digidentity.eu™

Certification Practice Statement
OID: 1.3.6.1.4.1.34471.1.2.1.1

Date : 20 April 2011

Version: 1.0

Document Control Page

Title	Certificate Practice Statement L3
Creator	Marcel A. Wendt
Date	20 April 2011
Type	Text
Format	Word
Identifier	CPS v10 Certification Practice Statement L3.doc
Source	N/A
Language	Dutch
Rights	Copyright “Digidentity”

Version number	1.0
Date	20 April 2011
Modified by	Boris Goranov
Comments	Final publication

Change history

Version	Date	Changed by	Changes made
1.0	20-04-11	Boris Goranov	Final publication

Distribution list

Name	Company	Department

Table of Contents

Terminology

Term	Definition
Audit (EDP)	A DP audit is the independent evaluation of an automated information service. EDP stands for Electronic Data Processing.
AuSO	Authentication Service Organization: The party Digidentity is working with for face to face verification.
Authentication	Verifies a person's identity.
Authorisation	Grants one or more permissions after identification and authentication.
CA	Certification Authority. Trusted entity that confirms (or repudiates) a user's identity.
CP	A written collection of rules that specifies the applicability of a certificate for a certain group and/or class with common security requirements. End users and relying parties can use a CP to determine how well they can trust the connection between the public key and the identity of the holder of the public key.
CPS	Certification Practice Statement: a document that explains the Digitentity's procedures and measures in all areas of its service.
CRL	Certificate Revocation List: a public list of revoked certificates.
CSP	Certification Service Provider: A natural person or legal entity that issues certificates or that provides other services in connection with electronic signatures (Definition translated from the Dutch Law on Electronic Signatures).
DID	A digital representation of a natural person or legal entity, which is always unique at Digidentity.
Distinguished Name	Unique name that is assigned to the Certificate Holder of an Advanced Certificate,
EFQM / INK	EFQM is the European Foundation for Quality Management, which was established in the 1980s by 14 large companies. INK is the Dutch Quality Institute. The Institute has adopted the international EFQM model. INK is raising further awareness for the model in the Netherlands through training sessions and supporting publications.
ETSI	European Telecom Standard Institute: an independent institute for standardisation in telecommunications.
Firewall	Hardware and/or software solution to prevent unauthorised access to a network.
FQDN	Fully Qualified Domain Name
Identification	The process that identifies a person.
LDAP	Lightweight Directory Access Protocol: The file maintained by Digidentity that contains the certificates that have been issued by Digidentity.
OID	Object Identifier: a row of numbers that permanently and uniquely identifies an object.
OSCP	Online Status Certificate Protocol: the standard protocol that is used to verify certificates online (in real time).
PKI	Public Key Infrastructure: A combination of architecture, technology, organization, procedures and rules based on public key cryptography. The purpose is to enable trusted electronic communication and trusted electronic service.
PUK	Personal Unlock Key: A code that is used to release or create cryptographic modules.
QCP	Qualified Certificate Policy: A Certificate Policy that specifies the requirements that are explained in article 18.15, the first and second paragraph of the Telecommunications Act.
RA	Registration Authority: A Registration Authority processes the certificate applications and handles all related tasks.
SHA-2-RSA encryption	Signing algorithm (encryption/unique protection) for all certificates and CRLs.

Term	Definition
SSCD	Secure Signature Creation Device. A device to create electronic signatures that meets the requirements specified in article 18.17, first paragraph of the Telecommunications Act. .
TTP	Trusted Third Party: Organization that acts as an independent third party between the parties involved in electronic transactions and message traffic by issuing keys and certificates as proof of authenticity of a transaction or message.
VIS	Verification Identification System. VIS is an automated information system that provides notifications regarding the unique codes of stolen, lost or otherwise invalid identity and travel documents at home and internationally.

Objective, services and organization

1.1. *Introduction*

The tremendous increase in electronic communications and transactions has resulted in a similarly large demand for a digital identity (DID). Before now, there has never been a standard DID and all service providers have had to arrange this DID themselves. Therefore, users have to manage and remember many different DIDs, preferably without writing them down, bearing all the consequences thereof (costs, loss, and difficult to manage, etc.). This is like having a "digital key ring full of keys" that keeps growing and growing.

For secure communications and transaction exchange, it is crucial for all parties involved that the absence of physical contact is overcome by a standard and trusted digital identity. In other words, how can the digital identity be authenticated and can this process be the same everywhere so that you know where you stand and that authentication becomes a predictable and perfectly common step in digital communications. The Digidentity service provides a solution to this problem.

1.2. *Organization*

The comprehensive service is provided by two different departments at Digidentity BV, which are Digidentity CA and Digidentity RA.

Digidentity CA is responsible for the technical side of the services provided and for its job as a Certification Authority. Digidentity CA provides the parties assurance about their identity and authority. Digidentity CA is responsible for all tasks involved in issuing, changing, renewing and revoking certificates. Before commencing these actions, Digidentity RA first performs the registration tasks explained in this document.

Digidentity RA is responsible for identity verification and for its duties as a Registration Authority (RA). Digidentity engages sub-contractors for a number of steps in the process. However, Digidentity maintains full responsibility.

Digidentity has internal approval procedures and a change advisory council. This council provides recommendations to management, who approves the change.

1.3. *Purpose of this Certification Practice Statement*

Digidentity operates in accordance with QCP public + SSCD, a Qualified Certificate Policy (QCP) for qualified certificates, which employs SSCD, a secure process for creating electronic signatures. This allows Digidentity to overcome the absence of physical contact by supplying a standard and trusted digital identity. This process secures digital communications and transactions in accordance with the ETSI TS 101 456 standard.

Digidentity acts as a Trusted Third Party (TTP) in terms of ETSI TS 101 456 in this case and, in its role as a Certificate Service Provider (CSP) it provides the service that enables the actual use of a Public Key Infrastructure (PKI). Digidentity operates according to European and Dutch laws and conforms to the European directive pertaining to electronic signatures (1999/93/EG) and to the Law and Administrative Order on Electronic Signatures the corresponding guidelines as well as the Compulsory Identification Act.

This document explains the activities of Digidentity, the organization for qualified certificates, and is the Digidentity Certification Practice Statement (CPS) for these certificates, in accordance with ETSI TS 101 456 standard. For the three star level, Digidentity follows all standards and the same procedures as ETSI TS 101 456, including the use of the SSCD; nevertheless, the identity is not validated face to face, which means that L3 certificates are not qualified certificates, but advanced certificates.

The ETSI TS 102 042 standards and Webtrust are observed for EV certificates.

Digidentity issues certificates with the following certificate policies.

Individual Domain:

Authentication	1.3.6.1.4.1.34471.1.2.3.1
Non-repudiation	1.3.6.1.4.1.34471.1.2.3.2
Trust	1.3.6.1.4.1.34471.1.2.3.3

Organization Domain:

Authentication	1.3.6.1.4.1.34471.1.2.5.1
Non-repudiation	1.3.6.1.4.1.34471.1.2.5.2
Trust	1.3.6.1.4.1.34471.1.2.5.3
Services – Authentication	1.3.6.1.4.1.34471.1.2.5.4
Services – Trust	1.3.6.1.4.1.34471.1.2.5.5
Services - Server	1.3.6.1.4.1.34471.1.2.5.6

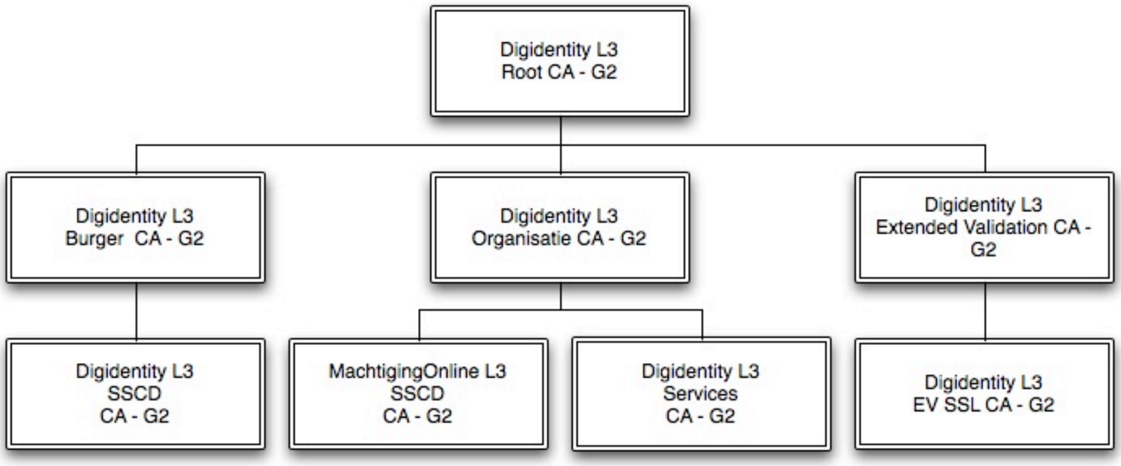
Extended Validation Domain:

Services – EV-SSL	1.3.6.1.4.1.34471.1.2.5.7

Trusted certificates can be generated technically, but will not actually be issued. Certificates related to a specific profession are not issued.

Certificates for organization domains are issued under the trade name MachtigingOnline and certificates for individual domains are issued under the trade name Digidentity.

In summary, Digidentity uses the following CA hierarchy; these CA profiles are available in appendix A:



1.4. *CPS availability and maintenance*

The Digidentity CPS is prepared and maintained periodically by:

Digidentity BV
P.O. Box 19148
2500 CC The Hague

Telephone : +31 (0)887 78 78 78
E-mail : info@digidentity.eu
Web : www.digidentity.eu

Digidentity ensures that this CPS is available 24x7 via the Digidentity website except in the event of system failures, maintenance activities or other factors that are beyond Digidentity's control. In the latter case, Digidentity will make every effort to ensure that a failure does not last longer than 24 hours. Revocation requests can be submitted at any time and will be processed immediately, or within 4 hours maximum, and placed on the published CRL.

Digidentity will also publish the following CRLs for all CAs it manages and make them available 24x7.

- pki.digidentity.eu/ L3 /root/latest.crl
- pki.digidentity.eu/ L3 /burger/latest.crl
- pki.digidentity.eu/ L3 /organisatie/latest.crl
- pki.digidentity.eu/ L3 /sscd-mo/latest.crl
- pki.digidentity.eu/ L3 /sscd-Digidentity/latest.crl
- pki.digidentity.eu/ L3 /services/latest.crl
- pki.digidentity.eu/ L3 /ev/latest.crl
-

1.5. *Audit*

Digidentity will examine whether it meets all requirements that certificate providers of qualified services must fulfil in terms of policy and operations, such as the ETSI TS 101 456 standard, by conducting an internationally standardised self-assessment (EFQM / INK). Digidentity will also assess any third parties involved in operations for this purpose to see if they meet all the requirements that certificate providers of qualified services must fulfil in terms of policy and operations, such as the ETSI TS 101 456 standard.

A certification institute designated by the Ministry of Economic Affairs, Agriculture and Innovation will also evaluate whether Digidentity and its third party sub-contractors meet the requirements set forth in this CPS, the legal regulations, the appendices to this CPS, the agreements that may contain this CPS, as well as the security policy.

1.6. *Changes to the CPS*

Editorial changes to this CPS or corrections of grammar and/or spelling can go into effect without prior notice.

In the event of changing market conditions, security requirements and changes to legal regulations, Digidentity BV reserves the right to make changes and adjustments to this documentation. Scheduled changes will be announced on the Digidentity website in a timely manner. The announcement will include the date the revised version of this CPS will go into effect. If applicable, the changes will also be made to the general terms and conditions that apply to the service provided by Digidentity, which are published on Digidentity's website.

The new CPS will be displayed upon logging in and it must be explicitly approved by the user. If a user does not or cannot read the modified documents due to the user's own actions or lack of actions, the user will be held fully responsible. Digidentity cannot accept any responsibility in this regard, or for any adverse effects on the user.

Users can provide comments to this CPS regarding its content. However, Digidentity BV retains the sole authority to make any changes to the documentation.

Changes to this CPS, whereby Digidentity is required to notify users, will appear as an announcement on the Digidentity website at least 30 days prior to the effective date of the new CPS.

Registration, identification and authentication

1.7. *Application method*

Digidentity provides an offer on its website, www.digidentity.eu. Upon acceptance of this offer by a prospective certificate holder, Digidentity is required to process a certificate application and to initiate a verification procedure as specified in section 2.3. If the Authentication process is successful, Digidentity produces the requested certificate and issues it to the certificate holder. This CPS is available to the user via the Digidentity website.

1.8. *Process steps*

- The registration process, whereby the applicant's identity is registered and whereby Digidentity acts as the Registration Authority (RA);
- The authentication process, whereby the applicant's identity is verified, whereby Digidentity acts as the Registration Authority;
- The certification process according to the requirements set forth by the ETSI TS 101 456, whereby Digidentity acts as the Certification Authority (CA).

1.9. *Verification*

The following user or subscriber information is registered in order to determine the user's identity:

a) Verification by Digidentity
   a. User name
      - Verifies that the user name only occurs once
   b. Password
      - Verifies password strength
   c. E-Mail address
      - The user receives an e-mail with a link to the e-mail address so that the e-mail address is verified upon clicking the link
   d. Mobile telephone number
      - The user receives an SMS code on his/her mobile phone; this code is to be entered during the registration process
   e. Secondary verification by submitting a payment of € 0.01 through iDeal
      - We use this to verify the user's name and city of residence

b) Verification by AuSO
   a. Surname
   b. First name with initials
   c. Date of birth
   d. Place of birth
   e. Postal code and street number
   f. Individual service number
   g. Type of identification and number

c) If there is a reason to do so, VIS investigates whether the identity card has been reported missing or stolen. If the VIS investigation results in a so-called HIT, the relevant agencies will be notified.

d) The copy of the identity card is examined for any fraudulent characteristics.

When applying for an organization domain certificate, an individual domain certificate is required and MachtigingOnline registers the following additional information:

e) Verification of company or organization via Chamber of Commerce
    a. Verification of name
    b. Verification of number
    c. Verification of directors
    d. If a company or organization is not registered with the Chamber of Commerce, the organization's statutes, memorandum of association or an order in council may also suffice
    e. If it is for EV, a call is made to the organization's telephone number.
    f. If it is for EV, the insolvency register of Judicial Services and the Supreme Court of the Netherlands are reviewed.
    g. If it is for EV, the EU terrorist list and the web trust list are checked.
    h. If a suspicious or fraudulent application is rejected, it will be maintained in our list, new applications will also be validated against this list.

f) FQDN Verification
    a. The domain name is verified by official registers such as the SIDN (Stichting Internet Domeinregistratie Nederland), IANA (Internet Assigned Numbers Authority and UnifiedRoot)
       - The domain name is checked to see if it is the property of the applicant organization.

g) When applying for a Services certificate within the organization domain, an authentication certificate linked to a person within the company domain is required.

h) The application process for EV certificates uses data that has already been validated if this data has been validated previously. If this data is older than 13 months, it will be revalidated.

1.10. *Purpose and types of certificates*

Digidentity can issue trusted certificates. They are actually only issued as server certificates. Besides the fact that encryption certificates are generally not issued, the private key is not escrowed. Messages that are encrypted with the private key will be lost of this key is lost or becomes defective. The holder of the private key bears full responsibility for any damages that occur due to this type of situation.

Furthermore, Digidentity does not issue any certificates linked to certain professions nor does it review any registers linked to certain professions before issuing a certificate.

A user can also create a SSCD alongside his existing SSCD with secondary credentials and can delegate the use of this alternate SSCD.

1.10.1. Digidentity

Personal authentication certificate

OID: 1.3.6.1.4.1.34471.1.2.3.1

The personal authentication certificate contains the public key for identifying and authenticating an individual. It can be used for the electronic, trusted identification and authentication of individuals. This applies to the identification of individuals by other individuals as well as to the identification between individuals and automated resources. A personal authentication certificate is valid for five years.

Personal signing certificate

OID: 1.3.6.1.4.1.34471.1.2.3.2

The personal signing certificate contains the public key for the advanced electronic signature. The personal signing certificate is valid for five years.

1.10.2. MachtigingOnline

Employee authentication certificate

OID: 1.3.6.1.4.1.34471.1.2.5.1

The personal authentication certificate contains the public key for identifying and authenticating an employee within an organization. It can be used for the trusted, electronic identification and authentication of employees. This applies to the identification of employees by other employees and to the identification between employees and automated resources. The employee authentication certificate is valid for five years. Authentication certificates that are issued under this CPS cannot be used for identifying individuals in those cases where the law requires that their identity can only be determined by the document specified in the Compulsory Identification Act.

Employee signing certificate

OID: 1.3.6.1.4.1.34471.1.2.5.2

The employee signing certificate contains the public key for the advanced electronic signature. The employee signing certificate is valid for five years.

1.10.3. Digidentity SSL

SSL authentication certificate

Authentication certificates that are issued under this CP can be used electronically for the trusted identification and authentication of the service that is provided by the organizational entity, which is responsible for the related service.

OID: 1.3.6.1.4.1.34471.1.2.5.4

SSL trusted certificate

Trusted certificates that are issued under this CP can be used for protecting the confidentiality of information that is exchanged and/or stored in electronic format.

OID: 1.3.6.1.4.1.34471.1.2.5.5

SSL Server certificate

Server certificates that are issued under this CP can be used for securing a connection between a certain client and a server that belongs to the organizational unit, which is designated as the subscriber in the corresponding certificate.

OID 1.3.6.1.4.1.34471.1.2.5.6

1.10.4. Digidentity EV

EV Server certificate

EV Server certificates that are issued under this CP can be used for securing a connection between a certain client and a server that belongs to the organizational unit, which is designated as the subscriber in the corresponding certificate.

OID: `1.3.6.1.4.1.34471.1.2.5.7`

Verification certificate by “relying parties”

Digidentity registers all generated and revoked certificates. Revoked certificates are published in a CRL for so-called “relying parties” for verification.

1.11. *Unique names*

The Distinguished Name (unique name), which is assigned to the Certificate Holder of an Advanced Certificate for a CA of Digidentity that is subject to this CPS, will always be unique for this Certificate Holder and will not be issued to another Certificate Holder. Pseudonyms are never permitted.

a) The spelling of a persons’ name must match the spelling on the identity card and must not have added or missing punctuation marks, like diaeresis.
b) If the same name occurs more than once, a numeric suffix will be added to differentiate the name with the aid of Subject.serialNumber.

Whenever parties do not agree to the use of the names registered in the certificate that identify the certificate holder, Digidentity BV will make the final decision after considering the interests of the parties involved, insofar as this is not bound by Dutch law or other applicable regulations.

1.12. *Certificate holder*

A certificate holder is the “subject” of a certificate, an entity recognised as the holder of the private key that is linked to the public key registered in the certificate. A certificate holder can determine and authenticate the identity within the boundaries of the applicable rules with the aid of the Digidentity certificates.

A natural person who is a certificate holder, is actually also the user at Digidentity. As such, he/she is the contracting party of Digidentity and is given the right to use his/her certificate together with the key pair in accordance with this CPS based on prescribed verifications and procedures. With MachtigingOnline the organization is the certificate holder and the natural person is the user.

A natural person can also create a secondary credential for a certificate and revoke it at any time. In this case, the use of the key can be explicitly delegated. A separate SSCD is created for a secondary credential. This SSCD is then only used for that purpose. An SSCD with secondary credential is for personal use and the user is free to use it as he wishes. An SSCD with secondary credential can also be delegated; in this case the SSCD will only be used for the delegated purpose.

Obligations

1.13. *Obligations of Digidentity*

All duties performed by Digidentity within the scope of this CPS and the agreements that may contain this CPS, are performed vigorously in consideration of the applicable procedures and in compliance with applicable laws and regulations.

Digidentity shall configure its TTP service, equipment, software, telecommunications facilities, system administration and procedures in accordance with the guidelines of ETSI TS 101 456 and Directive No. 1999/93/EG.

Digidentity operates according to European and Dutch laws and regulations and conforms to the European directive for electronic signatures (1999/93/EG) and to the Law and General Administrative Order on Electronic Signatures along with the corresponding guidelines and the Compulsory Identification Act.

Digidentity shall ensure that any AuSO engaged as a third party by Digidentity shall also configure its TTP service, equipment, software, telecommunications facilities, system administration and procedures in accordance with the ETSI TS 101 456 guidelines and Directive No. 1999/93/EG. In terms of identification, Digidentity will exchange personal information with its sub-contractors in order to be able to complete the identification process. Digidentity and its sub-contractors strictly comply with relevant laws and regulations when registering, processing and archiving personal information.

Digidentity will undergo an assessment each year by a certification institute, who can show that Digidentity and its entities fulfil the specified requirements.

Digidentity is responsible for the level and the quality of the resources they provide. The conformance to specified requirements is proven through certification.

Digidentity is responsible for the choice of systems and equipment and releases the subscriber or individual from violation of intellectual property by CPS.

1.14. *Certificate hierarchy*

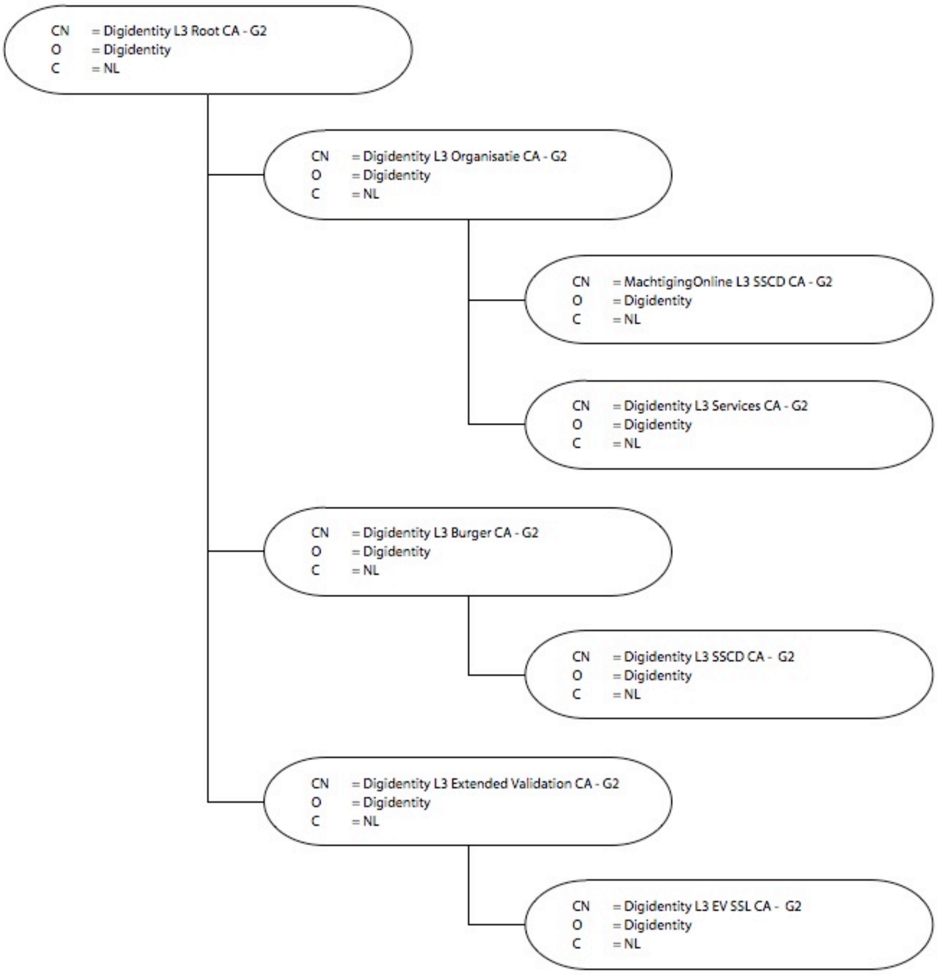
The Public Key Infrastructure of Digidentity is implemented in a “three-level certification hierarchy”.

At the highest level, Digidentity signs the root, “Digidentity L3 Root CA – G2” the Digidentity L3 (Individual, Organization or Extended Validation) CA – G2. This CA certificate then signs the Digidentity purpose-specific CA certificate. Digidentity CA then uses this Certificate to sign the Certificates of its users. Each Certificate that is issued under this CPS and the corresponding CP contains a DID that refers to this CPS.

The foundation is the following number that the Normaliseringinstituut (Dutch standardisation institute) has assigned to Digidentity. The DID structure is as follows:

Category	Number
ISO assigned OIDs	1
ISO Identified Organization	3
US Department of Defense	6
OID assignments from 1.3.6.1 - Internet	1
Internet Private	4
Digidentity	34471
CSP	1
Domain Organization	2 1
CA	1 L3 root 2 in organization domain 3 in individual domain 4 Machtiging Online L3 SSCD 5 Digidentity L3 Services 6 Digidentity L3 SSCD 7 in Extended Validation domain 8 Digidentity L3 EV SSL

Digidentity Hierarchy


CN = Digidentity L3 Root CA - G2
O = Digidentity
C = NL
CN = Digidentity L3 Organisatie CA - G2
O = Digidentity
C = NL
CN = MachtigingOnline L3 SSCD CA - G2
O = Digidentity
C = NL
CN = Digidentity L3 Services CA - G2
O = Digidentity
C = NL
CN = Digidentity L3 Burger CA - G2
O = Digidentity
C = NL
CN = Digidentity L3 SSCD CA - G2
O = Digidentity
C = NL
CN = Digidentity L3 Extended Validation CA - G2
O = Digidentity
C = NL
CN = Digidentity L3 EV SSL CA - G2
O = Digidentity
C = NL

User and subscriber obligations

Data accuracy and secure use

The user promises that:

a) The data copied from the Identity Card onto the Certificate is accurate and complete at all times
b) Any changes to the data will be applied to the information in the account as soon as possible
c) The Certificate will be used in accordance with applicable laws and regulations (such as privacy regulations, the Dutch Civil Code and the Telecommunications Act, etc.)
d) The Certificate will be used in accordance with this CPS and the agreements that may contain this CPS and that are connected with this CPS
e) The certificate holder(s) will comply with the provisions contained in this CPS and the contractual agreements that may contain this CPS
f) Reasonable precautions will be taken against unauthorised use of his or her private key
g) The CA will be notified without delay if one of the following events occurs before the certificate's expiration date:

   a. The subscriber has lost the private key or it has been stolen, or
   b. The verification of the subscriber's key is lost due to compromised activation information (for example the user name / password or PUK letter), and/or
   c. Inaccuracy or changes to the content of the certificate as reported to the subscriber

h) The user will only designate a SSCD to organizations that take additional precautions so that SSCDs with secondary credentials will only be implemented for their designated purpose, for example, Mass-Signing. The user must apply for a separate SSCD for the purpose of Mass-Signing. This certificate is expressly meant for Mass-Signing and can be revoked by the user in the Digidentity environment at any time. The user is always responsible for the proper use of his/her certificates.

The user exercises due diligence regarding the choice and (physical) security of software, equipment and telecommunications facilities, and is also responsible for the availability of the information and communications systems, which are deployed to receive and send electronic messages. The user will take adequate precautions to protect his/her system against viruses and other inappropriate software elements.

The subscriber promises that:

a) The certificate will be revoked as soon as possible after employment has been terminated
b) Authorisations granted according to permissions are issued and revoked in a timely manner
c) The equipment that generates and uses the private key for SSL certificates is adequately protected against access to the private key in conformance with guidelines and requirements
d) All SSL certificate applications are for domains and brand names that are the subscriber's property or that are licensed for the subscriber's use, and that the appropriate proof can be provided upon request
e) Subscriber will take additional precautions so that SSCDs with secondary credentials are only used for their designated purpose.

Limitations of use

The user will comply with applicable Dutch, European and other (inter)national laws, regulations and the provisions of this CPS with regard to the purpose for which he wishes to use this Certificate, the choice of the other party with whom he exchanges electronic messages and/or transactions, and in particular, the content of the message and/or transaction exchange that he would like to manage with the Certificate, including any agreements he may have concluded with other Parties and any resulting implementations. The user and the Certificate Holder(s) are prohibited from using the Certificate for any other purpose than the purpose stated in the CP, this CPS or in the Certificate itself.

Violations

The user and/or Certificate Holder will bear full responsibility for any violation of the scope or the purpose for which the Certificate has been issued.

Certificate property rights

The Certificate is and will remain the property of Digidentity BV. The user is only given the right to use the Certificate with the key pair in accordance with this CPS.

1.15. *Obligations of the relying parties*

A relying party is every natural person or legal entity that acts based on the trust of a received certificate. A relying party will only trust the Certificate if:

a) The validity of the certificate has been verified
b) The full chain of certificates up to the root certificate belonging to the official government of the Netherlands is valid
c) The Certificate has not been revoked
d) The party has made itself aware of the limitations regarding the use of the Certificate as stated in this CPS
e) The status information, authenticity of this information verified by the electronic signature that has signed the information and the corresponding certification path will be verified upon accessing the Certificate.

1.16. *Liability*

Digidentity is liable for the EV certificates it issues in accordance with the requirements of Webtrust. Dutch law (WEH) and the PvE of PKIoverheid are also applicable. This means that Digidentity can be held liable for damages that natural persons or legal entities encounter while they could have reasonably trusted this Certificate, in connection with:

a) The accuracy at the time the certificate was issued, of all information contained in the Qualified Certificate and the inclusion in the Qualified Certificate of all information that is prescribed for such a Certificate.

b) The assurance that the signer identified in the Qualified Certificate at the time the Certificate was issued, was the holder of the information for creating the signature, which matched the information provided or identified in the Certificate for verifying the signature.

c) The assurance that the information for creating the signature and for verifying the signature can be used to balance each other.

This above holds true unless Digidentity can prove it has not been negligent in its actions and the user has not fulfilled its obligations as stated in article 3.3. of this CPS. Digidentity is insured against this liability.

1.17. *Financial responsibility and liability*

Unless explicitly agreed otherwise, Digidentity does not set any limits to the value of the transactions for which qualified certificates can be used.

Except for those cases where Digidentity proves that it cannot be held liable and subject to the provisions of this CPS, Digidentity assumes liability for both direct and indirect damages resulting from a damaging event or series of damaging events up to a maximum amount of one million Euros. The above does not affect the option to take action against the party to whom the damage can be attributed.

1.18. *Confidentiality*

Digidentity will not disclose the information provided by the Certificate holders without the user's permission, a court order or other legal basis. Certificates can only be released if the Certificate Holder has given permission to do so.

If and where applicable, Digidentity shall ensure that the existing privacy laws and regulations are observed. The activities and administration of Digidentity are registered with the Dutch Data Protection Authority under reference m1451668.

1.19. *Enforcement*

The complaints procedure is published on Digidentity's website.
Any complaints regarding the services provided within the scope of this CPS can be submitted to Digidentity. This will activate the Digidentity complaints procedure.

Disputes can be presented to the ordinary competent court in the jurisdiction where Digidentity BV is headquartered. All agreements between the user and Digidentity are subject to Dutch law.

1.20. *Termination of service*

The Digidentity certification service can be terminated unilaterally by Digidentity BV in accordance with legal provisions. A planned termination shall be announced at least 2 months prior to termination to both the OPTA and Logius, as well as to all parties involved. Upon terminating the certification service, the CRL will still be accessible for relying parties for up to 6 months after termination.

If Digidentity ends the service, it will make every effort to arrange for its issued Advanced certificates to be acquired by a different, registered (with OPTA) service provider. If the activities are not acquired by a different certification service provider, all issued certificates will be blocked.

The Private keys of Digidentity will be destroyed or rendered useless in such a way that they can no longer be recovered or re-used.

The CRL and the archives will remain available for 7 years after the last certificate has expired. Digidentity has secured sufficient financial resources to meet this obligation at all times once the service has been terminated. This assurance is obtained by transferring this contractual obligation to a third party or by obtaining a statement from a third party who will promise to cover this obligation.

1.21. *Certificate management*

Issuing certificates

A certificate is produced by the Certification Authority (CA) of Digidentity upon acceptance of the application. This certificate is available as a SAAS (Signing as a Service) model. The user's Private Key is stored securely on the Digidentity servers and can be issued remotely for authentication and/non-repudiation.

As soon as the Certificate has been created, it is available to the user. The CA will publish the Certificate to the internal Digidentity certificates database and is made available to the user in his Digidentity safe. The user is responsible for publishing and distributing his certificate.

After the user has logged in for the first time with his user name and password, he will gain access to the key pairs for authentication and/or non-repudiation purposes. The private keys only work inside the HSM and can only perform an action after explicit approval by the user. Approval is given by entering the secret code that is only generated once. This guarantees that the use of the private key is only made available to authorised persons.

Acceptance

The Certificate is deemed to have been accepted by the user once it is issued. The Certificate will be displayed on the screen and the user can confirm acceptance after verifying the accuracy of the content. The certificate is only released for use once the content has been confirmed.

The user and the Certificate Holder must verify the information for accuracy before using the Certificate.
The user bears full risk and responsibility for inaccuracies in a Certificate that has not been revoked. The user must report any inaccuracies to Digidentity immediately, but in any case by the 3rd day after receipt of the Certificate. If not, Digidentity can never be held liable for such inaccuracies.

The user must realize that the Certificate can only be used for placing an electronic signature and for authentication, depending on the type and in compliance with the other limitations that have been communicated to the user.

Validity

A certificate's expiration date is specified in the certificate. The certificate holder is responsible for applying for new or replacement certificates in a timely manner. Digidentity notifies its users in a timely manner when a certificate is about to expire. Certificates that are issued to end users by Digidentity are valid for a period of up to 5 years from the date of issue, or up to the maximum time period specified by the issuing CA.

Change and renewal

A request to renew a Certificate must be submitted by the user. This always results in a new key pair once all information has been compared with the information from the old certificate. The request can only be submitted electronically with the old certificate that has not yet expired, for the same domain and/or organization at the same level. If the certificate has been revoked or has expired, the user will have to go through the whole registration process again.

Validation of revoked Certificates

All information for Certificate Holders and relying parties related to the process of issuing certificates, including the information regarding revocation of certificates (Revocation Status Information) is available via the published CRL.

Suspension and revocation of Certificates

Certificates issued under this CPS cannot be suspended.

Certificates issued under this CPS can be revoked. Revocation of a Certificate means that the Certificate has been invalidated permanently and can no longer be trusted.

A request for revocation of a Certificate must be submitted by an authorised person via the Digidentity website. The user can revoke his resource and his certificates at any time after logging in to the website. As an alternative, the user can also deactivate his safe with the aid of the PUK and PIN code that were provided to him for activation. A safe can also be reactivated once the entire registration process has been completed again. However, a new application will have to be submitted since the resource and the certificates have already been revoked, The certificate holder will receive an e-mail confirmation regarding the status change.

If the user no longer has a PUK and/or telephone and password, a request to revoke a certificate can also be presented to the Digidentity headquarters. The certificate owner must prove his identity with a valid identity card. A Digidentity employee will record the reason for revocation during this request for revocation. As an alternate method, the user can also e-mail his identity card referencing his user name.

Circumstances leading to revocation

The following circumstances lead to a certificate being revoked:

a) Legal regulations
b) Loss or possible theft of the PUK code
c) Loss or possible theft of mobile telephone
d) Loss or possible theft of SIM card
e) Certificate is no longer correct, the qualifications/data are no longer accurate
f) Private key has been compromised

Authority to revoke a certificate

A certificate can be revoked by:

a) The user or his legal representative
b) A third party represented by the certificate holder, whose representation is evidenced by an authorisation that has been submitted to Machtiging Online
c) The subscriber
d) Digidentity BV.

Digidentity RA must revoke a certificate if it receives notice and sufficient evidence of the user and/or certificate holder's death.

If an authorised employee of Digidentity B.V. revokes a certificate, he or she must specify the reason for revocation.

Actually, neither the RA nor the CA of Digidentity is required to take the initiative to revoke a certificate; nevertheless, they will start the revocation process after receiving the report and request for revocation from the certificate holder and after receiving Digidentity's positive identification. However, unlike revocation via the usual electronic means, this revocation will not always take place during the established 4 hour time frame.
In the event a CA is compromised, all remaining certificates will be revoked by Digidentity.

Repealing a revocation

The revocation of a certificate is final and cannot be reversed.
A certificate is considered to be revoked once the revocation has been published on the Digidentity website. This is maximum 4 hours after the request for revocation has been submitted..

Relationship between the different CA domains

All RA officers have Digidentity organization certificates.

All users have a Digidentity account. They are a prerequisite for a MachtigingOnline (online authorisation) account.

A MachtigingOnline account is a prerequisite for authorisation to apply for SSL certificates.

1.22. *CRL availability and issuing frequency*

Revocation status information is available 24 hours a day, 7 days a week via the website. In the event of system failures, maintenance activities or other factors that are beyond Digidentity's control, Digidentity will make every effort to ensure that this information does not remain unavailable for more than 4 hours.

The revocation status information is refreshed at least once every four hours in the Certificate Revocation List. The CRL can be reviewed at any time via the LDAP server. Inclusion of a certificate in the CRL is the final confirmation that a certificate has been blocked/revoked. Certificates are reported on the CRL for at least seven years, even once they have expired.

1.23. *Document archiving*

Digidentity shall record all registration information, including the following:

a) Logging the authentication process
b) Logging the lifecycle of the certificate
c) Logging the use of private keys
d) Logging the updates in the registration information

By entering into the agreement and/or actually using the certificate, the user and/or the certificate holder agrees to the above provisions.

1.24. *Physical and technical security*

Infrastructure

The information security infrastructure, which is necessary for managing security in CSP Digidentity, will be maintained at all times; each change that can have an effect on the security level must be approved by the Digidentity management team. The security management measures and the operational procedures for CSP facilities, systems and information resources that are employed for the purpose of providing certification services, have been documented, implemented and are being maintained.

Logs and Protocols

The following events are automatically logged along with the date and time:

a) All relevant data for logging a user into the system
b) All authentication data via the system
c) The generation of CA key pairs
d) All relevant events for the registration process of a certificate
e) All relevant data for publishing digital certificates
f) All relevant data for publishing revocation lists
g) All revocation details of a certificate, including the reason for revocation
h) All network traffic from and to the trusted computers

The following events are also added to the protocol:

a) Role changes
b) Report of suspected key abuse
c) Incident reports
d) All events related to managing the secured environment
e) All changes to the back-up configuration
f) All events related to the back-up process
g) All information related to the installation of new or updated software
h) All information related to hardware updates
i) Everything related to shutdowns and restarts.

Logs and Protocols are securely stored online. Only authorised personnel have access to these files. Backups are generated on a regular basis. Files are archived to CD after a certain time period. These CDs are stored in a secured area for 7 years. All issued public keys are kept on file for 7 years after the certificate has been terminated.

Identity cards

A copy of the certificate holder's identity card with signature is stored physically in a locked cabinet as well as online in a secure area. Only authorised personnel have access to these files. Backups are generated on a regular basis. The files are archived to CD after a certain period of time. These CDs are stored in a locked safe for 7 years.

Network security measures

The firewall and computer systems are kept at the current level of technology. All systems are minimally configured with only the most essential software. The systems and firewall configurations are regularly audited by an independent organization. All stored data is uniquely encrypted per user in the database.

Appendix A

The table below shows the profiles that are active in the above mentioned CAs

CA CN=	Active profiles
Digidentity L3 Root CA - G2	CA certificate
Digidentity L3 Organization CA - G2	CA certificate
Digidentity L3 Individual CA - G2	CA certificate
Machtiging Online L3 SSCD CA - G2	Authentication certificate Non-repudiation certificate
Digidentity L3 Services CA - G2	Authentication Trust Server
Digidentity L3 EV CA - G2	EV Server
Digidentity L3 SSCD CA - G2	Authentication certificate Non-repudiation certificate

End user certificates that are issued by a CA are valid for 5 years from the date of issue or until the maximum date provided by the issuing CA. SSL certificates are valid for 1 or 2 years.

Certificate Generation Component

Only keys that use SHA-256-RSA, 2048 bit RSA encryption are authorised. A key length of 4096 bit RSA applies to all (sub) CAs.

Basic attributes for all user certificates

Attribute		Description	Type	Details
Version	V	MUST be set to 2 (X.509v3).	Integer	Specifies the version of the certificate, the value 2 stands for X509 version 3.
SerialNumber	V	A unique serial number that MUST identify the certificate on the issuing CA domain.	Integer	-
Signature	V	MUST be configured for the algorithm that has been established by the PA.	OID	Must be the same as the signatureAlgorithm field. Only SHA-256 with RSA encryption is permitted for maximum interoperability.
Issuer	V	Must contain a Distinguished Name (DN). The field has the attributes listed below:		Attributes other than those listed below MUST NOT be used. The attributes that are used MUST be equal to the same attributes in the Subject field of the CSP certificate (for validation purposes).
Issuer .countryName	V	Must contain the country code of the country where the organization issuing the certificate is located.	Printable String	C = NL
Issuer. OrganizationName	V	Full name based on accepted document or basic registration	UTF8String	O=Digidentity B.V.
Issuer. commonName	V	Must contain the name of the CA in accordance with accepted document or basic registration, optionally supplemented by the Domain identifier and/or the types of certificates that are supported.	UTF8String	According to CAs table
Validity	V	MUST specify the validity period of the certificates according to RFC 5280.	UTCTime	Max 5 years or until expiration date of CA
Subject	V	The attributes that are used to describe the subject (end user) MUST assign a unique name to the subject. This field has the following attributes:		Must contain a Distinguished Name (DN). Attributes other than the ones named below MUST NOT be used.
Subject. countryName	V	Fixed value: C=NL, according to ISO 3166	PrintableString	C=NL
Subject. commonName	V	The commonName attribute must be entered in accordance with the above paragraph about Naming Convention Subject.commonName .	UTF8String	Identical to MRZ data from WID or If the service has a DNS name, it MUST be noted in the common-Name field as a "fully-qualified domain name"
Subject. organizationName	O	The use of organizationName is not permitted for certificates in the individual domain; the organization domain contains the organization name.	UTF8String	Required if in an organization hierarchy.
Subject. locality	O	Only for EV addres of organization		The same as with chamber of commerce
Subject. street address	O	Only for EV addres of organization		The same as with chamber of commerce

Subject. state/province	O	Only for EV address of organization		The same as with chamber of commerce
Subject. postal code	O	Only for EV address of organization		The same as with chamber of commerce
Subject. jurisdictionOfIncorporationCountryName	O	Only for EV		(OID: 1.3.6.1.4.1.311.60.2.1.3) always NL
Subject. business category	O	Only for EV		Private organization, Government organization
Subject. organizationalUnitName	O	Certificates in the individual domain are not permitted to use organizationalUnitName; the organization domain contains the organization name		
Subject. serialNumber	O	A number to be determined by the CSP. The combination of CommonName and Serialnumber MUST be unique within the CSP context.	Printable String	According to RA delivery. Numeric 10 numbers with leading zeros. Required, unless this is a services certificate. If this is an EV certificate, this is the organization's Chamber of Commerce number; it is blank for government organizations.
subjectPublicKeyInfo	V	Includes the public key.		Contains the public key. Identifies the algorithm that can be used with the key.

Standard extensions

Attribute		Description	Type	Details
authorityKeyIdentifier	V	The algorithm to generate the AuthorityKey MUST be configured for the algorithm that has been established by the PA.	BitString	The value must contain the SHA-1 hash from the authorityKey (the CSP/CA public key CSP/CA).
SubjectKeyIdentifier	V	The algorithm to generate the subjectKey MUST be configured for the algorithm that has been established by the PA.	BitString	The value must contain the SHA-1 hash from the subjectKey (the certificate holder's public key).
KeyUsage	V	This attribute extension specifies the intended purpose of the key that is registered in the certificate. The PKI for the government contains different bits in the keyUsage extension per certificate type. Authentication certificates must contain the digitalSignature bit and be marked as essential. No other keyUsage can be combined with this. Certificates for electronic signatures must contain the non-repudiation bit and be marked as essential. No other keyUsage can be combined with this.	BitString	In accordance with description
CertificatePolicies	V	MUST contain the OID from the certificate policy (CP), the URI from the certification practice statement (CPS), and a user note. The DID schema to be used in the PKI for the government is explained in the CP.	OID, String, String	In accordance with description
SubjectAltName	V	MUST be used with and must contain a unique, personal global number.		Must contain a unique identifier in the othername attribute. Attributes other than the ones mentioned here below MUST NOT be used.
SubjectAltName. otherName	V	MUST be used with a unique number that identifies the certificate holder.	Microsoft UPN	OID-UUID UUID is unique for each certificate.
SubjectAltName. DNSname	V	MUST be used for EV certificates with the server FQDN as registered in the Common name	FQDN	Server FQDN, the same as the Subject. commonName
CRLDistributionPoints	V	MUST contain the URI from a CRL distribution point.		Is identified in the certificate profile table.
ExtKeyUsage	O	Not used.		Not used in the Individual domain. This field is also referred to as the enhancedKeyUsage field. Is defined in the certificate profile table.

Private extensions

Attribute		Description	Type	Details
QcStatement	O	Certificates for electronic signatures MUST specify that these certificates are issued as Advanced Certificates that conform to the European Directive. This conformity is specified by registering the id-etsi-qcs-QcCompliance statement in this extension. The authenticity certificates and the trusted certificates are NOT allowed to use this extension.	OID	Not used

Basic attributes for all sub CA profiles

Attribute		Description	Type	Details
Version	V	MUST be set to 2 (X.509v3).	Integer	Specifies the certificate version; the value 2 stands for X.509 version 3.
SerialNumber	V	A serial number that MUST uniquely identify the certificate on the issuing CA domain.	Integer	-
Signature	V	MUST be set to the algorithm that has been established by the PA.	OID	Must be the same as the signatureAlgorithm field. Only SHA-256 with RSA encryption is allowed for maximum interoperability.
Issuer	V	Must contain a Distinguished Name (DN). The field has the attributes listed below:		Attributes other than the ones listed below MUST NOT be used. The attributes that are used MUST be the same as the attributes with the same name in the Subject field of the CSP certificate (for validation purposes).
Issuer .countryName	V	Must contain the country code of the country where the issuing organization of the certificate is located.	Printable String	C = NL
Issuer. OrganizationName	V	Full name in accordance with the accepted document or basic registration	UTF8String	O=Digidentity B.V.
Issuer. commonName	V	Must contain the name of the CA in accordance with the accepted document or basic registration, optionally supplemented by the Domain type and/or types of certificates that are supported.	UTF8String	In accordance with CA table
Validity	V	MUST define the validity period of the certificate in accordance with RFC 5280.	UTCTime	In accordance with CA table

Attribute		Description	Type	Details
Subject	V	The attributes that are used to describe the subject (end user) MUST give the subject a unique name. The field has the following attributes:		Must contain a Distinguished Name (DN). Attributes other than the ones specified below MUST NOT be used.
Subject. countryName	V	Fixed value: C=NL, according to ISO 3166	PrintableString	C=NL
Subject. commonName	V	The commonName attribute must be implemented according to the above naming convention Subject.commonName.	UTF8String	In accordance with CA table
Subject. organizationName	O	For certificates in the individual domain the use of organizationName is not permitted; it contains the organization name in the organization domain	UTF8String	O=Digidentity B.V.
subjectPublicKeyInfo	V	Includes the public key.		Contains the public key, identifies the algorithm that can be used with the key.

Standard extensions for CA profiles

Attribute		Description	Type	Details
SubjectKeyIdentifier	V	The algorithm that is used to generate the subjectKey MUST be set to the same algorithm that has been established by PA.	BitString	The value must contain SHA-1 hash from the subjectKey (public key from the certificate holder).
BasicContraint		The "CA" field MUST be set to "True" or it must be omitted. Pathlen=-1		
KeyUsage	V	This attribute extension specifies the intended purpose of the key registered in the certificate. The PKI for the government contains different bits per certificate type in the keyUsage extension. Authentication certificates must contain the digitalSignature bit and it must be marked as essential. No other keyUsage can be combined with this. Trusted certificates must contain keyEncipherment and dataEncipherment bits and must be marked as essential. As an option, this can be combined with the keyAgreement bit. No other keyUsage can be combined with this. Electronic signature certificates must contain a non-repudiation bit and they must be marked as essential. No other keyUsage can be combined with this.	BitString	CRL Signer, Certificate Signer.
CertificatePolicies	V		OID, String, String	Policy: 2.5.29.31.0 http://pki.digidenity.eu/validatie

All CAs conform to the below CRL profile

Attribute		Description	Type	Details
Version	V	MUST be set to 2 (X.509v3).	Integer	Describes the certificate version; value 2 stands for X.509 version 3.
Signature	V	MUST be set to the algorithm that has been established by the PA.	OID	Must be equal to the signatureAlgorithm field. Only SHA-256 met RSA encryption is allowed for maximum interoperability.
Issuer	V	Must contain a Distinguished Name (DN). The field has the following attributes:		Attributes other than the ones mentioned below MUST NOT be used. The attributes that are used MUST be equal to the same attributes in the Subject field of the CSP certificate (for validation purposes).
Issuer .countryName	V	Must contain the country code of the country where the certificate issuing organization is located.	Printable String	C = NL
Issuer. OrganizationName	V	Full name in accordance with accepted document or basic registration	UTF8String	O=Digidentity B.V.
Issuer. commonName	V	Must contain the name of the CA in accordance with the accepted document or basic registration, optionally supplemented by the Domain name and/or the types of certificates that are supported.	UTF8String	Conforms to CAs table
Issuer.organizationalUnitName	O	Optional name of a sub-organization. This field MUST NOT contain a function name or such information. It may contain the types of certificates that are supported.	ETSI TS 102280: 5.2.4	A possible future enhancement
ThisUpdate	V		UTCTime	CRL Issue date
NextUpdate	V		UTCTime	This is the latest date an update can be expected, Earlier updates are also possible. (4 hours from ThisUpdate)
RevokedCertificates	V		Serial number,UTC Time	

CRL

Attribute		Description	Type	Details
CRLNumber	V	This attribute MUST contain a sequentially incremental number that supports the establishment of the sequential order of CRLs (the CSP provides the numbering to the CRL).	Integer	

OID Numbers

Each CP is uniquely identified by the OID, in accordance with the table below.

	CA Profile	OID	KeyUsage	Qc_statement
Digidenitity L3 Root CA –G2	CSP-Root	1.3.6.1.4.1.34471.1.2.1.1		
Digidentity L3 Organisatie CA - G2	CSP-Organization	1.3.6.1.4.1.34471.1.2.1.2		
Digidentity L3 Burger CA - G2	CSP-Individual	1.3.6.1.4.1.34471.1.2.1.3		
Digidentity L3 Extended Validation CA - G2	CSP-EV SSL	1.3.6.1.4.1.34471.1.2.1.7		
MachtigingOnline L3 SSCD CA - G2		1.3.6.1.4.1.34471.1.2.1.4		
	SSCD-A-Organization	1.3.6.1.4.1.34471.1.2.5.1	0,2,4	
	SSCD-O-Organization	1.3.6.1.4.1.34471.1.2.5.2	-	
	SSCD-E-Organization	1.3.6.1.4.1.34471.1.2.5.3	0,4	
Digidentity L3 Services CA - G2		1.3.6.1.4.1.34471.1.2.1.5		
	SSL-A-Organization	1.3.6.1.4.1.34471.1.2.5.4	2,4	
	SSL-V-Organization	1.3.6.1.4.1.34471.1.2.5.5	2,4	
	SSL-S-Organization	1.3.6.1.4.1.34471.1.2.5.6	1,2,4	
Digidentity L3 SSCD CA - G2		1.3.6.1.4.1.34471.1.2.1.6		
	SSCD-A- Individual	1.3.6.1.4.1.34471.1.2.3.1,	-	
	SSCD-O- Individual	1.3.6.1.4.1.34471.1.2.3.2	-	
	SSCD-E- Individual	1.3.6.1.4.1.34471.1.2.3.3.	-	
Digidentity L3 EV SSL CA – G2		1.3.6.1.4.1.34471.1.2.1.8		
	SSL-EV	1.3.6.1.4.1.34471.1.2.5.7	1,2	

Key usage legend

Number	Meaning
0	Any keyusage
1	SSL server
2	SSL client
4	E-mail security

Certificate use for individuals

Certificates issued under this CP are for communication purposes by individual certificate holders.

[1.3.6.1.4.1.34471.1.2.3.1] Authentication certificates that are issued under this CP, can be used for the trusted identification and authentication of individuals electronically. This applies to the identification of individuals by other individuals and between individuals and automated devices.

[1.3.6.1.4.1.34471.1.2.3.2] Electronic signature certificates that are issued under this CP can be used to verify electronic signatures, which are subject to the "same legal consequences as a handwritten signature", as specified in article 15a, first and second paragraph, in Title 1 of Book 3 of the Dutch Civil Code under section 1A and are Advanced Certificates as stated in article 1.1, paragraph ss of the Telecommunications Act.

Certificate use for Organization

The use of certificates issued under this CP is related to communication by certificate holders in the role of employee with the subscriber.

Certificate use for Organization user certificates

The use of certificates issued under this CP is related to communication by certificate holders who act on behalf of the subscriber.

[1.3.6.1.4.1.34471.1.2.5.1] Authentication certificates that are issued under this CP can be used for the trusted identification and authentication of individuals, organizations and devices via electronic means. This applies to the identification of individuals by other individuals and between individuals and automated devices.

[1.3.6.1.4.1.34471.1.2.5.2] Signature certificates that are issued under this CP can be used to verify electronic signatures, which are subject to the "same consequences as a handwritten signature", as specified in article 15a, first and second paragraph, in Title 1 of Book 3 of the Dutch Civil Code under section 1A and are Advanced certificates as referred to in article 1.1, paragraph ss of the Telecommunications Act.

Certificate use services

The use of certificates issued under this CP is related to communication by certificate holders who act on behalf of the subscriber.

[1.3.6.1.4.1.34471.1.2.5.4] Authentication certificates that are issued under this CP can be used to identify and authenticate the service that belongs to the organizational unit that is responsible for the corresponding service.

[1.3.6.1.4.1.34471.1.2.5.5] Trusted certificates that are issued under this CP can be used to protect the confidentiality of the information that is exchanged and/or stored in electronic format.

[1.3.6.1.4.1.34471.1.2.5.6] Service certificates that are issued under this CP can be used for securing a connection between a certain client and a server that belongs to the organizational unit that has been named as the subscriber in the corresponding certificate.

EV Certificate use

[1.3.6.1.4.1.34471.1.2.5.7] EV Server Certificates that are issued under this CP can be used for securing a connection between a certain client and a server that belongs to the organizational unit that has been named as the subscriber in the corresponding certificate.