Bugzilla ID: 1015862
Bugzilla Summary: Staat der Nederlanden Root CA - G3 Inclusion Request

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	Staat der Nederlanden (represented by Logius)
Website URL	http://www.logius.nl/producten/toegang/pkioverheid/ (Dutch Language) http://www.logius.nl/english/products/access/pkioverheid/ (English language)
Organizational Type	The Netherlands national government CA
Primark Market / Customer Base	The Dutch governmental PKI (a.k.a. PKIoverheid) is the Public Key Infrastructure designed for trustworthy electronic communication within and with the Dutch government. The activities of PKIoverheid are primarily focused on the geographic region of The Netherlands.
Impact to Mozilla Users	The Dutch governmental PKI is the Public Key Infrastructure designed for trustworthy electronic communication within and with the Dutch government. To reach this goal a national PKI certificate hierarchy has been created. At present the national PKI hierarchy consists of four roots (1 based on SHA-1, 2 based on SHA-256 and 1 Extended Validation based on SHA-256). Each root has one or more sub CAs known as domain CAs or intermediate CAs. Each domain or intermediate CA services multiple Certificate Service Providers (CSPs). The purpose of the G3 Root is to enable CSPs to issue certificates to their customers. The CSPs (commercial and governmental organisations) will issue several types of certificates, such as authentication, encryption, non-repudiation and SSL, to end-users. End-users can be companies and governmental organisations. The PKIoverheid does not issue certificates directly to end-users, the PKIoverheid only issues certificates to CSPs. The Ministry of the Interior and Kingdom Relations (represented by Logius) is the owner of the PKIoverheid. Logius supports the Dutch Minister of the Interior and Kingdom Relations with the management and control of the PKI

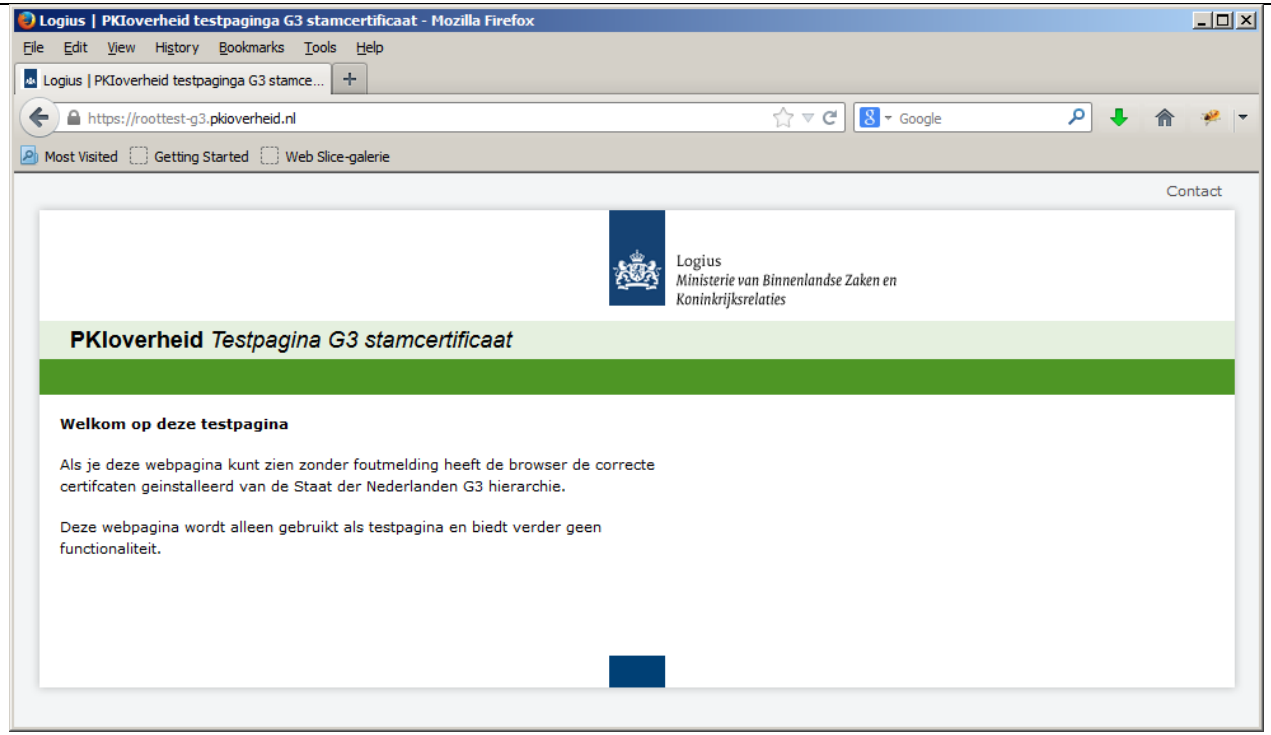
	system.
Inclusion in other major browsers	The Staat der Nederlanden has root certificates included in the products of the following vendors: • Mozilla (first and second generation Root certificate); • Microsoft; • Apple; • Adobe.
CA Primary Point of Contact (POC)	Douglas Skirving M: douglas.skirving@logius.nl T: +31 (0)6 534 255 06 Mark Janssen M: mark.janssen@logius.nl T: +31 – (0)70 8887 967

Technical information about each root certificate

Certificate Name	Staat der Nederlanden Root CA - G3
Certificate Issuer Field	CN = Staat der Nederlanden Root CA - G3 O = Staat der Nederlanden C = NL
Certificate Summary	The Staat der Nederlanden Root CA – G3 is the third generation Root CA of the Dutch governmental PKI (PKIoverheid). This Public Key Infrastructure was designed for trustworthy electronic communication within and with the Dutch government. The first and second generation Root CAs are included in the Mozilla Root Programme. The G3 Root CA acts as the successor of the presently included G2 Root CA. The Root CAs in the PKIoverheid have a validity of 15 years, and are replaced according to a fixed timetable. During the first 6 years of its validity the Root CA is used to issue sub-CAs. After 6 years a new generation Root CA is created leaving the previous generation to be used for validation purposes.
Root Cert URL	http://cert.pkioverheid.nl/RootCA-G3.cer
SHA1 Fingerprint	d8 eb 6b 41 51 92 59 e0 f3 e7 85 00 c0 3d b6 88 97 c9 ee fc
Valid From	2013-11-14
Valid To	2028-11-14
Certificate Version	v3
Certificate Signature Algorithm	sha256RSA

Signing Key Parameters	RSA modulus length 4096 bits.
Test Website URL (SSL)	https://roottest-g3.pkioverheid.nl
CRL URL	The PKIoverheid G3 hierarchy consists of three tiers which are detailed in the "CA hierarchy" section below. At present one CSP is in operation within the G3 hierarchy, in the Organization Services domain. The other CSPs in the PKIoverheid ecosystem have not yet been issued with subroots under the G3 hierarchy. More information on the other CSPs can be found here: https://bugzilla.mozilla.org/show_bug.cgi?id=551399 The following CRLs for the G3 root are presently available: **Validation of Domain (subordinate CA) certificates:** http://crl.pkioverheid.nl/RootLatestCRL-G3.crl **Validation of CSP (subordinate CA) certificates in the Organization Services domain:** http://crl.pkioverheid.nl/DomOrganisatieServicesLatestCRL-G3.crl **Validation of CSP (subordinate CA) certificates in the Organization Person domain:** http://crl.pkioverheid.nl/DomOrganisatiePersoonLatestCRL-G3.crl **Validation of CSP (subordinate CA) certificates in the Citizen domain:** http://crl.pkioverheid.nl/DomBurgerLatestCRL-G3.crl **Validation of CSP (subordinate CA) certificates in the Autonomous Devices domain:** http://crl.pkioverheid.nl/DomAutonomeApparatenLatestCRL-G3.crl **Validation of end-entity certificates issued by KPN Corporate Market in the Organization Services domain:** http://cert.managedpki.com/crl/KPNCorporateMarketCSPOrganisatieServicesCAG3/LatestCRL.crl This end-entity certificate CRL is updated and reissued every 4 hours and the nextUpdate field value is 24 hours (section 4.9.6 of the KPN PKIoverheid CPS: https://certificaat.kpn.com/files/CPS/KPN_PKIoverheid_CPS_v4.19.pdf). This is in conformance with requirement 4.9.7.1 of the CP (Part 3b of the Programme of Requirements: http://www.logius.nl/fileadmin/logius/product/pkioverheid/documenten/PoR_EN_part3b_v3.6.pdf) "The CSP has to update and reissue the CRL for end user certificates at least once every 7 calendar days and the date of the "Next update" field may not exceed the date of the "Effective date" field by 10 calendar days." **Test: Results of importing into Firefox browser**

	We were unable to import the CRL into Firefox as version 29 lacks the GUI to do so.
OCSP URL	The following OCSP URLs are in use within the PKIoverheid G3 hierarchy: **Validation of Domain Organisation Services subordinate CA certificate** http://rootocsp-g3.pkioverheid.nl **Validation of CSP (subordinate CA) certificate in the Organisation Services domain:** http://domorganisatieservicesocsp-g3.pkioverheid.nl **Validation of end-entity certificates issued by KPN Corporate Market:** http://ocsp3.managedpki.com **The maximum time elapsing from the revocation of an end entity or CA certificate until OCSP responders are updated to reflect that revocation.** Requirement 4.9.5-1 of the CP (Part 3b of the Programme of Requirements: http://www.logius.nl/fileadmin/logius/product/pkioverheid/documenten/PoR_EN_part3b_v3.6.pdf) states that "The maximum delay between receiving a revocation request or revocation report and the amendment of the revocation status information, that is available to all relying parties, is set at four hours." This requirement hold true for revocation status information by means of both CRL and OCSP. **Maximum expiration time of OCSP responses** Requirement 4.9.5-1 of the CP (Part 3b of the Programme of Requirements: http://www.logius.nl/fileadmin/logius/product/pkioverheid/documenten/PoR_EN_part3b_v3.6.pdf): "If the CSP supports OCSP, the CSP has to update the OCSP service at least once every 4 calendar days. The maximum expiry term of the OCSP responses is 10 calendar days". Test: Using OCSP validation in Firefox and treating the certificate as invalid when an OCSP server connection fails the webpage https://roottest-g3.pkioverheid.nl/ was requested, resulting in the following successful test:

	
Requested Trust Bits	Websites (SSL/TLS) Email (S/MIME)
SSL Validation Type	OV
Non-sequential serial numbers and entropy in cert	The PKIoverheid CP states the following regarding serial numbers and allowed hashing algorithms: **Basic Attribute: SerialNumber** All end user certificates have to contain at least 8 bytes of unpredictable random data in the certificate's serial number (SerialNumber). **Basic Attribute: Signature** For certificates under the G2 root certificate, only sha-256WithRSAEncryption is allowed. This requirement also applies on the G3 root hierarchy.

	Page 53 of the CP (Part 3b of the Programme of Requirements: http://www.logius.nl/fileadmin/logius/product/pkioverheid/documenten/PoR_EN_part3b_v3.6.pdf).

CA Hierarchy information for each root certificate

CA Hierarchy	The PKIoverheid G3 hierarchy consists of three tiers; Root CA, Domain Subroot CA and CSP Subroot CA. This hierarchy is described in further detail below: **Tier 1: Root CA** • Staat der Nederlanden Root CA – G3 This internally operated offline Root CA is the trust anchor of the third generation root hierarchy of PKIoverheid. This CA is only used to sign Domain Subroot CA's and corresponding status information. **Tier 2: Domain Subroot CAs** • Domain Organisation Person: Staat der Nederlanden Organisatie Persoon CA – G3 This internally operated offline Domain Subroot CA is used to sign CSP Subroot CAs in the domain Organisation Person. **Tier 3: Organisation Person CSP Subroot CA** • At present no CSP Subroot CA has been issued in the domain Organisation Person. • Domain Organisation Services: Staat der Nederlanden Organisatie Services CA – G3 This internally operated offline Domain Subroot CA is used to sign CSP Subroot CAs in the domain Organisation Services. **Tier 3: Organisation Person CSP Subroot CA** • CSP KPN Corporate Market: KPN Corporate Market CSP Organisatie Services CA - G3 This externally operated online CSP Subroot CA is operated by KPN Corporate Market to issue end entity certificates to their subscribers. • Domain Citizen: Staat der Nederlanden Burger CA – G3 This internally operated offline Domain Subroot CA is used to sign CSP Subroot CAs in the domain Citizen. **Tier 3: Citizen CSP Subroot CA** • At present no CSP Subroot CA has been issued in the domain Organisation Person. • Domain Autonomous Devices: Staat der Nederlanden Autonome Apparaten CA – G3 This internally operated offline Domain Subroot CA is used to sign CSP Subroot CAs in the

	domain Autonomous Devices. **Tier 3: Autonomous Devices CSP Subroot CA** • At present no CSP Subroot CA has been issued in the domain Organisation Person. Please see section 2.4 of part 1 of the PKIoverheid Programme of Requirements (http://www.logius.nl/fileadmin/logius/product/pkioverheid/documenten/PoR_EN_part1_v3.6.pdf) for more information on the PKI design.
Externally Operated SubCAs	**CA Policies about Third-Party Subordinate CAs** PKIoverheid issues sub-CA certificates to Certificate Service Providers. In turn those CSPs issue certificates to end users. The operation of PKIoverheid is governed by the Programme of Requirements. This collection of documents contains all requirements CSPs operating under PKIoverheid must adhere to. The English translation of this Programme of Requirements is available through http://www.logius.nl/english/products/access/pkioverheid/. The PoR consists of four parts: - Part 1: Introduction - Part 2: CSP Requirements - Part 3: Certificate Policies - Part 4: Definitions and abbreviations *1. General description of the sub-CAs operated by third parties.* The sub-CAs within PKIoverheid consist of governmental and commercial parties who issue end entity certificates to communicate with Dutch government These CSPs have to be reliable organizations that fulfil high requirements in respect of their operational procedures, technical devices, security of information, expertise and reliability of staff and the provision of information to their target group. For more information on the PKIoverheid setup please see part 1 of the PoR (http://www.logius.nl/fileadmin/logius/product/pkioverheid/documenten/PoR_EN_part1_v3.6.pdf). *2. Selection criteria for sub-CAs* CSPs within PKIoverheid have to adhere to the requirements laid out in part 2 of the Programme of Requirements (http://www.logius.nl/fileadmin/logius/product/pkioverheid/documenten/PoR_EN_part2_v3.6.pdf) . As stipulated in section 2.2 of part 2 of the PoR CSPs must demonstrate compliance by - certifying against ETSI EN 319 411-2, in accordance with the TTP.NL scheme. - certifying against ETSI TS 102 042, in accordance with the TTP.NL scheme, when issuing Services certificates - demonstrating the fulfilment of PKIoverheid requirement by means of an unqualified audit opinion.

	- certifying against WebTrust for Certification Authorities – Extended Validation audit, when issuing EV certificates - registering with the ACM (Autoriteit Consument en Markt – Authority for Consumers and Markets). Once a CSP can demonstrate compliance it can start the admittance process by making a formal application. This application is then vetted by PKIoverheid. See section 2.3 of part 2 of the PoR for more detail. *3. The CP/CPS that the sub-CAs are required to follow.* Depending on the types of certificates they issue CSPs have to follow one or more of the Certificate Policies stated below • Part 3a: Certificate policy Government, Companies and Organizations (http://www.logius.nl/fileadmin/logius/product/pkioverheid/documenten/PoR_EN_part3a_v3.6.pdf) • Part 3b: Certificate policy Services (http://www.logius.nl/fileadmin/logius/product/pkioverheid/documenten/PoR_EN_part3b_v3.6.pdf) • Part 3c: Certificate policy Citizen (http://www.logius.nl/fileadmin/logius/product/pkioverheid/documenten/PoR_EN_part3c_v3.6.pdf) • Part 3d: Certificate policy Autonomous Devices (http://www.logius.nl/fileadmin/logius/product/pkioverheid/documenten/PoR_EN_part3d_v3.6.pdf) • Part 3e: Certificate policy - Extended Validation (http://www.logius.nl/fileadmin/logius/product/pkioverheid/documenten/PoR_EN_part3e_v3.6.pdf) *4. Sub-CA constraints* 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 cannot 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. *5. Sub-CA verification requirements*

	Domain ownership/control: The requirements in the Programme of Requirements (http://www.logius.nl/fileadmin/logius/product/pkioverheid/documenten/PoR_EN_part3b_v3.6.pdf) regarding the subject.commonName (page 56) and subjectAltName.dNSName (page 64) state that "The subscriber MUST prove that the organization can use this name. In services server certificates [OID 2.16.528.1.1003.1.2.2.6 and 2.16.528.1.1003.1.2.5.6] the CSP MUST check recognized registers (Stichting Internet Domeinregistratie Nederland (SIDN) or Internet Assigned Numbers Authority (IANA)) to find out whether the subscriber is the domain name owner or whether the subscriber is exclusively authorized by the registered domain name owner to use the domain name on behalf of the registered domain name owner." Email address ownership/control : The email address of the certificate holder may be included in the certificate. The requirements on the SubjectAltName.rfc822Name attribute in part 3a of the PoR (http://www.logius.nl/fileadmin/logius/product/pkioverheid/documenten/PoR_EN_part3a_v3.6.pdf) (page 53) state that: "If the e-mail address is included in the certificate, the CSP MUST: - have the subscriber sign his/her approval for these and; - check that the e-mail address belongs to the subscriber's domain, or; - check that the e-mail address belongs to the subscriber (e.g. the professional) and that this person has access to the e-mail address (for example by performing a challenge response)." Digitally signing code: Not applicable. PKIoverheid does not intend to issue Code Signing certificates within the G3 hierarchy. 6. Description of audit requirements for sub-CAs (typically in the CP or CPS) In order to join the PKI for the government, a CSP is certified under the TTP.NL scheme. This scheme is applicable in the Netherlands when becoming certified under ETSI EN 319 411-2 and/or ETSI TS 102 042. The CSPs are responsible for their own certification. The certification audits can be performed by an auditor accredited for the auditing against the TTP.NL scheme. Currently BSI Group The Netherlands B.V. and PricewaterhouseCoopers Certification B.V. have obtained accreditation of the Raad voor Accreditatie (Dutch Accreditation Council) (http://www.rva.nl)

The TTP.NL schema certificate is valid for three years, with the obligation for the CSPs to undergo a yearly verification audit.

Third-Party Subordinate CAs that are not Technically Constrained

KPN Corporate Market CSP CA

Company name	KPN Corporate Market
Corporate URL	http://certificaat.kpn.com
Sub-CA certificate	see attachment to bug
URL to test website	https://roottest-g3.pkioverheid.nl
General CA hierarchy under the sub-CA	No sub-CAs have been issued under this sub-CA
CPS (Dutch)	https://certificaat.kpn.com/files/CPS/KPN_PKIoverheid_CPS_v4.19.pdf
Ownership verification	*Domain ownership/control:* Section 3.2.3.2.2 of KPN PKIoverheid CPS (https://certificaat.kpn.com/files/CPS/KPN_PKIoverheid_CPS_v4.19.pdf) states that: Translation: "The Subscriber must prove that the organisation is entitled to use the primary and additional names that identify the server or service. The primary and additional names of the server MUST be states as "fully-qualified domain name" (FQDN, see definitions)." (Original text: "De abonnee moet aantonen dat de organisatie de primaire en additionele namen die de server of de service identificeren, mag voeren. De primaire en additionele namen van de server MOETEN vermeld worden als "fully-qualified domain name" (FQDN, zie definities).") Section 4.2.2.3 of KPN PKIoverheid CPS describes the verification of Domain Name Ownership by the KPN Corporate Market CSP. Translation: "Among others, checks are made in recognized registers such as Stichting Internet Domeinregistratie Nederland (SIDN) or Internet Assigned Numbers Authority (IANA) to validate whether Subscriber owns the domain name as it appears in the e-mail address. In addition an assessment is made to determine URL-spoofing or phishing. http://www.phishtank.com or similar is consulted to see whether the domain name does not

		appears on a spam and/or phishing blacklist. If KPN suspects phishing or other potential abuse those suspicions will be reported to http://www.phishtank.com. ") ” (Original text: “KPN neemt de Certificaataanvraag in ontvangst en beoordeelt de volledigheid en de juistheid van de aanvraag. Onder andere wordt bij erkende registers als Stichting Internet Domeinregistratie Nederland (SIDN) of Internet Assigned Numbers Authority (IANA) gecontroleerd of Abonnee eigenaar is van de domeinnaam, zoals die onder deel uitmaakt van het e-mail adres. Daarnaast wordt beoordeeld of sprake is van url-spoofing of phishing. En zo wordt ook http://www.phishtank.com of vergelijkbaar geraadpleegd om te bezien of de domeinnaam niet voorkomt op een spam-en/of phishing blacklist. Als KPN een verdenking heeft van phishing of ander mogelijk misbruik zal het die verdenking melden bij http://www.phishtank.com.”) *Email address ownership/control:* Section 4.2.2.1 of KPN PKIoverheid CPS (https://certificaat.kpn.com/files/CPS/KPN_PKIoverheid_CPS_v4.19.pdf) describes the verification by the KPN Corporate Market CSP. Translation: “Checks are made in recognized registers such as Stichting Internet Domeinregistratie Nederland (SIDN) or Internet Assigned Numbers Authority (IANA) to validate whether Subscriber owns the domain name as it appears in the e-mail address.” (Original text: “Onder andere wordt bij erkende registers als Stichting Internet Domeinregistratie Nederland (SIDN) of Internet Assigned Numbers Authority (IANA) gecontroleerd of Abonnee eigenaar is van de domeinnaam, zoals die onderdeel uitmaakt van het e-mail adres.”) *Digitally signing code objects:* Not applicable, PKIoverheid does not intend to issue Code Signing certificates under the G3 hierachy.
	SSL category	OV
	Problematic Practises	None. KPN does not use PKCS#12 objects for distribution of key material.

		Please see the Problematic Practices section at the bottom of this document for a review of the other problematic practices.
	Audit report	Certificate of Registration: https://certificaat.kpn.com/files/ETSI/Getronics%20-%20ETSI%20certificate%20by%20BSI.pdf
Cross Signing	Not applicable. At present no cross signing has been performed in the PKIoverheid G3 hierarchy.	
Technical Constraints on Third-party Issuers	No technical constraints are in place for the CSP Subroot CAs within the PKIoverheid G3 hierarchy. CSPs that want to issue certificates under the PKIoverheid hierarchy have to be certified against ETSI EN 319 411 and/or ETSI TS 102 042 in accordance with the TTP.NL scheme. In addition the CSP must demonstrate that it fulfils the additional PKIoverheid requirements by means of an unqualified audit opinion. See section 2.2 of part 2 of the PKIoverheid Programme of Requirements (http://www.logius.nl/fileadmin/logius/product/pkioverheid/documenten/PoR_EN_part2_v3.6.pdf).	

Verification Policies and Practices

Policy Documentation	Language(s) that the documents are in: **Staat der Nederlanden Root and Domain CAs (Tier 1 and 2)** CP (English): • Part 3a: Certificate policy Government, Companies and Organizations (http://www.logius.nl/fileadmin/logius/product/pkioverheid/documenten/PoR_EN_part3a_v3.6.pdf) • Part 3b: Certificate policy Services (http://www.logius.nl/fileadmin/logius/product/pkioverheid/documenten/PoR_EN_part3b_v3.6.pdf) • Part 3c: Certificate policy Citizen (http://www.logius.nl/fileadmin/logius/product/pkioverheid/documenten/PoR_EN_part3c_v3.6.pdf) • Part 3d: Certificate policy Autonomous Devices (http://www.logius.nl/fileadmin/logius/product/pkioverheid/documenten/PoR_EN_part3d_v3.6.pdf) • Part 3e: Certificate policy - Extended Validation (http://www.logius.nl/fileadmin/logius/product/pkioverheid/documenten/PoR_EN_part3e_v3.6.pdf) CPS (Dutch): http://www.logius.nl/fileadmin/logius/product/pkioverheid/CPS_PA_PKIoverheid_v3.7.pdf **KPN Corporate Market CSP CA (Tier3)** CPS (Dutch):

	https://certificaat.kpn.com/files/CPS/KPN_PKIoverheid_CPS_v4.19.pdf Relying Party Agreement (English): https://certificaat.kpn.com/files/voorwaarden/Relying%20Party%20Agreement%20v1.3.1.pdf
Audits	**Staat der Nederlanden Root and Domain CAs (Tier 1 and 2)** Audit Type: • Trust Service Principles and Criteria for Certification Authorities • WebTrust®for Certification Authorities – SSL Baseline Requirements Audit Criteria, Version 1.1 – January 2013 Auditor: KPMG Advisory N.V. Auditor Website: http://www.kpmg.com/nl/nl/Pages/default.aspx URL to Audit Report and Management's Assertions: http://cert.webtrust.org/SealFile?seal=1652&file=pdf **KPN Corporate Market CSP CA (Tier3)** Audit Type: • Scheme for the certification of Certification Authorities against ETSI TS 101 456 Auditor: BSI Auditor Website: http://www.bsigroup.com/ URL to Certificate of Registration: https://certificaat.kpn.com/files/ETSI/Getronics%20-%20ETSI%20certificate%20by%20BSI.pdf
Baseline Requirements (SSL)	Commitment to Comply with the CA/Browser Forum Baseline Requirements is voiced as follows: **Staat der Nederlanden Root and Domain CAs (Tier 1 and 2)** Verification of compliance with the CA/Browser Forum Baseline Requirements is included in the WebTrust audit (http://cert.webtrust.org/SealFile?seal=1652&file=pdf) **KPN Corporate Market CSP CA (Tier 3)** Section 1.3 of KPN PKIoverheid CPS (https://certificaat.kpn.com/files/CPS/KPN_PKIoverheid_CPS_v4.19.pdf): Translation: KPN conforms to the current version of the Baseline Requirements for Issuance and Management of Publicly Trusted Certificates as published on http://www.cabforum.org. (Original text: "KPN conformeert zich aan de huidige versie van de Baseline Requirements for Issuance and Management of Publicly Trusted Certificates zoals gepubliceerd op http://www.cabforum.org.")
SSL Verification Procedures	The requirements in the Programme of Requirements

	(http://www.logius.nl/fileadmin/logius/product/pkioverheid/documenten/PoR_EN_part3b_v3.6.pdf) regarding the subject.commonName (page 56) and subjectAltName.dNSName (page 64) state that “The subscriber MUST prove that the organization can use this name. In services server certificates [OID 2.16.528.1.1003.1.2.2.6 and 2.16.528.1.1003.1.2.5.6] the CSP MUST check recognized registers (Stichting Internet Domeinregistratie Nederland (SIDN) or Internet Assigned Numbers Authority (IANA)) to find out whether the subscriber is the domain name owner or whether the subscriber is exclusively authorized by the registered domain name owner to use the domain name on behalf of the registered domain name owner.” Section 3.2.3.2.2 of KPN PKIoverheid CPS (https://certificaat.kpn.com/files/CPS/KPN_PKIoverheid_CPS_v4.19.pdf) states that: Translation:“The Subscriber must prove that the organisation is entitled to use the primary and additional names that identify the server or service. The primary and additional names of the server MUST be states as “fully-qualified domain name” (FQDN, see definitions).” (Original text: “De abonnee moet aantonen dat de organisatie de primaire en additionele namen die de server of de service identificeren, mag voeren. De primaire en additionele namen van de server MOETEN vermeld worden als “fully-qualified domain name” (FQDN, zie definities).”) Section 4.2.2.3 of KPN PKIoverheid CPS describes the verification of Domain Name Ownership by the KPN Corporate Market CSP. Translation: “Among others, checks are made in recognized registers such as Stichting Internet Domeinregistratie Nederland (SIDN) or Internet Assigned Numbers Authority (IANA) to validate whether Subscriber owns the domain name as it appears in the e-mail address. In addition an assessment is made to determine URL-spoofing or phishing. http://www.phishtank.com or similar is consulted to see whether the domain name does not appears on a spam and/or phishing blacklist. If KPN suspects phishing or other potential abuse those suspicions will be reported to http://www.phishtank.com. ") ” (Original text: “KPN neemt de Certificaataanvraag in ontvangst en beoordeelt de volledigheid en de juistheid van de aanvraag. Onder andere wordt bij erkende registers als Stichting Internet Domeinregistratie Nederland (SIDN) of Internet Assigned Numbers Authority (IANA) gecontroleerd of Abonnee eigenaar is van de domeinnaam, zoals die onder deel uitmaakt van het e-mail adres. Daarnaast wordt beoordeeld of sprake is van url-spoofing of phishing. En zo wordt ook http://www.phishtank.com of vergelijkbaar geraadpleegd om te bezien of de domeinnaam niet

	voorkomt op een spam-en/of phishing blacklist. Als KPN een verdenking heeft van phishing of ander mogelijk misbruik zal het die verdenking melden bij http://www.phishtank.com.")
Organization Verification Procedures	The Certificate Policies of PKIoverheid require the following regarding Organization verification: *Requirement 3.2.2.1* "In relation to organization-linked certificates, the CSP has to verify that the subscriber is an existing organization." *Requirement 3.2.2.2* "In terms of organization-linked certificates, the CSP has to verify that the name of the organization registered by the subscriber that is incorporated in the certificate, is correct and complete" The subject.organizationName attribute is filled with the "Full name of the subscriber in accordance with the accepted document or Basic Registry", according to page 48 of part 3a and page 58 of part 3b of the Programme of Requirements. (http://www.logius.nl/fileadmin/logius/product/pkioverheid/documenten/PoR_EN_part3a_v3.6.pdf and http://www.logius.nl/fileadmin/logius/product/pkioverheid/documenten/PoR_EN_part3b_v3.6.pdf) Section 3.2.2. of the KPN PKIoverheid CPS (https://certificaat.kpn.com/files/CPS/KPN_PKIoverheid_CPS_v4.19.pdf) describes the authentication of the Subscriber. Relevant sections have been translated below. Translation: "" If an organization wants to become a Subscriber of KPN it must complete the appropriate 'Subscriber Registration' form. This form comes with a detailed explanation . The Subscriber must include a number of supporting documents with the form. ... The evidence that must be submitted at the same time as the form is: - The existence of the organization and the accuracy and completeness of its name ; - If a government agency wants to make use of Digikoppeling : an extract from the Digikoppeling Service Registry; - The authority of the Legal Representative to represent the Subscriber ; - Copy of the identity of the Legal Representative that meets the requirements of the Law on Identification Act (hereinafter : WID) if the Legal Representative of the application provides a handwritten signature; - Copy of the identity of each contact that is authorized on the form. Also, this identification must meet the requirements of the WID. ...

	On receipt of the appropriate form and accompanying documents KPN will evaluate the completeness and accuracy thereof, including the reference of external sources. Separation of duties is applied between the assessor and the decision maker. Only if the form is complete and correct, KPN will approve the form, proceed to registration, assign a Subscriber number and inform the subscriber on the application. The Subscriber number should always be used in communication between Subscriber and KPN. Only if an organization is registered as KPN Subscriber it can submit certificate requests to KPN." (Original text: "Als een organisatie Abonnee wil worden van KPN dient het het daartoe bestemde formulier Abonnee Registratie in te vullen. Bij dit formulier is een uitgebreide toelichting gevoegd. Met het formulier dient de Abonnee een aantal bewijsstukken mee te sturen. … De bewijzen die tegelijk met het formulier aangeleverd moeten worden betreffen: - het bestaan van de organisatie en de juistheid en volledigheid van diens naam; - indien een overheidsorganisatie gebruik wil maken van Digikopppeling: een uittreksel uit het DigikoppelingServiceregister; - de bevoegdheid van de Bevoegde Vertegenwoordiger om de Abonnee te vertegenwoordigen; - kopie van het identiteitsbewijs van de Bevoegd Vertegenwoordiger dat voldoet aan de eisen uit de Wet op de identificatieplicht (verder: Wid) indien de Bevoegde Vertegenwoordiger de aanvraag voorziet van een handgeschreven handtekening; - kopie van het identiteitsbewijs van elke Contactpersoon die op het formulier wordt geautoriseerd. Ook dit identiteitsbewijs moet voldoen aan de eisen van de Wid. … KPN zal het betreffende formulier en de bijbehorende bewijsstukken in ontvangst nemen en de volledigheid en de juistheid ervan beoordelen, onder andere door externe bronnen te raadplegen. Hierbij wordt functiescheiding toegepast tussen hij/zij die beoordeelt (controle) en hij/zij die beslist (beschikken). Alleen indien het formulier volledig en juist is, zal KPN het formulier goedkeuren, overgaan tot registratie, een abonneenummer toekennen en de Abonnee hierover informeren. Het abonneenummer dient steeds bij de communicatie tussen Abonnee en KPN worden gebruikt. Alleen indien een organisatie bij KPN is geregistreerd als Abonnee kan het certificaataanvragen indienen bij KPN.")
Email Address Verification Procedures	**Email address verification** The requirements on the SubjectAltName.rfc822Name attribute in part 3a of the PoR (http://www.logius.nl/fileadmin/logius/product/pkioverheid/documenten/PoR_EN_part3a_v3.6.pdf) (page 53)

	state that: “If the e-mail address is included in the certificate, the CSP MUST: - have the subscriber sign his/her approval for these and; - check that the e-mail address belongs to the subscriber's domain, or; - check that the e-mail address belongs to the subscriber (e.g. the professional) and that this person has access to the e-mail address (for example by performing a challenge response).” Section 4.2.2.1 of the KPN PKIoverheid CPS (https://certificaat.kpn.com/files/CPS/KPN_PKIoverheid_CPS_v4.19.pdf) describes the verification by the KPN Corporate Market CSP. Translation: “Checks are made in recognized registers such as Stichting Internet Domeinregistratie Nederland (SIDN) or Internet Assigned Numbers Authority (IANA) to validate whether Subscriber owns the domain name as it appears in the e-mail address.” (Original text: “Onder andere wordt bij erkende registers als Stichting Internet Domeinregistratie Nederland (SIDN) of Internet Assigned Numbers Authority (IANA) gecontroleerd of Abonnee eigenaar is van de domeinnaam, zoals die onderdeel uitmaakt van het e-mail adres.”) **Subscriber Identity verification** The Certificate Policies of PKIoverheid require the following regarding Subscriber Identity verification: *Requirement 3.2.3.1* “In both organization-linked and profession-linked certificates, the CSP has to verify that the full name used by the certificate holder that is incorporated in the certificate is correct and complete, including the surname, first forename, initials or other forename(s) (if applicable) and surname prefixes (if applicable).” *Requirement 3.2.5.1* “In terms of organization-linked certificate holders, the CSP has to check that: - the proof that the certificate holder, authorized to receive a certificate on behalf of the subscriber, is authentic; - the name and identity markers mentioned in this proof correspond with the certificate holder's identity established under 3.2.3. In terms of profession-linked certificate holders, the CSP has to check that: - the proof, that the certificate holder is authorised to practise the recognized profession, is authentic; - the name and identity markers mentioned in this proof correspond with the certificate holder's identity

	established under 3.2.3. *Requirement 3.2.5.2* "Subscriber is a legal personality (organization-linked certificates): The agreement that the CSP enters into with the subscriber has to state that the subscriber is responsible for immediately informing the CSP of any relevant changes that have been made to the relationship between the subscriber and the certificate holder, by means of a revocation request. Relevant changes can, in this respect, for instance be termination of employment and suspension. Subscriber is a natural person (occupation-linked certificates): The agreement that the CSP enters into with the subscriber has to state that the subscriber is responsible for immediately informing the CSP of any relevant changes that have been made by means of a revocation request. A relevant change in this respect is, in any case, no longer having legal proof as outlined in PKI-OO 3.2.5-1."
Code Signing Subscriber Verification Procedures	Not applicable, PKIoverheid does not intend to issue Code Signing certificates under the G3 hierachy.
Multi-factor Authentication	The PKIoverheid Certificate Policies stipulate the following regarding multi-factor authentication: *Requirement 6.5.1.1:* The CSP has to use multi-factor authentication (e.g. smartcard with personal certificates and a personal password or biometry and a personal password) for the system or the user accounts which are used to issue or approve certificates. Multi-factor authentication tokens cannot be connected permanently or semi-permanently to the system (e.g. a permanently activated smartcard). That is because this would enable certificates to be issued or approved (semi) automatically, or for non-authorized staff to issue or approve certificates. " *Requirement 6.5.1.2* "The staff of external Registration Authorities (RA) or Resellers may not have access to the system or the user accounts of the CSP which enables issuance or approval of certificates. This function is restricted to authorized staff of the CSP. If an RA or a Reseller does have this access, the RA or the Reseller will be seen as part of the CSP and it/they have to comply with the PKI for the government Programme of Requirements fully and demonstrably." *Requirement 6.5.1.3*

	"The CSP prevents unauthorized access to the following core services: registration service, certificate generation service, subject device provision service, dissemination service, revocation management service and revocation status service. To this end, these core services are separated either physically or logically from the non-PKI network domains, or the various core services will be implemented on separate network domains, where there has to be a unique authentication for each core service. If core services use the same network domains, the CSP enforces a unique authentication for each core service. The CSP documents the organization of the network domains, at least in a graphical manner." The requirements mentioned above are an extension to the System Access Management requirements put forth by ETSI. CSPs undergo an annual audit against these requirements.
Network Security	The Certificate Policies of PKIoverheid require the following regarding Network Security: *Requirement 6.5.1.3* "The CSP prevents unauthorized access to the following core services: registration service, certificate generation service, subject device provision service, dissemination service, revocation management service and revocation status service. To this end, these core services are separated either physically or logically from the non-PKI network domains, or the various core services will be implemented on separate network domains, where there has to be a unique authentication for each core service. If core services use the same network domains, the CSP enforces a unique authentication for each core service. The CSP documents the organization of the network domains, at least in a graphical manner." *Requirement 6.7.1.1* "The CSP has to ensure that all PKIoverheid ICT systems relating to the registration service, certificate generation service, subject device provision service, dissemination service, revocation management service and revocation status service: - are equipped with the latest updates and; - the web application controls and filters all input by users and; - the web application codes the dynamic output and; - the web application maintains a secure session with the user and; - the web application uses a database securely." *Requirement 6.7.1.2*

	"Using an audit tool, at least each month the CSP performs a security scan on its PKIoverheid infrastructure. The CSP documents the result of every security scan and the measures that were taken in relation to this scan." *Requirement 6.7.1.3* "At least once a year, the CSP arranges for a pen test to be performed on the PKIoverheid internet facing environment, by an independent, experienced, external supplier. The CSP has to document the findings from the pen test and the measures that will be taken in this respect, or to arrange for these to be documented."

Response to Mozilla's CA Recommended Practices (https://wiki.mozilla.org/CA:Recommended_Practices)

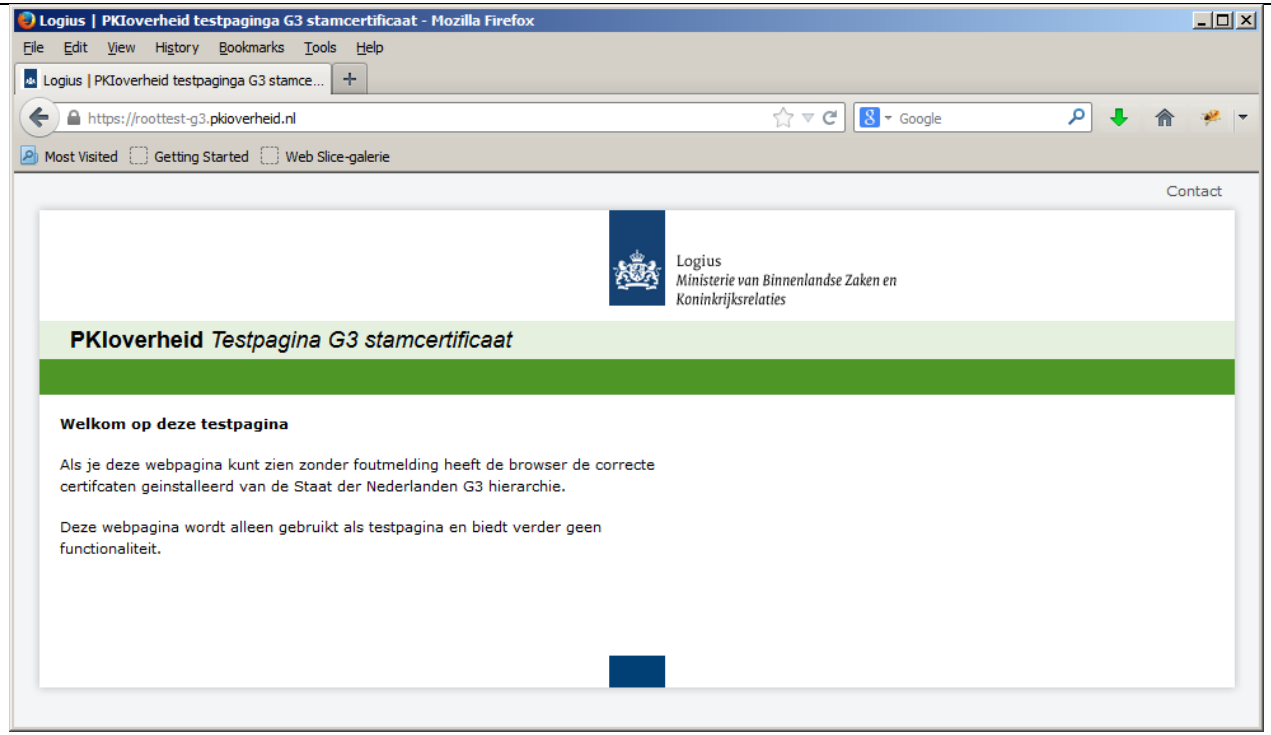
Publicly available CP and CPS	The Certificate Policies are available in PDF format. The Dutch language version can be obtained here: http://www.logius.nl/producten/toegang/pkioverheid/aansluiten-als-csp/programma-van-eisen/ The English language version can be obtained here: http://www.logius.nl/english/products/access/pkioverheid/ At present one CSP acts as subCA within the G3 (third generation) hierarchy of PKIoverheid. The Certificate Practice Statement of the KPN Corporate Market CSP CA is available in PDF format. The Dutch language version can be obtained here: https://certificaat.kpn.com/files/CPS/KPN_PKIoverheid_CPS_v4.19.pdf
CA Hierarchy	The PKIoverheid G3 hierarchy consists of three tiers; Root CA, Domain Subroot CA and CSP Subroot CA. This hierarchy is described in further detail below: **Tier 1: Root CA** • Staat der Nederlanden Root CA – G3 This internally operated offline Root CA is the trust anchor of the third generation root hierarchy of PKIoverheid. This CA is only used to sign Domain Subroot CA's and corresponding status information. **Tier 2: Domain Subroot CAs** • Domain Organisation Person: Staat der Nederlanden Organisatie Persoon CA – G3 This internally operated offline Domain Subroot CA is used to sign CSP Subroot CAs in the domain Organisation Person. **Tier 3: Organisation Person CSP Subroot CA** • At present no CSP Subroot CA has been issued in the domain Organisation Person. • Domain Organisation Services: Staat der Nederlanden Organisatie Services CA – G3 This internally operated offline Domain Subroot CA is used to sign CSP Subroot CAs in the

	domain Organisation Services. **Tier 3: Organisation Person CSP Subroot CA** • CSP KPN Corporate Market: KPN Corporate Market CSP Organisatie Services CA - G3 This externally operated online CSP Subroot CA is operated by KPN Corporate Market to issue end entity certificates to their subscribers. • Domain Citizen: Staat der Nederlanden Burger CA – G3 This internally operated offline Domain Subroot CA is used to sign CSP Subroot CAs in the domain Citizen. **Tier 3: Citizen CSP Subroot CA** • At present no CSP Subroot CA has been issued in the domain Organisation Person. • Domain Autonomous Devices: Staat der Nederlanden Autonome Apparaten CA – G3 This internally operated offline Domain Subroot CA is used to sign CSP Subroot CAs in the domain Autonomous Devices. **Tier 3: Autonomous Devices CSP Subroot CA** • At present no CSP Subroot CA has been issued in the domain Organisation Person.
Audit Criteria	Part 2 of the Programme of Requirements (http://www.logius.nl/fileadmin/logius/product/pkioverheid/documenten/PoR_EN_part2_v3.6.pdf) states that a CSP must be certified against the TTP.NL scheme. As per section 2.2.2 a TTP.NL certification is valid for three years and repeat audits have to be performed annually. Section 3.2.1 of part 2 of the PoR stipulates that CSPs have to submit the following documents annually: - Proof of compliance with ETSI EN 319 411-2 or TTP.NL certification for personal certificates; - Proof of compliance with ETSI TS 102 042 or TTP.NL certification for non-personal certificates issued under PoR parts 3b, 3d and 3e; - Instead of compliance with ETSI TS 102 042 or TTP.NL certification: an unqualified audit opinion concerning WebTrust for Certification Authorities – Extended Validation. Only if a CSP issues PKIoverheid EV SSL certificates; - Unqualified audit opinion for the PKIo requirements of the PKI for the government; - Unqualified audit opinion that fulfils the requirements based on ETSI TS 102 042 of the CP Services and/or Autonomous Devices and/or EV SSL.
Document Handling of IDNs in CP/CPS	Internationalized Domain Names (IDNs) are not allowed as described in the requirements regarding the subject.commonName (page 56) and subjectAltName.dNSName (page 64) in the Programme of Requirements (http://www.logius.nl/fileadmin/logius/product/pkioverheid/documenten/PoR_EN_part3b_v3.6.pdf)

Revocation of Compromised Certificates	The circumstances for the revocation of certificates are laid down in requirement 4.9.1.1 of the Programme of Requirements (http://www.logius.nl/fileadmin/logius/product/pkioverheid/documenten/PoR_EN_part3b_v3.6.pdf). “Certificates must be revoked when: - the subscriber states that the original request for a certificate was not allowed and the subscriber does not provide consent with retrospective force; - the CSP has sufficient proof that the subscriber's private key (that corresponds with the public key in the certificate) is compromised or if compromise is suspected, or if there is inherent security vulnerability, or if the certificate has been misused in any other way. A key is considered to be compromised in the event of unauthorized access or suspected unauthorized access to the private key, if the private key or SUD is lost or suspected to be lost, if the key or SUD is stolen or suspected to be stolen, or if the key or SUD is destroyed; - a subscriber does not fulfil its obligations outlined in this CP or the corresponding CPS of the CSP or the agreement that the CSP has entered into with the subscriber; - the CSP is informed, or otherwise become aware that the use of the domain name in the certificate is no longer legally permitted (e.g. by a judgement of a court); - the CSP is informed or otherwise becomes aware of a substantial change in the information that is provided in the certificate. An example of that is: a change in the name of the certificate holder (service); - the CSP determines that the certificate has not been issued in line with this CP or the corresponding CPS of the CSP or the agreement that the CSP has entered into with the subscriber; - the CSP determines that information in the certificate is incorrect or misleading; - the CSP ceases its work and the CRL and OCSP services are not taken over by a different CSP. - the subscriber uses a “code signing” certificate to digitally sign “hostile code” (including spyware, malware, Trojans, etc.). - The PA of PKIoverheid determines that the technical content of the certificate entails an irresponsible risk to subscribers, relying parties and third parties (e.g. browser parties).”
Verifying Domain Name Ownership	The requirements in the Programme of Requirements (http://www.logius.nl/fileadmin/logius/product/pkioverheid/documenten/PoR_EN_part3b_v3.6.pdf) regarding the subject.commonName (page 56) and subjectAltName.dNSName (page 64) state that “The subscriber MUST prove that the organization can use this name. In services server certificates [OID 2.16.528.1.1003.1.2.2.6 and 2.16.528.1.1003.1.2.5.6] the CSP MUST check

	recognized registers (Stichting Internet Domeinregistratie Nederland (SIDN) or Internet Assigned Numbers Authority (IANA)) to find out whether the subscriber is the domain name owner or whether the subscriber is exclusively authorized by the registered domain name owner to use the domain name on behalf of the registered domain name owner." Section 4.2.2.3 of KPN PKIoverheid CPS (https://certificaat.kpn.com/files/CPS/KPN_PKIoverheid_CPS_v4.19.pdf) describes the verification of Domain Name Ownership by the KPN Corporate Market CSP. Translation: "Among others, checks are made in recognized registers such as Stichting Internet Domeinregistratie Nederland (SIDN) or Internet Assigned Numbers Authority (IANA) to validate whether Subscriber owns the domain name as it appears in the e-mail address. In addition an assessment is made to determine URL-spoofing or phishing. http://www.phishtank.com or similar is consulted to see whether the domain name does not appears on a spam and/or phishing blacklist. If KPN suspects phishing or other potential abuse those suspicions will be reported to http://www.phishtank.com. ") " (Original text: "KPN neemt de Certificaataanvraag in ontvangst en beoordeelt de volledigheid en de juistheid van de aanvraag. Onder andere wordt bij erkende registers als Stichting Internet Domeinregistratie Nederland (SIDN) of Internet Assigned Numbers Authority (IANA) gecontroleerd of Abonnee eigenaar is van de domeinnaam, zoals die onder deel uitmaakt van het e-mail adres. Daarnaast wordt beoordeeld of sprake is van url-spoofing of phishing. En zo wordt ook http://www.phishtank.com of vergelijkbaar geraadpleegd om te bezien of de domeinnaam niet voorkomt op een spam-en/of phishing blacklist. Als KPN een verdenking heeft van phishing of ander mogelijk misbruik zal het die verdenking melden bij http://www.phishtank.com.")
Verifying Email Address Control	The email address of the certificate holder may be included in the certificate. The requirements on the SubjectAltName.rfc822Name attribute in part 3a of the PoR (http://www.logius.nl/fileadmin/logius/product/pkioverheid/documenten/PoR_EN_part3a_v3.6.pdf) (page 53) state that: "If the e-mail address is included in the certificate, the CSP MUST: - have the subscriber sign his/her approval for these and; - check that the e-mail address belongs to the subscriber's domain, or; - check that the e-mail address belongs to the subscriber (e.g. the professional) and that this person has access to the e-mail address (for example by performing a challenge response)." Section 4.2.2.1 of KPN PKIoverheid CPS (https://certificaat.kpn.com/files/CPS/KPN_PKIoverheid_CPS_v4.19.pdf)

	describes the verification by the KPN Corporate Market CSP. Translation: “Checks are made in recognized registers such as Stichting Internet Domeinregistratie Nederland (SIDN) or Internet Assigned Numbers Authority (IANA) to validate whether Subscriber owns the domain name as it appears in the e-mail address.” (Original text: “Onder andere wordt bij erkende registers als Stichting Internet Domeinregistratie Nederland (SIDN) of Internet Assigned Numbers Authority (IANA) gecontroleerd of Abonnee eigenaar is van de domeinnaam, zoals die onderdeel uitmaakt van het e-mail adres.”)
Verifying Identity of Code Signing Certificate Subscriber	Not applicable, PKIoverheid does not intend to issue Code Signing certificates under the G3 hierachy.
DNS names go in SAN	The requirements in the Programme of Requirements (http://www.logius.nl/fileadmin/logius/product/pkioverheid/documenten/PoR_EN_part3b_v3.6.pdf) state the following regarding the subject.commonName (page 56) and subjectAltName.dNSName. **subject.commonName** “Advised against; In services server certificates [OID 2.16.528.1.1003.1.2.2.6 and 2.16.528.1.1003.1.2.5.6] the use of this field is advised against. If this field is used, this MUST contain no more than 1 "fully-qualified domain name (FQDN)" (see the definition in part 4). This FQDN MUST also be included in the SubjectAltName.dNSName field.” **subjectAltName.dNSName.** “Compulsory; In services server certificates [OID 2.16.528.1.1003.1.2.2.6 and 2.16.528.1.1003.1.2.5.6] this field MUST include at least 1 "fully-qualified domain name (FQDN)"”
Domain owned by a Natural Person	Not applicable. PKIoverheid does not allow issuance of server certificates to natural persons.
OCSP	Using OCSP validation in Firefox and treating the certificate as invalid when an OCSP server connection fails the webpage https://roottest-g3.pkioverheid.nl/ was requested, resulting in the following successful test:

Response to Mozilla's list of Potentially Problematic Practices (https://wiki.mozilla.org/CA:Problematic_Practices)

Long-lived DV certificates	The CSPs in the PKIoverheid hierarchy do not issue DV certificates. The organizational identity of the subscriber must be verified as per section 3.2 of part 3b of the Programme of Requirements (http://www.logius.nl/fileadmin/logius/product/pkioverheid/documenten/PoR_EN_part3b_v3.6.pdf)
Wildcard DV SSL certificates	The CSPs in the PKIoverheid hierarchy do not issue DV certificates. The organizational identity of the subscriber must be verified as per section 3.2 of part 3b of of the Programme of Requirements (http://www.logius.nl/fileadmin/logius/product/pkioverheid/documenten/PoR_EN_part3b_v3.6.pdf)
Email Address Prefixes for DV Certs	The CSPs in the PKIoverheid hierarchy do not issue DV certificates. The organizational identity of the subscriber must be verified as per section 3.2 of part 3b of of the Programme of Requirements (http://www.logius.nl/fileadmin/logius/product/pkioverheid/documenten/PoR_EN_part3b_v3.6.pdf)
Delegation of Domain / Email	Within the PKIoverheid system the CSPs are responsible for the validation of information they include in the end entity

validation to third parties	certificates they issue. If a CSP chooses to delegate the RA function to another entity, they still need to conform to ETSI EN 319 411 and/or ETSI TS 102 042 and obtain certification to that effect.
Issuing end entity certificates directly from roots	PKIoverheid operates a three tier model of certificate issuance. Tier 1 and 2 are offline CAs operated by PKIoverheid. These tiers do not issue end entity certificates. Tier 3 is operated by the PKIoverheid CSPs and issues certificates to end users.
Allowing external entities to operate subordinate CAs	PKIoverheid issues certificates to CSPs. These CSP subordinate CAs are operated by external entities. The CSPs must be certified against ETSI EN 319 411 and/or ETSI TS 102 042 in accordance with the TTP.NL scheme. In addition the CSP must demonstrate that it fulfils the additional PKIoverheid requirements by means of an unqualified audit opinion.
Distributing generated private keys in PKCS#12 files	Within PKIoverheid CSPs are allowed to distribute private keys in PKCS#12 files. This distributions is governed by the requirements in section 6.1.1.4 of the Programme of Requirements (http://www.logius.nl/fileadmin/logius/product/pkioverheid/documenten/PoR_EN_part3b_v3.6.pdf)
Certificates referencing hostnames or private IP addresses	The requirements stipulated in the Programme of Requirements (http://www.logius.nl/fileadmin/logius/product/pkioverheid/documenten/PoR_EN_part3b_v3.6.pdf) regarding the subject.commonName (page 56) and subjectAltName.dNSName (page 64) state that FQDNs must be used. Furthermore "additional wildcard FQDNs, local domain names, private IP addresses, only a host name, internationalized domain names (IDNs) and null characters \0 MUST NOT be used".
Issuing SSL Certificates for Internal Domains	Issuing SSL Certificates for Internal Domains is not allowed under PKIoverheid. The requirements stipulated in the Programme of Requirements (http://www.logius.nl/fileadmin/logius/product/pkioverheid/documenten/PoR_EN_part3b_v3.6.pdf) regarding the subject.commonName (page 56) and subjectAltName.dNSName (page 64) state that "the CSP MUST check recognized registers (Stichting Internet Domeinregistratie Nederland (SIDN) or Internet Assigned Numbers Authority (IANA)) to find out whether the subscriber is the domain name owner or whether the subscriber is exclusively authorized by the registered domain name owner to use the domain name on behalf of the registered domain name owner."
OCSP Responses signed by a certificate under a different root	OCSP responses must either be signed by the issuing root, or a designated OCSP responder as per requirement 4.9.9-3 of the Programme of Requirements (http://www.logius.nl/fileadmin/logius/product/pkioverheid/documenten/PoR_EN_part3b_v3.6.pdf)
CRL with critical CIDP Extension	The CIDP extension is not part of the CRL profile used by PKIoverheid.
Generic names for CA's	The CA certificates issued within the PKIoverheid system to Tier 3 CSP CAs contain meaningful information on the CSP in question. This information is collected and vetted during phase 2 of the admittance process described in section 2.3 of part 2 of the Programme of Requirements (http://www.logius.nl/fileadmin/logius/product/pkioverheid/documenten/PoR_EN_part2_v3.6.pdf). The CSP fills out an admittance form

	(http://www.logius.nl/fileadmin/logius/product/pkioverheid/documenten/Aanvraagformulier_toetreding_pkioverheid.pdf) and suppies the CN, O and C fields they want to include in the CA certificate. This information is then vetted.
Lack of Communication With End Users	CSPs must publish their Certificate Practice Statements to the public at large in order to conform to section 2.4.1 of part 3b of the Programme of Requirements (http://www.logius.nl/fileadmin/logius/product/pkioverheid/documenten/PoR_EN_part3b_v3.6.pdf). These CPSs must conform to RFC3647 to satisfy section 2.2.5 of part 3b of the PoR. According to RFC 3647 the contact details of the CSP must be included in section 4.1.5 of the CPS.
Backdating the notBefore date	The Programme of Requirements does not contain a stipulation prohibiting the backdating of the notBefore date.