Digidentity Certification Practice Statement for Qualified Certificates and SSL

OID:	2.16.528.1.1003.1.5.8
Date:	18th May 2018
Version:	1.14

© Digidentity B.V. 2018

DIGIDENTITY

Document Control

Title	Digidentity Certification Practice Statement for Qualified Certificates
First Publication	19th May 2011
Rights	Copyright "Digidentity"

Change History

Version	*Date*	*Changes Overseen By*	*Changes Made*
1.0	*19-5-2011*	*Management*	*First Published Version in Dutch*
1.1	*7-9-2011*	*Management*	*SSL Additions*
1.2	*18-4-2012*	*Management*	*Addition of professional certificates*
1.3	*24-4-2013*	*SRC*	*Revocation of certificates*
1.4.1	*13-12-2013*	*SRC*	*Structure per RFC3647*
1.5	*18-2-2015*	*SRC*	*Removed professional certificates*
1.6	*30-8-2017*	*SRC*	*Text edits*
1.7	*12-1-2017*	*SRC*	*Text edits*
1.8	*3-4-2017*	*SRC*	*Certificate lifespan until 2020 and CSP changed to TSP*
1.9	*20-4-2017*	*SRC*	*WEH changed to eIDAS*
1.10	*2-6-2017*	*SRC*	*Update CA Structure G2*
1.11	*22-8-2017*	*SRC*	*Whois domain validation update, text edits*
1.12	*8-9-2017*	*SRC*	*CAA Records added*
1.13	*12-1-2018*	*SRC*	*Revocation Information edited, professional certificates added*
1.14	*20-3-2018*	*SRC*	*Complete revision and 1st English version – Approved MT 18-05-2018*

Contents

© Digidentity B.V. 2018

© Digidentity B.V. 2018

© Digidentity B.V. 2018

© Digidentity B.V. 2018

© Digidentity B.V. 2018

© Digidentity B.V. 2018

INTRODUCTION

Digidentity BV are a Certification Authority (CA) and a Trusted Service Provider (TSP) in the issuance, authentication, revocation and renewal of Public Key Infrastructure (PKI) certificates of the Dutch Government (Overheid). These types of certificates (PKIO) offer the highest level of reliability.

1.1 OVERVIEW

This Certification Practice Statement (CPS) describes the practices and procedures that Digidentity Certification Authority (CA) employ in the life-cycle management of Public Key Infrastructure certificates with "Staat der Nederlanden" as the root (Overheid).

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

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

This Certification Practice Statement is structured per RFC 3647, and is divided into 9 constituent parts that cover the security controls, practices and procedures for certificate issuance.

Digidentity is audited by external auditors and is certified for ETSI EN 319 411-1, ETSI EN 319 411-2 and ISO27001:2013. Digidentity is audited by the Dutch Government Organisation Agentschap Telecom for compliance with the EU Regulation on electronic signatures No. 910/2014 eIDAS.

This CPS document is for the following Certification Authorities of Digidentity:

CA	OID
TSP CA: Digidentity Organisation CA – G2	2.16.528.1.1003.1.3.5.8.1
TSP CA: Issuing CA: Digidentity Burger CA – G2	2.16.528.1.1003.1.3.3.2.1
Issuing CA: Digidentity Machtiging Online SSCD CA – G2	2.16.528.1.1003.1.3.5.8.2
Digidentity SSCD CA- G2	2.16.528.1.1003.1.3.3.2.2
Digidentity Services CA – G2	2.16.528.1.1003.1.3.5.8.3

The Certificate Hierarchy of Digidentity is available in the diagram below. (*Image 1)*

© Digidentity B.V. 2018

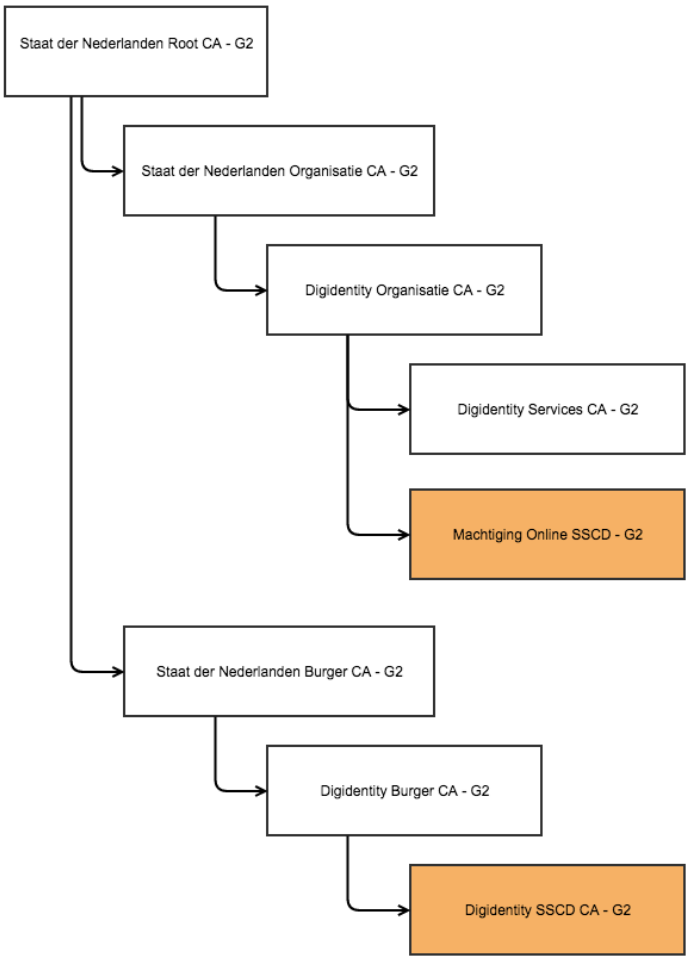

Image 1

1.2 Document Name and Identification

Document Title:	Digidentity Certification Practice Statement for Qualified Certificates
OID:	2.16.528.1.1003.1.5.8

1.3 PKI Participants

The following PKI Participants are applicable;

1.3.1 Certification Authorities

Certification Authorities are entities which issue digital certificates. The Certification Authorities relevant to this CPS are;

- The Root CA is Staat der Nederlanden Organisatie CA.
- The Domain CA is Staat der Nederlanden Burger CA.
- The TSP CA is Digidentity Organisatie CA and Digidentity Burger CA.
- The Issuing CA is Digidentity Machtiging Online SSCD CA and Digidentity SSCD CA.

1.3.2 Registration Authorities

The applicable Registration Authority (RA) for all issued Certificates is Digidentity RA. Digidentity RA verifies applicant requests for a digital certificate. Once the

© Digidentity B.V. 2018

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

Subscribers require the use of PKIO Certificates to support transactions and communications requiring an encrypted connection.
Subscribers can be;

- A natural person self
- A natural person with an associated profession
- A natural person in association with a legal person – a legal representative of an organisation
- A legal person (that can be an organisation, unit or department of the organisation) – where the subscriber is a legal representative applying for the certificate on behalf of the organisation
- A device or system operated by/on behalf on a natural or legal person.

1.3.4 Relying Parties

Are the parties who rely upon the trusted status of the certificate. Relying parties will assess the status of the certificates 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 have the following participants;

- Mitek – Identification document verification
- Kamer van Koophandel (Dutch Chambers of Commerce)
- NBA – Nederlandse Beroepsorganisatie van Accountants (Dutch Professional Organisation of Accountants)

1.4 Certificate Usage

1.4.1 Appropriate Certificate use

Within PKIO Digidentity CA issues certificates which may be used for the purposes explained in this CPS, in the user's Terms & Conditions and as identified in the Key Usage field on the certificate itself.

Personal Certificates/Profession Certificates: These certificates are issued and stored via a SSCD;

- Qualified Certificate: can be used to verify an electronic signature of the user. The signature has the same legal status as a handwritten signature. Digidentity conform to the EU regulations for electronic signatures No. 910/2014 (eIDAS).
- Authentication Certificate: can be used to reliably authenticate the identity of a user as being associated with an organisation.
- 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.

© Digidentity B.V. 2018

System Services Certificates: These are not personal certificates, but certificates which are used by systems;

- Server Certificate: can be used for securing the connection between a specific client and server which are related to an organisation.
- Service Certificate (Authentication): can be used to reliably authenticate the identity of an organisational entity, and additionally to encrypt data.
- Service Certificate (Trust Certificate): can be used for the securing of trusted information/details which are exchanged in electronic form.

1.4.2 Prohibited Certificate Use

Certificates issued under this CPS are prohibited from being used for any other purpose than described.

1.5 Policy Administration

1.5.1 Organisation Administering the Document

Digidentity B.V.
Waldorpstraat 17p
2521 CA
's Gravenhage

1.5.2 Contact Person

For questions about this document please contact;
Security, Risk and Compliance (SRC)
Digidentity B.V.
Waldorpstraat 17p
2521 CA
's Gravenhage
Tel: +31 (0)88 78 78 78
Email: info@digidentity.eu

1.5.3 CPS Approval

This CPS undergoes yearly review (at a minimum interval) and is included in the internal audit schedule. Compliance with CAB Forum Baseline Requirements, RFC 3647 and ETSI 319 411-1/-2 will be assessed, and any inconsistency remedied. Before publishing this CPS is approved by Digidentity Management, where the approval is recorded in the document history.

1.6 Definitions and Acronyms

See Appendix A for a table of acronyms and definitions.

© Digidentity B.V. 2018

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

Digidentity maintain a web-based repository and is responsible for the repository functions for its own CAs. The repository can be checked for enquiries about revocation and certificate status. The Certificate Revocation List (CRL) contains entries for all revoked (deleted) and non-expired certificates. Digidentity also provide OCSP services (Online Certificate Status Protocol).

Digidentity ensures that the repository;

- Accurately publishes information
- Publishes and archives information
- Publishes the status of certificates

2.2 Publication of Information

Digidentity maintain an online documentation repository, containing:

- Certification Practice Statement
- Public Disclosure Statement
- Certificate Revocation List
- OCSP
- Terms and Conditions
- Privacy Policy
- Test certificates – valid, expired and revoked (listed in this CPS).
- The revocation procedures

All information is available in a read-only format, and can be accessed via:
https://www.digidentity.eu/nl/home/#requirements
https://www.digidentity.eu/nl/home/#downloads

Digidentity host test webpages with subscriber certificates as follows:

Valid:	https://valid.digidentity.eu
Revoked:	https://revoked.digidentity.eu
Expired	https://expired.digidentity.eu

2.3 Time or Frequency of Publication

For every CA instance a new CRL will be generated instantly when a certificate is revoked (deleted). If no certificate revocation occurs the CRL will be published every 10 minutes. OCSP responses are valid for 12 hours.

2.4 Access Controls and Repositories

Digidentity provide all repository information and documentation in a read-only format. All publications are available 24 hours a day, 7 days a week, on the Digidentity website.

© Digidentity B.V. 2018

© Digidentity B.V. 2018

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of Names

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

CN – Common Name	Fully Qualified Domain Name to which the certificate and key pair are assigned. It is unique.
OU – Organisational Unit	A department of the organisation
O – Organisation Name	The Organisation Name itself
L – Locality	A geographic location relevant to the computer system
C – Country	A two-digit country code for the location
ST – State	The province/state location

3.1.2 Need for Names to be Meaningful

Distinguished names must be meaningful, unambiguous, and unique. Digidentity ensures that the Organisation (O) and Organisational Unit (OU) attributes in the Subject Field accurately identify the legal entity that is the subject of the Certificate.

3.1.3 Anonymity or Pseudonymity of Subscribers

The use of anonymous certificates, or the use of a pseudonym is not permitted.

3.1.4 Rules for Interpreting Various Name Forms

See paragraph 3.1.1.

3.1.5 Uniqueness of Names

The uniqueness of names is ensured via the Common Name attribute of the Subject Field, which contains a verified domain name. Domain names are always unique.

3.1.6 Recognition, authentication and Role of Trademarks

Certificate applicants shall not use names which infringe upon the intellectual property rights of others. Digidentity 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. Digidentity reserve the right, without liability, to reject any application for a certificate because of any dispute.

© Digidentity B.V. 2018

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

For SSL certificates, applicants must submit a digitally signed Certificate Signing Request (CSR) to prove possession of the private key, which corresponds to the public key in the certificate request.

3.2.2 Authentication of Organisation and Domain Identity

3.2.2.1 Identity

If an organisation wishes to apply for a certificate, then an online application should be made via the Digidentity website: https//www.digidentity.eu. The following details will be requested:

- **Email address of the applicant:**
  For organisations, this will be their chosen email address for contact/management of their certificates.
- **Telephone Number:**
  The telephone number of the contact person and/or certificate manager is required. Digidentity will telephone to check the validity and to make an appointment for identity checks.
- **Applicant;**
  To register for an account (for eventual PKI Overheid SSL Certificate requests) the applicant is a company. However, for the purposes of the application it is necessary to have a "Certificate Manager" and "Contact Person" who can legally represent the application on behalf of the company. In both cases a legitimate copy of identification document is required, as described in the WID – Dutch Identification Laws.
- **Legal Representative:**
  A legal representative is deemed to be the owner, the director, or an authorised representative person who is present on the Organisation's chamber of commerce registry.
- **The Contact Person;**
  Must be a legal representative of the company. The contact person must supply a copy of their identification document, their email address and contact telephone number. It is possible that the certificate manager and contact person are the same.
- **The Certificate Manager;**
  This is the person responsible for the handling of the certificate, its associated use and management. The certificate manager must supply a copy of their identification document, their email address and contact telephone number. If the certificate manager is not a legal representative of the organisation, then authorisation will be requested from the legal representative by means of an authorisation form.
- **Dutch Chamber of Commerce registration number (KVK Number):**

© Digidentity B.V. 2018

Applications can only be submitted by Dutch registered companies with a KVK number. The KVK number is entered, and then the details are retrieved automatically via a secure connection with KVK. The address and name details are taken directly from the KVK register.

- Face-to-Face:
  The certificate manager will undergo a meeting in person to check their identity/identity document.
- Certificate Signing Request (CSR);
  Requested via the online secure delivery interface form in the SSL Store.
- Common name;
  Digidentity confirm the Applicant's control over the 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 an Authorization Domain Name, (ii) including a Random Value in the email, and (iii) receiving a confirming response utilizing the Random Value.
- A Signed Contract;
  Once the registration details have been provided by an SSL applicant, a contract is automatically sent to the subscriber, containing the organisation name and contact person details. This document needs to be signed. If the document is signed digitally then the signature needs to conform to eIDAS EU Regulation No. 910/2014.
- A Signed Addendum;
  Once the SSL application CSR has been submitted an addendum is automatically sent to the applicant. This document needs to be signed. If the document is signed digitally then the signature needs to conform to eIDAS EU Regulation No. 910/2014.
- Terms and Conditions and associated Privacy Policy;
  It is necessary to agree with the Terms and Conditions and associated Privacy Policy to request a certificate. These are signed by the Certificate Manager during the face-to-face check, and the signature is checked against the identity document (written signature).
- Blacklist/Phishing check FQDN:
  All domain names provided as common name during registration will be checked for blacklist/phishing. If the result of the check is negative, then Digidentity will not issue any certificate, and the applicant will be placed on the blacklist.

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, then the application for a certificate will be terminated.

© Digidentity B.V. 2018

3.2.2.3 Verification of Country

Digidentity verify the domain is registered to the Organisation or the legal representative, and that both have the same country listed by checking the whois with the chamber of commerce registry information. Digidentity use reliable sources to verify the county – e.g. Dutch Chamber of Commerce registry.

3.2.2.4 Validation of Domain Authorisation or Control

Digidentity confirm the Applicant's control over the 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 an Authorization Domain Name, (ii) including a Random Value in the email, and (iii) receiving a confirming response utilizing the Random Value.

Once Digidentity receive a response from one of these email addresses, with a matching random value, then control over the domain name can be confirmed.

3.2.2.5 Agreed-Upon Changes to Website

Digidentity do not verify control of domain names using "agreed-upon changes to website".

3.2.2.6 Wildcard Domain Validation

Digidentity do not accept wildcards in common names.

3.2.2.7 Data Source Accuracy

Documentation relied upon by Digidentity RA for the verification of identity may not be older than 3 months old at the time of certificate issuance. This includes;

- Chamber of Commerce Information
- Domain name check and validation
- Identification checks
- Blacklist/phishing check

If the documentation is older than 3 months, then new documentation will be requested from the source by Digidentity RA. Digidentity have this time limit in place to ensure the accuracy and reliability of information.

3.2.2.8 CAA Records

CAA records of the domain name are checked within 8 hours of the issuance of any certificate. CAA records are checked to ensure there are no limitations on Digidentity issuing the certificate with the common name FQDN. If there are limitations on the issuance of a certificate using a specific FQDN then the applicant will be informed that no certificate can be issued for that application.

3.2.3 Authentication of Individual Identity

If the applicant is an individual person e.g. qualified signing certificate, then the applicant will be asked for the following information;

- Personal Details;

© Digidentity B.V. 2018

Full legal name as shown on an identification document which is recognised in Dutch law (WID – see below), date of birth, gender (optional), name history.

- **Address and telephone number;**
  Street, house number, postcode and place, and telephone number (mobile).
- **Identification Document;**
  To verify the identity of the applicant an initial check will be made, using the identification document. The applicant can submit a copy of their passport, driving licence or national identity card. The identification documents must be recognised per Dutch Laws of Identification (WID).
- **Face-to-face check;**
  For all qualified certificates an individual must be identity checked face-to-face. An appointment will be made by telephone for this purpose. The identification document will be checked, and the applicant will need to sign the terms and conditions – whereupon the signature is checked against that on the identification document.
- **Terms and Conditions and associated Privacy Policy;**
  It is necessary to agree with the Terms and Conditions and associated Privacy Policy to request a certificate.
- **Professional registration;**
  Using the records of professional registers to check the membership of the natural person to a regulated profession/job.

3.2.4 Non-Verified Subscriber Information

Non-verified subscriber information includes the Organisational Unit (OU). Digidentity do not verify any IP addresses, or intellectual property rights of applicants.

3.2.5 Validation of Authority

Digidentity verify the applicant's legal status (as described in 3.2.2.1 and 3.2.3) to apply for a certificate by;

- Checking the Chamber of Commerce registry for organisational applicants
- Checking the identity of the applicant in the face-to-face check.
- Checking any professional registers of a regulated profession/job.

3.2.6 Criteria for Interoperation or Certification

Digidentity do not have any stipulations since there is no interoperation or cross-certificates issued.

3.3 Identification and Authentication for Re-Key Requests

When the certificate is due to expire, the subscriber will need to apply for a renewal. Digidentity do not extend the usage of any certificate, but generate a new certificate and issue that to the subscriber, with a new key pair.

The subscriber's application will need to meet the requirements as if it were the first certificate request. If all details remain the same as the first certificate application, then the same contract and acceptance of the Terms and Conditions can be used.

© Digidentity B.V. 2018

The requirements to issue a certificate can change due to changes in the relative laws, regulations and requirements described in 1.1 Overview. Digidentity cannot guarantee the application process will remain the same as the initial application upon applying for renewal. Digidentity will ensure that any changes to the application process are recorded in this CPS.

3.3.1 Identification and Authentication for Re-Key Requests

The following can be requested;

- **Organisations:**
  A new Chamber of Commerce Registry check (if existing one is older than 3 months), a new copy of identification documents (if existing ones have expired), a new FQDN common name check, and associated blacklist/phishing check.
- **Individuals:**
  A new copy of the identification document (if existing one has expired).
  A new check of any professional registers which are applicable.

To issue any certificate to an existing subscriber, the subscriber must meet all requirements to fulfil the certificate application as if the first application. The use of any existing document(s) is acceptable if those documents meet the requirements of validity, age and relevance for application of the subsequent certificate.

1.1.1. Identification and Authentication for Re-Key after Revocation

When a certificate has been revoked, it is possible to request a new replacement certificate. The subscriber's application will need to meet the same requirements as if it were the first certificate request, except for the contract and terms and conditions which remain valid.

If the certificate has been revoked by Digidentity, due to non-payment, misuse or other reasons deemed by Digidentity to be outside of the terms of use of the certificate, then it is at Digidentity's discretion whether to issue a new certificate.

If the subscriber has been placed on the blacklist, then no certificate will be issued.

3.4 Identification and Authentication for Revocation Request

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

- **Organisational subscribers:**
  The certificate manager can request revocation by logging into the system and revoking the certificate(s). The certificate manager will need to log in using the email address and password which was created on creating an account. Alternatively, a request can be made to Digidentity for revocation. The request must originate from the subscriber's email address.
- **Individual subscribers:**
  Personal certificate subscribers can log into their account and revoke the certificates. Alternatively, personal users can contact Digidentity, from their confirmed email address, and request revocation.

© Digidentity B.V. 2018

4 CERTIFICATE LIFE-CYCLE OPERATION REQUIREMENTS

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

For organisational certificates, only legal representatives or those legally authorised can submit a certificate application.
For natural persons, the person self can apply.

All certificates issued by Digidentity CAs have applications handled by Digidentity RA. Once the applicant has registered via the online system (and thus submitted a certificate request), Digidentity RA will begin to process and verify the application. The following will be checked by Digidentity RA;

- The identity and identification document(s)
- The address details of the applicant
- The organisational information where applicable
- The FQDN status and registrant details where applicable
- The blacklist/phishing lists
- Any membership of a professional organisation

If any of the information required to issue a certificate produces a negative outcome e.g. the organisation is in bankruptcy, or the identification document is indicated to be falsified, then Digidentity RA will reject the application for a certificate.

Digidentity maintain an internal database of all previously revoked Certificates and previously rejected certificate applications. If the applicant is found on this list, then the certificate application will be rejected.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

During the application process, Digidentity RA will carry out verification procedures as described in this CPS.

4.2.2 Approval or Rejection of Certificate Applications

Digidentity RA will verify the information provided by the applicant during registration processes. Digidentity RA can only make assessments of whether to approve or reject applications based on the information provided by the applicant.

Applicants have a responsibility to ensure that all information is accurate and complete at the time of making the application, and Digidentity provide no guarantees to the issuance of any certificate. Refer to the Terms and Conditions of Digidentity for related responsibilities of the subscribers/applicants.

© Digidentity B.V. 2018

4.2.3 Time to Process Certificate Applications

Digidentity can process certificate application information on the day of receipt. 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 3-5 working days.

4.3 Certificate Issuance

4.3.1 CA Actions During Certificate Issuance

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

4.3.2 Notification of Certificate Issuance

Once an application for a certificate is successful, and Digidentity CA issue the certificate, the applicant is sent a notification via email.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

Once the certificate is approved the applicant is known as subscriber. The certificate is deemed to have been accepted by the subscriber once;

- The certificate has been downloaded, used and/or installed.
- A period of more than 1 calendar month has passed and no communication has been received from the subscriber.

4.4.2 Publication of the Certificate by the CA

All certificates are published as per the descriptions in this CPS under Chapter 2. Digidentity have conditions contained in the terms and conditions relating to the publishing of certificates.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

Digidentity do not notify other entities of the issuance of any certificate to the subscriber, but do publish the details of the certificate as per the repository information in Chapter 2 of this CPS. Relying parties can enquire about the certificate status via the CRL.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

Subscribers have obligations in the use of the certificate, which are set out in the terms and conditions and a contract where applicable. Prior to any certificate issuance the

© Digidentity B.V. 2018

subscriber will be required to accept the terms and conditions and the terms stated within any contract.

Subscribers are obliged to;

1. Ensure the validity and accuracy of all details provided to Digidentity for use within the certificate and registration process.
2. Ensure that the private key is secured and managed to prevent unauthorised use/access.
    - Immediately inform Digidentity of any theft/loss of the private key.
    - Immediately inform Digidentity of any theft/loss of passwords/log in details.
    - Immediately inform Digidentity of any inaccuracies within the certificate.
3. Ensure that the certificate details are checked upon issuance for any inaccuracies regarding registration details or details contained within the certificate and that these are reported to Digidentity within the time limits stipulated in the contract and terms and conditions.
4. Ensure that the certificate is used in accordance with relevant laws, regulations and agreements, and in accordance with the usage fields on the certificate itself.
5. Promptly request revocation of the certificate and cease the use of the private key if there is any actual or suspected misuse or compromise of the private key associated with the public key in the certificate, and to promptly request revocation of the certificate if any information in the certificate is or becomes incorrect or inaccurate.
6. Promptly cease all use of the Private Key corresponding to the Public Key included in the Certificate upon revocation of that Certificate for reasons of Key Compromise.
7. Ensure that all instructions provided by Digidentity, concerning key compromise or certificate misuse, are followed and carried out within a specific time.
8. Acknowledge that Digidentity reserve the right to immediately revoke the certificate if the applicant has violated the terms and conditions or any contractual agreement, or that Digidentity discovers the certificate has been used/is being used or will be used for any criminal activities, including phishing, fraud or for the distribution of malware/viruses.

All subscriber obligations are provided in the terms and conditions and any contract which is agreed between the subscriber and Digidentity.

4.5.2 Relying Party Public Key and Certificate Usage

Relying parties may only use the public key of the certificate for the purposes described in the relying party agreements in place with Digidentity, and as described in this CPS document. The appropriate certificate usage is denoted by the key usage field provided in the certificate itself.

Relying parties are responsible for:

1. Checking the certificate validity.
2. Checking the validity of the complete chain of certificates, up to the root certificate.
3. The revocation status of the certificate.
4. Limitations on any use of the certificate have been checked.

© Digidentity B.V. 2018

5. That the authenticity of all Certificate Status information is verified by the electronic signature by which the information has been signed.

4.6 Certificate Renewal

4.6.1 Circumstance for Certificate Renewal

Digidentity do not renew certificates.

4.6.2 Who May Request Renewal

Digidentity do not renew certificates.

4.6.3 Processing Certificate Renewal Requests

Digidentity do not renew certificates.

4.6.4 Notification of New Certificate Issuance to Subscriber

Digidentity do not renew certificates.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Digidentity do not renew certificates.

4.6.6 Publication of the Renewal Certificate by the CA

Digidentity do not renew certificates.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

Digidentity do not renew certificates.

4.7 Certificate Re-Key

4.7.1 Circumstance for Certificate Re-Key

Once the existing certificate is close to expiry, or that the existing certificate has been revoked – due to compromise (or other reasons), the subscriber will need to request a new certificate – and per Digidentity's procedure a new key pair. The key pair will expire/be revoked upon certificate expiration/revocation.

4.7.2 Who May Request Certification of a New Public Key

Subscribers described in 4.1.1 may submit a CSR.

4.7.3 Processing Certificate Renewal Requests

The process of a Certificate Renewal Request is the same as the initial certificate request. All conditions/requirements for certificate issuance as described in this CPS will need to be met before the issuance of any new certificate.

© Digidentity B.V. 2018

4.7.4 Notification of New Certificate Issuance to Subscriber

Once the new certificate is approved and issued to the subscriber, the subscriber will receive an email notification.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

The conditions constituting acceptance as the same as with the first certificate issuance process, as described in 4.4.1.

4.7.6 Publication of the Re-Keyed Certificate by the CA

All certificates are published as per the descriptions in this CPS under Chapter 2.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

Digidentity do not notify other entities of the issuance of any certificate to the subscriber, but do publish the details of the certificate as per the repository information in Chapter 2 of this CPS. Relying parties can enquire about the certificate status via the CRL.

4.8 Certificate Modification

4.8.1 Circumstance for Certificate Modification

Digidentity do not modify existing certificates. Digidentity will issue a new certificate and revoke the old one. Digidentity will replace certificates when;

- The common name is changed or authorisation is withdrawn from the registrant
- The company name is changed
- The address details are changed
- The chamber of commerce number is changed.

4.8.2 Who May Request Certificate Modification

Digidentity do not modify certificates.

4.8.3 Processing Certificate Modification Requests

Digidentity do not modify certificates.

4.8.4 Notification of New Certificate Issuance to Subscriber

Digidentity do not modify certificates.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

Digidentity do not modify certificates.

© Digidentity B.V. 2018

4.8.6 Publication of the Modified Certificate by the CA

Digidentity do not modify certificates.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

Digidentity do not modify certificates.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

Revocation occurs when the certificate is permanently disabled before the natural expiry time. Digidentity reserve the right to revoke certificates at its own discretion and/or based on information received. Digidentity will revoke a certificate when;

1. There is a legal requirement to do so;
2. The certificate subscriber has requested revocation per the process described in this CPS;
3. Where the legal representative has indicated that the original certificate request was not authorised, and that no retrospective authorisation will be given;
4. Where Digidentity has reasonable evidence that there has been loss, theft, modification, unauthorised disclosure, or other compromise of the Private Key corresponding to the Public Key within the Certificate, or that the Certificate has otherwise been misused;
5. Where the terms and conditions and/or contract have been infringed by the subscriber;
6. Where the authorisation/right to use the domain name (FQDN) is no longer permitted;
7. The certificate information related to subscriber information is no longer correct/accurate and therefore is misleading;
8. Where Digidentity in its sole discretion, knows/suspects/is informed that the Private Key corresponding to the Certificate was used to sign, publish or distribute spyware, Trojans, viruses, rootkits, browser hijackers, phishing, or other content, or that is harmful, malicious, hostile or downloaded onto a user's system without their consent;
9. Where the private key of the certificate has been compromised;
10. Where Digidentity has determined that the certificate was issued contrary to the processes/procedures described in this CPS;
11. Where the authorisation to issue certificates for Digidentity CA is revoked by the PA;
12. Where revocation is required by this CPS;
13. Where the technical content/format of the certificate poses an unacceptable risk to the application software.

4.9.2 Who Can request Revocation

The following people can request revocation;

- The subscriber
- A legal representative or authorised person of the organisation
- The user of the certificate
- Digidentity

© Digidentity B.V. 2018

- Authorities/regulators who are involved in the regulation of PKIO activities, e.g. Logius

Digidentity have the mandatory requirement to revoke certificates if there is notification that the subscriber/or legal representative in the certificate is deceased. Digidentity's service team will ensure the swift revocation of the certificate in this event. All certificates for PKIO are revoked within 4 hours.

4.9.3 Procedure for Revocation Request

In all cases the subscriber can log into their account and click revoke (delete) alongside the certificates in the account.

SSL certificates: Once the revoke button is clicked then the certificate is immediately revoked.
All other certificates:

- The user can click on revoke by the certificates and they are immediately revoked.
- The user can request the deactivation of the entire account, where all certificates will be revoked in approximately 3 hours (less than 4 hours), along with the account itself.

4.9.4 Revocation Request Grace Period

For SSL certificates the revocation is immediate. There is no grace period.
For all other certificates the revocation time is within 4 hours if via account revocation, where revocation occurs within 4 hours after the initial request. To stop the revocation from being processed the subscriber needs to log back into their account within 3 hours, where the process will be automatically halted.

4.9.5 Time Within Which CA Must Process the Revocation Request

Digidentity must process and complete the revocation of certificates for PKIO within 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 as described in repository information in Chapter 2 in this CPS. Relying parties that fail to check the status of the certificate cannot legitimately rely on the certificate.

4.9.7 CRL Issuance Frequency

The CRL is updated every 10 minutes and the OCSP response is valid for 12 hours. If a certificate is revoked the CRL is updated immediately, with a maximum latency of 10 seconds.

4.9.8 Maximum Latency for CRLs

The maximum latency for the CRL is 10 seconds.

4.9.9 Online Revocation/Status Checking Availability

© Digidentity B.V. 2018

Digidentity's online repository is available online, 24 hours' day, 7 days' week. All OCSP responses are 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

Digidentity update OCSP information at least every 4 days, with a maximum expiration time of 10 days, and within 24 hours upon revocation of a certificate.

4.9.11 Other Forms of Revocation Advertisements Available

This is not applicable to Digidentity.

4.9.12 Special Requirements Related to Key Compromise

Digidentity will take 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 do not suspend certificates, this is not applicable.

4.9.14 Who Can Request Suspension

Digidentity do not suspend certificates, this is not applicable.

4.9.15 Procedure for Suspension Request

Digidentity do not suspend certificates, this is not applicable.

4.9.16 Limits on Suspension Period

Digidentity do not suspend certificates, this is not applicable.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

Certificate Status information available in the CRL will be available until the actual given expiry date within the certificate.

4.10.2 Service Availability

The CRL and OCSP is available 24 hours per day, 7 days per week. The maximum latency is 10 seconds. For information regarding the frequency of publication refer to Chapter 2 of this CPS.

© Digidentity B.V. 2018

4.10.3 Optional Features

Digidentity do not have any stipulations.

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 and Recovery

Escrow is not applicable to Digidentity.

4.12.1 Key Escrow and Recovery Policy and Practices

Escrow is not applicable to Digidentity.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Escrow is not applicable to Digidentity.

© Digidentity B.V. 2018

5 MANAGEMENT, OPERATIONAL, AND PHYSICAL CONTROLS

5.1 Physical Security Controls

As mentioned in 1.1 Overview of this document, Digidentity are audited at least once per year for certification for ISO27001:2013, in which security measures are checked and evaluated. ISO27001:2013 is described by ISO: "This International Standard specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organisation. This International Standard also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organisation."

5.1.1 Site Location and Construction

Digidentity offices;
Digidentity's offices are located on the 7th and 8th floors of the Globe office building, Waldorpstraat in The Hague, Netherlands.

Data Centre;
Digidentity perform the CA functions via a secured data centre in Rotterdam, Netherlands. The data centre is also certified as meeting requirements for ISO27001:2013 and NEN7510, which are both requirements for information security, and ISO9001 for quality and ISO14001 for Environmental security.
Digidentity recognises the certification of the data centre as being reliable for the housing of its CA operational systems, meeting all conditions to ensure security, continuity and reliability.

5.1.2 Physical Access

Digidentity offices:
Access to the Digidentity offices is strictly controlled. Access is permitted to employees via a secure key tag system, and visitors gain access on appointment only. All visitors are required to bring their identification document, and register their arrival and departure from the offices.

Data Centre:
Physical access to the data centre is extremely strict, where permission is limited to specific employees in specific roles. All access to the data centre is logged. Employees accessing the data centre are subjected to dual authentication, using;

- An ID pass
- A finger print scan
- A face scan

5.1.3 Power and Air Conditioning

Data Centre;

© Digidentity B.V. 2018

All power and air conditioning requirements are met. The climate within the data centre is regulated to the international standard ASHRAE TC 9.9 2011. The data centre has two power circuits available to ensure continuity, where the power outage would be a maximum of 6 seconds.

5.1.4 Water Exposure

The data centre is within a contained non-exposed building.

5.1.5 Fire Prevention and Protection

All areas within the data centre are fire retardant up to a maximum time of 1 hour. The data centre halls are installed with highly sensitive smoke detection units, CO2 fire extinguishers and “dry” sprinkler systems.

5.1.6 Media Storage

At Digidentity media is stored within secured storage areas, accessible only to authorised personnel with the correct key tag or key.

5.1.7 Waste Disposal

Digidentity are very strict in the disposal of any paperwork or information (media). All information is handled per the information security policies;

- Paperwork – is cross shredded
- Media/hardware – is disposed of by permanent disabling of the apparatus by experts

5.1.8 Off-Site Backup

An external site is used for the storage and retention of data/information. The off-site location is only accessible by authorised personnel. The location is available 24 hours a day, 7 days per week. All locations of Digidentity (external and internal) are security audited for ISO27001:2013.

5.2 Procedural Controls

5.2.1 Trusted Roles

Digidentity have safeguards in place 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;

- **Chief Security Officer;**
  Oversees security, risk and compliance per the security regulations mentioned in 1.1 Overview.
- **Manager Development & IT Operations;**
  Manages the development team and manages the TSP systems.
- **System Operator/Administrator;**
  Responsible for the daily service provision from a technical aspect.

© Digidentity B.V. 2018

- **TSP Operator;**
  Responsible for the provision of client services and support.
- **System Auditor;**
  Provides an independent assessment on compliance.

5.2.2 Number of Individuals Required Per Task

Digidentity ensure 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.

5.2.3 Identification and Authentication for Trusted Roles

All employees at Digidentity undergo background screening, and all employees are verified and authenticated to the level of PKI0 (highest), including face-to-face checks and identification checks.

5.2.4 Roles Requiring Separation of Duties

Digidentity have a comprehensive list of roles and associated access rights. Privileges are assigned based on the tasks for the role, and a "need" for access, rather than a default permission. Digidentity keep a record of all access rights held by employees.

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. All employees need to have a clean and complete background screening check.

5.3.2 Background Check Procedures

Digidentity carry out the same check procedure for all employees;

- Previous employment and references
- Qualifications
- Criminal records

5.3.3 Training Requirements and Procedures

Upon employment, all new employees undergo 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
- Security awareness

5.3.4 Retraining Frequency and Requirements

All Digidentity employees receive information security awareness refresher training every 3 months.

© Digidentity B.V. 2018

5.3.5 Job Rotation Frequency and Sequence

Digidentity have no stipulation.

5.3.6 Sanctions for Unauthorized Actions

Digidentity have a disciplinary procedure in place. 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 do not employ any independent contractors in trusted roles. 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, re-key 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 and Archiving Audit Logs

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

© Digidentity B.V. 2018

5.4.3 Retention Period for Audit Logs

Logs associated with CA key lifecycle and Certificate Lifecycle management events are kept for 7 years, per the regulatory and legal requirements.

5.4.4 Protection of Audit Log

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. All audit logs are protected with encryption measures and subject to access restrictions.

5.4.5 Audit Log Backup Procedures

Digidentity have a comprehensive backup procedure for the backups which occur daily.

5.4.6 Audit Log Accumulation System (Internal vs External)

The system audit process logger is always available, and automatically record events. If the logger shuts down, then the system will also not function anymore, making it impossible to provide services.

5.4.7 Notifications to Event-Causing Subject

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

5.4.8 Vulnerability Assessments

Vulnerability of Digidentity's systems is assessed via internal and external vulnerability tests and penetration tests. The tests are carried out per the schedule. Vulnerability assessments are carried out by Dutch Government agencies at least once per year.

All foreseeable internal and external threats are assessed with the risk analysis of Digidentity at least once per year, with assessment of the potential damage proportionally to the sensitivity of the data concerned, and the assessment of the policies and procedures that Digidentity have in place to counteract such threats.

5.5 Records Archival

5.5.1 Types of Records Archived

Digidentity archive the following types of records;

- Registrations and verification data, certificate life cycle events, authorisations, configurations, authentications, deactivations, face-to-face checks, signing, reactivation, smartcard encryption, Name, common name, address.

5.5.2 Retention Period for Archive

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

5.5.3 Protection of Archive

© Digidentity B.V. 2018

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.
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 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 do not have any stipulations.

5.5.6 Archive Collection System (Internal or External)

The archive collection system is in the datacentre (external location). The datacentre is described in detail in this chapter of the CPS.

5.5.7 Procedures to Obtain and 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

At the end of Digidentity CA private key life cycle all signing of public keys with the private key will cease. Digidentity CA will only use the expiring private key for signing the CRLs and OCSP responses.

Digidentity have a procedure in place for the key changeover process, which is audited by external auditors for standards pertaining to ETSI EN 319 411-1/-2.

Once a new Digidentity CA signing key pair is issued, all newly issued certificates, thus public keys, and the CRLs and OCSP responses will be signed with the new CA private key.

5.7 Compromise and Disaster Recovery

Digidentity have a business continuity plan in place to prevent a disaster occurring and to ensure continuity if a disaster does occur. 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/customers affected.
The business continuity plan includes all criteria as required by CAB Forum Baseline Requirements.
The business continuity plan is a strictly confidential document, which has been audited and approved by external auditors.

5.8 CA or RA Termination

© Digidentity B.V. 2018

Digidentity have a CA Termination plan in place in the event of a CA operation coming to an end. This termination plan aims to keep the impact of the termination as small as possible, while carrying out actions per regulatory and legal requirements.

Digidentity's CA Termination plan is strictly confidential and has been audited and approved by external auditors.

6 TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

Digidentity have a prepared procedure for Root CA key pair generation. Digidentity have a record in place of any "key ceremony" which has taken place. All key ceremonies are audited by a qualified external auditor as being conform any requirements.

All attendees who have "roles" in the key ceremony are recorded, and sign-off the documentation pertaining to the key generation.

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.

6.1.2 Private Key Delivery to Subscriber

All private keys generated by Digidentity CAs are stored within the HSM until required for use. The private keys are protected via pin-codes which are 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.

For SSL certificates the subscriber generates their own private key and sends a CSR to Digidentity.

6.1.3 Public Key Delivery to Certificate Issuer

Public Keys within personal/professional certificates are generated at the HSM, within the SSCD. Public Keys for SSL 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 for that purpose.

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.
All CA public keys of Digidentity can be downloaded from the repository online: https://www.digidentity.eu

© Digidentity B.V. 2018

6.1.5 Key Sizes

All Digidentity CAs make use of a key length of 4096 or 2048 for RSA with Sha256 encryption.

6.1.6 Public Key Parameters Generation and Quality Checking

For Subscribers: The quality of the parameters, which are used for the production of public keys, is determined by the SSCD used and by the used software of the Certificate Holder.

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 and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

Digidentity use only certified FIPS 140-2 compliance hardware security modules for CA activity. FIPS is the Federal Information Processing Standard which is a standardisation used to approve and standardise cryptographic hardware. The hardware security module has the following features (a level 3 FIPS HSM);

- Tamper-evident seals
- Pick-resistant locks
- Detection and response actions to attempts at physical access
- Tamper-detection/response circuitry

All keys are generated conform the specified key lengths and algorithms as per ETSI TS 119 312.

6.2.2 Private Key Control

All actions are carried out in physically secure environments, and under dual control.

6.2.3 Private Key Escrow

Digidentity do not escrow CA private keys.

6.2.4 Private Key Backup

Digidentity CAs' private keys are backed up by authorised personnel in trusted roles, as described in this CPS.

6.2.5 Private Key Archival

Digidentity do not archive private keys.

6.2.6 Private Key Transfer

Digidentity do not generate keys for subordinate CAs.

© Digidentity B.V. 2018

6.2.7 Private Key Storage

Digidentity CAs' private keys are stored by authorised personnel in trusted roles, as described in this CPS. All private keys are stored and encrypted in the HSM until required for use.

6.2.8 Activating Private Keys

Digidentity CAs' private keys are activated per the documented procedure, and by authorised personnel in trusted roles. The activation of the keys is per the description in 6.1.2.

6.2.9 Deactivating Private Keys

The private keys of Digidentity's issuing CAs are not deactivated, but remain in a secure production environment. HSMs are deactivated when they are taken out of production, e.g. via manual logout or passive timeout. HSMs which are not used are decommissioned per a documented procedure.

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.

6.2.11 Cryptographic Module Capabilities

All aspects of key storage are in accordance with FIPS 140 level 3 and Common Criteria Protection Profile EAL 4+.

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 7 years once the key is expired.

6.3.2 Certificate Operational Periods and 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 key pair is also revoked.

- Digidentity's TSP CA is valid until 23-03-2020
- The validity of certificates issued by Digidentity TSP CA is 1 year.

To issue certificates the lifespan of Digidentity TSP CA must not be shorter than the validity span of the subscriber certificates.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

SSL certificates can be installed and activated by the certificate manager. The corresponding public key to the private key can be downloaded by the certificate manager from the secure account, which requires a log in to access.

© Digidentity B.V. 2018

For all other certificates the keys can be used and activated via use of a pin code.

6.4.2 Activation Data Protection

For SSL certificates the private key is in the management of the subscribing organisation, thus the certificate manager.

For all other certificates the keys are stored encrypted and wrapped in the HSM, until the subscriber enters the correct pin code upon use. The pin code is requested via the subscriber's mobile device and the Digidentity app, and not via the browser.

6.4.3 Other Aspects of Activation Data

Only subscribers with the correct credentials to log in/action the app can activate the use of keys.

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

Multifactor authentication tokens are not permitted on a permanent or temporary basis.

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

6.5.2 Computer Security Rating

All systems of Digidentity are audited per the designated schedule, and on a recurring cyclic basis, both internally and by external parties. All systems of Digidentity are approved and certified for ISO 27001:2013 and ETSI EN 319 411-1/-2 by external auditors at least once per year.

6.6 Life Cycle Technical Control

6.6.1 System Development Controls

All software development is carried out by Digidentity, by approved and screened Digidentity employees. The measures in place are strict so that Digidentity can meet the stringent legal and regulatory requirements e.g. CEN Workshop Agreement (CWA) 14167-1.

© Digidentity B.V. 2018

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 have procedures and schedules in place 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.

The CA software also provides a method for verifying the system, which provides the following guarantees;

- Confirmation of the supplier
- That no tampering has occurred
- That the version is correct.

6.6.3 Life Cycle Security Controls

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

6.7 Network Security Controls

Digidentity perform all technical actions, described in this CPS, using secure networking measures to prevent unauthorised and malicious activity. All access to systems is under the conditions of strict access controls. Digidentity protect sensitive information by using encryption and digital signatures.

The network security of Digidentity is internally audited to be compliant with CAB Browser Forum Network Security Controls (current version), and externally audited and certified to be compliant with ISO 27001:2013.

6.8 Time-Stamping

Digidentity do not perform time-stamping. All logs, data and other information does have the date on.

© Digidentity B.V. 2018

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 CERTIFICATE PROFILE

Digidentity have the following certificate profiles:

Digidentity Organisatie CA-G2

Content	OID	Description	Status
Version		x.509 version 3	Fixed
Serial Number	2.5.4.5	Automatically created	Mandatory
Signature Algorithm	1.2.840.113549.1.1.11	SHA-256 with RSA Encryption	Fixed
Subject Name: Country	2.5.4.6	NL	Fixed
Subject Name: Organisation	2.5.4.10	Organisation Name	Mandatory
Subject Name: Common Name	2.5.4.3	FQDN – Fully Qualified Domain Name	Fixed
Issuer Name: Country	2.5.4.6	NL	Fixed
Issuer Name: Organisation	2.5.4.10	Digidentity B.V.	
Issuer Name: Common Name	2.5.4.3	Digidentity Organisatie CA-G2	
Not valid before		Not valid before the date and time provided	Fixed
Not valid after		Not valid after the date and time provided	Fixed
Public Key Info: Algorithm	1.2.840.113549.1.1.1	SHA-256 with RSA Encryption	Fixed
Public Key Info: Key Size		4096 bits	Fixed
Signature		512 bytes	Fixed
Extension: Key Usage	2.5.29.15	Usage: Key Cert Sign CRL Sign	Critical
Extension: Basic Constraints	2.5.29.19	Certificate Authority: YES	Critical
Extension: Subject Key Identifier	2.5.29.14	Key ID	Not Critical
Extension: Authority Key Identifier	2.5.29.35	Key ID	Not Critical
Extension: Certificate Policies: • Policy ID #1	2.5.29.32.0	• Any policy identifier	Not Critical
Extension: Certificate Policies: Qualifier ID #1	1.3.6.1.5.5.7.2.1	Certification Practice Statement	Not Critical
Extension: CRL Distribution Points	2.5.29.31	CRL Publication http://pki.digidentity.eu/L4/organisatie/latestcrl.crl	Not Critical

MachtigingOnline SSCD CA-G2 - Authentication

Content	OID	Description	Status
Version		x.509 version 3	Fixed

© Digidentity B.V. 2018

Serial Number	2.5.4.5	Automatically created	Mandatory
Signature Algorithm	1.2.840.113549.1.1.11	SHA-256 with RSA Encryption	Fixed
Subject Name: Country	2.5.4.6	NL	Fixed
Subject Name: Organisation	2.5.4.10	Organisation Name	Mandatory
Subject Name: Common Name	2.5.4.3	Name of Subscriber	Fixed
Issuer Name: Country	2.5.4.6	NL	Fixed
Issuer Name: Organisation	2.5.4.10	Digidentity B.V.	
Issuer Name: Common Name	2.5.4.3	MachtigingOnline SSCD CA-G2	
Not valid before		Not valid before the date and time provided	Fixed
Not valid after		Not valid after the date and time provided	Fixed
Public Key Info: Algorithm	1.2.840.113549.1.1.1	SHA-256 with RSA Encryption	Fixed
Public Key Info: Key Size		4096 bits	Fixed
Signature		512 bytes	Fixed
Extension: Key Usage	2.5.29.15	Digital Signature	Critical
Extension: Basic Constraints	2.5.29.19	Certificate Authority: YES	Critical
Extension: Extended Key usage	2.5.29.37	Purpose #1: Client Authentication Purpose #2: Document Signing	Not Critical
Extension: Subject Key Identifier	2.5.29.14	Key ID	Not Critical
Extension: Authority Key Identifier	2.5.29.35	Key ID	Not Critical
Subject Alternative Name: NT Principle Name	2.5.29.17	OID ID	Not Critical
Extension: Certificate Policies: • Policy ID #1	2.5.29.32.0	• Any policy identifier	Not Critical
Extension: Certificate Policies: Qualifier ID #1	1.3.6.1.5.5.7.2.1	Certification Practice Statement	Not Critical
Extension: CRL Distribution Points	2.5.29.31	CRL Publication http://pki.digidentity.eu/L4/sscd-mo/latestcrl.crl	Not Critical

MachtigingOnline SSCD CA-G2 - Signing

Content	OID	Description	Status
Version		x.509 version 3	Fixed
Serial Number	2.5.4.5	Automatically created	Mandatory
Signature Algorithm	1.2.840.113549.1.1.11	SHA-256 with RSA Encryption	Fixed
Subject Name: Country	2.5.4.6	NL	Fixed
Subject Name: Organisation	2.5.4.10	Organisation Name	Mandatory
Subject Name:	2.5.4.3	Name of Subscriber	Fixed

© Digidentity B.V. 2018

Common Name			
Issuer Name: Country	2.5.4.6	NL	Fixed
Issuer Name: Organisation	2.5.4.10	Digidentity B.V.	
Issuer Name: Common Name	2.5.4.3	MachtigingOnline SSCD CA-G2	
Not valid before		Not valid before the date and time provided	Fixed
Not valid after		Not valid after the date and time provided	Fixed
Public Key Info: Algorithm	1.2.840.113549.1.1.1	SHA-256 with RSA Encryption	Fixed
Public Key Info: Key Size		4096 bits	Fixed
Signature		512 bytes	Fixed
Extension: Key Usage	2.5.29.15	Non-Repudiation	Critical
Extension: Basic Constraints	2.5.29.19	Certificate Authority: YES	Critical
Extension: Extended Key usage	2.5.29.37	Purpose #1: Document Signing	Not Critical
Extension: Subject Key Identifier	2.5.29.14	Key ID	Not Critical
Extension: Authority Key Identifier	2.5.29.35	Key ID	Not Critical
Subject Alternative Name: NT Principle Name	2.5.29.17	OID ID	Not Critical
Extension: Certificate Policies: • Policy ID #1	2.5.29.32.0	• Any policy identifier	Not Critical
Extension: Certificate Policies: Qualifier ID #1	1.3.6.1.5.5.7.2.1	Certification Practice Statement	Not Critical
Extension: **Certificate Policies** Qualifier ID #2	1.3.6.1.5.5.7.1.3	User Notice	Not Critical
Extension: CRL Distribution Points	2.5.29.31	CRL Publication http://pki.digidentity.eu/L4/sscd-mo/latestcrl.crl	Not Critical

Digidentity Services CA-G2 - Services

Content	OID	Description	Status
Version		x.509 version 3	Fixed
Serial Number	2.5.4.5	Automatically created	Mandatory
Signature Algorithm	1.2.840.113549.1.1.11	SHA-256 with RSA Encryption	Fixed
Subject Name: Country	2.5.4.6	NL	Fixed
Subject Name: Organisation	2.5.4.10	Organisation Name	Mandatory
Subject Name: Common Name	2.5.4.3	Name of Subscriber	Fixed
Issuer Name: Country	2.5.4.6	NL	Fixed
Issuer Name: Organisation	2.5.4.10	Digidentity B.V.	

© Digidentity B.V. 2018

Issuer Name: Common Name	2.5.4.3	Digidentity Burger CA-G2	
Not valid before		Not valid before the date and time provided	Fixed
Not valid after		Not valid after the date and time provided	Fixed
Public Key Info: Algorithm	1.2.840.113549.1.1.1	SHA-256 with RSA Encryption Usage: Encrypt, Verify, Wrap, Derive	Fixed
Public Key Info: Key Size		2048 bits	Fixed
Signature		512 bytes	Fixed
Extension: Key Usage	2.5.29.15	Digital Signature	Critical
Extension: Extended Key usage	2.5.29.37	Purpose #1: Client Authentication Purpose #2: Document Signing	Not Critical
Extension: Basic Constraints	2.5.29.19	Certificate Authority: YES	Critical
Extension: Subject Key Identifier	2.5.29.14	Key ID	Not Critical
Extension: Authority Key Identifier	2.5.29.35	Key ID	Not Critical
Extension: Certificate Policies: Qualifier ID #1	1.3.6.1.5.5.7.2.1	Certification Practice Statement	Not Critical
Extension: Certificate Policies Qualifier ID #2	1.3.6.1.5.5.7.1.3	User Notice	Not Critical
Extension: CRL Distribution Points	2.5.29.31	CRL Publication http://pki.digidentity.eu/L4/services/latestcrl.crl	Not Critical

Digidentity Services CA-G2 - Server

Content	OID	Description	Status
Version		x.509 version 3	Fixed
Serial Number	2.5.4.5	Automatically created	Mandatory
Signature Algorithm	1.2.840.113549.1.1.11	SHA-256 with RSA Encryption	Fixed
Subject Name: Country	2.5.4.6	NL	Fixed
Subject Name: Organisation	2.5.4.10	Organisation Name	Mandatory
Subject Name: Common Name	2.5.4.3	FQDN – Fully Qualified Domain Name	Fixed
Issuer Name: Country	2.5.4.6	NL	Fixed
Issuer Name: Organisation	2.5.4.10	Digidentity B.V.	
Issuer Name: Common Name	2.5.4.3	Digidentity Organisation CA-G2	
Not valid before		Not valid before the date and time provided	Fixed
Not valid after		Not valid after the date and time provided	Fixed
Public Key Info: Algorithm	1.2.840.113549.1.1.1	SHA-256 with RSA Encryption	Fixed
Public Key Info: Key Size		4096 bits	Fixed
Signature		512 bytes	Fixed

© Digidentity B.V. 2018

Extension: Key Usage	2.5.29.15	Usage: Key Cert Sign CRL Sign	Critical
Extension: Basic Constraints	2.5.29.19	Certificate Authority: YES	Critical
Extension: Subject Key Identifier	2.5.29.14	Key ID	Not Critical
Extension: Authority Key Identifier	2.5.29.35	Key ID	Not Critical
Extension: Certificate Policies: Policy ID #1	2.5.29.32.0	Any policy identifier	Not Critical
Extension: Certificate Policies: Qualifier ID #1	1.3.6.1.5.5.7.2.1	Certification Practice Statement	Not Critical
Extension: CRL Distribution Points	2.5.29.31	CRL Publication http://pki.digidentity.eu/L4/organisatie/latestcrl.crl	Not Critical

Digidentity SSCD CA-G2 - Authentication

Content	OID	Description	Status
Version		x.509 version 3	Fixed
Serial Number	2.5.4.5	Automatically created	Mandatory
Signature Algorithm	1.2.840.113549.1.1.11	SHA-256 with RSA Encryption	Fixed
Subject Name: Country	2.5.4.6	NL	Fixed
Subject Name: Organisation	2.5.4.10	Organisation Name	Mandatory
Subject Name: Common Name	2.5.4.3	FQDN – Fully Qualified Domain Name	Fixed
Issuer Name: Country	2.5.4.6	NL	Fixed
Issuer Name: Organisation	2.5.4.10	Digidentity B.V.	
Issuer Name: Common Name	2.5.4.3	Digidentity Organisation CA-G2	
Not valid before		Not valid before the date and time provided	Fixed
Not valid after		Not valid after the date and time provided	Fixed
Public Key Info: Algorithm	1.2.840.113549.1.1.1	SHA-256 with RSA Encryption Encrypt, Verify, Derive	Fixed
Public Key Info: Key Size		2048 bits	Fixed
Signature		512 bytes	Fixed
Extension: Key Usage	2.5.29.15	Digital Signature	Critical
Extension: Extended Key Usage	2.5.29.37	Purpose #1: Client Authentication Purpose #2: Document Signing	Not Critical
Extension: Basic Constraints	2.5.29.19	Certificate Authority: YES	Not Critical
Extension: Subject Key Identifier	2.5.29.14	Key ID	Not Critical
Extension: Authority Key Identifier	2.5.29.35	Key ID	Not Critical
Extension: Certificate Policies: Policy ID #1	2.5.29.32.0	Any policy identifier	Not Critical

© Digidentity B.V. 2018

Extension: Certificate Policies: Qualifier ID #1	1.3.6.1.5.5.7.2.1	Certification Practice Statement	Not Critical
Extension: **Certificate Policies** Qualifier #2	1.3.6.1.5.5.7.2.2	User Notice	Not Critical
Extension: CRL Distribution Points	2.5.29.31	CRL Publication http://pki.digidentity.eu/L4/sscd-digidentity/latestcrl.crl	Not Critical

Digidentity SSCD CA-G2 Encryption

Content	OID	Description	Status
Version		x.509 version 3	Fixed
Serial Number	2.5.4.5	Automatically created	Mandatory
Signature Algorithm	1.2.840.113549.1.1.11	SHA-256 with RSA Encryption	Fixed
Subject Name: Country	2.5.4.6	NL	Fixed
Subject Name: Organisation	2.5.4.10	Organisation Name	Mandatory
Subject Name: Common Name	2.5.4.3	FQDN – Fully Qualified Domain Name	Fixed
Issuer Name: Country	2.5.4.6	NL	Fixed
Issuer Name: Organisation	2.5.4.10	Digidentity B.V.	
Issuer Name: Common Name	2.5.4.3	Digidentity Organisation CA-G2	
Not valid before		Not valid before the date and time provided	Fixed
Not valid after		Not valid after the date and time provided	Fixed
Public Key Info: Algorithm	1.2.840.113549.1.1.1	SHA-256 with RSA Encryption Encrypt, Verify, Derive	Fixed
Public Key Info: Key Size		2048 bits	Fixed
Signature		512 bytes	Fixed
Extension: Key Usage	2.5.29.15	Key Encipherment, Data Encipherment	Critical
Extension: Extended Key Usage	2.5.29.37	Purpose #1: Email Protection Purpose #2: Encrypted File Systems	Not Critical
Extension: Basic Constraints	2.5.29.19	Certificate Authority: YES	Not Critical
Extension: Subject Key Identifier	2.5.29.14	Key ID	Not Critical
Extension: Authority Key Identifier	2.5.29.35	Key ID	Not Critical
Extension: Certificate Policies: Policy ID #1	2.5.29.32.0	Any policy identifier	Not Critical
Extension: Certificate Policies: Qualifier ID #1	1.3.6.1.5.5.7.2.1	Certification Practice Statement	Not Critical
Extension: **Certificate Policies** Qualifier #2	1.3.6.1.5.5.7.2.2	User Notice	Not Critical
Extension: CRL Distribution Points	2.5.29.31	CRL Publication http://pki.digidentity.eu/L4/sscd-digidentity/latestcrl.crl	Not Critical

© Digidentity B.V. 2018

Digidentity SSCD CA-G2 Signing Certificate

Content	OID	Description	Status
Version		x.509 version 3	Fixed
Serial Number	2.5.4.5	Automatically created	Mandatory
Signature Algorithm	1.2.840.113549.1.1.11	SHA-256 with RSA Encryption	Fixed
Subject Name: Country	2.5.4.6	NL	Fixed
Subject Name: Organisation	2.5.4.10	Organisation Name	Mandatory
Subject Name: Common Name	2.5.4.3	FQDN – Fully Qualified Domain Name	Fixed
Issuer Name: Country	2.5.4.6	NL	Fixed
Issuer Name: Organisation	2.5.4.10	Digidentity B.V.	
Issuer Name: Common Name	2.5.4.3	Digidentity Organisation CA-G2	
Not valid before		Not valid before the date and time provided	Fixed
Not valid after		Not valid after the date and time provided	Fixed
Public Key Info: Algorithm	1.2.840.113549.1.1.1	SHA-256 with RSA Encryption Encrypt, Verify, Derive	Fixed
Public Key Info: Key Size		2048 bits	Fixed
Signature		512 bytes	Fixed
Extension: Key Usage	2.5.29.15	Non-repudiation	Critical
Extension: Extended Key Usage	2.5.29.37	Purpose #1: Document Signing	Not Critical
Extension: Basic Constraints	2.5.29.19	Certificate Authority: YES	Not Critical
Extension: Subject Key Identifier	2.5.29.14	Key ID	Not Critical
Extension: Authority Key Identifier	2.5.29.35	Key ID	Not Critical
Extension: Certificate Policies: Policy ID #1	2.5.29.32.0	Any policy identifier	Not Critical
Extension: Certificate Policies: Qualifier ID #1	1.3.6.1.5.5.7.2.1	Certification Practice Statement	Not Critical
Extension: **Certificate Policies** Qualifier #2	1.3.6.1.5.5.7.2.2	User Notice	Not Critical
Extension: CRL Distribution Points	2.5.29.31	CRL Publication http://pki.digidentity.eu/L4/sscd-digidentity/latestcrl.crl	Not Critical

1.2. CRL Profile

Content	Description	Status
Version	x.509 version 3	Mandatory
Signature Algorithm	SHA-256 with RSA Encryption	Mandatory
Issuer	Must be a distinguished name	Mandatory

© Digidentity B.V. 2018

Issuer Country Name	NL	Mandatory
Issuer Name: Organisation	Digidentity B.V.	Mandatory
Issuer Name: Common Name	Should be set as the issuer CA	Mandatory
Issuer Organisational Unit	Department of the issuer e.g. ICT	Optional
This Update	UTC Time of next update to the CRL	Mandatory
Next Update	UTC Time of next update to the CRL	Mandatory
Revoked Certificate	Provides the status e.g. revoked	Mandatory
CRL Number	Provides the sequential order of the published CRLs	Mandatory
CRL Reason	Provides a reason for revocation	Optional

7.2 OCSP Profile

The OCSP responders are provided in the field of the relevant certificate.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency or Circumstances of Assessment

Digidentity are required to be audited by external auditors at least on an annual basis to assess compliance with national laws, regulations and standards mentioned in Chapter 1 of this CPS.

All certifications of Digidentity are publicly available on the website via: https://www.digidentity.eu.

8.2 Identity/Qualifications of Assessor

All activities related to qualified certificates, thus PKI Overheid, are strictly controlled. Digidentity must show compliance with multiple laws, regulations and requirements, and specifically for PKIOverheid the Programma van Eisen, as already mentioned in this CPS. Digidentity is compliance audited by the following external parties;

- **BSI – British Standards Institution**
  - Certified by around 20 local and international bodies including The Dutch Raad voor Accreditatie (Rva).
- **Agentschap Telecom** – Government Regulatory body of Telecommunications in The Netherlands.

8.3 Assessor's Relationship to Assessed Entity

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

© Digidentity B.V. 2018

8.4 Topics Covered by Assessment

Digidentity is audited to assess compliance with the laws, regulations and requirements associated with business activities of qualified certificates described in this CPS.
Digidentity is certified by BSI for;

- ISO 27001:2013
- ETSI EN 319 411-1/-2

Current certification status is available on the website of Digidentity.

The scope of the audit covers the following;

- Registration Service;
- Certificate Generation Service;
- Revocation Management Service;
- Revocation Status Service
- Dissemination Service;
- Subject Device Provision Service.

Digidentity are required to comply with national laws, regulations and standards mentioned in Chapter 1 of this CPS.

8.5 Actions Taken because of Deficiency

If the result of any audit produces a negative finding then Digidentity will produce a Corrective Action Plan (CAP), where the actions required to resolve/address the negative finding will recorded. The CAP will be submitted to the relevant auditor for approval, and then once approval is received the CAP will be carried out per any time limits set by the auditor. Reassessment of the initial non-conformity will be carried out by the auditor once the time limit has elapsed.

8.6 Communication of Results

All audit results are communicated to Digidentity via official reports.
Audit reports cover the relevant systems and processes used in the issuance of all Certificates. All certification related to audits can be found via the Digidentity website.

8.7 Self-Audits

Digidentity carry out regular internal audits to continuously assess compliance with the laws, regulations and requirements mentioned in this CPS. All internal audits are carried out per an approved and externally audited schedule.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

All fees are published on the Digidentity website by the corresponding product. The website is https://www.digidentity.eu

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

© Digidentity B.V. 2018

service Digidentity charge 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.

9.1.1 Certificate Issuance or Renewal Fees

All fees are published on the Digidentity website by the corresponding product. The website is https://www.digidentity.eu

9.1.2 Certificate Access Fees

Digidentity do not charge access fees.

9.1.3 Revocation or Status Information Access Fees

There are no fees for revocation or status information access.

9.1.4 Fees for Other Services

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 reserve the right to charge an administration fee at their discretion. The administration fee will be proportionate to the amount of work/costs to issue repeated replacement certificates.

9.1.5 Refund Policy

All policies regarding refunds can be found in the relevant terms and conditions and any contractual agreement between the subscriber and Digidentity.

9.2 Financial Responsibility

Digidentity have a dedicated financial department in place who are responsible for all financially related tasks and operations. Digidentity employ the services of an independent and non-affiliated accountancy bureau to check financial stability at least 1 time per year.

9.2.1 Insurance Coverage

Digidentity have a full liability insurance policy which provides coverage of more than the requirements of €1.000.000. More details about liability and insurance can be found in the relevant terms and 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 B.V. 2018

9.2.3 Insurance or Warranty Coverage for End-Entities

Digidentity do not provide for any other guarantees, undertakings, and/or commitments than those explicitly provided for in the terms and conditions, and any contractual agreements in place.

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 described in this CPS. All business information is classified in proportion to sensitivity, where access is controlled and limited to employees/individuals who have permission from Digidentity Management.

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 publically available information is outside the scope of confidential information.

9.3.3 Responsibility to Protect Confidential Information

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

9.4 Privacy of Personal Information

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

9.4.1 Privacy Plan

Digidentity have an Information Security Policy which is regularly reviewed and audited. The Information Security Policy identifies the information and data, and measures which are necessary to protect that information and data. Digidentity have a change management process in place 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.
Information supplied to Digidentity to meet the requirements of a certificate request is never shared with unauthorised 3rd parties.

© Digidentity B.V. 2018

9.4.3 Information Not Deemed Private

Information which is in the public domain is not deemed private. All other information will be handled per national data protection laws applicable to Digidentity and Dutch Law.

9.4.4 Responsibility to Protect Private Information

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.

9.4.5 Notice and Consent to Use Private Information

During the registration process all applicants are required to accept the terms and conditions of use, and any contractual terms associated with products provided by Digidentity.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

Digidentity will not publish, disclose or otherwise make sensitive data available for unauthorised view/use. Digidentity will only fulfil the requirements to supply information for forensic purposes as required by law enforcement and for the judicial process, per the legal administrative procedures.

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 Representations and Warranties

9.6.1 CA Representations and Warranties

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

1. That at the time of issuance Digidentity have 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. That at the time of issuance Digidentity have 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. That at the time of issuance Digidentity have followed the procedures in this CPS to verify the accuracy of the information provided by the applicant.
4. That at the time of issuance Digidentity have followed the procedures in this CPS to reduce the likelihood that the information contained in the certificate is misleading.
5. That Digidentity have followed the procedures in this CPS to verify the identity of any applicant for a certificate.

© Digidentity B.V. 2018

6. That Digidentity and the subscriber have a legally enforceable subscriber agreement in place, and that the terms and conditions have been accepted by the subscriber.
7. That Digidentity maintain a 24 x 7 publicly accessible repository available for checking certificate status.
8. That Digidentity will revoke a certificate for reasons already described in this CPS.

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 in place, including liability for negligence for the
maximum amount included in 9.2.1, for any event or series related events (in a period of 12 months).

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, 1.4.

The PKIOverheid can impose restrictions on the use of Signing Certificates, as long as those restrictions are clear to the 3rd party. Digidentity is not liable for the consequences of using a signing certificate in violation of those restrictions.

All questions of liability for subscribers, relying parties and other participants, are covered in contractual agreements, terms and conditions and privacy policy.

9.6.2 RA Representations and Warranties

Digidentity make 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 RA do not accept liability for damages incurred to the applicant because of no certificate being issued.

9.6.3 Subscriber Representatives and Warranties

Digidentity require 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 make no exceptions to the conditions of service provision.
The terms and conditions are available in the public repository online via the Digidentity website.

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

9.8.1 Limitation of liability

© Digidentity B.V. 2018

Digidentity will in no case be responsible for the loss of profit, loss of sales, loss 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 with relating to or related to other contracts, indirect damage or loss, consequential damage or loss, special loss or damage, and within this paragraph "Loss" means both a partial loss of or decrease in value as complete or total loss.

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 the PKI for the government (including, without limitation, the use of or relying on Certificates) votes for every person within the PKI for the government 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 the PKI government.

9.8.2 Liability Excluded

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 unauthorized disclosure or use of the Certificate, or any password or activation data that the access to do this;
- 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 circumstances lead to any 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;
- Power outages, power outages, or other interruptions of electricity, if Digidentity uses commercially reasonable methods to protect against such disturbances;

© Digidentity B.V. 2018

- Failure of one or more computer systems, communication infrastructure, processing, or storage media or mechanisms or any sub-component not under exclusive control of Digidentity and/or its subcontractors;
- One or more of the following events: a natural disaster or force majeure (including, without limitation, flooding, earthquake, or other natural or weather related cause); a work failure; war, uprising or overt military hostilities; contradictory legislation or government action, prohibition, embargo or boycott; riots or civil unrest; fire or explosion; catastrophic epidemic; trade embargo; limitation or impediment (including, without limitation, export controls); any lack of availability or integrity of telecommunications; legal coercion, including some decision, made by a court of competent jurisdiction, to which Digidentity is subject;

9.8.3 Limitation of Liability Digidentity

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 authorized personnel
- prohibit access to these sources by unauthorized 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 accept 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 known of any reason for the claim, and in all circumstances, no more than 3 years after the expiry of the Certificate which is included in the claim.

9.9 Indemnities

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

9.10 Term and Termination

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”.

© Digidentity B.V. 2018

9.10.1 Term

This CPS is valid until another more recent version takes its place in the Digidentity repository. This CPS will be reviewed and updated at least once per year.

9.10.2 Termination

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 then this CPS 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 the PKI Overheid, with relating to all actions based on the use of, or reliance on, one Certificate or other participation within the PKI for the government. 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 and Communications with Participants

Digidentity provide 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.
- Letter via post: Sent to the subscriber's confirmed address.

9.12 Amendments

All changes made to this CPS will be recorded in the document history. This CPS will be reviewed and changed when;

- A scheduled yearly review is necessary;
- There are changes to the process, procedures or policy described in this document;
- There are changes to the law, regulations or requirements;
- There are changes to the business interests of Digidentity and changes are required.

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.

In case of changing market conditions, safety requirements, legislative changes, etc., Digidentity reserve the right to make changes and modifications to this documentation. If applicable, the changes will be implemented in the general terms and 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.

9.12.1 Procedure for Amendment

© Digidentity B.V. 2018

All changes will be carried out per the change release management process, where final approval and consent is provided by management.

9.12.2 Notification Mechanism and Period

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

Digidentity will notify of any changes to this CPS at least 30 days prior to the publishing thereof.

9.13 Dispute Resolution Provisions

Digidentity have 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 CPS. 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

9.16.1Force Majeure

Digidentity are not obliged to perform any of the obligations under contracts or terms and conditions in the case of "force majeure". Force majeure is understood to be a turn of event which is out of the reasonable control of the affected party, and therefore, if Digidentity cannot perform actions associated with, and not limited to;

- Improper functioning materials provided by users
- Requirements under law
- Power cuts
- Improper functioning of internet, computer and or telecommunication resources
- Extreme Weather conditions – fire, flooding, war, strike, transportation
- Extreme circumstances which reduce/severely limit the availability of Digidentity employees to carry out tasks
- Acts of God
- Terrorism
- Failure of suppliers

Digidentity take measures to thwart the risk of any interruption to services, and have a business continuity plan and disaster recovery plan in place.

© Digidentity B.V. 2018

9.17 Other Provisions

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

© Digidentity B.V. 2018

10 Definitions and Acronyms

Term	Description
Account	The account is necessary to store the user's profile, products and authorisations.
ACM	Autoriteit Consument & Markt (Toezichthouder)
ARC	Account Recovery Code
Assertion	Identity information regarding a registrant.
Assured Identity	A Claimed Identity that is linked to an Applicant with a defined level of confidence that it is the Applicant's real identity
AP	Autoriteit Persoonsgegevens (regulator data protection)
AT	Agentschap Telecom (regulator Digital Identity Providers and Trusted Service Providers)
Biometric	A measure of a human body characteristic that is captured, recorded and/or reproduced in compliance with ICAO 9303, ISO/IEC 19794
Bit	Binary Unit: 0 or 1
CA	Certificate Authority - within a PKI area (TTP) the delivery and control of certificates.
CBP	College Bescherming Persoonsgegevens (College Protection Personal Details).
Claimed Identity	A declaration by the Applicant of their current Personal Name, date of birth and address
Cookie	A packet of data sent by an Internet server to a browser, which is returned by the browser each time it subsequently accesses the same server, used to identify the user or track their access to the server.
CP	Certificate Policy
CPS	Certification Practice Statement - a document describing how the CA operates within PKI.
Credential	An object that is verified when presented to the verifier in an authentication transaction. Credentials may be bound in some way to the individual to whom they were issued.
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.

© Digidentity B.V. 2018

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.
Data Integrity	Maintenance of, and the assurance of the accuracy and consistency of, data over its entire life-cycle.
ETSI	European Telecommunications Standards Institute. (ETSI).
FIPS	Federal Information Processing Standards
FQDN	Fully Qualified Domain Name
GBA	De Gemeentelijke basisadministratie persoonsgegevens (GBA) - The base register of all citizens in the gemeentes (town councils).
Hash Function	A hash function is any function that can be used to map data of arbitrary size to data of fixed size. The values returned by a hash function are called hash values, hashcodes, digests, or simply hashes. One use is a data structure called a hash table, widely used in computer software for rapid data lookup.
HSM	Hardware Security Module - special equipment which generates and stores digital keys securely.
Identity Assurance	Is the ability for a party to determine, with some level of certainty, that an electronic credential representing an entity (human or a machine) with which it interacts to effect a transaction, can be trusted to actually belong to the entity.
ISO	Internationale Organisation for Standardisation. Digidentity works extensively with standards in the ISO 27000 series.
LoA	Level of Assurance - the assurance that the person is who they claim to be after completing registration. 1 = lowest to 4 = highest.
NCSC	National Cyber Security Centre
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.
PIN	Personal Identification Number (Nederlands; Persoonlijk Identificatie Nummer)
PKC	Public Key Certificate
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.
Product	The user registers for the product e.g. GOV.UK verify, eHerkenning and Idensys.

© Digidentity B.V. 2018

Profile	An overview of the user's personal details, settings, activity and products. Available in the account once logged in.
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.
PUK	Personal Unlocking Key.
QCP	Qualified Certificate Policy
QES	Qualified Electronic Signature
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.
RP	Relying Party - the party which relies on the IDP to verify users and issue credentials so that they can access services.
SAML	Security Assertion Markup Language - based on XML framework for exchange of authentication and authorisation details.
Shared Secret	A secret which is known to the claimant of an identity and the verifier of the identity.
SSCD	Secure Signature Creation Device.
SSL	Secure Sockets Layer
Subscriber	A user who has been verified and been issued a credential.
SUD	Secure User Device.
Symmetric Key	An encryption system in which the sender and receiver of a message share a single, common key that is used to encrypt and decrypt the message.
TLS	Transport Layer Security
Token	In possession of the claimant for the authentication of identity e.g. password.
TSP	Trusted Service Provider
TWS	Trustworthy System - a computer system that is secure, reliable and available, and setup to carry out specific tasks.
TW4S	Trustworthy System Supporting Server Signing
Validation	The process of checking the validity of information e.g. validation of passport details.
Verification	The process of verifying the user's identity to complete registration for a product - to the required Level of Assurance (LoA).
VIS	Verification Identification System.
VPN	Virtual Private Network.

© Digidentity B.V. 2018

WBP	Wet Bescherming Persoonsgegevens. Data Protection Law.
WID	Wet op Identificatieplicht. Law regarding mandatory provision of identification.

© Digidentity B.V. 2018