Bugzilla ID: 369357
Bugzilla Summary: ADD DigiNotar EV Root CA certificates

CAs wishing to have their certificates included in Mozilla products must comply with the requirements of the Mozilla CA certificate policy (http://www.mozilla.org/projects/security/certs/policy/) and must supply the information necessary to determine whether or not the policy's requirements have been satisfied, as per http://wiki.mozilla.org/CA:Information_checklist.

General Information	Data
CA Name	DigiNotar
Website URL (English version)	http://www.diginotar.nl/
Organizational type. (E.g., whether the CA is operated by a private or public corporation, government agency, academic institution or consortium, NGO, etc.)	Public Corporation
Primary market / customer base. (Which types of customers does the CA serve? Are there particular vertical market segments in which it operates? Does it focus its activities on a particular country or other geographic region?)	DigiNotar is a Dutch CA operating primarily in the Netherlands, and issuing certificates to individuals and organizations. DigiNotar operates in partnership with Dutch civil-law notaries.

For Each Root CA whose certificate is to be included in Mozilla (or whose metadata is to be modified)

Info Needed	**Data**
Certificate Name	DigiNotar Root CA
Cert summary / comments	This request is to EV-enable this root which is already included in NSS. This is the top root, used only to issue CA certificates for five application-specific subordinate CAs: DigiNotar Public CA 2025 (non-qualified personal certificates), DigiNotar Qualified CA (qualified personal certificates), DigiNotar Services CA (SSL and object signing certificates), DigiNotar Extended Validation CA (EV certificates), and DigiNotar Private CA (CA certificates for organizational CAs).
The root CA certificate URL	http://www.diginotar.nl/files/Rootcertificaten/DigiNotar%20root%20CA2007.crt This root is already included in NSS.
SHA-1 fingerprint	C0:60:ED:44:CB:D8:81:BD:0E:F8:6C:0B:A2:87:DD:CF:81:67:47:8C
Valid from	2007-05-16
Valid to	2025-03-31

Cert Version	3
Modulus length	4096
CRL URL update frequency for end-entity certificates	http://service.diginotar.nl/crl/root/latestCRL.crl CRL published with validity of 24 hours. CPS section 6.10.3: "The DigiNotar CRL used for the CRL validation is never more than 25 (twenty-five) hours older than the current CRL." http://service.diginotar.nl/crl/extendedvalidation/latestCRL.crl
OCSP (if applicable) • OCSP Responder URL • Max time until OCSP responders updated to reflect end-entity revocation	http://validation.diginotar.nl/ See section 6.10 of the CPS. Comment #79: The OCSP service of DigiNotar contains the most accurate revocation information as possible. The CRL is published every half hour to the OCSP server. This is audited and approved by our auditors to be in line with the CABforum requirements. On which the provided EV statement is issued.
List or description of subordinate CAs operated by the CA organization associated with the root CA. (For example, this might include subordinate CAs created to issue different classes or types of end entity certificates: Class 1 vs. class 2 certificates, qualified vs. non-qualified certificates, EV certificates vs. non-EV certificates, SSL certificates vs. email certificates, and so on.) For internally-operated subordinate CAs the key is to confirm that their operation is	DigiNotar operates five subordinate CAs corresponding to the different types of certificates issued: 1) DigiNotar Public CA 2025 Issues medium trust, non-qualified personal and organizational certificates. https://bugzilla.mozilla.org/attachment.cgi?id=254028 2) DigiNotar Qualified CA Issues qualified certificates conforming to EU regulations. https://bugzilla.mozilla.org/attachment.cgi?id=254029 3) DigiNotar Services CA Issues certificates for SSL, Code Signing, S/Mime. https://bugzilla.mozilla.org/attachment.cgi?id=254032 4) DigiNotar Extended Validation CA https://bugzilla.mozilla.org/attachment.cgi?id=254031 For issuing EV SSL certs.

addressed by the relevant CPS, and that any audit covers them as well as the root.	Maximum number of intermediate CAs: 0 5)Private subCA (Customers have a private subCA) Issues private sub-CAs for companies, internal certs. They have a few important organizations as a client like the ministry of justice, kadaster (the Offices of the land registry), the commercial register,etc.
For subordinate CAs operated by third parties, if any: General description of the types of third-party subordinates that exist, and what the general legal/technical arrangements are by which those subordinates are authorized, controlled, and audited.	None operated by third-parties. Comment #79: The subordinated CA's are operated as a managed PKI hosted in the Diginotar environment.
List any other root CAs that have issued cross-signing certificates for this root CA	Comment #79: Like other CA's the Diginotar root CA is cross-signed by the Entrust CA to make sure the SSL certificates are trusted if the end-user is not using an EV enabled webbrowser. https://www.diginotar.nl/Portals/7/Rootcertificaten/DigiNotar%20Root%20CA%20Entrust.crt
Requested Trust Bits One or more of: • Websites (SSL/TLS) • Email (S/MIME) • Code Signing	Websites Code Signing
If SSL certificates are issued within the hierarchy rooted at this root CA certificate: • Whether or not the domain name referenced in the certificate is verified to be owned/controlled by the certificate subscriber.	OV, EV CPS section 4.2: “The DigiNotar TTP civil-law notary is the RA in the DigiNotar partnership. The RA is responsible for the verification of the identity of the Client and/or the User and the other data to be included in the Certificate,” CPS section 4.3, Verification: the registration of a company will be checked in the commercial register

(DV) • Whether or not the value of the Organization attribute is verified to be that associated with the certificate subscriber in addition to verifying the domain name. (OV) • Whether verification of the certificate subscriber conforms to the Extended Validation Certificate Guidelines issued by the CAB Forum. (EV)	CPS section 4.3.2.6, Verification of SSL Server Certificate and Signing Server Certificate: “For an application for an SSL Server Certificate PLUS, an independent registration service checks whether the Client is registered as the owner of the domain name or the IP address provided. If it emerges that the domain name or the IP address provided belongs to another organisation than the Client, then the Client must provide a statement that demonstrates that permission has been obtained from this organisation to use the domain name and/or the IP address.” CPS section 4.3.2.6.4 Verification of EV SSL Server Certificate: “For an application for an EV SSL Server Certificate, an independent registration service checks whether the Client is registered as the owner of the domain name of the IP address provided. For an application for an EV SSL Server Certificate, an extra control measure will be performed by telephone to the number provided by the Client. One goal of this check is to ensure that the telephone number provided is the same as the telephone number of the location where the company is operated. In any case, the above-mentioned controls and the other controls to be conducted are performed while talking into account the most recent guidelines in the ‘Guidelines for Extended Validation Certificates’ (drawn up by the CA/Browser Forum and published at: http://www.cabforum.org) which are set out as mandatory (and generally designated in the Guidelines by MUST) and taking into account the instructions in which certain issues are expressly forbidden (generally designated in the Guidelines by MUST NOT). To this extent, the Guidelines for Extended Validation Certificates apply directly to the issue of EV SSL Server Certificates.”
EV policy OID	2.16.528.1.1001.1.1.1.12.6.1.1.1
Example certificate(s) issued within the hierarchy rooted at this root, including the full certificate chain(s) where applicable. For SSL certificates this should also include URLs of one or more web servers using the certificate(s).	https://www.evssl.nl https://www.polisdirect.nl
CP/CPS	Certification Practice Statement pointer: http://www.diginotar.nl/cps CPS DigiNotar 30 October 2007, Version 3.5: http://www.diginotar.com/Portals/0/General%20terms/DigiNotar_CPS_3.5_-_EN.pdf
AUDIT	Audit Type: WebTrust EV

Auditor: Price Waterhouse Coopers
Auditor Website: http://www.pwc.nl/
Assertion of Management and Audit Report:
https://bugzilla.mozilla.org/attachment.cgi?id=357961
11/17/2008

Issue noted:

In the course of our examination, we noted that DigiNotar did not include the Business Category attribute in the certificates published in this period of time. This is due to early implementation of the certificate profile against the early version of the CAB Forum guidelines.

According to DigiNotar management all new certificates will be issued against the new current certificate profile as defined in the CAB Forum guidelines. Furthermore, DigiNotar defined an action plan to address our audit findings.

Audit Type: ETSI 101.456
Auditor: Price Waterhouse Coopers
Auditor Website: http://www.pwc.nl/
ETSI Certificate:
http://www.diginotar.nl/Portals/7/ETSI/Certificate.pdf
Statement of ETSI Compliance:
http://www.ecp.nl/download/Reg._Cert._op_basis_van_TTP.NL,_3dec08.pdf?PHPSESSID=f23ec42c909cc2bf1107372430d46d08

The schedule is based on ETSI TS 101 456 (Version 6, March 2006) and is managed by the Central Executive Experts on Information Security (CCvD-IB).

Certificate Registry
https://bugzilla.mozilla.org/attachment.cgi?id=357962

We also note that the scheme and the Certification Bodies (like PricewaterhouseCoopers Certification) that work in it, are supervised by the Dutch Accreditation Council (www.rva.nl). To verify that an audit organization is accredited in the Netherlands to perform audits against ETSI TS 101456 according the TTP.NL scheme one visits the RVA website and verifies that the audit organization is listed with a scope that contains the TTP.NL schema.

> From: adri.de.bruijn@nl.pwc.com <adri.de.bruijn@nl.pwc.com>
> Subject: Re: Verification of DigiNotar WebTrust for EV Audit Report
> To: kathleen95014@yahoo.com
> Date: Wednesday, March 11, 2009, 1:39 AM
> Dear Kathleen Wilson,

	> I confirm that I issued the audit report as attached in the url below. > The audit report is authentic. > If you need more information, please let me know. > Kind regards > Adri de Bruijn > PricewaterhouseCoopers > The Netherlands

Review CPS sections dealing with subscriber verification (COMPLETE)
(section 7 of http://www.mozilla.org/projects/security/certs/policy/)

- Verify the domain referenced in an SSL cert is owned/controlled by the subscriber. In addition to verification of subscriber's legal identity.
    - DigiNotar verifies identity for applicants issued certificates suitable for use with SSL-enabled servers, with verification for EV SSL certificates done according to the CAB Forum Guidelines. (See sections 4.3.1 and 4.3.2.6 of the CPS, including section 4.3.2.6.4 for EV.)
        - For an application for an SSL Server Certificate PLUS, an independent registration service checks whether the Client is registered as the owner of the domain name or the IP address provided. If it emerges that the domain name or the IP address provided belongs to another organisation than the Client, then the Client must provide a statement that demonstrates that permission has been obtained from this organisation to use the domain name and/or the IP address.
        - For an application for an SSL Server Certificate BASIS, an independent registration service checks whether the Client is registered as the owner of the domain name or the IP address provided. If it emerges that the domain name or the IP address provided belongs to another organisation than the Client, then the Client must provide a statement that demonstrates that permission has been obtained from this organisation to use the domain name and/or the IP address.
        - For an application for an EV SSL Server Certificate, an independent registration service checks whether the Client is registered as the owner of the domain name of the IP address provided.
        - For an application for an EV SSL Server Certificate, an extra control measure will be performed by telephone to the number provided by the Client. One goal of this check is to ensure that the telephone number provided is the same as the telephone number of the location where the company is operated.
        - In any case, the above-mentioned controls and the other controls to be conducted are performed while talking into account the most recent guidelines in the 'Guidelines for Extended Validation Certificates' (drawn up by the CA/Browser Forum and published at: http://www.cabforum.org) which are set out as mandatory (and generally designated in the Guidelines by MUST) and taking into account the instructions in which certain issues are expressly forbidden (generally designated in the Guidelines by MUST NOT). To this extent, the Guidelines for Extended Validation Certificates apply directly to the issue of EV SSL Server Certificates.
        - The Guidelines for Extended Validation Certificates are published on the DigiNotar website. Insofar as a difference arises at any time between the applicable version published by the CA/Browser Forum and the version published on the DigiNotar website, the version published on the CA/Browser Forum shall prevail.

- Verify the email account associated with the email address in the cert is owned by the subscriber. In addition to verification of subscriber's legal identity.
    - Not requesting email trust bit.
    - Comment #45: Based on discussion during the public comment period, I've decided to consider this application as applying to SSL and code signing uses only, and to postpone any approval for email use until such time as we determine that DigiNotar is in compliance with our current policy requirements regarding verifying that email addresses referenced in certificates actually belong to the entity holding the certificate.
- Verify identity info in code signing certs is that of subscriber
    - DigiNotar verifies identity for applicants issued certificates suitable for code signing. (See sections 4.3.1 and 4.3.2.6 of the CPS.)
        - 4.3.2.6.5 Verification of Signing Server Certificate PLUS (person-specific/not person-specific)
        - 4.3.2.6.6 Verification of Signing Server Certificate BASIS (person-specific/not person-specific)
- Make sure it's clear which checks are done for which context (cert usage)
- All documents supplied as evidence should be publicly available and must be addressed in any audit. Any substantial omissions submitted afterwards may need to be confirmed by auditor, at Mozilla's discretion.

Flag Problematic Practices
(http://wiki.mozilla.org/CA:Problematic_Practices)

- Long-lived DV certificates
    - SSL certs are OV or EV.
    - CPS, section 5.3: The Certificate is issued for a maximum period of validity of four years, commencing at the time of issue. The period of validity for the Certificate is stated in the Certificate.
- Wildcard DV SSL certificates
    - SSL certs are OV or EV.
    - Diginotar only issues wildcard SSL certificates if the organisation is validated.
- Delegation of Domain / Email validation to third parties
    - No.
- Issuing end entity certificates directly from roots
    - No, root only issues sub-CAs.
- Allowing external entities to operate unconstrained subordinate CAs
    - No.
- Distributing generated private keys in PKCS#12 files
    - Comment #79: In some cases Diginotar is issuing PKCS#12 files. PKCS#12 files are send in a secure way using certified snail-mail. Some end-user request this type of certificate because of back-up/ key archiving services.
- Certificates referencing hostnames or private IP addresses

  - Comment #79: In some cases, for working functionality, it is an obligation to include a hostname in the subject altname, like outlook 2007 mail certificates. See: http://technet.microsoft.com/en-us/library/bb851505.aspx
- OCSP Responses signed by a certificate under a different root
  - OCSP tested without error in Firefox using the test urls provided.
- CRL with critical CIDP Extension
  - CRLs have been successfully downloaded into Firefox.

Verify Audits (COMPLETE)
(Sections 8, 9, and 10 of http://www.mozilla.org/projects/security/certs/policy/)

- Validate contact info in report, call to verify that they did indeed issue this report.
  - The authenticity of the WebTrust EV audit report was confirmed via email exchanged with the auditor.
- For EV CA’s, verify current WebTrust EV Audit done.
  - Yes.
- Review Audit to flag any issues noted in the report
  - **One issue noted and resolved. See above for details.**