Bugzilla ID: 551399
Bugzilla Summary: Request enabling email trust bit for Staat der Nederlanden Root CA - G2

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.

CA's are also encouraged to review the Recommended Practices at https://wiki.mozilla.org/CA:Recommended_Practices.

General Information	**Data**
CA Name	Staat der Nederlanden (Logius)
Website URL	http://www.logius.nl/english/
Organizational type	Netherlands national government CA
Primary market / customer base	Staat der Nederlanden is the Netherlands national government CA. The Dutch governmental PKI hierarchy consists of 2 roots, Staat der Nederlanden Root CA and Staat der Nederlanden Root CA – G2, both of which are included in NSS. The organization operating these roots is called Logius as of January 2010, it used to be called GBO.Overheid. Logius is the digital government service of the Netherlands Ministry of the Interior and Kingdom Relations (BZK).
CA Contact Information	CA Email Alias: servicecentrum@logius.nl CA Phone Number: 0900 - 555 4555 Title / Department: Policy Authority PKIoverheid

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

Info Needed	**Data**
Certificate Name	Staat der Nederlanden Root CA - G2
Cert summary / comments	This request is to enable the email trust bit for the "Staat der Nederlanden Root CA - G2" root certificate authority. This root was approved for inclusion in bug #436056. 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 signed by a specified representative of a government organization or commercial company.
Root CA certificate URL	https://bugzilla.mozilla.org/attachment.cgi?id=413393
SHA-1 fingerprint.	59:af:82:79:91:86:c7:b4:75:07:cb:cf:03:57:46:eb:04:dd:b7:16
Valid from	2008-03-26
Valid to	2020-03-25

Cert Version	3
Modulus length	4096
Test Cert	End-user cert: https://bugzilla.mozilla.org/attachment.cgi?id=447309 Intermediate certs: https://bugzilla.mozilla.org/attachment.cgi?id=447310
CRL	http://crl.pkioverheid.nl/RootLatestCRL-G2.crl http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl http://crl.pkioverheid.nl/DomBurgerLatestCRL-G2.crl In each CP, section 4.9.5: The maximum delay … of the revocation status information, for all relying parties available, is set at four hours. This requirement applies to all types of certificate status information (OCSP and CRL)
OCSP (if applicable)	All of the CSPs provide OCSP. The CP indicates that the CRL and OCSP update frequency for end-entity certificates has to take place at least every 4 hours. See https://bugzilla.mozilla.org/attachment.cgi?id=407385 for specifics of each CSP.
CA Hierarchy	The certificate hierarchy diagram is shown in section 4 of the CPS. http://www.logius.nl/fileadmin/logius/product/pkioverheid/documenten/CPS%20PA%20PKIoverheid%20v3.2.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.
Subordinate CAs operated by third parties	See https://bugzilla.mozilla.org/attachment.cgi?id=407385 for the details of the CSPs currently in operation under the "Staat der Nederlanden Root CA". These CSPs will be migrated to the new root. There is a new CSP, QuoVadis; information for the new CSP is provided below. Based on the original Staat der Nederlanden Root CA, around 6 subordinate CA's, created underneath and signed by a CSP, will be created under this second generation root before the end of 2010. Sub-CAs within the PKIoverheid who issue end-entity certificates can only be created 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 must have permission from the Policy Authority (PA) of PKIoverheid, as is stated in the CP's paragraph 9.12.2.2. 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.
Cross-signing certificates	None
Requested Trust Bits	Email (S/MIME) Note: Websites and Code Signing trust bits are currently enabled.
If SSL, verification type: DV, OV, and/or EV	OV
EV Policy OID	Not EV
CP/CPS	All documents are in Dutch CPS of the Policy Authority PKI Overheid: http://www.logius.nl/fileadmin/logius/product/pkioverheid/documenten/CPS%20PA%20PKIoverheid%20v3.2.pdf The PKIoverheid has developed a Schedule of Requirements (Certificate Policy). The Schedule of Requirements can be found at: http://www.logius.nl/producten/toegang/pkioverheid/aansluiten/programma-van-eisen/#c1618 CP for CSPs (Dutch): http://www.logius.nl/fileadmin/logius/product/pkioverheid/documenten/pve/PvE%20deel2%20v2.1.pdf This document describes how a CSP can join the PKI for the government can demonstrate compliance with the requirements and formalities which must be met. It also describes how the PA monitors joined the CSP 's. CP Part 3a for employees of governmental organizations or commercial companies: http://www.logius.nl/fileadmin/logius/product/pkioverheid/documenten/pve/PvE%20deel3a%20v2.1.pdf CP Part 3b for SSL services of governmental organizations or commercial companies:

	http://www.logius.nl/fileadmin/logius/product/pkioverheid/documenten/pve/PvE%20deel3b%20v2.1.pdf CP Part 3c for personal use of civilians: http://www.logius.nl/fileadmin/logius/product/pkioverheid/documenten/pve/PvE%20deel3c%20v2.1.pdf
CP/CPS of each CSP	DigiNotar: https://www.diginotar.nl/LinkClick.aspx?fileticket=KYQoXTpWkD4%3d&tabid=321 https://www.diginotar.nl/Portals/7/Voorwaarden/CPS%20DigiNotar%20PKIoverheid%20Services%20v1.2.2.pdf GetronicsPinkRoccade: http://www.pki.getronicspinkroccade.nl/website/files/Getronics_PKIoverheid_CPS_v4.5.pdf CIBG/UZI-register: https://www.uzi-register.nl/pdf/20081001_CPS_UZI-register_4.1d.pdf ESG: http://cps.csp4.eu/downloads/CPS_3.2.pdf Defensie: http://cps.dp.ca.mindef.nl/mindef-ca-dp-cps/CPS%20Certificatie%20Autoriteit%20Defensie%20v.1.2.pdf QuoVadis: http://www.quovadisglobal.nl/nl-NL.aspx?sc_lang=en-GB http://www.quovadisglobal.nl/Beheer/~/media/Files/Repository/QV_CPS_PKI_Overheid_V1_0.ashx
AUDIT	Auditor: KPMG Auditor Website: http://www.kpmg.com/Global/Pages/default.aspx Audit: http://cert.webtrust.org/SealFile?seal=1015&file=pdf (2009.12.31) The CSPs undergo regular audits based on the ETSI TS 101 456 requirements and additional requirements from PKIoverheid (as described in the CP). ETSI 101 456 Certificate for each CSP: DigiNotar: http://www.diginotar.nl/Portals/7/ETSI/Certificate.pdf (expires: 2010.09.26) GetronicsPinkRoccade: https://www.pki.getronicspinkroccade.nl/website/files/Getronics%20-%20ETSI%20certificate%20by%20BSI.pdf.pdf (expires: 2011.01.11) CIBG/UZI-register: https://bugzilla.mozilla.org/attachment.cgi?id=447313 (expires: 2010.11.22) ESG: http://www.de-electronische-signatuur.nl/downloads/ETS006.pdf (expires: 2012.06.29) Defensie: https://bugzilla.mozilla.org/attachment.cgi?id=447311 (expires: 2011.02.28) QuoVadis: http://www.quovadisglobal.nl/~/media/Files/Files_NL/BSI_quovadis_certificate.ashx (expires: 2011.08.07)

Organization Identity Verification	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. Google Translations: CP Part 3b for SSL services of governmental organizations or commercial companies 3.2 Initial Identity Validation 3.2.2 Authentication of organizational entity The CSP shall verify that the subscriber is an existing organization. The CSP shall verify that the organization notified the subscriber name is included in the certificate correctly and completely. 3.2.3 Authentication of individual identity The CSP is under Dutch laws and regulations and the identity, if any, specific properties to check the license manager. Proof of identity must be verified on the basis of physical appearance of the person, either directly or indirectly, by the same means by which security can be obtained as to personal presence. Proof of identity may be on paper or electronically delivered. For specification of the set in 3.2.3-1, the identity of the certificate manager can only be determined by Article 1 of the Act on the obligation to identify appropriate valid documents. The CSP is the validity and authenticity of this check. If the control of the personal identity of the certificate manager is implemented when applying for a license in the Public Domain, Business and Organization, then the verification of the identity of the certificate manager under this CP alleged to have found place. The license manager is a person whose identity should be determined in conjunction with an organizational entity. There is evidence to be made of: • full name, including surname, first name, initials or other forename (s) name (s) (if applicable) and inserts (if applicable); • date and place, an appropriate national registration, or other characteristics of the license manager that can be used for extent possible, the person of other people with similar names to distinguish; • proof that the license manager is entitled to a certificate holder to receive on behalf of the legal person or other organizational entity. 3.2.5 Authorization of the certificate holder The CSP shall verify that: · Proof that the certificate holder is authorized on behalf of the subscriber to receive a certificate, is authentic; · Or the certificate administrator has obtained permission from the subscriber actions assigned to him to perform (if the license manager performs the registration).
Domain Name Ownership / Control	Domain Name Verification is specified in CP Part 3b. CSPs within the PKIoverheid hierarchy verify, on the basis of The Dutch Trade Register (http://www.kvk.nl/english/traderegister/default.asp) whether the subscriber may represent the organization, whether the name of the organization is true and whether the address of the organization is correct. At the

	request of SSL certificates CSPs verify the records of the SIDN (aka www.domain-registry.nl) or the Internet Assigned Numbers Authority (IANA) whether the subscriber is the owner of the domain name. CSPs within the PKIoverheid only issue certificates to organizations operating within the Netherlands. Google Translations: CP Part 3b for SSL services of governmental organizations or commercial companies Table: Personal certificates, Basic Attributes Field/Attribute: Subject.commonName Criteria: V (Required; the attribute is mandatory and MUST be used in the certificate.) Description: Name that identifies the service or server. Standard reference: RFC 3739, ETSI TS 102 280, PKIo Type: UTF8String Remarks: The subscriber must demonstrate that the organization may carry this name. The service MUST have a DNS name that the common name mentioned as a fully-qualified domain name (see the definition in section 4). A certificate for such pkioverheid.nl what is requested is not valid for secure.pkioverheid.nl. It is not allowed to use wildcards in this attribute. The CSP MUST register with authorized (Stichting Internet Domain Registration Netherlands (SIDN) or Internet Assigned Numbers Authority (IANA)) check whether the subscriber is the owner of the domain.
Email Address Ownership / Control	Staat der Nederlanden has updated their practices and CP documents to address the following concern: 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.” Bug #436056, Comment #24: PKIoverheid does not allow the email address to be included in the Subject.emailAddress field. The email address is deprecated but permitted in the SubjectAltName.rfc822Name field. It only may be used to support certain applications (legacy implementations) who need the email address (according to RFC 5280 page 25). This is sometimes necessary for (legacy) applications within companies and governmental organizations. Therefore it is applicable with regard to our CP part 3a. But it will not be necessary for the use of certs issued to civilians (CP Part 3c). Staat der Nederlanden updated CP Part 3a (for employees of governmental organizations or commercial companies) to include the following: If the e-mail address is included in the certificate then the CSP MUST: - let the subscriber agree on this by signing an agreement and; - verify that the e-mail address belongs to the domain of the subscriber.

	Google Translations: ANNEX A CERTIFICATES AND LICENSE STATUS INFORMATION PROFILES Profile of the certificate for the Public Domain / Business and Organization CP Part 3a, 3b, and 3c Table: Personal certificates, Basic Attributes Field/Attribute: Subject.emailAddress Criteria: N (Not allowed, indicates that use of the attribute in the PKI for the government is not allowed.) Description: Operation is not allowed. Standard reference: RFC 5280 Type: IA5String Remarks: This field CAN NOT be used in new certificates. CP Part 3a for employees of governmental organizations or commercial companies Table: Personal certificates, Standard Extensions Field/Attribute: SubjectAltName.rfc822Name Criteria: A (not recommended; indicates that the attribute is not recommended but may be included in the certificate) Description: May be used to e-mail address of the holder, for applications that need e-mail address to function properly. Standard reference: RFC 5280 Type: IA5String Remarks: For PKIoverheid certificates in Public Domain / Companies Organization and the use of e-mail addresses not recommended as e-mail addresses of holders and also often exchange privacy sensitive (spam). If the e-mail address is included in the certificate the CSP must: • let the subscriber agree on this by signing an agreement and; • verify that the e-mail address belongs to the domain of the subscriber. Note: 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.
Identity of Code Signing Subscriber	Verification procedures for Code Signing certificates are described in CP part 3b. CSPs within the PKIoverheid hierarchy perform an extensive identity validation check and organizational validation check regarding the subscriber (governmental organization or commercial company) and the end-user.

	Bug #436056, Comment #24: 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. Before a CSP may provide a certificate to (a representative of) a subscriber they have to verify that the subscriber: 1. is an existing organization and; 2. provides an organization name, to be included in the certificate, which is accurate and complete. Google Translation of CP part 3b: 3.2.2 Authentication of organizational entity 3.2.2.1 The CSP shall verify that the subscriber is an existing organization. 3.2.2.2 The CSP shall verify that the organization notified the subscriber name is included in the certificate correctly and completely. Bug #436056, Comment #24: In addition in paragraph 3.2.3.1, 3.2.3.2 and 3.2.3.3 requirements are described about the verification of the identity of the person (=certificaatbeheerder) who may act on entity's behalf. This certificaatbeheerder (in English Certificate Manager) is the ONLY person who may act as a representative of the subscriber/on entity's behalf. In paragraph 3.2.3.1 it is stated that the CSP has to perform a face-to-face verification with regard to the identity of the Certificate Manager. In paragraph 3.2.3.2 it is stated that the CSP may only verify the identity of the Certificate Manager using a document based on the Dutch law for identification ("Wet identificatie bij dienstverlening") e.g a passport. Finally the subscriber/entity has to hand over to the CSP: - proof of the full name (surname etc.) of the Certificate Manager; - proof of date and place of birth of the Certificate Manager; - proof that the Certificate Manager may receive a cert on behalf of the subscriber/entity/organization. This is described in paragraph 3.2.3.3. Google Translation of CP part 3b: 3.2.3 Authentication of individual identity 3.2.3.1 The CSP is under Dutch laws and regulations and the identity, if any, specific properties to check the license manager. Proof of identity must be verified on the basis of physical appearance of the person, either directly or indirectly, by the same means by which security can be obtained as to personal presence. Proof of identity may be on paper or electronically delivered. 3.2.3.2 For specification of the set in 3.2.3-1, the identity of the certificate manager can only be determined by Article 1 of the Act on the obligation to identify appropriate valid documents. The CSP is the validity and authenticity of this check.

	If the control of the personal identity of the certificate manager is implemented when applying for a license in the Public Domain, Business and Organization, then the verification of the identity of the certificate manager under this CP alleged to have found place. 3.2.3.3 The license manager is a person whose identity should be determined in conjunction with an organizational entity. There is evidence to be made of: • full name, including surname, first name, initials or other forename (s) name (s) (if applicable) and inserts (if applicable); • date and place, an appropriate national registration, or other characteristics of the license manager that can be used, where possible, the person of other people with similar names to distinguish; • proof that the license manager is entitled to a certificate holder to receive on behalf of the legal person or other organizational entity.
CSP Information	Summary of CSP Information: https://bugzilla.mozilla.org/attachment.cgi?id=407385 This document covers the following CSPs, which were evaluated during the root inclusion request in bug #436056: DigiNotar, GetronicsPinkRoccade, CIBG/UZI-register, ESG, Defensie The information remains the same, but some of them have updated CP/CPS documents as listed above. The updated ETSI audit certificates are also listed above. There is one new CSP chaining up to this root, which was introduced after the evaluation in the document listed above. The summary of the new CSP is provided here. QuoVadis URL: http://www.quovadisglobal.nl/nl-NL.aspx?sc_lang=en-GB CPS: http://www.quovadisglobal.nl/Beheer/~/media/Files/Repository/QV_CPS_PKI_Overheid_V1_0.ashx Audit Certificate: http://www.quovadisglobal.nl/~/media/Files/Files_NL/BSI_quovadis_certificate.ashx CRL: http://crl.quovadisglobal.com/qvocag2.crl (NextUpdate: 24 hours) OCSP: http://ocsp.quovadisglobal.com/ Test site: https://irisklic.delta.nl/ (page displays the message "under construction", SSL cert chains to this root) Domain Name Ownership / Control -- page 16 CPS English: "Concerning SSL certificates: domain name and ownership are verified at SIDN (the Foundation for Internet Domain Registration in the Netherlands) or Internet Assigned Numbers Authority." Email Address Ownership / Control -- page 16 CPS English: "In the situation that an email address is included in the certificate QuoVadis will verify the email address by sending a verification email to this address with a request to the end user to confirm the validity of the e-mail address." Additional info: QuoVadis does fully comply with all the PKIoverheid requirements. In addition: QuoVadis has not delegated parts of their process regarding the organization and end-user identity check to third parties.

Potentially Problematic Practices	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: "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 CP Part 3a and 3c in paragraph 9.12.2.2 and in Part 3b in paragraph 9.12.2.2. 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 CP:
	  ▪ CP Part 3a and Part 3b 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.
	• 1.6 Certificates referencing hostnames or private IP addresses
	  ○ CP Part 3b 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 CP Part 3b. 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
	  ○ No.