generated by ABZ and assigned to the legal person.

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.

3.2.3.4 Phone number

Mobile phone number is used to send messages or contact you for a face-to-face meeting. Digidentity sends a confirmation code to the mobile phone using the applicant's supplied mobile phone number.

3.2.3.5 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 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
- 9.3 Use case for identity proofing of legal person
- 9.4 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 service 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

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

3.2.3.5.1 Validation of Identity Documents using NFC

Digidentity supports the use of Near Field Communication (NFC) to read the NFC chip in modern identity documents (e.g. passports, identity cards and driver's 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 validation of the ID and verification of the data using cryptographic controls.

The Applicant uses the Digidentity mobile app (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 services but is mandatory for Qualified certificates, Seals and eIDAS High or other Level of Assurance level 4 services.

3.2.3.5.2 Validation of Identity Documents using images

Digidentity supports the validation of identity documents using photos of the physical identity document. The Applicant uses the Digidentity mobile app (iOS and Android) to take photos of the identity document. The images are uploaded to Digidentity.

An automated 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 services with a level of assurance 3 and lower.

3.2.3.5.3 Verification of natural person using Liveness Detection

Digidentity uses liveness detection 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 mobile app starts a video stream of the Applicant where the Applicant must move his/her head in a randomly selected direction. The mobile app extracts to images from the video stream which are used for the liveness detection. The 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.

The biometric service uses artificial intelligence in several instances of Deep Convolutional Neural Networks (DCNN) to provide Digidentity with a true or false response. The DCNN for face comparison and liveness detections are trained on datasets using more than five million face images.

3.2.3.5.4 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.

3.2.3.6 Face-to-face verification

For eHerkenning Level 4, Digidentity must verify the identity of the natural person and the identity of a legal representative or authorised representative of an organisation with a face-to-face check. We will make an appointment by phone for this check. During the F2F, Digidentity will verify the identity document.

3.2.3.7 General Terms & Conditions and Privacy Statement

During registration, it is required to agree with the General Terms & Conditions and Privacy Statement.

3.2.3.8 General verifications

For all applications, Digidentity verifies:

- Organisational information 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 Manager. The delegated person will be verified via the process described above, including a face-to-face check or 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 Manager. The delegated person will be verified via the process described above, including a face-to-face check or 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.

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

If the Applicant for a Certificate containing Subject Identity Information is an organisation, the CA will use a Reliable Method of Communication to verify the authenticity of the Applicant Representative's certificate request.

The CA will use the sources listed in section 3.2.2.1 to verify the Reliable Method of Communication.
In addition, the CA have established a process that allows an Applicant to specify the individuals who may request certificates.

If the request is for a certificate that asserts an organisational affiliation between a human Subscriber and an organisation, the CA shall obtain documentation from the organisation that recognises the affiliation and obligates the organisation to request revocation of the certificate if that affiliation ends.

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

- Checking the Chamber of Commerce registry for organisational applicants
- Checking the identity of the applicant in the face-to-face check.
- 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 Requests

The CA SHALL make revocation information for Subordinate Certificates and Subscriber Certificates available in accordance with this Policy. The CA shall revoke certificates in a timely manner based on authorised and validated certificate revocation requests.

Only the Subscriber or an authorised representative of the Subscriber MAY request certificate revocation on behalf of the Subscriber.

The RA SHALL implement identification and authentication procedure that provide reasonable assurance that the requestor of the revocation is the Subscriber or an authorised representative of the Subscriber acting on behalf of the Subscriber.

If the Subscriber or authorised representative of the Subscriber wishes to make a request for revocation, then the following is applicable;

3.4.1 Website

Subscribers can log into their account and revoke personal certificate(s). If a Subscriber is able to log into their account, the identity is verified. After selecting 'delete smartcard 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 Automotive Authentication certificates, the Subscriber or Company Manager must log into their account to access the Self-Service Portal (SSP). In the SSP, the Subscriber or Company Manager can select the certificate to be revoked. A confirmation of the revocation is sent via email.

To revoke eDelivery certificates, the Company Manager must use the ABC tool and revoke the certificate. A confirmation of the revocation is displayed in the ABC tool.

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 email 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. After the account recovery, the Subscriber can revoke the certificate themselves in the account as described above.

3.4.3 Recover smart cards

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 Virtual Smart Card to revoke 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 Virtual Smart Card 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 smartcard and certificates by scanning a QR-code and uploading an identity document. After verification, a QR code can be scanned to create the Virtual Smart Card with Certificates as well as a new five-digit PIN code. The Virtual Smart Card with new certificates is then activated.

3.4.4 Phone

If the Subscribers or Company Managers 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 smartcard on the mobile device is lost, we support the Subscriber with the recovery process as described in section 3.4.1.

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

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

- Official Name
- KvK number
- Organisation name
- Email address
- Certificate to be revoked

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

3.4.5 Email

Digidentity does not accept revocation requests via email 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 email address in the account, the account cannot be recovered.

4 Certificate Life-Cycle Operation Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

The Subject SHALL register with an RA either prior to, or at the time of, applying for a Certificate. 3.2 defines necessary requirements for identification and authentication.

A certificate application can be submitted by a:

[1] Natural person applying for a personal qualified certificate or a personal advanced certificate.

[2] Natural person legally representing an Organisation (legal entity) and applying for a business qualified certificate for electronic seals, or Automotive Authentication or eDelivery certificate for the organisation.

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

4.1.2 Enrolment Process and Responsibilities

The Subject SHALL accept the terms and conditions regarding the use of Digidentity certificates including to the storing of records by the CA of data used in the registration.

Digidentity will obtain any additional documentation determined necessary to meet Requirements.

The certificate request MUST contain a request from, or on behalf of, the Applicant for the issuance of a Certificate, and a certification by, or on behalf of, the Applicant that all of the information contained therein is correct.

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.

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

Section 4.2 of a CA's Certificate Policy and/or Certification Practice Statement (section 4.1 for CAs still conforming to RFC 2527) SHALL state the CA's policy or practice on processing CAA Records for Fully Qualified Domain Names.

It shall clearly specify the set of Issuer Domain Names that the CA recognises in CAA "issue" or "issuewild" records as permitting it to issue. The CA SHALL log all actions taken, if any, consistent with its processing practice.

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

Digidentity does not issue certificates that contain FQDN so no CAA Records for FQDN are processed.

4.2.1 Performing Identification and Authentication Functions

The CA has established and follow a documented procedure for verifying all data requested for inclusion in the Certificate by the Applicant.

The CA can use documents and data provided in Section 3.2 to verify certificate information, or may reuse previous validations themselves, provided that the previous completed validation is no more than 825 days old prior to issuing the certificate.

The CA SHALL develop, maintain, and implement documented procedures that identify and require additional verification activity for High Risk Certificate Requests prior to the Certificate's approval, as reasonably necessary to ensure that such requests are properly verified under these Requirements.

See section 3.2.

4.2.2 Approval or Rejection of Certificate Applications

CAs SHALL NOT issue certificates containing Internal Names (see section 7.1.4.2.1).

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 and Advanced Certificates, and Seals, once the Virtual Smart Card creation is completed, the Subscriber has possession. The Virtual Smart Card 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 and the Self-Service Portal. Company Managers are able to download certificates by signing into the Self-Service Portal using their account credentials.

4.3.1 CA Actions During Certificate Issuance

Certificate issuance by the Root CA SHALL require an individual authorized by the CA (i.e. the CA system operator, system officer, or PKI administrator) to deliberately issue a direct command in order for the Root CA to perform a certificate signing operation.

Certificate issuance by the Root CA's is only performed by authorised employees within the CA operations facility.

4.3.2 Notification of Certificate Issuance

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

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 once:

- The Virtual Smart Card is linked with a PIN code to the mobile device
- 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.

4.4.2 Publication of the Certificate by the CA

Issuing CAs of Digidentity shall publish all CA Certificates to the repository.

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:

[1] certificate validity
[2] validity of the complete chain of certificates, up to the root certificate
[3] revocation status of the certificate
[4] limitations on any use of the certificate
[5] 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.

4.6.1 Circumstance for certificate renewal

No stipulation

4.6.2 Who may request renewal

No stipulation

4.6.3 Processing certificate renewal requests

No stipulation

4.6.4 Notification of new certificate issuance to subscriber

No stipulation

4.6.5 Conduct constituting acceptance of a renewal certificate

No stipulation

4.6.6 Publication of the renewal certificate by the CA

No stipulation

4.6.7 Notification of certificate issuance by the CA to other entities

No stipulation

4.7 Certificate Re-Key

Digidentity does not perform re-key of certificates.

4.7.1 Circumstance for certificate re-key

No stipulation

4.7.2 Who may request certification of a new public key

No stipulation

4.7.3 Processing certificate re-keying requests

No stipulation

4.7.4 Notification of new certificate issuance to subscriber

No stipulation

4.7.5 Conduct constituting acceptance of a re-keyed certificate

No stipulation

4.7.6 Publication of the re-keyed certificate by the CA

No stipulation

4.7.7 Notification of certificate issuance by the CA to other entities

No stipulation

4.8 Certificate Modification

Digidentity does not perform modification of certificates.

4.8.1 Circumstance for certificate modification

No stipulation

4.8.2 Who may request certificate modification

No stipulation

4.8.3 Processing certificate modification requests

No stipulation

4.8.4 Notification of new certificate issuance to subscriber

No stipulation

4.8.5 Conduct constituting acceptance of modified certificate

No stipulation

4.8.6 Publication of the modified certificate by the CA

No stipulation

4.8.7 Notification of certificate issuance by the CA to other entities

No stipulation

4.9 Certificate Revocation & Suspension

The CA make revocation information for Subordinate Certificates and Subscriber Certificates available in accordance with policy requirements.

4.9.1 Circumstances for Revocation

The CA will process and complete the revocation of certificates within four (4) hours of receiving the request to revoke from the Subscriber for circumstances described in this CPS

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.

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 that the certificate was not issued in accordance with the requirements or the CAs Certificate Policy or Certification Practice Statement;
[7] CA determines that any of the information appearing in the certificate is inaccurate or misleading;
[8] CA ceases operation for any reason and has not made arrangements for another CA to provide support for revocation of the Certificate;
[9] Revocation is required by the CA's Certificate Policy and/or Certification Practice Statement; or
[10] Technical content or format of the certificate presents an unacceptable risk to Subscribers, Relying Parties and third parties (e.g. that a deprecated cryptographic/signature algorithm or key size presents an unacceptable risk and that such Certificates should be revoked and replaced within a given period of time);
[11] The Subscriber ceases operation;
[12] The Subscriber is deceased

4.9.1.2 Reasons for Revoking a Subordinate CA Certificate

Digidentity will revoke a Subordinate CA certificate when:

[1] CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the certificate;
[2] CAs right to issue certificates under these requirements expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP Repository;
[3] CA is made aware of a possible compromise of the Private Key of the Subordinate CA used for issuing the certificate;
[4] Revocation is required by the CA's Certificate Policy and/or Certification Practice Statement; or
[5] Technical content or format of the certificate presents an unacceptable risk

4.9.2 Who can request Revocation?

The Subscriber or authorised representative of the Subscriber, RA, or CA can initiate revocation. Additionally, Subscribers, Relying Parties, Application Software Suppliers, and other third parties may submit Certificate Problem Reports informing the issuing CA of reasonable cause to revoke the certificate.

Revocation can be requested by:

[a] Subscriber (or Certificate Holder)
[b] Legal representative or authorised person of the organisation (Company Manager)
[c] Digidentity
[d] Authorities/regulators who are involved in the regulation of PKI activities, e.g. Agentschap Telecom

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

4.9.3 Procedure for Revocation Request

The CA provides a process for Subscribers to request revocation of their own certificates. The process of revocation request is described in this Certification Practice Statement. The CA maintain the continuous 24x7 ability to accept and respond to revocation requests and Certificate Problem Reports.

The CA provides Subscribers, Relying Parties and other third parties with clear instructions for reporting suspected Private Key Compromise, certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to certificates.

Subject or Subscriber MAY submit revocation requests to an RA either in person, by writing, by telephone or through electronic communication. The possibilities that are offered SHALL be made available to the Subject and Subscriber.

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 (8.30 – 17.00 hours) by calling the Service Desk at +31 (0)88 78 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 Virtual Smart Cards which contains their certificates. By deleting a specific Virtual Smart Card, all three (3) associated certificates (authentication, encryption and non-repudiation) will be revoked. Revocation occurs immediately.

To revoke Automotive Authentication certificates, the Company Manager must log into their account in the Self-Service Portal (SSP) using two factor authentication. In the SSP, the certificates to be revoked. To revoke eDelivery certificates, the Company Manager must use the ABC tool to revoke the certificate.

The Subscriber or Company Manager 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

Within 24 hours after receiving a Certificate Problem Report, Digidentity will investigate the facts and circumstances related to a Certificate Problem Report and provide a preliminary report on its findings to both the Subscriber and the entity who filed the Certificate Problem Report.

The maximum delay between receipt of a revocation request and the decision to change its status information being available to all relying parties shall be at most 24 hours.

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

Following certificate issuance, a certificate may be revoked for reasons stated in Section 4.9.1. Therefore, relying parties should check the revocation status of all certificates that contain an OCSP pointer.

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

For the status of Subscriber Certificates: Digidentity publishes a CRL which is updated and reissued at least once every seven days. For the status of the Root CA and Subordinate CA Certificates: Digidentity updates and reissues CRLs at least (i) once every twelve months and (ii) within 24 hours after revoking a Subordinate CA Certificate.

Digidentity publishes the CRL for the issuing CA every ten (10) minutes, whereby the CRL is valid for 24 hours. The CRL for the Digidentity Roots will be published once a year and are valid for one year.

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

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

The CA shall ensure that the certificate status information distributed by it on-line meets or exceeds the requirements for CRL issuance and latency stated in sections 4.9.5, 4.9.7 and 4.9.8.

OCSP responses must conform to RFC6960 and/or RFC5019. OCSP responses must either:

[1] *Be signed by the CA that issued the Certificates whose revocation status is being checked, or*

[2] *Be signed by an OCSP Responder whose certificate is signed by the CA that issued the Certificate whose revocation status is being checked.*

Digidentity does not use OCSP services for certificates issued from Digidentity issuing CA.

4.9.10 Online Revocation checking Requirements

A relying party shall confirm the validity of a certificate via CRL or OCSP in accordance with section 4.9.6 prior to relying on the certificate. OCSP responders operated by the CA SHALL support the HTTP GET method, as described in RFC 6960 and/or RFC 5019.

If the OCSP responder receives a request for the status of a certificate serial number that is "unused", then the responder SHOULD NOT respond with a "good" status. If the OCSP responder is for a CA that is not Technically Constrained in line with Section 7.1.5, the responder MUST NOT respond with a "good" status for such requests.

The CA SHOULD monitor the OCSP responder for requests for "unused" serial numbers as part of its security response procedures. The OCSP responder MAY provide definitive responses about "reserved" certificate serial numbers, as if there was a corresponding Certificate that matches the Precertificate [RFC6962].

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.

4.9.11 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.

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

The CA shall make certificate status information available via CRL or OCSP. The CA shall list revoked certificates on the appropriate CRL where they remain until one additional CRL is published after the end of the certificate's validity period.

Digidentity makes certificate status information available on the CRL. 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

CAs shall provide certificate status services 24x7 without interruption. This includes the online repository that application software can use to automatically check the current status of all unexpired certificates issued by the CA.

The CA operates and maintains its CRL and OCSP capability with resources sufficient to provide a response time of ten seconds or less under normal operating conditions. The CA shall maintain a continuous 24x7 ability to respond internally to a high-priority Certificate Problem Report.

Digidentity operates and maintains a CRL 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

Digidentity subscribers can end their subscription by allowing the certificate to expire, or by revoking their own certificate(s). Subscribers are still subject to contractual/agreement costs associated with the certificates - end of subscription is not related to financial agreements.

4.12 Key Escrow & Recovery

Digidentity does not provide key escrow and key recovery.

4.12.1 Key escrow and recovery policy and practices

No stipulation

4.12.2 Session key encapsulation and recovery policy and practices

No stipulation

Digidentity

5 Facility, Management & Operational Controls

The CA SHALL develop, implement, and maintain a comprehensive security program designed to:

[1] Protect the confidentiality, integrity, and availability of certificate data and certificate management processes;

[2] Protect against anticipated threats or hazards to the confidentiality, integrity, and availability of the certificate data and certificate management processes;

[3] Protect against unauthorized or unlawful access, use, disclosure, alteration, or destruction of any certificate data and certificate management processes;

[4] Protect against accidental loss or destruction of, or damage to, any certificate data and certificate management processes; and

[5] Comply with all other security requirements applicable to the CA by law.

The Certificate Management Process MUST include:

[1] physical security and environmental controls;

[2] system integrity controls, including configuration management, integrity maintenance of trusted code, and malware detection/prevention;

[3] network security and firewall management, including port restrictions and IP address filtering;

[4] user management, separate trusted-role assignments, education, awareness, and training; and

[5] logical access controls, activity logging, and inactivity time-outs to provide individual accountability.

The CA's security program MUST include an annual Risk Assessment that:

[1] Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any certificate data and certificate management processes;

[2] Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the certificate data and certificate management processes; and

[3] Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the CA has in place to counter such threats.

Based on the Risk Assessment, the CA SHALL develop, implement, and maintain a security plan consisting of security procedures, measures, and products designed to achieve the objectives set forth above and to manage and control the risks identified during the Risk Assessment, commensurate with the sensitivity of the certificate data and certificate management processes;. The security plan MUST include administrative, organisational, technical, and physical safeguards appropriate to the sensitivity of the certificate data and certificate management processes.

Digidentity has implemented and maintains an Information Security Management System (ISMS) which is certified against ISO27001:2013 and a Privacy Information Management System (PIMS) which is certified against ISO27701:2019 and subject to annual audit by an external auditor.

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.

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. All visitors are required to identify themselves with a legal identity document and register their arrival and departure from the offices.

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 authorisation.

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 Personal Data Breach/Leakage.

5.2.2 Number of Individuals required per task

Certificate issuance by the root CA shall be under at least dual control by authorized, trusted personnel such that one person cannot sign subordinate certificates on his/her own

All maintenance operations involving CA private keys SHALL be under at least dual control by authorised, trusted personnel.

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.

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

Prior to the engagement of any person in the Certificate Management Process, whether as an employee, agent, or an independent contractor of the CA, the CA verifies the identity and trustworthiness of such person.

CA personnel SHALL provide proof of their identity, background, qualifications and experience, as well as any other information required by the CA.

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 performs a background check 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.

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 CA SHALL ensure that records of all relevant events and related information regarding the services are retained for an appropriate period of time, in particular for the purpose of providing evidence of certification for the purposes of legal proceedings. The CA SHALL record in detail every action taken to process a certificate application and to issue a certificate, including all information generated or received in connection with a certificate application, and every action taken to process the application, including time, date, and personnel involved in the action. These records SHALL be available as auditable proof of the CA's practices. The foregoing also applies to all Registration Authorities (RAs) and subcontractors as well.

All registration information including the following shall be recorded:
[1] *type of document(s) presented by the applicant to support registration;*
[2] *record of unique identification data, numbers, or a combination thereof (e.g. subject's identity card or passport) of identification documents, if applicable;*
[3] *method used to validate identification documents*

The CA shall record all the information necessary to verify the subject's identity and if applicable, any specific attributes of the subject, including any reference number on the documentation used for verification, and any limitations on its validity.

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 data and 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
[3] Security Events;
  [a] Access attempts
  [b] System actions performed
  [c] Profile changes
  [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 for Processing & Archiving Audit Logs

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 with. 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 Accumulation 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

A risk assessment is carried out to evaluate business requirements and determine the security requirements to be included in the CP for the stated community and applicability. Digidentity selects the appropriate risk treatment measures, taking account of the risk assessment results. The risk treatment measures shall ensure that the level of security is commensurate to the degree of risk. The risk assessment is regularly reviewed and revised. Digidentity's management approve the risk assessment and accept the residual risk identified.

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.

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 records related to CA activities.

5.5.6 Archive Collection System (Internal or External)

The archive collection systems are in the Digidentity 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.

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 services for the Subscriber affected. The business continuity plan includes all criteria as required by CA/Browser Forum Baseline Requirements. 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

No Stipulation

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.

6 Technical Security Controls

6.1 Key Pair Generation & Installation

6.1.1 Key Pair Generation

6.1.1.1 CA Key Pair Generation

Digidentity shall:

[1] generate the keys in a physically secured environment as described;

[2] generate the CA keys using personnel in trusted roles under the principles of multiple person control and split knowledge;

[3] generate the CA keys within cryptographic modules meeting the applicable technical and business requirements as disclosed in the Certification Practice Statement;

[4] log its CA key generation activities; and

[5] maintain effective controls to provide reasonable assurance that the Private Key was generated and protected in conformance with the procedures described in its Certificate Policy and/or Certification Practice Statement and (if applicable) its Key Generation Script.

Digidentity has a procedure for key pair generation. Digidentity maintains a record of all key ceremonies 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.

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

The CA SHALL ensure that any Subject keys are generated securely, and the secrecy of the Subject Private Key is assured.

Digidentity generates and stores the key pair for qualified, advanced and seals in the HSM. For Automotive Authentication 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

The Subject private key SHALL be made available to the Subject making sure that the secrecy and integrity of the key is not compromised and, once made available to the Subject, the private key can be maintained under the Subject's sole control. If the CA or any of its designated RAs become aware that a Subject's Private Key has been communicated to an unauthorized person or an organisation not affiliated with the subject, then the CA shall revoke all certificates that include the public key belonging to the private key.

See section 3.2.1.

6.1.3 Public Key Delivery to Certificate Issuer

Public Keys for Automotive Authentication 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

Digidentity CA public keys can be downloaded from the repository online: https://cps.digidentity-pki.com/.

6.1.5 Key sizes

Certificates MUST meet the following requirements for algorithm type and key size.

All Digidentity CA certificates (Root CA, Subordinate CA and Subscriber CA) make use of 2.048 bits or 4.096 bits RSA keys.

All Digidentity Subscriber Certificates makes use of 2.048 bits or 4.096 bits RSA keys.

6.1.6 Public Key Parameters Generation & Quality Checking

RSA: CA confirms that the value of the public exponent is an odd number equal to 3 or more. Additionally, the public exponent SHOULD be in the range between 2^16+1 and 2^256-1. The modulus SHOULD also have the following characteristics: an odd number, not the power of a prime, and have no factors smaller than 752. [Source: Section 5.3.3, NIST SP 800-89].

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 2.048 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 CP/CPS. These linters are available for:

- Issuance of Qualified certificates
- Issuance of Advanced certificates
- Issuance of Automotive Authentication certificates

Digidentity has implemented these linters for pre-issuance and post-issuance of final certificates.

6.1.7 Key Usage Purposes

Private Keys corresponding to Root Certificates MUST NOT be used to sign Certificates except in the following cases:

[1] *Self-signed Certificates to represent the Root CA itself;*

[2] *Certificates for Subordinate CAs and Cross Certificates;*

[3] *Certificates for infrastructure purposes (administrative role certificates, internal CA operational device certificates); and*

[4] *Certificates for OCSP Response verification.*

Digidentity specifies the practice regarding the use of CA keys for signing certificates, CRLs and OCSP.

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.

6.2 Private Key Protection & Cryptographic Module Engineering Controls

The CA SHALL implement physical and logical safeguards to prevent unauthorized certificate issuance. Protection of the CA Private Key outside the validated system or device specified above MUST consist of physical security, encryption, or a combination of both, implemented in a manner that prevents disclosure of the CA Private Key. The CA SHALL encrypt its Private Key with an algorithm and key-length that, according to the state of the art, are capable of withstanding cryptanalytic attacks for the residual life of the encrypted key or key part.

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

The CA private signing key SHALL be backed up, stored and recovered only by personnel in trusted roles using, at least, dual control in a physically secured environment. The number of personnel authorised to carry out this function shall be kept to a minimum and be consistent with the CA's practices.

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

CA Private Keys SHALL be archived by the CA when they are no longer used.

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.

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.

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 Capabilities

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

Subscriber Certificates issued after 1 March 2018 MUST have a Validity Period No greater than 825 days.

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 SSCD Root CA is valid until 4 July 2043
- Digidentity Personal Qualified CA is valid until 4 July 2043
  - Certificates are valid for 365 days

- Digidentity Business Qualified CA is valid until 4 July 2043
  - Certificates are valid for 365 days
- Digidentity Personal Advanced CA is valid until 4 July 2043
  - Certificates are valid for 365 days

- Digidentity Assurance Root CA is valid until 4 July 2043

- Digidentity G2 CA is valid until 9 September 2041
  - Automotive Authentication certificates are valid for 365 days
  - eDelivery certificates are valid for 365 days

To issue certificates the lifespan of the issuing CA must not be shorter than the validity span of the Subscriber certificates.

6.4 Activation Data

See section 3.2.

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 Security 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.

6.6.3 Life Cycle Security Controls

Digidentity ensures that all ICT 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.

6.8 Timestamping

Digidentity does not perform time-stamping.

Digidentity

7 Certificate, CRL & OCSP Profiles

Digidentity use only approved Certificate Profiles for the issuance of certificates. This document describes the approved certificate profiles for all certificates issued from Digidentity Root and Issuing CA. CA Hierarchy is documented in section 1.1.2.

7.1 Certificate Profiles

The certificates shall meet the requirements, specified in Recommendation ITU-T X.509 or IETF RFC 5280. CAs shall generate non-sequential Certificate serial numbers greater than zero (0) containing at least 64 bits of output from a CSPRNG.

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)

Certificates MUST be of type X.509 v3.

All certificates are of type X.509 v3.

7.1.2 Certificate Extensions

This section specifies the additional requirements for Certificate content and extensions for Certificates generated after the Effective Date.

7.1.2.1 Root CA Certificate

All Root Certificates are configured per Baseline Requirements and/or ETSI EN 319 411-1/411-2.

All Root Certificates are configured per Baseline Requirements and/or ETSI EN 319 411-1/411-2.

7.1.2.2 Subordinate CA Certificates

All CA Certificates are configured per Baseline Requirements, eIDAS and/or ETSI EN 319 411-1/411-2.

All CA Certificates are configured per Baseline Requirements, eIDAS and/or ETSI EN 319 411-1/411-2.

7.1.2.3 Subscriber Certificates

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

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

7.1.2.4 All Certificates

All other fields and extensions MUST be set in accordance with RFC 5280. Digidentity will NOT issue a Certificate that contains a keyUsage flag, extendedKeyUsage value, Certificate extension, or other data not specified in section 7.1.2.1, 7.1.2.2, or 7.1.2.3 unless the CA is aware of a reason for including the data in the Certificate.

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

7.1.2.5 Application of RFC 5280

No stipulation.

7.1.3 Algorithm Object Identifiers

CAs MUST NOT issue any Subscriber certificates or Subordinate CA certificates using the SHA-1 hash algorithm.

Subscriber certificates SHOULD NOT chain up to a SHA-1 Subordinate CA Certificate.

Digidentity uses RSA encryption with SHA-2 algorithm.

7.1.3.1 SubjectPublicKeyInfo

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

7.1.3.1.1 RSA

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

7.1.3.1.2 ECDSA

Digidentity does not use ECDSA.

7.1.3.1.3 RSA

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

7.1.3.1.4 ECDSA

Digidentity does not use ECDSA.

7.1.4 Name Forms

The content of the certificate Issuer Distinguished Name field MUST match the Subject DN of the Issuing CA to support Name chaining as specified in RFC 5280, section 4.1.2.4.

By issuing the certificate, CA represents that it followed the procedure set forth in its Certificate Policy and/or Certification Practice Statement to verify that, as of the certificate's issuance date, all of the Subject Information was accurate. Underscore characters ("_") MUST NOT be present in dNSName entries.

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

7.1.4.1 Name Encoding

See Certificates Profiles in section 7.1.10.

7.1.4.2 Subject Information – Subscriber certificates

See Certificates Profiles in section 7.1.10.

7.1.4.2.1 Subject Alternative Name Extension

See Certificates Profiles in section 7.1.10.

7.1.4.2.2 Subject Distinguished Name Fields

See Certificates Profiles in section 7.1.10.

7.1.4.3 Subject Information – Root Certificates and Subordinate CA Certificates

See Certificates Profiles in section 7.1.10.

7.1.4.3.1 Subject Distinguished Name Fields

No stipulation

7.1.5 Name Constraints

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

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

7.1.6 Certificate Policy Object Identifier

All policy object identifiers are described in section 1.2

7.1.6.1 Reserved Certificate Policy Identifiers

See section 1.2.

7.1.6.2 Root CA Certificates

A Root CA Certificate SHOULD NOT contain the certificatePolicies extension.

Root certificates do not contain the certificatePolicies extension.

7.1.6.3 Subordinate CA Certificates

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

All Certificates are configured per Baseline Requirements, eIDAS and/or ETSI EN 319 411-1/411-2

7.1.6.4 Subscriber Certificates

A Certificate issued to a Subscriber MUST contain a certificatePolicies extension.

The extension MUST contain one or more policy identifiers that indicate adherence to and compliance with these Requirements. CAs MUST either use a CA/Browser Forum identifier reserved for this purpose or MUST use a policy identifier documented by the CA in its Certificate Policy and/or Certification Practice Statement to indicate the Certificate's compliance with these Requirements.

The issuing CA SHALL document in its Certificate Policy or Certification Practice Statement that the Certificates it issues containing the specified policy identifier(s) are managed in accordance with these Requirements.

See Certificates Profiles in section 7.1.10.

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.

7.1.10 Certificate Tables

7.1.10.1 Digidentity SSCD Root CA

Field	OID	Value	Critical	Type
Version		x.509 version 3		Required
SerialNumber	2.5.4.5	77 76 F4 39 51 CA 70 98 99 B5 D0 C7 FB 22 62 3B		Required
SignatureAlgorithm	1.2.840.113549.1.1.11	sha256WithRSAEncryption		Required
Validity				
NotValidBefore		10 July 2018		Required
NotValidAfter		4 July 2043		Required
Issuer DN				
commonName	(2.5.4.3) {id-at-3}	CN=Digidentity SSCD Root CA		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=Digidentity SSCD Root CA		Required
organizationName	(2.5.4.10)	O=Digidentity B.V.		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		4.096 bits		Required
signature		512 bytes		Required
Extensions				
basicConstraints	(2.5.29.19) {id-ce 19}	CA=True	Yes	Required
keyUsage	(2.5.29.15) {id-ce 15}	keyCertSign , cRLSign	Yes	Required
subjectKeyIdentifier	(2.5.29.14) {id-ce 14}	42 A2 2F 12 11 F3 8E 7E CD 7E C4 C9 E8 17 42 85 CB 31 21 9D	No	Required
Fingerprints				
SHA-256	C2 04 51 BD 93 D8 FD 6D 0C 43 CD 5C E8 32 87 7F D5 61 40 55 87 51 26 D1 70 91 0E 12 09 C9 B7 7D			
SHA-1	D3 8A 52 2C A2 CE 20 92 68 B8 93 CD 8C 29 EE 58 90 83 53 9F			

7.1.10.2 Digidentity Personal Qualified CA (Issuing CA)

Field	OID	Value	Critical	Type
Version		x.509 version 3		Required
SerialNumber	2.5.4.5	44 A0 79 92 C5 E6 B0 5B 88 60 D3 89 41 D1 F1 BA		Required
SignatureAlgorithm	1.2.840.113549.1.1.11	sha256WithRSAEncryption		Required
Validity				
NotValidBefore		27 February 2019		Required
NotValidAfter		4 July 2043		Required
Issuer DN				
commonName	(2.5.4.3) {id-at-3}	CN=Digidentity SSCD Root CA		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=Digidentity Personal Qualified CA		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
Public Key				
algorithm	(1.2.840.113549.1.1.1)	sha256WithRSAEncryption		Required
keySize		4.096 bits		Required
signature		512 bytes		Required
Extensions				
basicConstraints	(2.5.29.19) {id-ce 19}	cA=True, PathLenConstraint=0	Yes	Required
keyUsage	(2.5.29.15) {id-ce 15}	keyCertSign, cRLSign	Yes	Required
extKeyUsage	(2.5.29.37) {id-ce 37}	id-kp-clientAuth (1.3.6.1.5.5.7.3.2) id-kp-emailProtection (1.3.6.1.5.5.7.3.4) szOID_KP_DOCUMENT_SIGNING (1.3.6.1.4.1.311.10.3.12) szOID_EFS_CRYPTO (1.3.6.1.4.1.311.10.3.4)	No	Required
certificatePolicies	(2.5.29.32) {id-ce 32}	PolicyID1=1.3.6.1.4.1.34471.3.1.1 (Authentication/NCP+) PolicyID2=1.3.6.1.4.1.34471.3.1.2 (Encryption/NCP+) PolicyID3=1.3.6.1.4.1.34471.3.1.3 (Non-repudiation/QCP-n-qscd) 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}	97 F6 F6 B1 62 6A A3 8B 39 F1 5F 2F B4 BB 2E 23 59 21 C3 87	No	Required
authorityKeyIdentifier	(2.5.29.35) {id-ce 35}	42 A2 2F 12 11 F3 8E 7E CD 7E C4 C9 E8 17 42 85 CB 31 21 9D	No	Required
authorityInfoAccess	{id-pe 1}	Method#1: 1.3.6.1.5.5.7.48.2 (caIssuers) Contains CA Issuers 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
Fingerprints				
SHA-256	03 E1 AA EF 72 32 9B 4D A1 FC F0 BA 75 FC B7 B2 F2 F3 4B 25 AA DE 70 1A AA EA CC 0F 65 A3 B4 C4			
SHA-1	A4 83 40 72 4E EF B4 31 64 32 50 FA 7B 90 04 86 7E 42 8C DB			

Digidentity

Personal Qualified Authentication (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		< +365 days>		Required
Issuer DN				
commonName	(2.5.4.3) {id-at-3}	CN=Digidentity Personal Qualified CA		Required
organisationName	(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=<Given Names and Surname as registered on ID>		Required
serialNumber	(2.5.4.5)	SERIALNUMBER=<pseudonym>		Required
givenName	(2.5.4.42)	GN=<Given names as displayed on ID>		Required
surname	(2.5.4.4)	SN=<Surname as displayed on ID>		Required
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 bits or 4.096 bits		Required
signature		512 bytes		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) id-kp-emailProtection (1.3.6.1.5.5.7.3.4) 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=1.3.6.1.4.1.34471.3.1.1 (authentication/NCP+) 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 (calssuers) Contains CA Issuers 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

Digidentity

Personal Qualified Encryption (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		< +365 days>		Required
Issuer DN				
commonName	(2.5.4.3) {id-at-3}	CN=Digidentity Personal Qualified CA		Required
organisationName	(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=<Given Names and Surname as registered on ID>		Required
serialNumber	(2.5.4.5)	SERIALNUMBER=<pseudonym>		Required
givenName	(2.5.4.42)	GN=<Given names as displayed on ID>		Required
surname	(2.5.4.4)	SN=<Surname as displayed on ID>		Required
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 bits or 4.096 bits		Required
signature		512 bytes		Required
Extensions				
keyUsage	(2.5.29.15) {id-ce 15}	keyEncipherment, dataEncipherment	Yes	Required
extKeyUsage	(2.5.29.37) {id-ce 37}	id-kp-emailProtection (1.3.6.1.5.5.7.3.4) szOID_EFS_CRYPTO (1.3.6.1.4.1.311.10.3.4)	No	Required
certificatePolicies	(2.5.29.32) {id-ce 32}	PolicyID1=1.3.6.1.4.1.34471.3.1.2 (encryption/NCP+) 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 (calssuers) Contains CA Issuers 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

Digidentity

Personal Qualified Non-repudiation (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		<+365 days>		Required
Issuer DN				
commonName	(2.5.4.3) {id-at-3}	CN=Digidentity Personal Qualified CA		Required
organisationName	(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=<Given Names and Surname as registered on ID>		Required
serialNumber	(2.5.4.5)	SERIALNUMBER=<pseudonym>		Required
givenName	(2.5.4.42)	GN=<Given names as displayed on ID>		Required
surname	(2.5.4.4)	SN=<Surname as displayed on ID>		Required
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 bits or 4.096 bits		Required
signature		512 bytes		Required
Extensions				
keyUsage	(2.5.29.15) {id-ce 15}	nonRepudiation	Yes	Required
extKeyUsage	(2.5.29.37) {id-ce 37}	id-kp-emailProtection (1.3.6.1.5.5.7.3.4) 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=1.3.6.1.4.1.34471.3.1.3 (non-repudiation/QCP-n-qscd) 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)	No	Required

		Contains CA Issuers URL. URLs vary based on Issuing CA.		
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= 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

7.1.10.3 Digidentity Business Qualified CA (Issuing CA)

Field	OID	Value	Critical	Type
Version		x.509 version 3		Required
SerialNumber	2.5.4.5	4C 7A 70 99 16 30 CB 45 16 9B 04 32 E0 DC ED C0		Required
SignatureAlgorithm	1.2.840.113549.1.1.11	sha256WithRSAEncryption		Required
Validity				
NotValidBefore		28 February 2019		Required
NotValidAfter		4 July 2043		Required
Issuer DN				
commonName	(2.5.4.3) {id-at-3}	CN=Digidentity SSCD Root CA		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=Digidentity Business Qualified CA		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
Public Key				
algorithm	(1.2.840.113549.1.1.1)	sha256WithRSAEncryption		Required
keySize		4.096 bits		Required
signature		512 bytes		Required
Extensions				
basicConstraints	(2.5.29.19) {id-ce 19}	cA=True, PathLenConstraint=0	Yes	Required
keyUsage	(2.5.29.15) {id-ce 15}	keyCertSign, cRLSign	Yes	Required
extKeyUsage	(2.5.29.37) {id-ce 37}	id-kp-clientAuth (1.3.6.1.5.5.7.3.2) id-kp-emailProtection (1.3.6.1.5.5.7.3.4) szOID_KP_DOCUMENT_SIGNING (1.3.6.1.4.1.311.10.3.12) szOID_EFS_CRYPTO (1.3.6.1.4.1.311.10.3.4)	No	Required
certificatePolicies	(2.5.29.32) {id-ce 32}	PolicyID1=1.3.6.1.4.1.34471.3.2.1 (Authentication/NCP+) PolicyID2=1.3.6.1.4.1.34471.3.2.2 (Encryption/NCP+) PolicyID3=1.3.6.1.4.1.34471.3.2.3 (Non-repudiation/QCP-l-qscd) 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}	D9 57 6B 30 38 31 1C 27 74 45 A8 9F 41 8B DE 6D FA 7C 34 BB	No	Required
authorityKeyIdentifier	(2.5.29.35) {id-ce 35}	42 A2 2F 12 11 F3 8E 7E CD 7E C4 C9 E8 17 42 85 CB 31 21 9D	No	Required
authorityInfoAccess	{id-pe 1}	Method#1: 1.3.6.1.5.5.7.48.2 (caIssuers) Contains CA Issuers 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
Fingerprints				
SHA-256	21 E5 D8 CF BC 24 30 AA 45 AD 86 D3 83 94 AE 97 B3 59 C0 E8 88 35 E4 DE 5E 0A D1 CE 92 A8 20 1D			
SHA-1	56 7F 67 9E 8A F6 9A D2 AB F0 4C 39 A2 69 23 55 A6 A0 09 FA			

Digidentity

Business Qualified Authentication (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		< +365 days>		Required
Issuer DN				
commonName	(2.5.4.3) {id-at-3}	CN=Digidentity Business Qualified CA		Required
organisationName	(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=<name commonly used by the subject to represent itself>		Required
organisationName	(2.5.4.10)	O=<full registered name of the legal person>		Required
organisationIdentifier	(2.5.4.97)	Unique number identifying Organisation		Required
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 bits, 3.072 bits or 4.096 bits		Required
signature		512 bytes		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) id-kp-emailProtection (1.3.6.1.5.5.7.3.4) 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=1.3.6.1.4.1.34471.3.2.1 (Authentication/NCP+) 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) Contains CA Issuers 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

Business Qualified Encryption (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		< +365 days>		Required
Issuer DN				
commonName	(2.5.4.3) {id-at-3}	CN=Digidentity Business Qualified CA		Required
organisationName	(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=<name commonly used by the subject to represent itself>		Required
organisationName	(2.5.4.10)	O=<full registered name of the legal person>		Required
organisationIdentifier	(2.5.4.97)	Unique number identifying Organisation		Required
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 bits, 3.072 bits or 4.096 bits		Required
signature		512 bytes		Required
Extensions				
keyUsage	(2.5.29.15) {id-ce 15}	keyEncipherment, dataEncipherment	Yes	Required
extKeyUsage	(2.5.29.37) {id-ce 37}	id-kp-emailProtection (1.3.6.1.5.5.7.3.4) szOID_EFS_CRYPTO (1.3.6.1.4.1.311.10.3.4)	No	Required
certificatePolicies	(2.5.29.32) {id-ce 32}	PolicyID1=1.3.6.1.4.1.34471.3.2.2 (Encryption/NCP+) 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) Contains CA Issuers 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

Digidentity

Business Qualified Non-repudiation (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		< +365 days>		Required
Issuer DN				
commonName	(2.5.4.3) {id-at-3}	CN=Digidentity Business Qualified CA		Required
organisationName	(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=<name commonly used by subject to represent itself>		Required
organisationName	(2.5.4.10)	O=<full registered name of the legal person>		Required
organisationIdentifier	(2.5.4.97)	Unique number identifying Organisation		Required
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 bits, 3.072 bits or 4.096 bits		Required
signature		512 bytes		Required
Extensions				
keyUsage	(2.5.29.15) {id-ce 15}	nonRepudiation	Yes	Required
extKeyUsage	(2.5.29.37) {id-ce 37}	id-kp-emailProtection (1.3.6.1.5.5.7.3.4) 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=1.3.6.1.4.1.34471.3.2.3 (non-repudiation/QCP-l-qscd) 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) Contains CA Issuers 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)		Required

7.1.10.4 Personal Advanced CA (Issuing CA)

Field	OID	Value	Critical	Type
Version		x.509 version 3		Required
SerialNumber	2.5.4.5	58 BA 8A 98 2A 30 7E 3D DE FA 42 BE 8F 9F C9 A0		Required
SignatureAlgorithm	1.2.840.113549.1.1.11	sha256WithRSAEncryption		Required
Validity				
NotValidBefore		28 February 2019		Required
NotValidAfter		4 July 2043		Required
Issuer DN				
commonName	(2.5.4.3) {id-at-3}	CN=Digidentity SSCD Root CA		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=Digidentity Personal Advanced CA		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
Public Key				
algorithm	(1.2.840.113549.1.1.1)	sha256WithRSAEncryption		Required
keySize		4.096 bits		Required
signature		512 bytes		Required
Extensions				
basicConstraints	(2.5.29.19) {id-ce 19}	cA=True, PathLenConstraint=0	Yes	Required
keyUsage	(2.5.29.15) {id-ce 15}	keyCertSign, cRLSign	Yes	Required
extKeyUsage	(2.5.29.37) {id-ce 37}	id-kp-clientAuth (1.3.6.1.5.5.7.3.2) id-kp-emailProtection (1.3.6.1.5.5.7.3.4) szOID_KP_DOCUMENT_SIGNING (1.3.6.1.4.1.311.10.3.12) szOID_EFS_CRYPTO (1.3.6.1.4.1.311.10.3.4)	No	Required
certificatePolicies	(2.5.29.32) {id-ce 32}	PolicyID1=1.3.6.1.4.1.34471.3.3.1 (Authentication/NCP+) PolicyID2=1.3.6.1.4.1.34471.3.3.2 (Encryption/NCP+) PolicyID3=1.3.6.1.4.1.34471.3.3.3 (Non-repudiation/NCP+) 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}	D1 1B 2E 9F AE FF EB C1 BF E4 7D FD BF AE A6 F4 D4 0A 4E 77	No	Required
authorityKeyIdentifier	(2.5.29.35) {id-ce 35}	42 A2 2F 12 11 F3 8E 7E CD 7E C4 C9 E8 17 42 85 CB 31 21 9D	No	Required
authorityInfoAccess	{id-pe 1}	Method#1: 1.3.6.1.5.5.7.48.2 (caIssuers) Contains CA Issuers 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
Fingerprints				
SHA-256	E1 52 89 25 76 F4 B4 0B 14 96 F6 0F 67 11 AA 14 C2 AD 54 BA FE 35 53 31 EE 6E 47 39 73 01 E9 62			
SHA-1	0C 1D 42 28 42 53 1C D3 65 B0 14 27 D6 CA 8B CA 4C BD 1C E0			

Digidentity

Personal Advanced Authentication (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		< +365 days>		Required
Issuer DN				
commonName	(2.5.4.3) {id-at-3}	CN=Digidentity Personal Advanced CA		Required
organisationName	(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=<Given Names and Surname as registered on ID>		Optional
serialNumber	(2.5.4.5)	SERIALNUMBER=<pseudonym>		Required
givenName	(2.5.4.42)	GN=<Given names as displayed on ID>		Required
surname	(2.5.4.4)	SN=<Surname as displayed on ID>		Required
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 bits or 4.096 bits		Required
signature		512 bytes		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) id-kp-emailProtection (1.3.6.1.5.5.7.3.4) 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=1.3.6.1.4.1.34471.3.3.1 (Authentication/NCP+) 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 (calssuers) Contains CA Issuers 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

Digidentity

Personal Advanced Encryption (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		< +365 days>		Required
Issuer DN				
commonName	(2.5.4.3) {id-at-3}	CN=Digidentity Personal Advanced CA		Required
organisationName	(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=<Given Names and Surname as registered on ID>		Optional
serialNumber	(2.5.4.5)	SERIALNUMBER=<pseudonym>		Required
givenName	(2.5.4.42)	GN=<Given names as displayed on ID>		Required
surname	(2.5.4.4)	SN=<Surname as displayed on ID>		Required
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 bits or 4.096 bits		Required
signature		512 bytes		Required
Extensions				
keyUsage	(2.5.29.15) {id-ce 15}	dataEncipherment, keyEncipherment	Yes	Required
extKeyUsage	(2.5.29.37) {id-ce 37}	id-kp-emailProtection (1.3.6.1.5.5.7.3.4) szOID_EFS_CRYPTO (1.3.6.1.4.1.311.10.3.4)	No	Required
certificatePolicies	(2.5.29.32) {id-ce 32}	PolicyID1=1.3.6.1.4.1.34471.3.3.2 (Encryption/NCP+) 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) Contains CA Issuers 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

Digidentity

Personal Advanced Non-repudiation (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		< +365 days>		Required
Issuer DN				
commonName	(2.5.4.3) {id-at-3}	CN=Digidentity Personal Advanced CA		Required
organisationName	(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=<Given Names and Surname as registered on ID>		Optional
serialNumber	(2.5.4.5)	SERIALNUMBER=<pseudonym>		Required
givenName	(2.5.4.42)	GN=<Given names as displayed on ID>		Required
surname	(2.5.4.4)	SN=<Surname as displayed on ID>		Required
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 bits or 4.096 bits		Required
signature		512 bytes		Required
Extensions				
keyUsage	(2.5.29.15) {id-ce 15}	nonRepudiation	Yes	Required
extKeyUsage	(2.5.29.37) {id-ce 37}	id-kp-emailProtection (1.3.6.1.5.5.7.3.4) 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=1.3.6.1.4.1.34471.3.3.3 (Non-repudiation/NCP+) 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 (calssuers) Contains CA Issuers 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

7.1.10.5 Digidentity Assurance Root CA

Field	OID	Value	Critical	Type
Version		x.509 version 3		Required
SerialNumber	2.5.4.5	1C 8B AE 30 39 88 76 26 90 31 E1 6B 56 A6 2D A8		Required
SignatureAlgorithm	1.2.840.113549.1.1.11	sha256WithRSAEncryption		Required
Validity				
NotValidBefore		10 July 2018		Required
NotValidAfter		4 July 2043		Required
Issuer DN				
commonName	(2.5.4.3) {id-at-3}	CN=Digidentity Assurance Root CA		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=Digidentity Assurance Root CA		Required
organizationName	(2.5.4.10)	O=Digidentity B.V.		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		4.096 bits		Required
signature		512 bytes		Required
Extensions				
basicConstraints	(2.5.29.19) {id-ce 19}	CA=True	Yes	Required
keyUsage	(2.5.29.15) {id-ce 15}	keyCertSign , cRLSign	Yes	Required
subjectKeyIdentifier	(2.5.29.14) {id-ce 14}	8F E3 55 6B F7 7C 6F B7 E0 B2 C2 99 30 2F B4 D6 CD E3 D9 84	No	Required
Fingerprints				
SHA-256	75 0C C6 55 7F 38 21 DA 9C 5B EF 04 AF 06 5D 74 62 96 51 D8 C6 75 7E 76 9F 62 FF 3C 9A CA 7D EF			
SHA-1	DD 10 5B 66 D2 B2 E0 E2 63 6C D3 07 54 44 59 35 FE F6 D7 C3			

Digidentity

7.1.10.6 Digidentity G2 CA (Issuing CA)

Field	OID	Value	Critical	Type
Version		x.509 version 3		Required
SerialNumber	2.5.4.5	21 D4 F3 8D 8F 76 64 B8 1F 6B 20 0B CE 66 BD 1D		Required
SignatureAlgorithm	1.2.840.113549.1.1.11	sha256WithRSAEncryption		Required
Validity				
NotValidBefore		14 September 2021		Required
NotValidAfter		9 September 2041		Required
Issuer DN				
commonName	(2.5.4.3) {id-at-3}	CN=Digidentity Assurance CA		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=Digidentity G2 CA		Required
organizationName	(2.5.4.10)	O=Digidentity B.V.		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		4.096 bits		Required
signature		512 bytes		Required
Extensions				
basicConstraints	(2.5.29.19) {id-ce 19}	cA=True, PathLenConstraint=0	Yes	Required
keyUsage	(2.5.29.15) {id-ce 15}	keyCertSign, cRLSign	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=1.3.6.1.4.1.34471.4.1.1 (Authentication/NCP) PolicyID2=1.3.6.1.4.1.34471.4.1.2 (Authentication/NCP) QualifierID1: 1.3.6.1.5.5.7.2.1 (id-qt-cps) URI=https://cps.digidentity-pki.com	No	Required
subjectKeyIdentifier	(2.5.29.14) {id-ce 14}	A2 47 0E F0 1C 1A D5 68 AD 45 C1 62 74 7C 33 42 B0 70 1C FD	No	Required
authorityKeyIdentifier	(2.5.29.35) {id-ce 35}	8F E3 55 6B F7 7C 6F B7 E0 B2 C2 99 30 2F B4 D6 CD E3 D9 84	No	Required
authorityInfoAccess	{id-pe 1}	Method#1: 1.3.6.1.5.5.7.48.2 (caIssuers) Contains CA Issuers 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
Fingerprints				
SHA-256	20 E2 24 2B 84 B5 04 52 50 CD 64 1A 3E 77 55 75 D0 34 D0 91 11 62 E1 3F F7 9A FB E4 5E 69 4E AA			
SHA-1	97 51 26 6C 23 F4 37 75 02 79 A0 7A 6B A4 1F 1A A8 CA 21 36			

Digidentity

Automotive Authentication certificate (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		< +365 Days>		Required
Issuer DN				
commonName	(2.5.4.3) {id-at-3}	CN=Digidentity G2 CA		Required
organisationName	(2.5.4.10)	O=Digidentity B.V.		Required
countryName	(2.5.4.6) {id-at-6}	C=NL		Required
Subject DN				
emailAddress		E=<validated email address>		Required
commonName	(2.5.4.3) {id-at-3}	CN=<validated email address>		Required
pseudonym	(2.5.4.65)	<Subscriber Pseudonym>		Required
organisationName	(2.5.4.10)	O=<Organisation Name as validated from KvK>		Required
organizationIdentifier	(2.5.4.97)	<Number of KvK> (optional <Office Number>)		Required
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 bits		Required
signature		512 bytes		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=1.3.6.1.4.1.34471.4.1.1 (Authentication/NCP) 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) Contains CA Issuers 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

Digidentity

eDelivery certificate (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		< +365 days>		Required
Issuer DN				
commonName	(2.5.4.3) {id-at-3}	CN=Digidentity G2 CA		Required
organisationName	(2.5.4.10)	O=Digidentity B.V.		Required
countryName	(2.5.4.6) {id-at-6}	C=NL		Required
Subject DN				
emailAddress		E=<validated assigned email address>		Required
commonName	(2.5.4.3) {id-at-3}	CN=<Organisation name preferred presentation format>		Required
organizationIdentifier	(2.5.4.97)	<Number of KvK>		Required
organisationName	(2.5.4.10)	O=<Organisation Name as validated from KvK>		Required
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 bits		Required
signature		512 bytes		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=1.3.6.1.4.1.34471.4.1.2 (Authentication/NCP) 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) Contains CA Issuers 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

7.2 CRL Profile

7.2.1 Root CA CRL

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
Issuer DN				
commonName	(2.5.4.3) {id-at-3}	CN=<Root CA Name>		Required
organisationName	(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
Extensions				
ThisUpdate		UTC Time of next update to the CRL		Required
NextUpdate		+ 1 year		Required
revokedCertificates		Provides the status e.g. revoked		Required
CRlNumber		Provides the sequential order of the published CRLs		Required
CRlReason		Provides a reason for revocation		Optional

7.2.2 Issuing CA CRL

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
Issuer DN				
commonName	(2.5.4.3) {id-at-3}	CN=<Issuer CA Name>		Required
organisationName	(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
Extensions				
ThisUpdate		Issue date and time of this CRL		Required
NextUpdate		<+ ten minutes>		Required
revokedCertificates		Provides the status e.g. revoked		Required
expiredCertsOnCrl (*)		Revoked certificates remain on CRL after expiration		Optional
CRlNumber		Provides the sequential order of the published CRLs		Required
reasonCode	(2.5.29.21) {id-ce 21}	Provides a reason for revocation		Optional

(*) The expiredCertsOnCrl is only applicable for the Digidentity Personal Qualified CA and Digidentity Business Qualified CA.

7.3 OCSP Profile

Digidentity does not provide OCSP services for Digidentity certificates.

7.3.1 Version number(s)

No stipulation

7.3.2 OCSP extensions

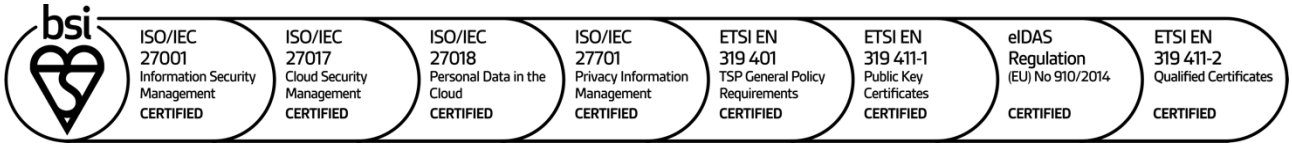
No stipulation

8 Compliance Audit & Other Assessments

The CA SHALL at all times:
[1] Issue Certificates and operate its PKI in accordance with all laws applicable to its business and the Certificates it issues in every jurisdiction in which it operates;
[2] Comply with applicable requirements;
[3] Comply with the audit requirements; and
[4] Are licensed as a CA.

Digidentity is a Qualified Trust Service Provider (QTSP) as defined in EU Regulation 910/2014 also known as eIDAS. Digidentity is compliant to the applicable requirements of the following standards, requirements and regulations:

ISO27001:2013	Information Security Management System (ISMS)
ISO27701:2019	Privacy Information Management System (PIMS)
ISO27017:2015	Information Security in the Cloud
ISO27018:2019	Securing Personal Data in the. Cloud
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) N 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
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)
CA/Browser Forum	Baseline Requirements
CA/Browser Forum	Network and Certificate System Security Requirements



8.1 Frequency or Circumstances of Assessment

Digidentity undergoes an audit for ETSI EN 319 411-1 and ETSI EN 319 411-2, which includes normative references to ETSI EN 319 401 (the latest version of the referenced ETSI documents should be applied). The audit is conducted by a Qualified Auditor, as specified in Section 8.2.

The period during which THE CA issues Certificates is divided into an unbroken sequence of audit periods. An audit period MUST NOT exceed one year in duration. If the CA does not have a currently valid Audit Report indicating compliance with one of the audit schemes listed in Section 8.1, then, before issuing Publicly-Trusted Certificates, the CA must successfully complete a point-in-time readiness assessment performed in accordance with applicable standards under one of the audit schemes listed in Section 8.1.

Digidentity is under supervision and may be audited by the Dutch government organisation Agentschap Telecom 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, ISO27001:2013, ISO27701:2019, ISO27017:2015 and ISO27018:2019 standards and audited annually by an independent auditor.

8.2 Identity/Qualifications of Assessor

The CA's audits are performed by a Qualified Auditor. A Qualified Auditor means a natural person, Legal Entity, or group of natural persons or Legal Entities who possess the correct qualifications and skills. Omissions insurance with policy limits of at least one million US dollars in coverage

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

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.

8.4 Topics Covered by Assessment

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

- 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

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.

8.6 Communication of Results

The Audit Report states explicitly that it covers the relevant systems and processes used in the issuance of all certificates that assert one or more of the policy identifiers listed in Section 7.1.6.1. The CA make the Audit Report publicly available.

All Conformity Assessment Reports meet the requirement of the Baseline Requirements and are available in the repository https://cps.digidentity-pki.com/.

8.7 Self-Audits

During the period in which the CA issues certificates, it monitors its adherence to its Certificate Policy, Certification Practice Statement and these Requirements and strictly control its service quality by performing self audits on at least a quarterly basis against a randomly selected sample of the greater of one certificate or at least three percent of the Certificates issued by it during the period commencing immediately after the previous self-audit sample was taken.

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.

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 services.

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 this CPS are subject to face-to-face checks, where the identity of the applicant is checked in person, along with the identity document. For this service Digidentity charges a fee. Fees related to the face-to-face checks are available online.

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

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

In cases where it has been necessary to repeatedly replace certificates due to the fault of the Subscriber, Digidentity reserves the right to charge an administration fee at their discretion. The administration fee will be proportionate to the amount of work/costs to issue repeated replacement certificates.

9.1.5 Refund Policy

Digidentity does not have a refund policy.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

Digidentity has an 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

9.3 Confidentiality of Business Information

9.3.1 Scope of confidential information

All business data, which is not released for public view, is confidential. This applies to all information which is exchanged and communicated in procedures and processes with participants.

9.3.2 Information Not within the scope of confidential information

Information which is available for public view, including information on the Digidentity website, the information and documentation in the repository online and other publicly available information is outside the scope of 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 Privacy of Personal Data

9.4.1 Privacy Plan

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

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

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/use. Digidentity has implemented appropriate technical and organizational 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 use of personal data is based on 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 fulfil the requirements to supply data for forensic purposes as required by law enforcement and for the judicial process, per the legal administrative procedures. Digidentity has the right to inform the relevant authorities of fraudulent or other criminal activity, in accordance with Digidentity's Terms.

9.4.7 Other information disclosure circumstances

There are no other information disclosure circumstances.

9.5 Intellectual Property Rights

Any intellectual property rights associated with products and services supplied by Digidentity, and associated materials, remain the property of Digidentity, the licensee or supplier. 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 and Warranties

By issuing a Certificate, Digidentity makes the certificate warranties listed herein to the following Certificate Beneficiaries:

[1] The Subscriber that is a party to the Subscriber Agreement or Terms of Use for the Certificate;
[2] All Application Software Suppliers with whom the Root CA has entered into a contract for inclusion of its Root Certificate in software distributed by such Application Software Supplier; and
[3] All Relying Parties who reasonably rely on a Valid Certificate.

Digidentity represents and warrants to the Certificate Beneficiaries that, during the period when the Certificate is valid, that Digidentity has complied with these Requirements and its Certificate Policy and/or Certification Practice Statement in issuing and managing the Certificate.

Upon the issuance of a certificate Digidentity make the following warranties that;

[1] at the time of issuance Digidentity has followed the procedures in this CPS and verified that the subject authorised the issuance of the certificate, and that the applicant representative of the subject was authorised to request the certificate.
[2] at the time of issuance Digidentity has followed the procedures in this CPS to verify the accuracy of the information provided by the applicant.
[3] 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.

[4] Digidentity has followed the procedures in this CPS to verify the identity of any applicant for a certificate.
[5] Digidentity and the subscriber have a legally enforceable subscriber agreement, and that Digidentity's General Terms & Conditions have been provided to the subscriber so that these apply to the agreement.
[6] Digidentity maintains a 24 x 7 publicly accessible repository available for checking certificate status.
[7] Digidentity will revoke a certificate for reasons already described in this CPS.

Digidentity is only liable for actions carried out which are contrary to the provisions of this CPS, law, regulation, requirement or contract, including liability for negligence for the maximum amount included in 9.2, for any event or series related events (in a period of 12 months).

9.6.2 RA Representations & Warranties

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

9.6.3 Subscriber Representations & Warranties

Digidentity require, as part of the Subscriber Agreement or Terms of Use, that the Applicant make the commitments and warranties in this section for the benefit of the CA and the Certificate Beneficiaries. Prior to the issuance of a Certificate, Digidentity will obtain, for the express benefit of the Digidentity and the Certificate Beneficiaries, either:

[1] The Applicant's agreement to the Subscriber Agreement with the CA, or
[2] The Applicant's acknowledgement of the Terms of Use.

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 law, and will never 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 organization, and

9.6.4 Relying Party Representations and Warranties

No stipulation

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 remain fully responsible for the performance of all parties in accordance with these Requirements, regardless as whether tasks have been delegated.

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 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;
- 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 is valid until a new version takes its place in the Digidentity repository. This CPS will remain applicable to the services of Digidentity if services are still offered by Digidentity. If Digidentity cease to issue certificates from Digidentity CA, this document will cease to be relevant.

9.10.3 Effect of termination and survival

The provisions within this CPS terminate in the event of termination by Digidentity of its provision of Digidentity certificates.

9.11 Individual Notices & Communications with Participants

Digidentity provides notifications to participants in the following ways;

- Website: Notifications and announcements.
- Emails: Sent to the Subscriber's confirmed email address.
- Telephone calls: Made to the Subscriber's confirmed telephone number.

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.

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/home/#complaints-procedure.

Complaints will be handled with by Digidentity per the described procedure. Complaints can be handled via email: 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.

9.15 Compliance with Applicable Law

Digidentity currently comply 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

Digidentity

Appendix A — Definitions & Abbreviations

Term	Description
Applicant	New customer that applies for a certificate.
AT	Agentschap Telecom (regulator Trust Service Providers)
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 emails 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.
Pseudonym	The use of a unique string of characters (numbers and letters) to identify a specific user. A name substitute.
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.
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

Term	Description
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 services. 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.