Bugzilla ID: 436056
Bugzilla Summary: Add second Staat der Nederlanden root certificate

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	Staat der Nederlanden GBO.Overheid
Website URL (English version)	http://gbo.overheid.nl/english/ http://www.pkioverheid.nl/english
Organizational type. (E.g., whether the CA is operated by a private or public corporation, government agency, academic institution or consortium, NGO, etc.)	Netherlands national government CA
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?)	Staat der Nederlanden is the Netherlands national government CA. The Dutch governmental PKI hierarchy consists of 2 roots. This first root, Staat der Nederlanden Root CA, is already included in NSS. The second root is the next generation, Staat der Nederlanden Root CA – G2.

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

Info Needed	Data	Status / Notes
Certificate Name	Staat der Nederlanden Root CA - G2	COMPLETE
Cert summary / comments	This is the next generation of the Staat der Nederlandend Root CA that is currently in the Mozilla store. The PKIoverheid issues two internally operated subordinate CAs, which issue subordinate CAs to CSPs. The CSPs are commercial and governmental organizations. Each CSP has to prove that it complies with ETSI TS 101 456 and the Dutch law on electronic signatures. CSPs must conclude a contract with a representative of a government organization or commercial company before issuing end-entity certificates. A request for a certificate is always performed by a specified representative of a government organization or commercial company.	COMPLETE
The root CA certificate URL	http://www.pkioverheid.nl/fileadmin/PKI/PKI_certifcaten/staatdernederlandenrootca-g2.crt	COMPLETE

Download into FireFox and verify		
SHA-1 fingerprint.	59:af:82:79:91:86:c7:b4:75:07:cb:cf:03:57:46:eb:04:dd:b7:16	COMPLETE
Valid from	2008-03-26	COMPLETE
Valid to	2020-03-25	COMPLETE
Cert Version	3	COMPLETE
Modulus length / key length	4096	COMPLETE
CRL • URL • update frequency for end-entity certificates	http://crl.pkioverheid.nl/ CP Part 3a and 3c in paragraph 4.9.5.1 (Tijdsduur voor verwerking intrekkingsverzoek) on page 11 indicates that the CRL and OCSP update frequency for end-entity certificates has to take place at least every 4 hours. The same statement is made in CP Part 3b in paragraph 4.9.5.1 (Tijdsduur voor verwerking intrekkingsverzoek) on page 13.	COMPLETE (Verified using Google Translate)
OCSP (if applicable) • OCSP Responder URL • Max time until OCSP responders updated to reflect end-entity revocation	The CSPs provide OCSP. See 436056-subCA-review for specifics. CP Part 3a and 3c in paragraph 4.9.5.1 (Tijdsduur voor verwerking intrekkingsverzoek) on page 11 indicates that the CRL and OCSP update frequency for end-entity certificates has to take place at least every 4 hours. The same statement is made in CP Part 3b in paragraph 4.9.5.1 (Tijdsduur voor verwerking intrekkingsverzoek) on page 13.	COMPLETE
List or description of subordinate CAs operated by the CA organization associated with the root CA.	The certificate hierarchy diagram can be found in our CPS, page 8 at http://www.pkioverheid.nl/fileadmin/PKI/CPS_PA_PKIoverheid_v3.0.pdf There are two internally-operated subordinate CAs. 1) a domain-CA for Government-Organization 2) a domain-CA for Government-Citizen These sub-CAs issue the subordinate CAs for the CSPs.	COMPLETE
For subordinate CAs operated by third parties, if any: General description of the types of third-party subordinates that exist, and what the general	At this moment no CSP or subordinate CA, created underneath and signed by a CSP, is active yet underneath our 2nd root Staat der Nederlanden Root CA – G2. Based on our current root Staat der Nederlanden Root CA, I expect that around 6 subordinate CA's, created underneath and signed by a CSP, will be created before the end of 2010. Sub-CAs within the PKIoverheid who issue end-entity certificates can only be created	**See 436056-subCA-review for the details of the CSPs currently in operation under the "Staat der Nederlanden Root CA". These CSPs will be migrated to the**

legal/technical arrangements are by which those subordinates are authorized, controlled, and audited.	underneath and signed by CSPs within the PKIoverheid hierarchy. So Sub-CAs can only issue certificates within the same domains as where the CSPs issue their certificates. Sub-CAs can not create their own subordinates. The only reason that a CSP within the PKIoverheid creates a Sub-CA is to differentiate between the different usages of certificates. This means that, if applicable, a Sub-CA is created for certificates meant for personal use (authentication, encryption and non-repudiation) and a Sub-CA for certificates meant for services (e.g. SSL). Before a CSP can create a Sub-CA they have to have permission from the Policy Authority (PA) of PKIoverheid, as is stated in our CP part 3a and 3c in paragraph 9.12.2.2 on page 25 and in part 3b in paragraph 9.12.2.2 on page 27. The PA grants its permission by assigning a separate OID for the Sub-CA. Each CSP can issue several types of certificates (e.g. authentication, encryption, non-repudiation, service (such as SSL)). Before being allowed as a CSP in the hierarchy of the PKIoverheid the CSP has to prove that it complies with ETSI TS 101 456 (standard for issuing qualified certificates in accordance with the EU-directive on electronic signatures) and the Dutch law on electronic signatures. The CSP needs also to provide a certificate from the Chamber of Commerce and has to sign a contract with the Dutch Ministry of Interior and Kingdom Relations. CSPs will always conclude a contract with (a representative of) a subscriber before issuing any end-entity certificate. This means that a request for a certificate always takes place by (a representative of) a subscriber. So it is not possible that an employee from a government organization or commercial company can directly request a certificate from a CSP. Furthermore (the representative of) the subscriber is responsible for the accuracy and completeness of the request for a certificate. The only exception is the CSP Defensie. They only issue certificates to their own employees. So the conclusion of a contract with a subscriber is not applicable here. In theory end-users can also be civilians. However, so far no certificates have been issued directly to civilians and this will probably not happen in the coming years.	**new root.**
List any other root CAs that have issued cross-signing	Not applicable.	COMPLETE

certificates for this root CA		
Requested Trust Bits One or more of: • Websites (SSL/TLS) • Email (S/MIME) • Code (Code Signing)	Websites Email Code	COMPLETE
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. (This is commonly referred to as a DV certificate.) • Whether or not the value of the Organization attribute is verified to be that associated with the certificate subscriber. (This is commonly referred to as an OV certificate.)	OV	COMPLETE
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).	No (SSL) end-entity certificates have been issued yet underneath the Staat der Nederlanden Root CA - G2.	We will need this for testing purposes.

• There should be at least one example certificate for each of the major types of certificates issued, e.g., email vs. SSL vs. code signing, or EV vs. OS vs. DV. • Note: mainly interested in SSL, so OK if no email example.		
CP/CPS • Certificate Policy URL • Certificate Practice Statement(s) (CPS) URL (English or available in English translation)	CP Part 3a: http://www.pkioverheid.nl/fileadmin/PKI/pve/PvE_deel3a_v1.2.pdf Certificates for personal use issued to employees working in governmental organizations or commercial companies CP Part 3b: http://www.pkioverheid.nl/fileadmin/PKI/pve/PvE_deel3b_v1.2.pdf Certificates for services (e.g. SSL) issued to governmental organizations or commercial companies CP Part 3c: http://www.pkioverheid.nl/fileadmin/PKI/pve/PvE_deel3c_v1.2.pdf Certificates for personal use issued to civilians CPS: http://www.pkioverheid.nl/fileadmin/PKI/CPS_PA_PKIoverheid_v3.0.pdf The PKIoverheid has developed a Schedule of Requirements (Certificate Policy). The Schedule of Requirements can be found at: http://www.pkioverheid.nl/voor-certificaatverleners/programma-van-eisen/programma-van-eisen-2008/ The parts 3a, b, c are the certificate policies (CP). In the other parts specific requirements (for instance regarding interoperability) are stated.	COMPLETE
. AUDIT: The published document(s) relating to independent audit(s) of the	Auditor: KPMG Auditor Website:	COMPLETE Audit Date: 1/28/2009

root CA and any CAs within the hierarchy rooted at the root. (For example, for WebTrust for CAs audits this would be the "audit report and management assertions" document available from the webtrust.org site or elsewhere.)	http://www.kpmg.com/Global/Pages/default.aspx Audit Document URL(s): https://cert.webtrust.org/ViewSeal?id=683	

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

- See 436056-subCA-review for details about how each CSP's CP/CPS addresses the ownership/control of domain name and email address.
- Each application form is signed by the representative of the government organization or commercial company of the end-user. Each CSP performs an extensive identity validation check and organizational validation check. So there can be absolutely no doubt that the employee is working within that specific organization and that the employee is the one who he/she claims to be.
- CP Part 3b page 31 underneath the attribute Subject.commonName declares that the subscriber is responsible for the correctness of the FQDN.
    - "The subscriber has to demonstrate that the organization may carry this name. If the service has a DNS (Domain Name System) than this should be mentioned in the commonName as "fully-qualified domain name" (FQDN). For example if a certificate is requested for pkioverheid.nl than the certificate is not valid for secure.pkioverheid.nl."
- CP Part 3a page 33 (SubjectAltName.rfc822Name) does not recommend the use of an email address for applicants: "The use of email addresses for PKIoverheid certificates within the domain Government and Companies is not recommended, because email addresses of applicants change a lot and it can harm the privacy of the applicants (spam)."
    - Nevertheless some CSPs include an email address. This is sometimes necessary for authentication (access control) purposes within government organizations or commercial companies.
    - In the CPSs of the CSPs DigiNotar, Getronics and ESG no real statement is made about the verification of the email address of the end-user. However, each application form is signed by the representative of the government organization or commercial company of the end-user. Each CSP performs an extensive identity validation check and organizational validation check. So there can be absolutely no doubt that the employee is working within that specific organization and that the employee is the one who he/she claims to be. This means that the CSP can trust the submitted email address on the application form.
- See bug 431085: "Bug 369357 comment 37 suggests that Staat der Nederlanden does not verify that the subscriber (Subject) has access/control to the email address(es) that it puts into certs, yet it's CA certs are trusted for email. At least one other person concurs with that assessment. So Mozilla needs to review that CA's practices to see if they comply with Mozilla's policy for email trust, and consider what action to take if they do not."

Flag Problematic Practices (COMPLETE – The translations have been verified using Google Translate)
(http://wiki.mozilla.org/CA:Problematic_Practices)

- 1.1 Long-lived DV certificates
    - SSL Certs are IV/OV, not DV.
- 1.2 Wildcard DV SSL certificates
    - CP Part 3b page 31 underneath Subject.commonName declares that "It is not allowed to use wildcards within this attribute".
- 1.3 Delegation of Domain / Email validation to third parties
    - The CSPs DigiNotar, Getronics and ESG have delegated parts of their process regarding the organization and end-user identity check to third parties. Nevertheless when a CSP within the PKIoverheid hierarchy uses a RA or LRA for e.g. an identity check than this process will also be included in the audit. The audit info for CSPs is provided in See 436056-subCA-review.
- 1.3 Issuing end entity certificates directly from roots
    - The root does not issue certificates directly to end-users.
- 1.4 Allowing external entities to operate unconstrained subordinate CAs
    - CSP sub-CAs can only issue certificates within the same domains as where the CSPs issue their certificates. Sub-CAs can not create their own subordinates. The only reason that a CSP within the PKIoverheid creates a Sub-CA is to differentiate between the different usages of certificates. This means that, if applicable, a Sub-CA is created for certificates meant for personal use (authentication, encryption and non-repudiation) and a Sub-CA for certificates meant for services (e.g. SSL). Before a CSP can create a Sub-CA they have to have permission from the Policy Authority (PA) of PKIoverheid, as is stated in our CP Part 3a and 3c in paragraph 9.12.2.2 on page 25 and in Part 3b in paragraph 9.12.2.2 on page 27. The PA grants its permission by assigning a separate OID for the Sub-CA.
- 1.5 Distributing generated private keys in PKCS#12 files
    - Subscribers generate their own key pairs (PKCS#10). Furthermore the CSPs may not archive or make a back-up from the private key of the subscriber. This is stated in our CP:
        - CP Part 3a (page 18) and Part 3b (page 20) in paragraph 6.2.4.2.1 and 6.2.5.1.
        - CP Part 3c in paragraph 6.2.4.2.1 and 6.2.5.1 on page 18.
- 1.6 Certificates referencing hostnames or private IP addresses
    - Our CP Part 3b on page 31 describes that the "Subject" field has to contain an Distinguished Name (DN). In addition the Subject.commonName field has to contain the fully-qualified domain name (FQDN).
- 1.7 OCSP Responses signed by a certificate under a different root
    - The requirements regarding the OCSP are described in our CP Part 3b. On page 39 regarding the "Issuer" field it is stated that "An OCSPSigning certificate must be issued within the hierarchy of the PKIoverheid".
- 1.8 CRL with critical CIDP Extension
    - CP Part 3b page 38: issuingDistributionPoint attribute is optional.
    - Only the CSP ESG uses this attribute. We will inform them about Mozilla's recommendation.

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.
    - Posted on cert.webtrust.org
- For EV CA’s, verify current WebTrust EV Audit done.
    - Not EV
- Review Audit to flag any issues noted in the report
    - No issues noted in report.