Root CA Bugzilla ID: 335197
Root CA Company/Organization Name: Staat der Nederlanden

This document summarizes the information gathered and verified for subordinate CAs for companies who use their sub-CA to sign other sub-CAs or certificates for other companies or individuals not affiliated with their company. For instance, this document is necessary when the root issues sub-CAs that are used by Certificate Service Providers (CSP). For more background information, see

- https://wiki.mozilla.org/CA:How_to_apply
- https://wiki.mozilla.org/CA:SubordinateCA_checklist

Info Needed	**Data**
Root Name	Staat der Nederlanden Root CA - G2
List or Description of all of the Subordinate CA's operated by third parties	The Dutch governmental PKI (hereafter PKIoverheid) is the name for the Public Key Infrastructure designed for trustworthy electronic communication within and with the Dutch government. To reach the latter goal a national PKI certificate hierarchy has been realised. This hierarchy consists of 2 roots and 4 domains. The CSPs (commercial and governmental organizations) issue several types of certificates (e.g. authentication, encryption, non-repudiation, service (SSL)) to end-users. End-users can be employees (or in the case of service/SSL certificates: a server) within governmental organizations or employees working at commercial companies ((or in the case of service/SSL certificates: a server). 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. The PKIoverheid only issues certificates to CSPs. The Ministry of Interior and Kingdom Relations is the owner of the PKIoverheid. The Policy Authority PKIoverheid supports the Dutch Minister of Interior and Kingdom Relations with the management and control of the PKI system. The PKIoverheid hierarchy consists of a root based on the SHA-1 algorithm (Staat der Nederlanden Root CA) and two subordinate domain-CAs (a domain-CA for Government-Government and Government-Business and a domain-CA for Government-Citizen), with several CSPs underneath, and of a root based on the SHA-256 algorithm (Staat der Nederlanden Root CA – G2) and two subordinate domain-CAs (a domain-CA for Government-Organization and a domain-CA for Government-Citizen). Note: "Staat der Nederlanden Root CA" is already included in NSS. This request is to include "Staat der Nederlanden Root CA – G2", which is the next generation of the root. Both our roots and our 4 domains have been evaluated by the Dutch General Intelligence and Security Service and are classified as Stg. Confidentieel (Nato Confidential). The private key of both our roots and our 4 domains are held at a location which is classified by the Dutch General Intelligence and Security Service as Stg. Geheim (Nato Secret). So Mozilla customers can have full confidence that the private key of our roots and 4 domains will not be compromised.

	CSPs only issue certificates to end-users working within governmental organizations or end-users working at commercial companies. 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. 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. This is stated in CP: - part 3a; in paragraph 3.2.1, 3.2.2, and 3.2.3 and; - part 3b; in paragraph 3.2.2.1 and 3.2.2.2 When the subscriber is a natural person (civilian) the CSP has to verify that the name, which will be included in the certificate, is complete and correct, including surname, first name, initials or other forename(s)(if applicable). This is stated in CP part 3c; in paragraph 3.2.3.1 In addition the CSPs also have to verify the identity of an end-user. In the CPSs of the CSPs is described how the verification of the identity of (the representative of) the subscriber and the verification of the identity of the end-user takes place. See below. Exception to this is the situation if the subscriber is a natural person (CP part 3c). This can not be found in the CPSs of the CSPs because so far no certificates have been issued directly to civilians and this will probably not happen in the coming years.
Requirements (technical and contractual) for subordinate CAs in regards to whether or not subordinate CAs are constrained to issue certificates	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-

only within certain domains, and whether or not subordinate CAs can create their own subordinates.	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.
Requirements for sub-CAs to take reasonable measures to verify the ownership of the domain name and email address for end-entity certificates chaining up to the root, as per section 7 of http://www.mozilla.org/projects/security/certs/policy/. a) domain ownership/control b)email address ownership/control c) digitally signing code objects -- entity submitting the certificate signing request is the same entity referenced in the certificate	All CSPs perform an extensive identity validation check and organizational validation check regarding the (representative of the) subscriber (governmental organization or commercial company) and the end-user. Domain Ownership/Control: CP Part 3b: 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). 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: 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 CP Part 3a: 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. Code Signing Subscriber Identity: CP part 3b: 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. 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.
CRL and OCSP	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)
Description of audit requirements for sub-CAs (typically in the CP or CPS)	The CSPs within the PKIoverheid hierarchy also have to comply with the ETSI TS 101 456 standard. This is audited annually by the auditor. When a CSP uses a RA or LRA for e.g. an identity check than this process will also be included in the audit. PKIoverheid has a number of additional requirements for the CSPs which are also annually reviewed by the auditor. See the tables below for the audit certificates for each CSP.

5 CSP are evaluated below. The first table contains the 3 CSPs that issue SSL certificates. The second table contains the 2 CSPs that do not currently issue SSL certificates. The sub-CAs for these CSPs are currently signed by the “Staat der Nederlanden Root CA” which is already included in NSS. They are evaluated here because they will be migrated to the new root, “Staat der Nederlanden Root CA – G2”, which is under evaluation for inclusion.

Table of CSP’s that issue SSL certificates

Info	**Data**	**Data**	**Data**
Sub-CA	DigiNotar	GetronicsPinkRoccade	CIBG/UZI-register
URL	http://www.diginotar.nl	http://www.getronicspinkroccade.nl/	http://www.cibg.nl/
Sub-CA CP/CPS	CPS: https://www.diginotar.nl/Portals/7/Voorwaarden/CPS%20DigiNotar%20PKIoverheid%20domein%20overheid%20v1.2.3.pdf CPS services: https://www.diginotar.nl/Portals/7/Voorwaarden/CPS%20DigiNotar%20PKIoverheid%20Services%20v1.2.2.pdf	http://www.pinkroccadecsp.nl/website/files/Getronics_PinkRoccade_PKIoverheid_CPS_v4.2.pdf	https://www.uzi-register.nl/pdf/20081001_CPS_UZI-register_4.1d.pdf
Subscriber verification Section 7 of Mozilla Policy	No statement is made in the CPS services from CSP DigiNotar about the verification of a domain name. However in the application form for PKIoverheid SSL certificates the subscriber has to fill in who is the domain owner. In paragraph 2 of the form it is stated that “a proof of ownership of the domain name of the organization is	In CPS paragraph 3.2.3.2.2 it is stated that “the subscriber has to provide evidence about the identifier (aka the domain name) of the server. Getronics will then assess if the supplied evidence is accurate and complete”. In CPS paragraph 3.2.2 it is stated that a	In CPS paragraph 3.2.3 it is stated that “At the request of server certificates UZI Register will verify the records of the SIDN (aka www.domain-registry.nl more info can be found here: http://www.sidn.nl/ace.php/c,728,122,,,,Home.html) or the Internet Assigned Numbers Authority (IANA)) whether the

	required. The subscriber has to fulfil this request by handing over evidence of this ownership which can be obtained at www.domain-registry.nl” English: http://www.domain-registry.nl/ace.php/c,728,122,,,,Home.html (aka SIDN). The application form can be found here: https://www.diginotar.com/Portals/7/Aanvraagformulier/Aanvraagformulier%20PKIoverheid%20Services%20certificaat%20SSL%20V4.1.pdf In CPS paragraph 4.3 it is stated that the Registration Authority (in the case of DigiNotar that is a solicitor) will verify the surname, first name, date of birth, birth place, ID number, Location ID Issuance and the validity of the ID (of the representative) of the subscriber. Furthermore the RA will verify, on the basis of The Dutch Trade Register (http://www.kvk.nl/english/traderegister/default.asp) whether the (representative of) subscriber may represent the organization, whether the name of the organization is true and whether the address of the organization is correct. In CPS paragraph 4.9 it is stated that DigiNotar checks the identity of the end-user. Evidence of the identity is checked by the RA on the basis of physical appearance of the end-user.	(representative of a) subscriber has to fill in a form to become registered as a subscriber. This form can be found here: http://www.pinkroccadecsp.nl/website/files/PKIoverheid%20-%20Abonnee%20Registratie.doc) CSP Getronics will then verify whether the (representative of) subscriber may represent the organization, whether the name of the organization is true and whether the address of the organization is correct. Regarding the verification the CSP Getronics will use The Dutch Trade Register or, if it is a government organization, the constitution. This is stated in the form on page 2. In addition CSP Getronics will verify the ID (of the representative) of the subscriber. They verify the surname, first name, date of birth, birth place, ID number, Location ID Issuance, the validity of the ID, the signature and the photo (of the representative) of the subscriber. The subscriber will receive a message when all the information is in order. In CPS paragraph 4.2.2.1it is stated that Getronics checks the identity of the end-user. Evidence of the identity is checked by the RA (in the case of Getronics that is an employee of GWK Travelex (http://www.travelex.com/nl/Default.asp?content=&lang=ENG)) on the basis of	subscriber is the owner of the domain name.” In CPS paragraph 7.1.3 it is stated that “the email address is not included within the certificate profile for the UZI-register.” In CPS paragraph 3.2.2 and 3.2.3 it is stated that CSP CIBG/UZI-register will verify the surname, first name, ID number and the validity of the ID (of the representative) of the subscriber. Furthermore the CSP CIBG/UZI-register will verify, on the basis of The Dutch Trade Register whether the (representative of) subscriber may represent the organization, whether the name of the organization is true and whether the address of the organization is correct. In CPS paragraph 3.2.3 it is stated that CIBG/UZI-register checks the identity of the end-user. Evidence of the identity is checked on the basis of physical appearance of the end-user.

		physical appearance of the end-user.	
DV or OV?	OV	OV	OV
Potentially Problematic Practices	The one particular to DigiNotar is 1.3 Delegation of Domain / Email validation to third parties DigiNotar has 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 one particular to Getronics is 1.3 Delegation of Domain / Email validation to third parties Getronics has 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.	There are none that are specific to CIBG/UZI-register.
Audit	Auditor: PricewaterhouseCoopers Statement of Audit based on ETSI 101 456 criteria: http://www.diginotar.nl/Portals/7/ETSI/Certificate.pdf	Auditor: BSI Management Systems Statement of compliance with ETSI 101 456 criteria: https://www.pki.getronicspinkroccade.nl/website/files/Getronics%20-%20ETSI%20certificate%20by%20BSI.pdf	Auditor: BSI Management Systems Statement of compliance with ETSI 101 456 criteria: https://bugzilla.mozilla.org/attachment.cgi?id=360053
CRL	In CPS paragraph 5.6.8 it is stated that "The Revocation status information is updated at least every half hour."	In CPS paragraph 4.9.6 it is stated that "CRL issuance frequency is once every four hours"	In CPS paragraph 4.10 it is stated that "UZI-register issues a new CRL every 3 hours"
OCSP	http://validation.diginotar.nl/ In CPS paragraph 5.5.3 it is stated that "the OCSP validation information is at least equal to, and as current as the information provided on the basis of CRL validation".	http://ocsp.pinkroccade.com/ In CPS paragraph 4.9.8 it is stated that "the OCSP validation information is as current as the information provided on the basis of CRL validation but it can be more accurate than the information that is communicated through the CRL. This is only the case if a withdrawal of a certificate has taken place and the regular renewal of the CRL has not yet taken place".	http://ocsp.uzi-register.nl In CPS paragraph 4.9.9 it is stated that "the OCSP validation information is as current as the information provided on the basis of CRL validation but it can be more accurate than the information that is communicated through the CRL. This is only the case if a withdrawal of a certificate has taken place and the regular renewal of the CRL has not yet taken place".

Table of CSP's that do not issue SSL certificates

Info Needed	**Data**	**Data**
Sub-CA Name	ESG	Defensie
Sub-CA URL	http://www.de-electronische-signatuur.nl/cms/	http://www.mindef.nl/en/
Sub-CA CP/CPS	http://www.de-electronische-signatuur.nl/downloads/CPS_080213.pdf	http://cps.dp.ca.mindef.nl/mindef-ca-dp-cps/CPS%20Certificatie%20Autoriteit%20Defensie%20v.1.2.pdf
Subscriber verification Section 7 of Mozilla Policy	At this moment the CSP ESG does not issue server certificates (e.g. SSL certificates). They only issue certificates for personal use (authentication, encryption and non-repudiation) to end users. In CPS paragraph 2.3 it is stated that (a representative of) a subscriber has to fill in a form. In this form (the representative of) the subscriber (government organization or commercial company) has to fill in the registration number of The Dutch Trade Register (KvK nummer). The form can be found here: http://www.de-electronische-signatuur.nl/downloads/reg_formulieren/OCD.pdf The form and the supplied information are checked by a Local Registration Authority (LRA). In the same paragraph of the CPS from ESG it is stated that ESG checks the identity of the end-user. Evidence of the identity is checked by the LRA on the basis of physical appearance of the end-user. A list of LRAs used by CSP ESG can be found here: http://www.de-electronische-signatuur.nl/cms/nl/lrao-partneroverzicht.html	The CSP Defensie does not issue server certificates (e.g. SSL certificates). They only issue certificates for personal use (authentication, encryption and non-repudiation) to end users. CPS Paragraph 9.4.2 describes which attributes are included in the certificates issued by the CSP Defensie. The attributes are: surname, initials, name, employee number, public encryption key, public authentication and signing key. **So no email address is included in the certificate.** In CPS paragraph 3.2.2 it is stated that only the system used for HRM purposes within the Ministery of Defense organization (PeopleSoft that is) can be used to request a certificate. It is not possible to request a certificate without the use of the PeopleSoft system. In paragraph 3.2.3 it is stated that CSP Defensie checks the identity of the end-user. Evidence of the identity is checked on the basis of physical appearance of the end-user.
DV or OV?	N/A – not issuing SSL certs.	N/A – not issuing SSL certs
Potentially Problematic Practices	There is one that applies to ESG: 1.3 Delegation of Domain / Email validation to third parties ESG has delegated parts of their process regarding the organization and end-user identity check to third parties. Nevertheless when a CSP within the PKIoverheid	There are none that are specific to Defensie.

	hierarchy uses a RA or LRA for e.g. an identity check than this process will also be included in the audit.	
Audit	Auditor: BSI Management Systems Statement of compliance with ETSI 101 456 criteria: http://www.de-electronische-signatuur.nl/downloads/BSI%20Certificaat.pdf	Auditor: BSI Management Systems Statement of compliance with ETSI 101 456 criteria: https://bugzilla.mozilla.org/attachment.cgi?id=360055
CRL	In CPS paragraph 4.1.2.2 it is stated that “The CRL is renewed every 4 hours.”	In CPS paragraph 4.9.7 it is stated that “The CRL is issued once every 4 hours”
OCSP	http://pks.esg4.eu/ocspesgnl In the CPS from ESG no real statement is made about the update frequency from the OCSP. Nevertheless ESG has to comply with the requirement as described in the PKIoverheid CP. Furthermore the auditor will check this during the annual audit. The auditor has stated that ESG meets the additional requirements from PKIoverheid.	http://ocsp.dp.ca.mindef.nl In the CPS from Defensie no real statement is made about the update frequency from the OCSP. Nevertheless Defensie has to comply with the requirement as described in the PKIoverheid CP. Furthermore the auditor will check this during the annual Audit. The auditor has stated that Defensie meets the additional requirements from PKIoverheid.