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	Indicate whether the CA is operated by a private or public corporation, government agency, international organization, academic institution or consortium, NGO, etc. Note that in some cases the CA may be of a hybrid type, e.g., a corporation established by the government. For government CAs, the type of government should be noted, e.g., national, regional/state/provincial, or municipal.
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. Why does Digidentity need to have this root certificate directly included in Mozilla's products, rather than being signed by another CA's root that is already included in NSS? Is this root certificate included in any other major browsers? If yes, which? If no, why not?
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	http://pki.digidentity.eu/validatie I have not been able to find the URL to download this "Digidentity L3 Root CA - G2" root certificate. Please provide the exact URL for downloading the certificate, or attach it to the bug.
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	
Signing key parameters	4096 bits

Test Website URL (SSL)	https://pki.digidentity.eu/validatie I cannot connect to this website. Please provide a website whose SSL certificate chains up to this root. If you are requesting EV treatment, then the website cert must be EV.
CRL URL	pki.digidentity.eu/ L3 /root/latest.crl (this URL doesn't work for me.) CPS section 1.4: nextUpdate for CRLs for end-entity certs is 4 hours.
OCSP URL	OCSP URI in the AIA of end-entity certs Maximum expiration time of OCSP responses Testing results a) Browsing to test website with OCSP enforced in Firefox browser b) If requesting EV: https://wiki.mozilla.org/PSM:EV_Testing_Easy_Version
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): Coming 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=companyXeqXDigidentity

	https://pgplus.bsigroup.com/cert/default.asp?certnumber=ETS+015&crdate=27%2F01%2F2011&certtemplate=cemea_en
SSL Verification Procedures	CPS, section 1.11 and beyond (Kathleen to review when English CPS is available.) - 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 (Kathleen to review when English CPS is available.)
Email Address Verification Procedures	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	?
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	?
Domain owned by a Natural Person	?
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	?
Wildcard DV SSL certificates	?
Email Address Prefixes for DV Certs	? If DV SSL certs, then list the acceptable email addresses that are used for verification.
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	?
Certificates referencing hostnames or private IP addresses	?
Issuing SSL Certificates for Internal Domains	?
OCSP Responses signed by a certificate under a different root	?
CRL with critical CIDP Extension	?
Generic names for CAs	No
Lack of Communication With End Users	