Digidentity

PKI Disclosure Statement

PKIoverheid Certificates

Title	PKI Disclosure Statement - PKIoverheid Certificates
Date	8 August 2023
Valid from	15 August 2023
Version	2023-v1
Location	https://www.digidentity.eu/en/documentation/
Classification	Public

Digidentity

Revisions

Version	Date	Changes Made (*)
2019-v1	27 February 2019	Full revision and first publication in English
2019-v2	6 December 2019	Review and added Self Service Portal
2020-v1	9 September 2020	Added Remote Identification
2021-v1	25 May 2021	Add notification to end issuance of SSL/TLS PKIo
2022-v1	31 January 2022	Removed PKIo Server 2020 CA
2022-v2	7 October 2022	Updated links
2023-v1	8 August 2023	Annual review - no changes

(*) All changes are marked in grey highlight.

03 Aug 2023 20:28 +0200
Den Haag

Digidentity B.V.
QUALIFIED BUSINESS SEAL

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 PKIoverheid 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
Dutch Service Desk: +31 (0)70 700 79 76

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

Digidentity Opening Hours

Office/Reception: Monday – Friday 9.00 until 17.00

Service Desk NL:
Monday – Friday 8.30 until 17.00

Public Holidays

The office/reception is closed on Dutch public holidays.
The Dutch Service Desk is closed on Dutch public holidays.

Digidentity Website & Email Addresses

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

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

Dutch Service Desk: helpdesk@digidentity.eu
English Service Desk: helpdesk@digidentity.co.uk

Certificate Types

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

Domain Burger: Personal Qualified

- 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.

Domain Organisation Services: 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 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.

Applicants of these products 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.

Digidentity

Domain Organisatie Persoon: Personal 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 a Qualified Secure Signature Creation Device (QSCD). Digidentity complies to the EU regulations for electronic signatures No. 910/2014 (eIDAS).

Within this domain, Digidentity issues personal qualified certificates for Registered Professionals (Accountants). For these certificates, we verify the registration of the professional with the Nederlandse Beroepsorganisatie van Accountants (NBA). Applicants will need to supply their NBA registration number during the process.

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.

Applicants of these products 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.

Private Server Certificates

These certificates are SBR/Digipoort server certificates attached to an organisation. Server certificates are used for PKIoverheid SBR/Digipoort services. These certificates are issued from the PKIoverheid Private Root hierarchy.

To request a SBR/Digipoort certificate, the applicant can visit the website: https://www.digidentity.eu/en/home/ and select the SBR Certificates. In the SSL Store, 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.

For the certificate the following is checked;

- Identity of the Certificate Manager and Legal Representative of the Organisation;
  - Identity document;
  - Remote Identification of Certificate Manager and Legal Representative;
- A valid Kamer van Koophandel (Chamber of Commerce) registration;

Certificate Usage

Digidentity issues subscriber certificates for:

- Server certificates for Digipoort (Digidentity BV PKIoverheid Private Services CA - G1) – OID 2.16.528.1.1003.1.3.15.1.1
  - Server (OVCP) – OID 2.16.528.1.1003.1.2.8.6
- Personal certificates for Registered Professionals (Digidentity BV PKIoverheid Organisatie Persoon CA - G3) – OID 2.16.528.1.1003.1.3.5.8.1
  - Professional Authentication (NCP+) – OID 2.16.528.1.1003.1.2.5.1
  - Professional Encryption (NCP+) – OID 2.16.528.1.1003.1.2.5.3
  - Professional Non-Repudiation (QCP-n-qscd) – OID 2.16.528.1.1003.1.2.5.2
- Personal certificates (Digidentity BV PKIoverheid Burger CA - 2021) – OID 2.16.528.1.1003.1.3.3.2.1
  - Personal Authentication (NCP+) – OID 2.16.528.1.1003.1.2.3.1
  - Personal Encryption (NCP+) – OID 2.16.528.1.1003.1.2.3.3
  - Personal Non-Repudiation (QCP-n-qscd) – OID 2.16.528.1.1003.1.2.3.2
- Organisation certificates (Digidentity BV PKIoverheid Organisatie Services CA - 2021) – OID 2.16.528.1.1003.1.3.5.8.3
  - Organisation Authentication (NCP+) – OID 2.16.528.1.1003.1.2.5.4
  - Organisation Encryption (NCP+) – OID 2.16.528.1.1003.1.2.5.5
  - Organisation Non-Repudiation (QCP-l-qscd) – OID 2.16.528.1.1003.1.2.5.7

Digidentity PKIoverheid 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

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

[3] Natural person applying for a personal qualified certificate for Registered Professionals

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

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 Terms & Conditions, and the CPS.

The Applicant is required to accept the 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 identification document is indicated not to be genuine, then Digidentity will reject the application for a certificate. For certificates for Registered Professionals, 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
- Organisations of Registered Professionals
- Authorities/regulators involved in the regulation of PKIo activities, e.g. Logius

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

Revocation of certificates can be performed:

[1] By Subscriber themselves by logging in their account and requesting the revocation of issued 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.

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

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 & 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.

We refer to the General Terms & Conditions and the CPS (https://cps.digidentity-pki.com/) for further detail on liability and warranties

Applicable Agreements & CPS

Terms & Conditions

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

Dutch:	https://www.digidentity.eu/nl/documentation/
English:	https://www.digidentity.eu/en/documentation/

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/documentation/

Refund Policy

Digidentity does not refund paid invoices.

Applicable Law, Complaints and Dispute Resolution

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

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

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/certification/) for all audits and certifications.