Certificate Practice Statement

PKIoverheid Certificates

Title	Certificate Practice Statement – PKIoverheid certificates
Date	16 March 2020
Valid from	30 March 2020
Version	2020-v1
Classification	Public

Revisions

Version	Date	Author	Changes Made
2019-v1	25 February 2019	Digidentity	
2019-v2	6 December 2019	Digidentity	Alligned with CPS for Digidentity Certificates (*)
2020-v1	16 March 2020	Digidentity	Updated to recent requirements (*)

(*) Changes are marked in grey highlight and detailed in Appendix B.

DIGIDENTITY

Contents

1   Introduction

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

1.1   Overview

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

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

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

Personal certificates and personal certificates for Registered Professionals are also EU Qualified Certificates issued to natural persons according to Regulation (EU) No 910/2014.

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

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), PKIoverheid Programma van Eisen parts 3a (Organisatie & Organisatie Persoon), 3c (Burger), 3e (Server – Organisatie Services) and 3h (Server – Private Services), ISO27001:2013, and Root Store policies of Mozilla and Microsoft.

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

This CPS covers the following Certificate Authorities of Digidentity:

CA	OID
Digidentity BV PKIoverheid Private Services CA – G1	2.16.528.1.1003.1.2.8.1
Digidentity BV PKIoverheid Organisatie Server CA - G3	Not Applicable
Digidentity BV PKIoverheid Burger CA - G3	2.16.528.1.1003.1.3.3.2.1
Digidentity BV PKIoverheid Organisatie Persoon CA - G3	2.16.528.1.1003.1.3.5.8.1

1.1.1 Intended audience

This document is intended for:
- Subscribers
- Certificate Holders
- Certificate Managers
- Relying parties

1.1.2 CA Hierarchy
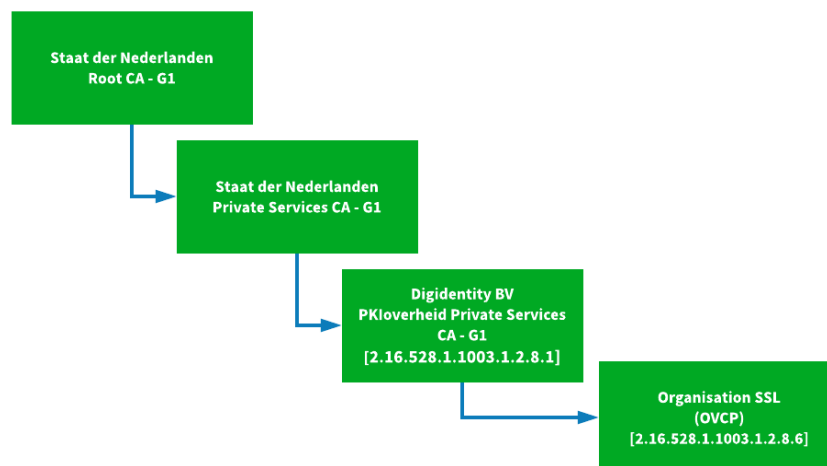
Figure 1 - PKIoverheid G1 hierarchy
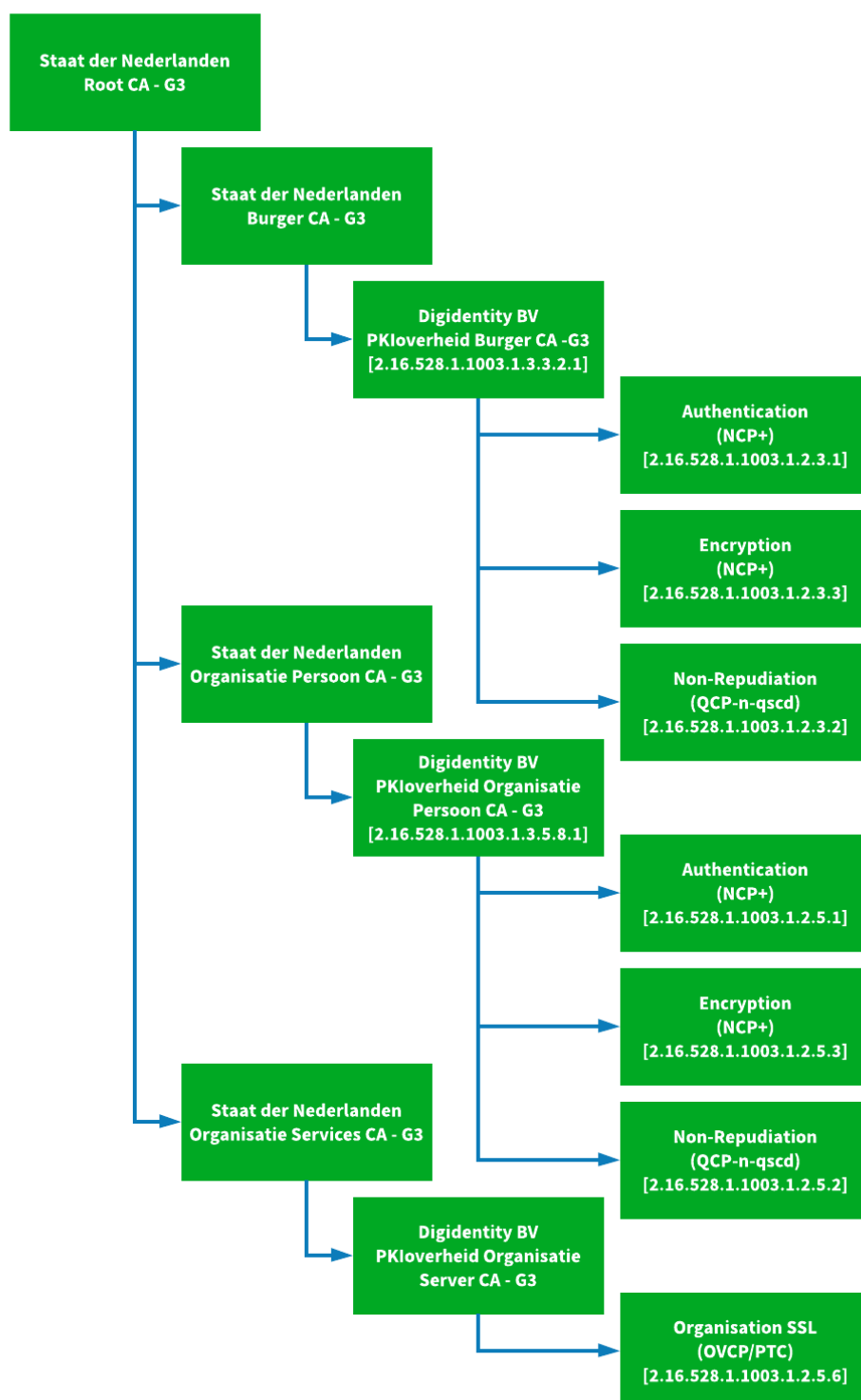
Figure 2 - PKIoverheid G3 hierarchy

1.2   Document Name & Identification

This Certificate Practice Statement is identified as Certificate Practice Statement for PKIoverheid Certificates.

The Certificate Policies adopted by Digidentity are found in the list within brackets and are equal to the same certificate policies defined in ETSI EN 319 411-1 and ETSI EN 319 411-2.

Digidentity issues subscriber certificates for:

- Server certificates for Digipoort (Digidentity BV PKIoverheid Private Services CA - G1) – OID 2.16.528.1.1003.1.3.15.1.1
  + Server (OVCP) – OID 2.16.528.1.1003.1.2.8.6
- Personal certificates for natural persons (Digidentity BV PKIoverheid Burger CA -G3)- OID 2.16.528.1.1003.1.3.3.2.1
  + Personal Authentication (NCP+) – OID 2.16.528.1.1003.1.2.3.1
  + Personal Encryption (NCP+) – OID 2.16.528.1.1003.1.2.3.3
  + Personal Non-Repudiation (QCP-n-qscd) – OID 2.16.528.1.1003.1.2.3.2
- Personal certificates for Registered Professionals (Digidentity BV PKIoverheid Organisatie Persoon CA - G3) – OID 2.16.528.1.1003.1.3.5.8.1
  + Professional Authentication (NCP+) – OID 2.16.528.1.1003.1.2.5.1
  + Professional Encryption (NCP+) – OID 2.16.528.1.1003.1.2.5.3
  + Professional Non-Repudiation (QCP-n-qscd) – OID 2.16.528.1.1003.1.2.5.2
- Server certificates (Digidentity BV PKIoverheid Organisatie Server CA - G3)
  + Server (PTC, OVCP) – OID 2.16.528.1.1003.1.2.5.6

Relying Parties shall recognize 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 PKIoverheid Certificates listed in section 1.2.

1.3.2   Registration Authorities

The applicable Registration Authority (RA) for all issued certificates is Digidentity. Digidentity verifies applicant requests for a digital 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.

1.3.3 Subscribers, Certificate Holder, Certificate Manager

Subscribers can be a;

- natural person
- natural person with a registered profession
- natural person in association with a legal person – a legal representative of an organisation

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;

- natural person
- legal person (e.g. Organisation)
- 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. The Certificate 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;

- Kamer van Koophandel (Dutch Chamber of Commerce)
- Identity document verification services
- Nederlandse Beroepsorganisatie van Accountants (NBA)

1.4 Certificate usage

1.4.1 Appropriate certificate usage

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

Personal Certificates/ Personal Certificates for Registered Professionals

- 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).

Server Certificates

Server certificates can be used for securing the connection between a specific client and server which are related to 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, Subscribers, Relying Parties, Application Software Suppliers, and other third parties can contact Digidentity.

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

1.5.3 CPS Approval

This document is subject to a review at least once a year and is included in the internal audit schedule. Compliance of this document with CA/B Forum Baseline Requirements, RFC 3647, ETSI EN 319 401, ETSI EN 319 411-1, ETSI EN 319 411-2, PKIoverheid Programma van Eisen and eIDAS will be assessed, and any inconsistency remedied. Before publishing, this document is approved by Digidentity Management with a digital signature.

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

1.6 Definitions & Acronyms

See Appendix A – Definitions & Acronyms for a table of acronyms and definitions.

2   Publication & Repository Responsibilities

2.1   Repositories

Digidentity maintains an online repository, containing:

- Certificate Practice Statement, PKI Disclosure Statement
- General Terms & Conditions, Privacy Statement, Product Specific Terms & Conditions
- Certificates of Digidentity TSP CAs and issuing CAs for PKIoverheid

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

2.2   Publication of Information

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

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

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

Subscriber test certificates are hosted by the Policy Authority (see section 2.2 of the applicable CPS of PKIoverheid at https://cps.pkioverheid.nl/).

Subscribers are able to download their certificates in their Digidentity account.

2.3   Time or Frequency of Publication

Digidentity publishes updates of this document and other documents in the repository at least once per year or when significant changes are implemented.

2.4   Access Control & Repositories

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

DIGIDENTITY

3 Identification & Authentication

3.1 Naming

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

3.1.1 Types of Names

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

Personal Certificates

Field	Description	Max. Length
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 for the location	2
GN – Given Name	Given Names as registered on ID	64
S - Surname	Surname as registered on ID	64

Personal Certificates for Registered Professionals

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 for the location	2
GN – Given Name	Given Names as registered on ID	64
S - Surname	Surname as registered on ID	64
T - Title	Official registered professional title of subscriber	64
O – Organisation Name	Given Names and Surname as registered on ID	64

Server (G1) certificates

Field	Description	Max. Length
CN – Common Name	SBR Digipoort	64
O – Organisation Name	Name of the Organisation as registered in Trade Register	64
C – Country	Two-digit country code for the location	2
Serial Number	Organisation Trade Register number	64

Server (G3) certificates

Field	Description	Max. Length
CN – Common Name	Fully Qualified Domain Name to which the certificate and key pair are assigned.	64
O – Organisation Name	Name of the Organisation as registered in Trade Register	64
Serial Number	National Trade Register registration number	64
L – Locality	Place the Organisation is located	128
C – Country	Two-digit country code for the location	2
ST – State	Province/state the Organisation is located	128
Optional		
OU – Organisational Unit	Department of the Organisation	64

3.1.2   Need for Names to be Meaningful

The naming of the Distinguished Name in the certificates based on the tables above, should result in:

▪ Names to be meaningful, unambiguous, and unique and allows any relying party to identify the subscriber.

3.1.3   Anonymity or Pseudonymity of Subscribers

No stipulation.

3.1.4   Rules for Interpreting Various Name Forms

No stipulation.

3.1.5   Uniqueness of Names

No stipulation.

3.1.6   Recognition, Authentication and Role of Trademarks

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

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

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

3.2 Initial Identity Validation

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

In the Digidentity Self-Service Portal (https://selfservice.digidentity.eu), server certificates can be 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). As part of the registration process for server certificates, Digidentity performs email, organisation and domain validation (see 3.2.2).

3.2.1 Method to prove possession of Private Key

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

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

For server certificates, applicants or subscriber generate their own private key and send a signed Certificate Signing Request (CSR) to prove possession of the private key, which corresponds to the public key in the certificate request. For server certificates the private key is in the management by the Certificate Manager of the subscribing organisation.

3.2.2 Authentication of Organisation & Domain Identity

Digidentity verifies certificate requests for high-risk domain names with the Fully Qualified Domain Name (FQDN) contained within the CSR is checked against a list of top 500 global domains names and a list of top 500 Dutch domains names as well as a Phishtank check. The Security Officer has to approve or reject certificate requests that are marked as high risk.

3.2.2.1   Identity

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).

Digidentity verifies that the domain name is registered to the Organisation as described in section 3.2.2.4.

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

3.2.2.2   DBA/Tradename

The organisation tradename is checked via the 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

Digidentity uses the method in section 3.2.2.1.

3.2.2.4   Validation of Domain Authorisation or Control

Digidentity uses the method described in 3.2.2.4.4.

3.2.2.4.1   Validating the Applicant as a Domain Contact

This method is retired and not used by Digidentity.

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

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

(ii)   including a random confirmation code in the email, and

(iii)   receiving a confirming response utilizing the random confirmation code.

Once Digidentity receives a response from one of these email addresses, with a matching random value (confirmation code), then control over the domain name is confirmed. The confirmation code is valid for seven (7) days. This method of verification is per CA/Browser Forum Baseline Requirements (section 3.2.2.4.4). When used, this validation method is recorded during the application for a certificate.

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

3.2.2.4.5   Domain Authorisation Document

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

Requirement removed by CA/Browser Forum.

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 this method.

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

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 forty-five (45) days
- Domain name check and validation (including high risk domain check) – always performed on issuance
- Phishing check – always performed on issuance

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.

For server certificate applications, all other documentation used in applications e.g. ID validation, should never be older than 825 days. Upon request for a new certificate it may or may not be necessary to request a new identity document in order to reverify information included in the certificate.

3.2.2.8   CAA Records

For server certificates, Certification Authority Authorization (CAA) records of the domain name are checked before of issuance. CAA records are checked to ensure there are no limitations on Digidentity issuing the certificate with the domain name (FQDN). If there are limitations on the issuance of a certificate using a specific FQDN, Digidentity will inform the applicant that the certificate cannot be issued.

Digidentity only issues PKIoverheid server certificates for domains if:

(1) CAA identifier "digidentity.com" is entered for the domain requested
(2) PKIoverheid system-wide CAA identifier "www.pkioverheid.nl" or "pkioverheid.nl" is entered for the domain requested
(3) DNS of the domain requested, does not contain a CAA identifier

Digidentity cannot issue certificates for other domain requests.

3.2.3   Authentication of Individual Identity

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

3.2.3.1   Personal Details

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

Digidentity uses the records of professional registrars to verify the natural person is allowed to use the title of the recognised profession.

3.2.3.2   Email address

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.

3.2.3.3   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.

3.2.3.4   Face-to-face verification

For Personal Qualified certificates, Digidentity must verify the identity of the natural person with face-to-face (F2F) check. Digidentity must verify 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.

3.2.3.5   Terms & Conditions and Privacy Statement

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

3.2.3.6   General verifications

For all applications, Digidentity verifies:
▪ Organisational information where applicable
▪ FQDN status and registrant details where applicable
▪ Blacklist/phishing lists

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 Certificate Manager. The delegated person will be verified via the process described above, including a face-to-face check. The delegated person also needs to submit a signed authorisation letter from the legal representative, stating the authorisation for the delegated person. Digidentity verifies the authorisation letter by name and signature match of the legal representative.

If the legal representative of an organisation approves, it is possible to authorise another person to handle the authorisations of the organisation as the Company Administrator. The delegated person will be verified via the process described above, including a face-to-face check. 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

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 Request

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

3.4.1 Website

Subscribers can log into their account and revoke personal certificate(s). If a Subscriber 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 server certificates, the Subscriber or Certificate Manager must log into their account to access the Self-Service Portal (SSP). In the SSP, the Subscriber or Certificate Manager can select the certificate to be revoked. A confirmation of the revocation is sent via email.

To revoke server certificates issued before 23 March 2020, the Subscriber or Certificate Manager must log into the SSL Store with their account and select the certificate to be revoked. A confirmation of the revocation is sent via email.

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.

Recover smartcards

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, and the 'lost' certificates are automatically revoked.

3.4.2 Phone

If the Subscribers or Certificate 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 3.4.1.

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

Certificate 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 Certificate Manager's email address, as shown in the account or SSL Store. The certificate manager must reply to this for the revocation to take place. If the Certificate Manager no longer has the email address in the account, we request a copy of their identity document to verify their identity.

Nederlandse Beroepsorganisatie van Accountants (NBA)

The NBA can request revocation of certificates for Registered Professionals issued to a natural person. Digidentity and NBA agreed on a procedure for revocation requests to revoke these certificates in case a registered accountant is no longer entitled to the title of the registered profession.

3.4.3 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

A certificate application can be submitted by a:

(1) Natural person applying for a personal qualified certificate
(2) Natural person applying for a personal qualified certificate for Registered Professionals
(3) Natural person applying for a personal qualified certificate which is authorised by a natural person legally representing an organisation
(4) Natural person legally representing an Organisation (legal entity) and applying for a server certificate for that Organisation.

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

4.1.2 Enrolment Process and Responsibilities

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

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

For certificates for Registered Professionals, a KvK registration is required.

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

4.2 Certification Application Processing

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

4.2.1 Performing Identification and Authentication Functions

See section 3.2.

4.2.2   Approval or Rejection of Certificate Applications

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

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

4.2.3   Time to Process Certificate Applications

Digidentity can process certificate application information during Service Desk opening hours. Completion of the certification issuing process is dependent on the availability of both parties (Digidentity and applicant) to make an appointment for the face-to-face identity check. The total processing time from application to issuance of a certificate is approximately three (3) to five (5) working days.

4.3   Certificate Issuance

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

For Qualified Certificates, 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 . Certificate Managers are able to download server certificates by signing into the SSL store or Self Service Portal using their account credentials.

4.3.1   CA Actions During Certificate Issuance

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

4.3.2   Notification of Certificate Issuance

Upon successful application and issuance of a certificate, the applicant will receive a notification via 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 by the subscriber 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

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 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 certificates.

4.7 Certificate Re-Key

Digidentity does not perform re-key of certificates.

4.8 Certificate Modification

Digidentity does not perform modification of certificates.

4.9 Certificate Revocation & Suspension

4.9.1 Circumstances for Revocation

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

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

(6) CA is made aware of a material change in the information contained in the certificate;

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

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

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

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

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

(12) The Subscriber ceases operation;

(13) The Subscriber is deceased

4.9.1.2   Reasons for Revoking a Subordinate CA Certificate

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

4.9.2   Who can request Revocation?

Revocation can be requested by:

- The subscriber (or Certificate Holder)
- A legal representative or authorised person of the organisation
- Digidentity
- Organisations of Registered Professions
- Authorities/regulators who are involved in the regulation of PKIoverheid activities, e.g. Logius

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

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 server certificates, the Subscriber or Certificate Manager must log into their account in the Self-Service Portal (SSP) using two factor authentication. In the SSP, the Subscriber or Certificate Manager can select the certificate to be revoked. A confirmation of the revocation is sent via email.

To revoke server certificates issued before 23 March 2020, the Subscriber or Certificate Manager must log into the SSL Store with their account and select the certificate to be revoked.

The Subscriber or Certificate 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

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

4.9.6   Revocation Checking Requirement for Relying Parties

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

4.9.7   CRL Issuance Frequency

Digidentity publishes the CRL for the issuing CA every ten (10) minutes, whereby the CRL is valid for 24 hours.

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

4.9.8   Maximum Latency for CRLs

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

4.9.9   Online Revocation/Status checking Availability

All Digidentity server certificates have an Authority Information Access extension that contains an URL for the OCSP service. OCSP is updated immediately when a certificate is revoked. OCSP responses are valid for eight (8) hours. All OCSP responses conform to RFC6960.

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

4.9.10 Online Revocation checking Requirements

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

Digidentity supports an OCSP capability using the HTTP GET method for certificates issued in accordance with the Baseline Requirements. OCSP Responders under Digidentity's control will respond to a request for the status of a certificate serial number that is "unused" with an "unknown" status.

4.9.11 Other Forms of Revocation Advertisements available

No stipulation

4.9.12 Special Requirements related to Key Compromise

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

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

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

4.10.2 Service Availability

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

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

4.10.3 Optional Features

No stipulation.

4.11 End of Subscription

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 use key escrow and key recovery.

5 Management, Operational & Physical Controls

Digidentity has implemented and maintains an Information Security Management System (ISMS) which is certified against ISO27001:2013 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 are 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 Information Security Officer (CISO): overall responsibility for maintenance and implementation of the security policies and practices.
- Data Protection Officer (DPO) - Responsible for the handling of all security incidents involving Person Data Breach/Leakage.

5.2.2 Number of Individuals required per task

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

All Qualified certificates issued are signed off by two persons in separate trusted roles, namely the RA1 and RA2 officers. It is not possible for either RA1 or RA2 officers to act alone and agree to issue a certificate.

5.2.3 Identification & Authentication for Trusted Roles

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

5.2.4   Roles requiring Separation of Duties

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

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

5.3   Personnel Controls

5.3.1   Qualifications, Experience, and Clearance Requirements

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

5.3.2   Background Check Procedures

Digidentity carries out background check procedure for all employees. These checks will consist of;
- Previous employment and references
- Qualifications
- Criminal records
- 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 logging system records the following types of events;
(1) Key Lifecycle Events;
    (a) Key generation, backup, storage, recovery, archival and destruction
    (b) Cryptographic device lifecycle management events
(2) Certificate Lifecycle Events;
    (a) Certificate requests and revocation
    (b) Verification activities
    (c) Date, time, phone numbers, contact persons, and verification of those
    (d) Acceptance and rejection of certificate requests
    (e) Issuance of certificates

     (f)   Generation of CRLs and OCSPs
(3) Security Events;
     (a)   Access attempts
     (b)   System actions performed
     (c)   Profile changes
     (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

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:

- Registrations and verification data,
- certificate life cycle events,
- authorisations,
- configurations,

- authentications,
- revocation,
- face-to-face checks,
- name,

5.5.2 Retention Period for Archive

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

5.5.3 Protection of Archive

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

5.5.4 Archive Backup Procedures

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

5.5.5 Requirement for Time-Stamping of Records

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

5.5.6 Archive Collection System (Internal or External)

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

5.5.7 Procedures to Obtain & Verify Archive Information

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

5.6   Key Changeover

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

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 Controls

6.1 Key Pair Generation & Installation

6.1.1 Key Pair Generation

6.1.1.1 CA Key Pair Generation

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

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

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

6.1.1.2 RA Key Pair Generation

No stipulation.

6.1.1.3 Subscriber Key Pair Generation

Digidentity generates and stores the key pair for qualified, advanced and seals in the HSM. For server certificates and email certificates, the Subscriber generates the key pair and are 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).

6.1.2 Private Key Delivery to Subscriber

See section 3.2.1.

6.1.3 Public Key Delivery to Certificate Issuer

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

6.1.4 CA Public Key Delivery to Relying Parties

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

6.1.5 Algorithm type and key sizes

All PKIoverheid CAs makes use of 4.096 bits RSA keys.

6.1.5.1 Root CA Certificates

All PKIoverheid Root Certificates are defined and configured by PKIoverheid.

6.1.5.2 Subordinate CA Certificates

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

6.1.5.3 Subscriber Certificates

All Digidentity Subscriber Certificates makes use of 2.048 bits, 3.072 bits or 4.096 bits RSA keys.

6.1.6 Public Key Parameters Generation & Quality Checking

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

CABLint, CertLint & ZLint

The CABLint, CertLint and ZLint linters verify compliance to X.509 RFCs, CA/Browser Forum Baseline Requirements, root store policies, and ETSI standards. Digidentity has implemented these linters for distinct issuance phases: pre-issuance of Subscriber certificates, post-issuance of pre-certificates (if applicable) 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, 3.072 or 4.096 bits,
- the value of the public exponent is an odd number equal to 3 or more;
- the public exponent is in the range between 2^{16+1} and 2^{256-1}
- the modulus is an odd number, not the power of a prime, and have no factors smaller than 752
- Key passes a ROCA vulnerability test (recovery of Private Key from the Public Key)
- Key is not a Debian Weak Key (entropy check)

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

CAA Validator (SSL)

The CAA Validator queries the domain name in the certificate for its DNS CAA records to determine which CA is allowed to issue the certificate.

Digidentity has implemented the CAA Validator on issuance of all SSL certificates.

Digidentity Linters

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

- Issuance of PKIoverheid Organisation SSL certificates (PvE 3e)
- Issuance of PKIoverheid Private Root SSL certificates (PvE 3h)
- Issuance of PKIoverheid Qualified certificates (PvE 3a and PvE 3c)

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

6.1.7   Key Usage Purposes

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

6.2   Private Key Protection & Cryptographic Module Engineering Controls

6.2.1   Cryptographic Module Standards and Controls

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

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

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

6.2.3   Private Key Escrow

Digidentity do not use escrow.

6.2.4   Private Key Backup

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

6.2.5 Private Key Archival

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

6.2.6 Private Key Transfer into or from a Cryptographic Module

Digidentity does not do key transfer.

6.2.7 Private Key Storage on Cryptographic Module

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

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

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

- Digidentity BV PKIoverheid Private Services CA – G1 is valid until 12 November 2028
  + Certificates are valid for three (3) years

- Digidentity BV PKIoverheid Organisatie Persoon CA – G3 is valid until 12 November 2028
  + Certificates are valid for five (5) years
- Digidentity BV PKIoverheid Organisatie Server CA – G3 is valid until 12 November 2028
  + Certificates are valid for 395 days
- Digidentity BV PKIoverheid Burger CA – G3 is valid until 12 November 2028
  + Certificates are valid for five (5) years

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
- Multifactor authentication on systems
- Multifactor authentication for online portals/interfaces
- The use of encryption certificates (SSL/TLS) on all systems
- Separation of duties and use of trusted roles

▪ Use of x.509 certificates for all administrators

6.5.2 Computer Security Rating

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

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

All software development is carried out by Digidentity, by approved and screened Digidentity employees. The measures are strict so that Digidentity can meet the stringent legal and regulatory requirements. Access to code and systems related to development is strictly limited to personnel approved to carry out their roles.

6.6.2 Security Management Controls

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

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

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 Time Stamping

Digidentity does not perform time-stamping.

7 Certificate, CRL & OCSP Profiles

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

7.1 Certificate Profiles

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

7.1.1 Version Number(s)

All certificates are of type X.509 v3.

7.1.2 Certificate Extensions

7.1.2.1 Root CA Certificate

All Root Certificates are defined and configured by PKIoverheid.

7.1.2.2 Subordinate CA Certificates

All Subordinate Certificates are defined and configured by PKIoverheid.

7.1.2.3 Subscriber Certificates

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

7.1.2.4 All Certificates

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

Digidentity uses RSA encryption with SHA-2 algorithm.

7.1.4 Name Forms

7.1.4.1 Issuer Information

See Subscriber Certificates in section 7.1.10.

7.1.4.2 Subject Information

See Subscriber Certificates in section 7.1.10.

7.1.4.2.1 Subject Alternative Name Extension

See Subscriber Certificates in section 7.1.10.

7.1.4.2.2 Subject Distinguished Name Fields

See Subscriber Certificates in section 7.1.10.

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.

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

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/ETSI EN 319 411-2.

7.1.6.4 Subscriber Certificates

See Subscriber Certificates 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.

DIGIDENTITY

7.1.10 Certificate Tables

7.1.10.1 PKIoverheid Private Services CA – G1

Certificate Profile CA managed by PKIoverheid.

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

Field	OID	Value	Critical	Type
Version	(0x02)	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		< +3 years >		Required
Issuer DN				
commonName	(OID 2.5.4.3) {id-at-3}	CN=Digidentity BV PKIoverheid Private Services CA – G1		Required
organizationName	(OID 2.5.4.10)	O=Digidentity B.V.		Required
countryName	(OID 2.5.4.6) {id-at-6}	C=NL		Required
organizationIdentifier	(OID 2.5.4.97)	NTRNL-27322631		Required
Subject DN				
commonName	(OID 2.5.4.3) {id-at-3}	CN=SBR Digipoort		Required
organizationName	(OID 2.5.4.10)	O=<Organisation Name>		Required
countryName	(OID 2.5.4.6) {id-at-6}	C=<Two letter Country Code e.g. NL>		Required
serialNumber	(OID 2.5.4.5)	SERIALNUMBER=<OIN or KVK filled out>		Optional
Public Key				
algorithm	(1.2.840.113549.1.1.1)	sha256WithRSAEncryption		Required
keySize		2048 bits, 3072 bits or 4096 bits		Required
signature		512 bytes		Required
Extensions				
keyUsage	(2.5.29.15) {id-ce 15}	digitalSignature, keyEncipherment	Yes	Required
extKeyUsage	(2.5.29.37) {id-ce 37}	id-kp-serverAuth (1.3.6.1.5.5.7.3.1) id-kp-clientAuth (1.3.6.1.5.5.7.3.2)	No	Required
certificatePolicies	(2.5.29.32) {id-ce 32}	PolicyID1=2.16.528.1.1003.1.2.8.6 (server) QualifierID1=1.3.6.1.5.5.7.2.2 (id-qt-unotice) UserNotice=For the use of this certificate the associated CPS applies. QualifierID2: 1.3.6.1.5.5.7.2.1 (id-qt-cps) URl=https://cps.ca.digidentity.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	Optional

Field	OID	Value	Critical	Type
		URl: http://certificates.pkio-private.ca.digidentity.com/Digidentity-BV-PKIoverheid-Private-Services-CA-G1.pem Method#2: 1.3.6.1.5.5.7.48.1 (ocsp) URl=http://ocsp.pkio-private.ca.digidentity.com		
subjectAltName	(2.5.29.17) {id-ce 17}	<Permanent Identifier: UUID, TSP-OID>	No	Required
cRLDistributionPoints	(2.5.29.31) {id-ce 31}	URl: http://crl.pkio-private.ca.digidentity.com/Digidentity-BV-PKIoverheid-Private-Services-CA-G1.der	No	Required

7.1.10.2 PKIoverheid Burger CA – G3

Certificate Profile CA managed by PKIoverheid.

Personal Authentication – G3 (Subscriber certificate)

Field	OID	Value	Critical	Type
Version	(0x02)	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		< <5 years>		Required
Issuer DN				
commonName	(OID 2.5.4.3) {id-at-3}	CN= Digidentity BV PKIoverheid Burger CA – G3		Required
organisationName	(OID 2.5.4.10)	O= Digidentity B.V.		Required
countryName	(OID 2.5.4.6) {id-at-6}	C=NL		Required
organizationIdentifier	(OID 2.5.4.97)	NTRNL-27322631		Required
Subject DN				
commonName	(OID 2.5.4.3) {id-at-3}	CN=< Full Name as displayed on identity document>		Required
countryName	(OID 2.5.4.6) {id-at-6}	C=<Two letter Country Code e.g. NL>		Required
givenName	(OID 2.5.4.42)	GN=<Given names as displayed on identity document>		Required
surname	(OID 2.5.4.4)	SN=<Surname as displayed on identity document>		Required
serialNumber	(OID 2.5.4.5)	SERIALNUMBER=<pseudonym >		Required
Public Key				
algorithm	(1.2.840.113549.1.1.1)	sha256WithRSAEncryption		Required
keySize		2048 bits or 3072 bits or 4096 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

Field	OID	Value	Critical	Type
		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)		
certificatePolicies	(2.5.29.32) {id-ce 32}	PolicyID1=2.16.528.1.1003.1.2.3.1 (authentication) 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.ca.digidentity.com	No	Required
subjectAltName	(2.5.29.17) {id-ce 17}	SAN= <Permanent Identifier: UUID, TSP-OID>	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) URl: http://certificates.ca.digidentity.com/Digidentity-BV-PKIoverheid-Burger-CA-G3.pem	No	Required
cRLDistributionPoints	(2.5.29.31) {id-ce 31}	URl: http://crl.ca.digidentity.com/Digidentity-BV-PKIoverheid-Burger-CA-G3.der	No	Required

Personal Encryption – G3 (Subscriber certificate)

Field	OID	Value	Critical	Type
Version	(0x02)	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		< <5 years>		Required
Issuer DN				
commonName	(OID 2.5.4.3) {id-at-3}	CN= Digidentity BV PKIoverheid Burger CA – G3		Required
organisationName	(OID 2.5.4.10)	O= Digidentity B.V.		Required
countryName	(OID 2.5.4.6) {id-at-6}	C=NL		Required
organizationIdentifier	(OID 2.5.4.97)	NTRNL-27322631		Required
Subject DN				
commonName	(OID 2.5.4.3) {id-at-3}	CN=< Full Name as displayed on identity document>		Required
countryName	(OID 2.5.4.6) {id-at-6}	C=<Two letter Country Code e.g. NL>		Required
givenName	(OID 2.5.4.42)	GN=<Given names as displayed on identity document>		Required
surname	(OID 2.5.4.4)	SN=<Surname as displayed on identity document>		Required
serialNumber	(OID 2.5.4.5)	SERIALNUMBER=<pseudonym >		Required
Public Key				
algorithm	(1.2.840.113549.1.1.1)	sha256WithRSAEncryption		Required
keySize		2048 bits or 3072 bits or 4096 bits		Required

Field	OID	Value	Critical	Type
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=2.16.528.1.1003.1.2.3.3 (encryption) 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.ca.digidentity.com	No	Required
subjectAltName	(2.5.29.17) {id-ce 17}	SAN= <Permanent Identifier: UUID, TSP-OID>	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) Url: http://certificates.ca.digidentity.com/Digidentity-BV-PKIoverheid-Burger-CA-G3.pem	No	Required
cRLDistributionPoints	(2.5.29.31) {id-ce 31}	URl: http://crl.ca.digidentity.com/Digidentity-BV-PKIoverheid-Burger-CA-G3.der	No	Required

Personal Non-Repudiation – G3 (Subscriber certificate)

Field	OID	Value	Critical	Type
Version	(0x02)	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		< <5 years>		Required
Issuer DN				
commonName	(OID 2.5.4.3) {id-at-3}	CN= Digidentity BV PKIoverheid Burger CA – G3		Required
organisationName	(OID 2.5.4.10)	O=Digidentity B.V.		Required
countryName	(OID 2.5.4.6) {id-at-6}	C=NL		Required
organizationIdentifier	(OID 2.5.4.97)	NTRNL-27322631		Required
Subject DN				
commonName	(OID 2.5.4.3) {id-at-3}	CN=< Full Name as displayed on identity document>		Required
countryName	(OID 2.5.4.6) {id-at-6}	C=<Two letter Country Code e.g. NL>		Required
givenName	(OID 2.5.4.42)	GN=<Given names as displayed on identity document>		Required
surname	(OID 2.5.4.4)	SN=<Surname as displayed on identity document>		Required
serialNumber	(OID 2.5.4.5)	SERIALNUMBER=<pseudonym >		Required

Field	OID	Value	Critical	Type
Public Key				
algorithm	(1.2.840.113549.1.1.1)	sha256WithRSAEncryption		Required
keySize		2048 bits or 3072 bits or 4096 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=2.16.528.1.1003.1.2.3.2 (non-repudiation) 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.ca.digidentity.com	No	Required
subjectAltName	(2.5.29.17) {id-ce 17}	SAN= <Permanent Identifier: UUID, TSP-OID>	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) URl: http://certificates.ca.digidentity.com/Digidentity-BV-PKIoverheid-Burger-CA-G3.pem	No	Required
cRLDistributionPoints	(2.5.29.31) {id-ce 31}	URl: http://crl.ca.digidentity.com/Digidentity-BV-PKIoverheid-Burger-CA-G3.der	No	Required
qcStatements				
esi4-qcStatement-1	(0.4.0.1862.1.1) id-etsi-qcs-1	id-etsi-qcs-QcCompliance		Required
esi4-qcStatement-4	0.4.0.1862.1.4) id-etsi-qcs-4	id-etsi-qcs-QcSSCD		Required
esi4-qcStatement-5	(0.4.0.1862.1.5) id-etsi-qcs-5	id-etsi-qcs-QcPDS URL= https://cps.ca.digidentity.com Language = EN		Required
esi4-qcStatement-6	(0.4.0.1862.1.6) id-etsi-qcs-6	id-etsi-qct-esign {id-etsi-qcs-QcType 1}		Required

DIGIDENTITY

7.1.10.3 PKIoverheid Organisatie Persoon CA – G3

Certificate Profile CA managed by PKIoverheid.

Registered Professional Authentication – G3 (Subscriber certificate)

Field	OID	Value	Critical	Type
Version	(0x02)	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		< <5 years>		Required
Issuer DN				
commonName	(OID 2.5.4.3) {id-at-3}	CN= Digidentity BV PKIoverheid Organisatie Persoon CA - G3		Required
organisationName	(OID 2.5.4.10)	O= Digidentity B.V.		Required
countryName	(OID 2.5.4.6) {id-at-6}	C=NL		Required
organizationIdentifier	(OID 2.5.4.97)	NTRNL-27322631		Required
Subject DN				
commonName	(OID 2.5.4.3) {id-at-3}	CN=< Full Name as displayed on identity document>		Required
countryName	(OID 2.5.4.6) {id-at-6}	C=<Two letter Country Code e.g. NL>		Required
givenName	(OID 2.5.4.42)	GN=<Given names as displayed on identity document>		Required
surname	(OID 2.5.4.4)	SN=<Surname as displayed on identity document>		Required
serialNumber	(OID 2.5.4.5)	SERIALNUMBER=<pseudonym >		Required
organizationName	(OID 2.5.4.10)	O=<Identical to CommonName>		Required
title	(OID 2.5.4.12)	TITLE=<Recognised Profession>		Required
Public Key				
algorithm	(1.2.840.113549.1.1.1)	sha256WithRSAEncryption		Required
keySize		2048 bits or 3072 bits or 4096 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=2.16.528.1.1003.1.2.5.1 (authentication) 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.ca.digidentity.com	No	Required
subjectAltName	(2.5.29.17) {id-ce 17}	SAN= <Permanent Identifier: UUID, TSP-OID>	No	Required

Field	OID	Value	Critical	Type
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) URl: http://certificates.ca.digidentity.com/Digidentity-BV-PKIoverheid-Organisatie-Persoon-CA-G3.pem	No	Required
cRLDistributionPoints	(2.5.29.31) {id-ce 31}	URl: http://crl.ca.digidentity.com/Digidentity-BV-PKIoverheid-Organisatie-Persoon-CA-G3.der	No	Required

Registered Professional Encryption – G3 (Subscriber certificate)

Field	OID	Value	Critical	Type
Version	(0x02)	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		< <5 years>		Required
Issuer DN				
commonName	(OID 2.5.4.3) {id-at-3}	CN= Digidentity BV PKIoverheid Organisatie Persoon CA - G3		Required
organizationName	(OID 2.5.4.10)	O= Digidentity B.V.		Required
countryName	(OID 2.5.4.6) {id-at-6}	C=NL		Required
organizationIdentifier	(OID 2.5.4.97)	NTRNL-27322631		Required
Subject DN				
commonName	(OID 2.5.4.3) {id-at-3}	CN=< Full Name as displayed on identity document>		Required
countryName	(OID 2.5.4.6) {id-at-6}	C=<Two letter Country Code e.g. NL>		Required
givenName	(OID 2.5.4.42)	GN=<Given names as displayed on identity document>		Required
surname	(OID 2.5.4.4)	SN=<Surname as displayed on identity document>		Required
serialNumber	(OID 2.5.4.5)	SERIALNUMBER=<pseudonym >		Required
organizationName	(OID 2.5.4.10)	O=<Identical to CommonName>		Required
title	(OID 2.5.4.12)	TITLE=<Recognised Profession>		Required
Public Key				
algorithm	(1.2.840.113549.1.1.1)	sha256WithRSAEncryption		Required
keySize		2048 bits or 3072 bits or 4096 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=2.16.528.1.1003.1.2.5.3 (encryption) QualifierID1: 1.3.6.1.5.5.7.2.2 (id-qt-unotice)	No	Required

Field	OID	Value	Critical	Type
		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.ca.digidentity.com		
subjectAltName	(2.5.29.17) {id-ce 17}	SAN= <Permanent Identifier: UUID, TSP-OID>	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) URl: http://certificates.ca.digidentity.com/Digidentity-BV-PKIoverheid-Organisatie-Persoon-CA-G3.pem	No	Required
cRLDistributionPoints	(2.5.29.31) {id-ce 31}	URl: http://crl.ca.digidentity.com/Digidentity-BV-PKIoverheid-Organisatie-Persoon-CA-G3.der	No	Required

Registered Professional Non-Repudiation – G3 (Subscriber certificate)

Field	OID	Value	Critical	Type
Version	(0x02)	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		< <5 years>		Required
Issuer DN				
commonName	(OID 2.5.4.3) {id-at-3}	CN= Digidentity BV PKIoverheid Organisatie Persoon CA - G3		Required
organisationName	(OID 2.5.4.10)	O=Digidentity B.V.		Required
countryName	(OID 2.5.4.6) {id-at-6}	C=NL		Required
organizationIdentifier	(OID 2.5.4.97)	NTRNL-27322631		Required
Subject DN				
commonName	(OID 2.5.4.3) {id-at-3}	CN=< Full Name as displayed on identity document>		Required
countryName	(OID 2.5.4.6) {id-at-6}	C=<Two letter Country Code e.g. NL>		Required
givenName	(OID 2.5.4.42)	GN=<Given names as displayed on identity document>		Required
surname	(OID 2.5.4.4)	SN=<Surname as displayed on identity document>		Required
serialNumber	(OID 2.5.4.5)	SERIALNUMBER=<pseudonym >		Required
organizationName	(OID 2.5.4.10)	O=<Identical to CommonName>		Required
title	(OID 2.5.4.12)	TITLE=<Recognised Profession>		Required
Public Key				
algorithm	(1.2.840.113549.1.1.1)	sha256WithRSAEncryption		Required
keySize		2048 bits or 3072 bits or 4096 bits		Required
signature		512 bytes		Required
Extensions				

Field	OID	Value	Critical	Type
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=2.16.528.1.1003.1.2.5.2 (non-repudiation) 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.ca.digidentity.com	No	Required
subjectAltName	(2.5.29.17) {id-ce 17}	SAN= <Permanent Identifier: UUID, TSP-OID>	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) URl: http://certificates.ca.digidentity.com/Digidentity-BV-PKIoverheid-Organisatie-Persoon-CA-G3.pem	No	Required
cRLDistributionPoints	(2.5.29.31) {id-ce 31}	URl: http://crl.ca.digidentity.com/Digidentity-BV-PKIoverheid-Organisatie-Persoon-CA-G3.der	No	Required
qcStatements				
esi4-qcStatement-1	(0.4.0.1862.1.1) id-etsi-qcs-1	id-etsi-qcs-QcCompliance		Required
esi4-qcStatement-4	0.4.0.1862.1.4) id-etsi-qcs-4	id-etsi-qcs-QcSSCD		Required
esi4-qcStatement-5	(0.4.0.1862.1.5) id-etsi-qcs-5	id-etsi-qcs-QcPDS URL= https://cps.ca.digidentity.com Language = EN		Required
esi4-qcStatement-6	(0.4.0.1862.1.6) id-etsi-qcs-6	id-etsi-qct-esign {id-etsi-qcs-QcType 1}		Required

7.1.10.4 PKIoverheid Organisatie Server CA – G3

Certificate Profile CA managed by PKIoverheid.

PKIoverheid Organisatie Server CA - G3 (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		< + 395 days >		Required
Issuer DN				
commonName	(OID 2.5.4.3) {id-at-3}	CN=Digidentity BV PKIoverheid Organisatie Server CA - G3		Required

Field	OID	Value	Critical	Type
organisationName	(OID 2.5.4.10)	O=Digidentity B.V.		Required
countryName	(OID 2.5.4.6) {id-at-6}	C=NL		Required
organizationIdentifier	(OID 2.5.4.97)	NTRNL-27322631		Required
Subject DN				
commonName	(OID 2.5.4.3) {id-at-3}	CN= <FQDN>		Optional
serialNumber	(OID 2.5.4.5)	SERIALNUMBER=< OIN or KvK >		Optional
organisationName	(OID 2.5.4.10)	O=<Organisation Name>		Required
organisationUnitName	(OID 2.5.4.11)	OU=		Optional
localityName	(OID 2.5.4.7)	L=<City of Residence>		Required
stateOrProvinceName	(OID 2.5.4.8)	ST=<Province of subscriber)		Required
countryName	(OID 2.5.4.6) {id-at-6}	C=<Country Code>		Required
Public Key				
algorithm	(1.2.840.113549.1.1.1)	sha256WithRSAEncryption		Required
keySize		2048 bits or 3072 bits or 4096 bits		Required
signature		512 bytes		Required
Extensions				
keyUsage	(2.5.29.15) {id-ce 15}	digitalSignature, keyEncipherment	Yes	Required
extKeyUsage	(2.5.29.37) {id-ce 37}	id-kp-serverAuth (1.3.6.1.5.5.7.3.1) id-kp-clientAuth (1.3.6.1.5.5.7.3.2)	No	Required
certificatePolicies	(2.5.29.32) {id-ce 32}	PolicyID1=2.16.528.1.1003.1.2.5.6 (server) PolicyID2=2.23.140.1.2.2 (BR OVCP) 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 url=https://cps.ca.digidentity.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) URl= http://certificates.ca.digidentity.com/Digidentity-BV-PKIoverheid-Organisatie-Server-CA-G3.pem Method#2: 1.3.6.1.5.5.7.48.1 (ocsp) URl=http://ocsp.ca.digidentity.com	No	Required
subjectAltName	(2.5.29.17) {id-ce 17}	SAN= < Fully-Qualified Domain Name >	No	Required
cRLDistributionPoints	(2.5.29.31) {id-ce 31}	URl: http://crl.ca.digidentity.com/Digidentity-BV-PKIoverheid-Organisatie-Server-CA-G3.der	No	Required
CT Extensions				
SignedCertificateTimestampList	1.3.6.1.4.1.11129.2.4.2	Log Key ID Timestamp – Day, Date, Month, Year, TIME CET Signature Algorithm: SHA-259 ECDSA Signature: 72 bytes		

7.2 CRL Profile

7.2.1 G1 & G3 CRL Profiles

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	(OID 2.5.4.3) {id-at-3}	CN=<Issuer CA Name>		Required
organisationName	(OID 2.5.4.10)	O=Digidentity B.V.		Required
countryName	(OID 2.5.4.6) {id-at-6}	C=NL		Required
organizationIdentifier	(OID 2.5.4.97)	NTRNL-27322631		Required
Extensions				
ThisUpdate		UTC Time of next update to the CRL		Required
NextUpdate		UTC Time of next update to the CRL		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

7.3 OCSP Profile

The OCSP responses and OCSP signing certificates fulfil the requirements laid down in IETF RFC 6960. OCSP signing certificates are compliant with the X.509v3 standard for public key certificates.

7.3.1 PKIoverheid Private Services CA – G1 (OCSP Signing certificate)

Field	OID	Value	Critical	Type
Version	(0x02)	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		<+ 2 years>		Required
Issuer DN				
commonName	(OID 2.5.4.3) {id-at-3}	CN=Digidentity BV PKIoverheid Private Services CA - G1		Required
organisationName	(OID 2.5.4.10)	O=Digidentity B.V.		Required
countryName	(OID 2.5.4.6) {id-at-6}	C=NL		Required
organizationIdentifier	(OID 2.5.4.97)	NTRNL-27322631		Required

Field	OID	Value	Critical	Type
Subject DN				
commonName	(OID 2.5.4.3) {id-at-3}	CN=Digidentity BV PKIoverheid Private Services CA - G1 OCSP		Required
organisationName	(OID 2.5.4.10)	O=Digidentity B.V.		Required
countryName	(OID 2.5.4.6) {id-at-6}	C=NL		Required
Public Key				
algorithm	(1.2.840.113549.1.1.1)	sha256WithRSAEncryption		Required
keySize		4096 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-OCSP-signing (1.3.6.1.5.5.7.3.9)	Yes	Required
certificatePolicies	(2.5.29.32) {id-ce 32}	PolicyID1=2.16.528.1.1003.1.2.8.6 (server) 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.ca.digidentity.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
ocspNoRevocationCheck		1.3.6.1.5.5.7.48.1.5 (id-pkix-ocsp-nocheck)	No	Required

7.3.2 PKIoverheid Organisatie Server CA – G3 (OCSP Signing certificate)

Field	OID	Value	Critical	Type
Version	(0x02)	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		<+ 2 years>		Required
Issuer DN				
commonName	(OID 2.5.4.3) {id-at-3}	CN= Digidentity BV PKIoverheid Organisatie Server CA - G3		Required
organisationName	(OID 2.5.4.10)	O=Digidentity B.V.		Required
countryName	(OID 2.5.4.6) {id-at-6}	C=NL		Required
organizationIdentifier	(OID 2.5.4.97)	NTRNL-27322631		Required
Subject DN				
commonName	(OID 2.5.4.3) {id-at-3}	CN=Digidentity BV PKIoverheid Organisatie Server CA - G3 OCSP		Required
organisationName	(OID 2.5.4.10)	O=Digidentity B.V.		Required
countryName	(OID 2.5.4.6) {id-at-6}	C=NL		Required

Field	OID	Value	Critical	Type
Public Key				
algorithm	(1.2.840.113549.1.1.1)	sha256WithRSAEncryption		Required
keySize		4096 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-OCSP-signing (1.3.6.1.5.5.7.3.9)	Yes	Required
certificatePolicies	(2.5.29.32) {id-ce 32}	PolicyID1=2.16.528.1.1003.1.2.8.6 (server) QualifierID1: 1.3.6.1.5.5.7.2.1 (id-qt-cps) URl=https://cps.ca.digidentity.com QualifierID2=1.3.6.1.5.5.7.2.2 (id-qt-unotice) UserNotice=For the use of this certificate the associated CPS applies.	No	Required
subjectKeyIdentifier	(2.5.29.14) {id-ce 14}	160-bit SHA-1 hash	No	Required
authorityKeyIdentifier	(2.5.29.35) {id-ce 35}	160-bit SHA-1 hash	No	Required
ocspNoRevocationCheck		1.3.6.1.5.5.7.48.1.5 (id-pkix-ocsp-nocheck)	No	Required

8   Compliance Audit & Other Assessments

Digidentity is a Trust Service Provider (TSP) as defined in EU Regulation 910/2014 also known as eIDAS. As a TSP within PKIoverheid, Digidentity must comply to the applicable requirements from Dutch government defined in the Program of Requirements (Programma van Eisen – PvE).

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

- ISO27001:2013   Information Security Management System (ISMS)
- 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
- 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
- PKIoverheid   Programma van Eisen (PvE)
  - PvE Part 3   General requirements
  - PvE Part 3   Additional requirements
  - PvE Part 3a   Organisatie (G2) & Organisatie Persoon (G3)
  - PvE Part 3c   Certificate Policy – Domein Burger
  - PvE Part 3e   Certificate Policy server certificaten – Domein Organisatie Services (G3)
  - PvE Part 3h   Certificate Policy Server Certificaten – Domein Private Services

8.1 Frequency or Circumstances of Assessment

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 319 411-1, ETSI EN 319 411-2 (including normative references to ETSI EN 319 401), eIDAS and ISO27001:2013 standards on a yearly basis.

8.2 Identity/Qualifications of Assessor

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 Netherlands is accredited by UKAS for assessments under ISO17065 and the requirements defined in ETSI EN 319 403.

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;
- 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

All certificates (conformity assessment reports) of Digidentity are available in the repository https://cps.digidentity-pki.com/.

8.7 Self-Audits

Digidentity carries out regular internal audits to continuously assess compliance with the laws, regulations, internal policies and requirements mentioned in this document. At least once per quarter (4 x year) Digidentity checks a 3% sample of all server certificates issued for internal auditing purposes.

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).

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 product (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.

Digidentity does not have a refund policy.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

Digidentity has a full liability insurance policy which provides coverage of more than the required €1.000.000. More details about liability can be found in the relevant Terms & Conditions and any contractual agreement between the subscriber, relying parties and Digidentity.

9.2.2 Other Assets

All assets of Digidentity are managed internally and strictly controlled/maintained. All property of Digidentity is deemed an asset. Digidentity does not provide for any other guarantees, undertakings, and/or commitments than those explicitly provided for in the terms and conditions, and any contractual agreements.

9.2.3 Insurance or Warranty Coverage for End-Entities

Digidentity has a dedicated financial department who are responsible for all financially related tasks and operations. Digidentity employs the services of an independent and non-affiliated accountancy bureau to check financial stability at least once per year.

9.3 Confidentiality of Business Information

9.3.1 Scope of confidential information

All business information, 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 Protection of Personal Data

9.4.1 Privacy Plan

Digidentity is fully compliant with Data Protection laws and European Regulations currently in force for the protection of personal data.

Digidentity has an Information Security Policy which is annually reviewed and audited. The Information Security Policy identifies the information and data, and controls which are necessary to protect that information and data. Digidentity has a change management process to track changes to the laws, and to update systems, procedures, policies and processes as required.

The information security policy includes measures necessary to meet the strict requirements of data protections laws in the European jurisdiction of Digidentity.

9.4.2   Information Treated as Private

Information which is not released for public review, and information contained in the repository is not treated as private. All other types of information are treated as private and handled with the strictest confidentiality. Data supplied to Digidentity to meet the requirements of a certificate request is never shared with unauthorised third parties.

9.4.3   Information Not Deemed Private

Information which is in the public domain is not deemed private. All other information will be handled according to applicable data protection laws. Digidentity have the legal obligation to protect data, per the relevant data protection laws. Digidentity undergo regular internal and external audits to check compliance with relevant data protection laws.

9.4.4   Responsibility to protect private information

Digidentity will not publish, disclose or otherwise make data available for unauthorised view/use.

9.4.5   Notice and consent to use private information

During the registration process all applicants are required to accept the applicable Terms & Conditions, the Privacy Statement and any contractual terms associated with products provided by Digidentity. The use of private information is based on execution of a contract.

9.4.6   Disclosure pursuant to judicial or administrative process

Digidentity will only fulfil the requirements to supply data for forensic purposes as required by law enforcement and for the judicial process, per the legal administrative procedures.

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

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 subscriber has the right to use or has control of the Domain Name described in the certificate.

(2) 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.

(3) at the time of issuance Digidentity has followed the procedures in this CPS to verify the accuracy of the information provided by the applicant.

(4) 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.

(5) Digidentity has followed the procedures in this CPS to verify the identity of any applicant for a certificate.

(6) Digidentity and the subscriber have a legally enforceable subscriber agreement, and that the terms and conditions have been accepted by the subscriber.

(7) Digidentity maintains a 24 x 7 publicly accessible repository available for checking certificate status.

(8) Digidentity will revoke a certificate for reasons already described in this CPS.

(9) Digidentity, as the issuing CA for Root Staat der Nederlanden certificates takes no other responsibilities which are for the Root CA.

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).

PKIoverheid can impose restrictions on the use of Non-Repudiation Certificates, as long as those restrictions are clear to the third party. Digidentity is not liable for the consequences of using a Non-Repudiation certificate that violate these restrictions.

9.6.2 RA Representations and Warranties

Digidentity operate the Digidentity CA and RA functions. Please refer to 9.6.1.

9.6.3 Subscriber Representations and Warranties

Digidentity do not accept liability for damages incurred as a result of improper use of the certificate. Proper use of the certificate is described in this CPS.

Digidentity requires that all applicants accept the relevant terms and conditions, however, can make no guarantee that an applicant will be successful. Successful applicants are required to meet the requirements as described in this CPS. Digidentity makes no exceptions to the conditions of service provision. The terms and conditions are available in the public repository online via the Digidentity website.

Digidentity makes no guarantee than an applicant will be successful. All conditions and requirements must be met by the applicant so that any certificate can be issued. Digidentity is limited to assessing information which the applicant provides and takes no responsibility for inaccurately provided information. Digidentity does not accept liability for damages incurred to the applicant because of no certificate being issued.

9.6.4 Relying Party Representations and Warranties

All questions of liability for subscribers, relying parties and other participants, are covered in contractual agreements, Terms & Conditions and Privacy Statement.

9.6.5 Representations and Warranties of Other Participants

No stipulation

9.7 Disclaimers of Warranties

To the extent permitted by the applicable legislation, this CPS, the Certificate holder agreement and any other contractual documentation, applicable within the PKI for the government, exclude guarantees from Digidentity.

9.8 Limitations of Liability

Digidentity will in no case be liable for the loss of profit, loss of sales, damage to reputation, loss of contracts, loss of customers, loss of use of any software or data, loss or use of any computer or other equipment (unless directly due to breakage of this CPS), wasted time of management or other personnel, losses or liabilities relating to or related to other contracts, indirect damage or loss, consequential damage or loss, special loss or damage. Loss includes full or partial loss or decrease in value.

Digidentity's liability for personal damages, when a person has acted in any way under, on behalf of, within or in relation to this CPS, Certificate holder agreement, the applicable contract or related contract, whether in contract, warranty, tort or any other legal theory, subject to what is explained below, are limited to actual damage suffered by this person. Digidentity will not be liable for indirect, consequential, incidental, special, example or punitive damages with respect to any person, even if Digidentity is pointed out on the possibility of such damage, regardless of how such damage or responsibility has occurred, whether in tort, negligence, justice, contract, statute, customary law or the other.

As a condition, participation within PKIoverheid (including, without limitation, the use of or relying on Certificates) votes for every person within PKIoverheid participates irrevocably in that he/she do not want to claim, or in any other way search for, example, consequence, special, incidental or punitive damages and irrevocably confirms to Digidentity the acceptance of the foregoing as one condition and incentive to allow this person to participate within PKIoverheid.

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 requirement, is compromised by unauthorised disclosure or use of the Certificate, or if any password or activation data is compromised;
- If the Certificate, held by the claimant or otherwise subject of any claim, has been issued to misrepresentation, error or fact which is due to the negligence of any person, entity or organisation;
- If the Certificate, held by the claimant or otherwise subject of any claim, has expired or been withdrawn before the date of the claim;
- If the Certificate, held by the claimant or otherwise subject has been changed in any way or has been used in other ways than the conditions of this CPS and/or the relevant Certificate holder agreement or any applicable legislation or regulations;
- If the private key, which corresponds to the Certificate, held by the claimant or otherwise subject to any claim, is compromised;
- If the Certificate, issued by the plaintiff, is issued in a manner that is in violation with any applicable legislation or regulations;
- Computer hardware or software, or mathematical algorithms, have been developed that tend to have public key cryptography or asymmetric make cryptosystems uncertain, provided Digidentity have reasonable practices used to protect against security breaches because of such hardware, software or algorithms;

Digidentity has introduced several measures to reduce and limit its liabilities if security measures and protection measures fail. Namely to:

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

These measures include, but are not limited to:
- identifying unforeseen events and appropriate remedial actions in a business continuity plan and Disaster Recovery Plan (IT contingency);
- regular backup of system data;
- performing a back-up of the current working software and certain software configuration files;
- storing all backups in secured local and decentralized storage;
- maintaining secure decentralized storage of other materials, needed for disaster recovery;
- The periodic testing of local and centralised backups to ensure that information is available in case of system faults;
- The periodic review of the business continuity plan and disaster recovery plan, including the identification, evaluation and prioritisation of risks;
- The periodic review of any faults in power supply.

Digidentity accepts no liability, in accordance with any requirement, for any violation of obligations, unless the claimant notifies Digidentity within ninety (90) days of the claimant knowing of, or ought to reasonably have known of any reason for the claim, and in all circumstances, no more than three (3) years after the expiry of the Certificate which is included in the claim.

9.9   Indemnities

9.9.1   Indemnification by CAs

No stipulation.

9.9.2   Indemnification by Subscribers

The provisions and obligations concerning damages are included in the relevant contractual documentation.

9.9.3   Indemnification by Relying Parties

The provisions and obligations concerning damages are included in the relevant contractual documentation.

9.10 Term & Termination

9.10.1 Term

The current and valid version of this CPS is available in the Digidentity website repository and is applicable to the services of Digidentity which have the Root certificate "Staat der Nederlanden".

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 which have the Root certificate "Staat der Nederlanden" if services are still offered by Digidentity. If Digidentity cease to issue certificates with Root Staat der Nederlanden, this document will cease to be relevant.

9.10.3 Effect of termination and survival

The provisions within this CPS terminate upon withdrawal of a Certificate holder or relying party within PKIoverheid, with relating to all actions based on the use of, or reliance on, one Certificate or other participation within PKIoverheid. Any termination or withdrawal does not imply any right to action or remedy, to affect or influence any person who has been affected up to and including the date of withdrawal or termination.

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

If applicable, the changes will be implemented in the Terms & Conditions that apply to the service of Digidentity and which are published via the Digidentity website.

Subscribers can comment on the content of this CPS, however, Digidentity reserve the right of whether a change to the document is necessary or not. 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 14 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

Digidentity, situated in The Netherlands, is subject to national Dutch Laws and European Regulations for the provision of services and products.

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

Digidentity is not obliged to perform any of the obligations under contracts in the case of "force majeure" as defined in our General Terms & Conditions.

9.17 Other Provisions

Any provision within this document that is declared invalid or unenforceable will be outside operation. This does not affect the applicability of the remaining provisions in this CPS.

DIGIDENTITY

Appendix A – Definitions & Acronyms

Term	Description
Applicant	New customer that applies for a certificate.
AT	Agentschap Telecom (regulator Trust Service Providers)
GDPR	General Data Protection Regulation
CA	Certificate Authority - within a PKI area the delivery and control of certificates.
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. (ETSI).
FIPS	Federal Information Processing Standards
FQDN	Fully Qualified Domain Name
HSM	Hardware Security Module - special equipment which generates and stores digital keys securely.
OCSP	Online Certificate Status Protocol
PA	Policy Authority
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.

Term	Description
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.
QCP	Qualified Certificate Policy
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
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.

Term	Description
Verification	The process of verifying the user's identity in order to complete registration for a product - to the required Level of Assurance (LoA).
VSC	Virtual Smart Card
WID	Wet op Identificatieplicht. Law regarding mandatory provision of identification.

Appendix B – Revision Details

Version	Date	Description
2019-v1	25 February 2019	PKIoverheid certificate services in one CPS Added G3 Qualified certificates Added G1 Server certificates
2019-v2	6 December 2019	1.5.1 & 1.5.2 Digidentity address modified, 2.2 Removed URL to test certificates G2, aligned CPS with CPS for Digidentity Certificates, added missing sections and removed empty sections to comply to RFC3647 and Mozilla Root Store Policy, updated to Baseline requirements 1.6.6
2020-v1	16 March 2020	Updated to BR 1.6.8, updated to Mozilla Root Store Policy 2.7, updated to PKIoverheid PvE 4.8, removed G2 certificates and references (CA expired), updated section on linters (6.1.6), minor text updates, updated Appendix A

All changes in the latest version are marked in the document grey highlight.