**Bugzilla ID:** 693273
**Bugzilla Summary:** Request to add CA "Digidentity" to Mozilla

CAs wishing to have their certificates included in Mozilla products must

1) Comply with the requirements of the Mozilla CA certificate policy (http://www.mozilla.org/projects/security/certs/policy/)
2) Supply all of the information listed in http://wiki.mozilla.org/CA:Information_checklist.
    a. Review the Recommended Practices at https://wiki.mozilla.org/CA:Recommended_Practices
    b. Review the Potentially Problematic Practices at https://wiki.mozilla.org/CA:Problematic_Practices

**General information about the CA's associated organization**

| | |
|---|---|
| CA Company Name | Digidentity |
| Website URL | http://www.digidentity.eu/ |
| Organizational type | Private company often working for the Dutch Government.<br>A Certificate Service Provider through a 'Besloten Vennootschap', the Dutch equivalent to a Private Limited company. |
| Primark Market / Customer Base | Digidentity BV caters to (mostly Dutch) companies, governmental entities and consumers. |
| Impact to Mozilla Users | Digidentity will be selling certificates to one of the Netherlands' largest webhosting providers (400,000+ websites), not to the owners of websites themselves.<br>Digidentity is a provider of certificate services for the Dutch government, insurance companies and financial institutes.<br>Because of this, a large number of Dutch citizens are confronted with the certificates provided by Digidentity. |
| CA Contact Information | CA Email Alias: ca-root@digidentity.eu<br>CA Phone Number: +31-(0)88-778 78 78<br>Title / Department: CTO, Security Officer |

**Technical information about each root certificate**

| | |
|---|---|
| Certificate Name | Digidentity L3 Root CA - G2 |
| Certificate Issuer Field | CN = Digidentity L3 Root CA - G2<br>O = Digidentity B.V.<br>C = NL |
| Certificate Summary | The root is offline, and signs internally-operated subordinate CAs. |
| Root Cert URL | https://www.digidentity.eu/static/nl/downloads/downloads.html#3<br>https://www.digidentity.eu/static/nl/downloads/level%203/der/Digidentity%20L3%20Root%20CA%20-%20G2.der |
| SHA1 Fingerprint | F1:38:A3:30:A4:EA:98:6B:EB:52:0B:B1:10:35:87:6E:FB:9D:7F:1C |
| Valid From | 2011-04-29 |
| Valid To | 2031-11-10 |
| Certificate Version | 3 |
| Cert Signature Algorithm | PKCS #1 SHA-256 With RSA Encryption |
| Signing key parameters | 4096 bits |

| | |
|---|---|
| Test Website URL (SSL) | https://ca-root-test.digidentity.eu |
| CRL URL | http://pki.digidentity.eu/L3/root/latestCRL.crl<br>http://pki.digidentity.eu/L3/services/latestCRL.crl<br>CPS section 1.22: The revocation status information is refreshed at least once every four hours in the Certificate Revocation List. |
| OCSP URL | Not currently available. In planning. |
| Requested Trust Bits | Websites (SSL/TLS) |
| SSL Validation Type | OV |
| EV Policy OID(s) | Not requesting EV treatment at this time. |

### CA Hierarchy information for each root certificate

| | |
|---|---|
| CA Hierarchy | CA Hierarchy diagrams provided in CPS sections 1.3 and 1.14.<br>The 7 internally-operated sub-CAs in this CA hierarchy are:<br>- Digidentity L3 Organisatie: used for identifying organisations<br>- Machtigingonline: dedicated for use with the Staat der Nederlanden PKI-infrastructure (qv.)<br>- Digidentity L3 Services: used for signing and SSL<br>- Digidentity L3 Burger: used for identifying natural persons<br>- L3 SSCD CA: Used for creating "virtual smartcards"<br>- L3 Extended Validation: used for EV SSL<br>- Digidentity L3 EV SSL CA - G2: Used for Digidentity specific web-services. |
| Externally Operated SubCAs | None |
| Cross-Signing | None |

### Verification Policies and Practices

| | |
|---|---|
| Policy Documentation | Document Repository: http://pki.digidentity.eu/validatie<br>CPS (Dutch): https://www.digidentity.eu/downloads/Certification%20Practice%20Statement%20L3.pdf<br>CPS (English): https://bugzilla.mozilla.org/attachment.cgi?id=623056 |
| Audits | Audit Type: ETSI TS 101 456<br>Auditor: British Standards Institution (BSI), http://www.bsigroup.com<br>Statement of valid ETSI Certificate (2011.01.27):<br>http://www.bsigroup.com/en/Assessment-and-certification-services/Client-directory/CertificateClient-Directory-Search-Results/?pg=1&licencenumber=ETS+015&searchkey=companyXeqXDigidentity<br>https://pgplus.bsigroup.com/cert/default.asp?certnumber=ETS+015&crdate=27%2F01%2F2011&certtemplate=cemea_en |
| Organization Verification | CPS Section 1.9 |
| SSL Verification | CPS Section 1.9: 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. |

| | |
|---|---|
| | Comments:<br>- All checks are face-to-face<br>- High-profile websites are filtered out.<br>- We will not be issuing certs automatically. DNS checks, as well as checks with the hosting provider will take place to verify ownership etc. If a request is blocked, all involved parties will be notified personally.<br>- We use DNS, Chamber of Commerce and other publicly accessible records. Also, since we will not be providing SSL certificates directly (only through the hosting company i referred to earlier) we will have access to their database. |
| Email Address Verification | N/A. Not requesting the Email trust bit at this time. |
| Code Signing Subscriber Verification | N/A. Not requesting the code signing trust bit at this time. |
| Multi-factor Authentication | Confirm that multi-factor authentication is required for all accounts capable of directly causing certificate issuance. See # 6 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices<br>**Where is this Documented? What form of multi-factor authentication is used?** |
| Network Security | CPS Section 1.24.<br>An ISO 27001 audit is performed annually to review network security. |

**Response to Mozilla's CA Recommended Practices** (https://wiki.mozilla.org/CA:Recommended_Practices)

| | |
|---|---|
| Publicly Available CP and CPS | Yes |
| CA Hierarchy | Yes. Root offline; internally-operated intermediate issuing CAs. |
| Audit Criteria | Yes |
| Document Handling of IDNs in CP/CPS | N/A, IDNs are not supported |
| Revocation of Compromised Certificates | Probably in CPS – Kathleen to check when English version available. |
| Verifying Domain Name Ownership | See above. |
| Verifying Email Address Control | N/A |
| Verifying Identity of Code Signing Certificate Subscriber | N/A |
| DNS names go in SAN | Yes |
| Domain owned by a Natural Person | N/A, not supported. |
| OCSP | In progress. |

**Response to Mozilla's list of Potentially Problematic Practices** (https://wiki.mozilla.org/CA:Problematic_Practices)

| | |
|---|---|
| Long-lived DV certificates | SSL certs are OV or EV. Maximum of 3 years. |
| Wildcard DV SSL certificates | N/A, not supported. |
| Email Address Prefixes for DV Certs | SSL certs are OV or EV. |
| Delegation of Domain / Email validation to third parties | ??? **Can anyone outside of DigiIdentity directly cause the issuance of SSL certs?** |
| Issuing end entity certificates directly from | N/A |

| | |
|---|---|
| roots | |
| Allowing external entities to operate subordinate CAs | N/A |
| Distributing generated private keys in PKCS#12 files | N/A |
| Certificates referencing hostnames or private IP addresses | Not found – FQDN only |
| Issuing SSL Certificates for Internal Domains | Not found – FQDN only |
| OCSP Responses signed by a certificate under a different root | No |
| CRL with critical CIDP Extension | No |
| Generic names for CAs | No |
| Lack of Communication With End Users | No |