DIGIDENTITY

PKI Disclosure Statement

Digidentity Certificates

Title	PKI Disclosure Statement – Digidentity Certificates
Date	9 September 2020
Author	Digidentity
Version	2020-v1
Classification	Public

Revisions

Version	Date	Author	Changes Made
2019-v1	25 March 2019	SRC	First publication
2019-v2	12 September 2019	SRC	Added DDY Assurance Root CA and certificates
2019-v3	6 December 2019	SRC	Added Self Service Portal
2020-v1	9 September 2020	SRC	Added Remote Identification, removed Organisation Validated Certificates, updated Issuing CA

Introduction

This PKI Disclosure Statement (PDS) is an informational document which aims to provide information about PKI services, summarising the Certification Practice Statement (CPS) for Digidentity certificates. The PDS is not intended as a replacement for the CPS and the CPS should be read if you want to use our products and services (see paragraph CPS).

Contact Information

Addresses

Digidentity B.V.
Waldorpstraat 13-F,
2521 CA, 's Gravenhage (The Hague)
Netherlands

Digidentity B.V.
Postbus 19148
2500 CC 's Gravenhage (The Hague)
Netherlands

Telephone Numbers

Reception: +31 (0)887 78 78 78
Service Desk NL: +31 (0)70 700 79 76
Service Desk UK: +44 (0)330 05 83 454

Emergency revocation line for certificates (outside of office hours): +31 (0)88 778 78 00

Digidentity Opening Hours

Office/Reception: Monday – Friday 9am until 5pm
Service Desk NL:
Monday – Friday 8.30am until 5pm

Service Desk UK:
Monday – Friday 8am until 10pm (GMT)
Saturday and Sunday 8am until 5pm (GMT)

Public Holidays

The office/reception are unavailable on Dutch public holidays.
The Service Desk NL are unavailable on Dutch public holidays.
The Service Desk UK are unavailable on UK public holidays.

Digidentity Website and Email Addresses

Dutch website: https://www.digidentity.eu/nl/home/
English website: https://www.digidentity.eu/en/home/

Dutch support pages: https://helpdesk.digidentity.eu/hc/nl
English support pages: https://helpdesk.digidentity.com/hc/en-us

Service Desk NL: helpdesk@digidentity.eu
Service Desk UK: helpdesk@digidentity.co.uk

Certificate Types

All certificates have a policy identifier, which identifies the use. The identifiers are as follows;

Personal Qualified & Personal Advanced

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

- Encryption Certificate: can be used for the securing of trusted information/details which are exchanged in electronic form. This includes exchanges between people as well as people and automated systems.

- Non-repudiation Certificate: can be used to digitally sign documents. These certificates are issued as Advanced or Qualified certificates and are issued and stored on a Qualified Secure Signature Creation Device (QSCD). Digidentity complies to the EU regulations for electronic signatures No. 910/2014 (eIDAS).

At Digidentity an application can be made via the Digidentity website. Applicants will need to create an account and add personal details during the registration, including an ID via a mobile app. For products in this domain all Applicants will be required to perform a remote identification process. Once Applicants are approved and the certificate is issued to them, and they become Subscribers. For eHerkenning level 4, a physical identification is required. The physical identification will be during the Face-to-Face meeting.

Seals for Organisations (Qualified)

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

- Encryption Certificate: can be used for the securing of trusted information/details which are exchanged in electronic form.

- Non-repudiation Certificate: can be used to digitally sign documents on behalf of an organisation. These certificates are issued as qualified certificates for electronic seals. The certificates are issued and stored on Secure Signature Creation Device (SSCD) or Qualified Secure Signature Creation Device (QSCD). Digidentity complies to the EU regulations for electronic signatures No. 910/2014 (eIDAS).

At Digidentity an application can be made via the Digidentity website. Applicants will need to create an account and add personal details during the registration, including an ID via a mobile app. For products in this domain all applicants will be required to perform a remote identification process.

Digital Passport Certificates

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

Business Authentication Certificates

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

Applicants of certificates which include the organisation name in the Subject field, will need to add the details of their organisation. This may involve the request of authorisation from an employer who has legal representation of the company. Once applicants are approved, and the certificate is issued to them, they become subscribers.

Secure Email

These personal certificates can be used for encrypting and/or singing email messages. An application can be made via the Digidentity website. Applicants will need to create an account and add personal details during registration.

Server Certificates

Server Certificate: can be used for securing the connection between a specific client and server. These certificates are server certificates linked to a domain name. Server certificates are used for SSL/TLS certificates.

SSL means ‘Secure Sockets Layer’. It is a protocol which creates a secure connection between a client and the server to which information is sent. The Subscriber of the certificate is a natural person.

To request a certificate, the applicant can visit the website: https://www.digidentity.eu/en/home/ and select the SSL Certificates. In the Self-Service Portal, you can make an account and fill in the required data. For all requests a Certificate Signing Request (CSR) is required. Full instructions can be obtained from the Service Desk, or the support pages NL.

Domain Validated Certificate

A Domain Validated certificate is an SSL certificate used for securing the connection between a client and server. These certificates contain a Fully Qualified Domain Name (FQDN), which is validated during the application process. The Subscriber of the certificate is an organisation or a natural person.

To request a certificate, the applicant can visit the website: https://www.digidentity.eu/en/home/ and select the SSL Certificates. In the Self-Service Portal, you can make an account and fill in the required data. For all requests a Certificate Signing Request (CSR) is required.

For the certificate the following is checked;

- In all certificate requests, the use of a Fully Qualified Domain Name (FQDN) will require a validation that the domain is under the control of the Subscriber or its legal representatives.

Certificate Usage

Digidentity issues subscriber certificates for:

- Server certificates (Digidentity TLS CA) – OID 1.3.6.1.4.1.34471.2.3
  - Domain validated (DVCP) – OID 1.3.6.1.4.1.34471.2.3.7
- Email certificates (Digidentity Secure Mail CA) – OID 1.3.6.1.4.1.34471.2.2.4
  - Secure Email (S/MIME) (LCP) – OID 1.3.6.1.4.1.34471.2.2.4.6
- Qualified certificates for natural persons (Personal Qualified CA) – OID 1.3.6.1.4.1.34471.3.1
  - Personal Authentication (NCP+) – OID 1.3.6.1.4.1.34471.3.1.1
  - Personal Encryption (NCP+) – OID 1.3.6.1.4.1.34471.3.1.2
  - Personal Non-Repudiation (QCP-n-qscd) – OID 1.3.6.1.4.1.34471.3.1.3
- Qualified certificates for legal persons – Seals (Business Qualified CA) – OID 1.3.6.1.4.1.34471.3.2
  - Business Authentication (NCP+) – OID 1.3.6.1.4.1.34471.3.2.1
  - Business Encryption (NCP+) – OID 1.3.6.1.4.1.34471.3.2.2
  - Business Non-Repudiation (QCP-l-qscd) – OID 1.3.6.1.4.1.34471.3.2.3
- Advanced certificates for natural persons (Personal Advanced CA) – OID 1.3.6.1.4.1.34471.3.3
  - Personal Authentication (NCP+) – OID 1.3.6.1.4.1.34471.3.3.1
  - Personal Encryption (NCP+) – OID 1.3.6.1.4.1.34471.3.3.2
  - Personal Non-Repudiation (NCP+) – OID 1.3.6.1.4.1.34471.3.3.3
- Authentication certificates (SIVI CA) – OID 1.3.6.1.4.1.34471.4.1
  - Digital Passport (NCP) – OID 1.3.6.1.4.1.34471.3.4.1.1
  - Business Authentication (NCP) – OID 1.3.6.1.4.1.34471.3.4.1.2

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

Certificate Application

A certificate application can be submitted by a:

(1) Natural person applying for a personal qualified certificate, a personal advanced certificate, a secure email certificate or a server certificate for a domain.

(2) Natural person legally representing an Organisation (legal entity) and applying for a business qualified certificate for electronic seals or a Digital Passport certificate or Business Authentication certificate for the organisation.
(3) Natural person applying for a personal qualified certificate which is authorised by a natural person legally representing an organisation (eHerkenning Level 4)

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

The Applicant is required to accept the General Terms & Conditions and Privacy Statement. If any of the information required to issue a certificate is missing/incomplete or produces a negative outcome e.g. the organisation is in bankruptcy, or the identification document is indicated not to be genuine, then Digidentity will reject the application for a certificate. For eHerkenning, a KvK registration is required.

Subscribers have obligations in the use of the certificate, which are set out in the General Terms & Conditions. Prior to any certificate issuance the subscriber will be required to accept the General Terms & Conditions.

Certificate Revocation

Revocation can be requested by:

- The subscriber
- A legal representative or authorised person of the organisation
- Digidentity
- Authorities/regulators who are involved in the regulation of PKI activities, e.g. Agentschap Telecom

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

Revocation of certificates can be performed:

(1) By Subscriber themselves by logging in their account and requesting the revocation of issued certificates. The subscriber is able to click “Change two-factor authentication”, “Revoke Certificates”.
(2) During office hours (8.30 – 17.00 hours) by calling the Service Desk at +31 (0)88 78 78 78
(3) Outside of office hours by calling the emergency revocation line at +31 (0)88 778 78 00

Subscriber is able to log into their account and click “Revoke certificates” or “Change two-factor authentication”. The subscriber is able view their virtual smartcard which contain their certificates. By

deleting a specific virtual smartcard, all three (3) associated certificates (authentication, encryption and non-repudiation) will be revoked. Revocation occurs immediately.

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

For server and email certificates, the Certificate Manager will need to log in their account in the Self-Service Portal using two factor authentication. From the list of certificates, you can click on “Revoke certificate” next to the associated certificate to revoke the certificate.

The Subscriber or Certificate Manager will receive confirmation of the revocation of the certificates.

Limitations of Use

Certificates issued may only be used for the purposes that they were issued, as explained in corresponding CPS, in the General Terms & Conditions and as identified in the key usage field of the certificate itself. Certificates are prohibited from being used for any other purpose that described, and all certificate usage must be done within the limits of applicable laws.

Obligations of Subscribers

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

The Subscriber is required to accept the General Terms & Conditions, Privacy Statement and if applicable, sign the certificate contract. If any of the information required to issue a certificate is missing/incomplete or produces a negative outcome e.g. the organisation is in bankruptcy, or the identity document is indicated not to be genuine, then Digidentity will reject the application for a certificate.

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

Acknowledge that Digidentity reserve the right to immediately revoke the certificate if the applicant has violated the terms and conditions, contractual agreements or used the certificate for other purposes than provided in the CPS;

Acknowledge that Digidentity reserve the right to immediately revoke the certificate if it is discovered the certificate has been used/is being used, or will be used for any criminal activity, including phishing, fraud or for the distribution of malware/viruses.

Certificate Status Checking Obligations of Relying Parties

Relying parties may only use the public key of the certificate for the purposes described in the relying party agreements with Digidentity, and as described in the CPS.

Relying parties are responsible for verifying:

(1) certificate validity.
(2) validity of the complete chain of certificates, up to the root certificate.
(3) revocation status of the certificate.
(4) limitations on any use of the certificate
(5) authenticity of all Certificate Status information is verified by the electronic signature by which the information has been signed

Relying parties that fail to check the status of the certificate cannot legitimately rely on the certificate.

Limitations of Warranty and Liability

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

Digidentity's liability for personal damages, when a person has acted in any way under, on behalf of, within or in relation to this CPS, Certificate holder agreement, the applicable contract or related contract, whether in contract, warranty, tort or any other legal theory, subject to what is explained below, are limited to actual damage suffered by this person. Digidentity will not be liable for indirect, consequential, incidental, special, example or punitive damages with respect to any person, even if Digidentity is pointed out on the possibility of such damage, regardless of how such damage or responsibility has occurred, whether in tort, negligence, justice, contract, statute, customary law or the other. As a condition, participation (including, without limitation, the use of or relying on Certificates) votes for every person 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. We refer to the CPS (https://cps.digidentity-pki.com/) for further detail on liability and warranties

Applicable Agreements & CPS

Terms & Conditions

The General Terms & Conditions are applicable to all services of Digidentity, and can be found on the website:

Dutch:	https://www.digidentity.eu/nl/home/#terms-and-conditions
English:	https://www.digidentity.eu/en/home/#terms-and-conditions

CPS

The applicable CPS, product specific terms and this document link, are available on the Digidentity website via this link: https://cps.digidentity-pki.com/

Privacy Statement

The Privacy Statement is available on the Digidentity website via this link: https://www.digidentity.eu/en/home/#privacy-statement

Refund Policy

Digidentity does not have a refund policy.

Applicable Law, Complaints and Dispute Resolution

Digidentity B.V. is subject to laws of The Netherlands, EU and International Law. These laws include, but are not limited to;

- General Data Protection Regulation EU;
- eIDAS Regulation (EU) 910/2014;
- The Data Protection Act 2018 (UK);

Our complaints procedure is available on our website at: https://www.digidentity.eu/en/home/#complaints-procedure

Any information we receive about our services and products is taken seriously. Any complaints will be handled with the ultimate aim of resolving the issue.

Repository Licences, Trust Marks and Audit

See our website (https://www.digidentity.eu/en/home/#certifications) for all audits and certifications.