DIGIDENTITY

PKI Disclosure Statement

Digidentity PKIoverheid certificates

Title	PKI Disclosure Statement – Digidentity PKIoverheid Certificates
Date	27 February 2019
Author	Digidentity
Version	2019-v1
Classification	Public

Revisions

Version	Date	Author	Changes Made
2019-v1	27 February 2019	SRC	Full revision and first publication in English

Introduction

This PKI Disclosure Statement (PDS) is an informational document which aims to provide information about PKI services, summarising the Certification Practice Statement (CPS). 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 17p,
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

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;

Domain Burger

These certificates are personal qualified certificates used for our eSGN Qualified and eHerkenning Level 4 products:

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 document via a mobile app. For products in this domain all applicants will be required to attend a physical meeting with a Digidentity agent to verify their identity during a face-to-face check.

Certificate usage:	
Personal authentication certificates:	OID 2.16.528.1.1003.1.2.3.1
Personal signing certificates:	OID 2.16.528.1.1003.1.2.3.2
Personal encryption certificates:	OID 2.16.528.1.1003.1.2.3.3

Domain Organisatie Persoon

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 document via a mobile app. For products in this domain all applicants will be required to attend a physical meeting with a Digidentity agent to check identity. This is called a face-to-face check.

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.

Certificate usage:	
Personal authentication certificates:	OID 2.16.528.1.1003.1.2.5.1
Personal signing certificates:	OID 2.16.528.1.1003.1.2.5.2
Personal encryption certificates:	OID 2.16.528.1.1003.1.2.5.3

Domain Services

These certificates are server certificates attached to an organisation. Server certificates are used for PKIoverheid SSL/TLS certificates.

Certificate usage: Server certificates (PKIo public root): OID 2.16.528.1.1003.1.2.5.6

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 an organisation (and not 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 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;
  - ID document;
  - Physical meeting with a Digidentity agent, called a face-to-face check;
- A valid Kamer van Koophandel (Chamber of Commerce) registration;

Digidentity will also require a signed contract, Terms & Conditions and where applicable, authorisations for non-legal representatives to carry out PKI certificate related tasks. 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.

Domain Private Services

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.

Certificate usage: Private Server Certificates: OID 2.16.528.1.1003.1.2.8.6

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;
  - ID document;
  - Physical meeting with a Digidentity agent, called a Face-to-face check;
- A valid Kamer van Koophandel (Chamber of Commerce) registration;

Digidentity will also require a signed contract, Terms & Conditions and where applicable, authorisations for non-legal representatives to carry out PKI certificate related tasks. 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 Application

A certificate application can be submitted by a:

(1) Natural person applying for a personal qualified certificate
(2) Natural person applying for a personal qualified certificate for Registered Professionals
(3) Natural person applying for a personal qualified certificate which is authorised by a natural person legally representing an organisation (eHerkenning Level 4)
(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.

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 who are 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 via three (3) methods
(2) During office hours (8.30 – 17.00 hours) by calling the Service Desk at +31 (0)88 78 78 78
(3) Outside of office hours by calling the emergency revocation line at +31 (0)88 778 78 00

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

Limitations of Use

Certificates issued may only be used for the purposes that they were issued, as explained in corresponding CPS, in the 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 Terms & Conditions, and the CPS.

The Subscriber 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 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 Terms & Conditions and a contract where applicable. Prior to any certificate issuance the subscriber will be required to accept the 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 within PKIo (including, without limitation, the use of or relying on Certificates) votes for every person within PKIo 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 PKIo. We refer to the CPS (https://cps.ca.digidentity.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/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.ca.digidentity.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);
- Wet op de Identificatieplicht.

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.