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	We are a private company often working for the Dutch Government 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). Digidentity will not be selling certificates to the owners of websites directly. Digidentity is a provider of certificate services for the Dutch government, insurance companies and financial institutes. Because of this, a large number of Dutch citizens is confronted with the certificates provided by Digidentity.
CA Contact Information	CA Email Alias: ca-root@digidentity.eu CA Phone Number: +31-(0)88-778 78 78 Title / Department: CTO, Security Officer

Technical information about each root certificate

Certificate Name	Digidentity L3 Root CA - G2
Certificate Issuer Field	
Certificate Summary	The root is offline, and signs internally-operated subordinate CAs.
Root Cert URL	New URL coming soon
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 2031-
Valid To	11-10
Certificate Version	3
Cert Signature Algorithm	
Signing key parameters	4096 bits

Test Website URL (SSL)	https://ca-root-test.digidentity.eu
CRL URL	pki.digidentity.eu/L3/root/latestCRL.crl
OCSP URL	OCSP planned
Requested Trust Bits	Websites (SSL/TLS)
SSL Validation Type	DV and 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. The 7 sub-CAs in this CA hierarchy are: - Digidentity L3 Organisatie: used for identifying organisations - Machtigingonline: dedicated for use with the Staat der Nederlanden PKI-infrastructure (qv.) - Digidentity L3 Services: used for signing and SSL - Digidentity L3 Burger: used for identifying natural persons - L3 SSCD CA: Used for creating "virtual smartcards" - L3 Extended Validation: used for EV SSL - Digidentity L3 EV SSL CA - G2: Used for Digidentity specific web-services.
Externally Operated SubCAs	None
Cross-Signing	None
Technical Constraints on Third-party Issuers	N/A

Verification Policies and Practices

Policy Documentation	Document Repository: http://pki.digidentity.eu/validatie CPS (Dutch): https://www.digidentity.eu/downloads/Certification%20Practice%20Statement%20L3.pdf CPS (English): Comming soon
Audits	Performed annually. Audit Type: ETSI TS 101 456 Auditor: British Standards Institution (BSI) Auditor Website: http://www.bsigroup.com/ Statement of valid ETSI Certificate (2011.01.27): http://www.bsigroup.com/en/Assessment-and-certification-services/Client-directory/CertificateClient-Directory-Search-

	Results/?pg=1&licencenumber=ETS+015&searchkey=companyXeqXDigidentit y https://pgplus.bsigroup.com/cert/default.asp?certnumber=ETS+015&crdate=27%2F01%2F2011&certtemplate=cem ea_en
SSL Verification Procedures	CPS, section 1.11 and beyond - All checks are face-to-face - High-profile websites are filtered out. - 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. - 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.
Organization Verification Procedures	CPS, section 1.11 and beyond
Email Address	N/A. Not requesting the Email trust bit at this time.
Code Signing Subscriber Verification Procedures	N/A. Note 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
Network Security	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
Verifying Domain Name Ownership	See above.
Verifying Email Address Control	N/A
Verifying Identity of Code Signing Certificate	N/A
DNS names go in SAN	Yes
Domain owned by a Natural Person	N/A, not supported
OCSP	OCSP not provided? Please see the CAB Forum Baseline requirements - OCSP will be required

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

Long-lived DV certificates	Maximum of 3 years
Wildcard DV SSL certificates	N/A, not supported
Email Address Prefixes for DV Certs	If DV SSL certs, then list the acceptable email addresses that are used for verification. e) e) **Checking organisation by means of Chambers of Comerce** a. Verification name; b. Verification number; c. Verification CEO/directors d.If an organisation has not been registered in KvK a law, establishment certificate or a general measure of governing board also can be enough. e. If for EV, the phone number of the organisation is rung. f. If for EV insolvency register of the internet site of the jurisdiction and the Supreme Court is consulted of the Netherlands. g. If for EV, then the EU terror list and the web trust list is verified. h. If or fraudulent application are rejected these suspected in their own list are then kept up, new applications are also validated against this list. f) **Verification FQDN** a. The field name is checked at recognised registers as SIDN (foundation Internet Domeinregistratie the Netherlands), IANA (Internet Assigned Numbers Authority and UnifiedRoot); - it is checked if the field name concerned property is of the organisation requesting.

Delegation of Domain / Email validation to third parties	
Issuing end entity certificates directly from roots	N/A
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	Digidentiy don't do any domain verification pur sang, but what Digidentity does is the validation. See our translated CPS (Comming Soon)
Issuing SSL Certificates for Internal Domains	See our translated CPS (Comming Soon)
OCSP Responses signed by a certificate under a different root	No
CRL with critical CIDP Extension	N/A
Generic names for CAs	No
Lack of Communication With End Users	