Bugzilla ID: 1016568
Bugzilla Summary: Staat der Nederlanden G3 and EV Root CA 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	https://www.logius.nl/languages/english/pkioverheid/
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 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

Cert Name	Staat der Nederlanden Root CA - G3	Staat der Nederlanden EV Root CA
Cert Issuer Field	CN = Staat der Nederlanden Root CA - G3 O = Staat der Nederlanden C = NL	CN = Staat der Nederlanden EV Root CA 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.	The Staat der Nederlanden EV Root CA is the Extended Validation Root CA of the Dutch governmental PKI (PKIoverheid). This Public Key Infrastructure was designed for trustworthy electronic communication within and with the Dutch government. A number of Staat der Nederlanden Root CAs are already included in the Mozilla Root Programme.
Root Cert	http://cert.pkioverheid.nl/RootCA-G3.cer	http://cert.pkioverheid.nl/EVRootCA.cer
SHA1 Fingerprint	D8:EB:6B:41:51:92:59:E0:F3:E7:85:00:C0:3D:B6:88:97:C9:EE:FC	76:E2:7E:C1:4F:DB:82:C1:C0:A6:75:B5:05:BE:3D:29:B4:ED:DB:BB
Valid From	2013-11-14	2010-12-08
Valid To	2028-11-13	2022-12-08
Cert Version	3	3
Cert Signature Algorithm	SHA-256	SHA-256
Signing key parameters	4096	4096
Test Website	https://roottest-g3.pkioverheid.nl	https://pkioevssl-v.quovadisglobal.com/
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:	The PKIoverheid Extended Validation hierarchy consists of three tiers which are detailed in the “CA hierarchy” section below. At present one CSP is in operation within the EV hierarchy. The other CSPs in the PKIoverheid ecosystem have not yet been issued with a sub-root under the EV 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 EV root are presently available: Validation of Staat der Nederlanden Intermediair CA (subordinate

	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: 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."	CA) certificate: http://crl.pkioverheid.nl/EVRootLatestCRL.crl Validation of Extended Validation CSP (subordinate CA) certificates: http://crl.pkioverheid.nl/EVIntermediairLatestCRL.crl Validation of end-entity certificates issued by QuoVadis CSP: http://crl.quovadisglobal.com/pkioevca.crl This end-entity certificate CRL is updated at least once every 7 calendar days and the date of the "Next update" field exceeds the date of the "Effective date" field by 10 calendar days at the most (section 4.9.7 of the QuoVadis PKIoverheid Extended Validation CPS: https://www.quovadisglobal.com/~/media/Files/Repository/QV_CPS_PKI_Overheid_EV_V1_0.ashx). This is in conformance with requirement 4.9.7.1 of the Extended Validation CP (Part 3e of the Programme of Requirements: PoR_EN_part3e_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."
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	The following OCSP URLs are in use within the PKIoverheid Extended Validation hierarchy: Validation of Staat der Nederlanden Intermediair CA (subordinate CA) certificates: http://evrootocsp.pkioverheid.nl Validation of Extended Validation CSP (subordinate CA) certificates: http://ocsp.pkioverheid.nl Validation of end-entity certificates issued by QuoVadis CSP: http://ocsp.quovadisglobal.com

	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: 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: 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".	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 3e of the Programme of Requirements: PoR_EN_part3e_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 4.9.9-4 of the CP (Part 3e of the Programme of Requirements: PoR_EN_part3e_v3.6.pdf): "The CSP must update the OCSP service at least once every 4 calendar days. The maximum expiry term of the OCSP responses is 10 calendar days.".
Requested Trust Bits	Websites (SSL/TLS) Email (S/MIME)	Websites (SSL/TLS)
SSL Validation Type	OV	EV
EV Policy OID(s)	N/A	2.16.528.1.1003.1.2.7 EV Testing Completed and screen shot added to attachment in bug.
Non-sequential serial numbers and entropy in cert	Page 53 of the CP (Part 3b of the Programme of Requirements: PoR_EN_part3b_v3.6.pdf) 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.	On page 57 of the PKIoverheid EV CP (Part 3e of the Programme of Requirements: PoR_EN_part3e_v3.6.pdf) 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 MUST be the same as the field signatureAlgorithm. For maximum interoperability, for certificates issued under this CP, only sha-256WithRSAEncryption is allowed.

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. **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 (PoR_EN_part1_v3.6.pdf) for more information on the PKI design.	The PKIoverheid EV hierarchy consists of three tiers; Root CA, Intermediate Subroot CA and CSP Subroot CA. **Tier 1: Root CA** · Staat der Nederlanden EV Root CA This internally operated offline Root CA is the trust anchor of the Extended Validation root hierarchy of PKIoverheid. This CA is only used to sign the Intermediate Subroot CA and corresponding status information. **Tier 2: Intermediate Subroot CA** · Staat der Nederlanden EV Intermediair CA This internally operated offline Intermediate Subroot CA is used to sign CSP Subroot CAs. **Tier 3: CSP Subroot CA** · CSP QuoVadis: QuoVadis CSP - PKI Overheid EV CA This externally operated online CSP Subroot CA is operated by QuoVadis to issue EV end entity certificates to their subscribers.

Externally Operated SubCAs	See below	See below
Cross-Signing	Not applicable. At present no cross signing has been performed in the PKIoverheid G3 hierarchy.	Not applicable. At present no cross signing has been performed in the PKIoverheid EV 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 (PoR_EN_part2_v3.6.pdf).	No technical constraints are in place for the CSP Subroot CAs within the PKIoverheid EV 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 (PoR_EN_part2_v3.6.pdf).

CA Policies about Third-Party Subordinate CAs

General description of the sub-CAs operated by third parties.	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 https://www.logius.nl/languages/english/pkioverheid/ The PoR consists of four parts: - Part 1: Introduction - Part 2: CSP Requirements - Part 3: Certificate Policies - Part 4: Definitions and abbreviations 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 fulfill 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 (PoR_EN_part1_v3.6.pdf).
Selection criteria for sub-CAs	CSPs within PKIoverheid have to adhere to the requirements laid out in part 2 of the Programme of Requirements (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 **– [Comment #6: the CSPs will be audited against the NCP- combined with OVCP- and PTC-BR requirements as stated in ETSI TS 102 042.]** - 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.
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 (PoR_EN_part3a_v3.6.pdf) · Part 3b: Certificate policy Services (PoR_EN_part3b_v3.6.pdf) · Part 3c: Certificate policy Citizen (PoR_EN_part3c_v3.6.pdf) · Part 3d: Certificate policy Autonomous Devices (PoR_EN_part3d_v3.6.pdf) · Part 3e: Certificate policy - Extended Validation (PoR_EN_part3e_v3.6.pdf)
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 (and in the EV CP) 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.
Sub-CA verification requirements non-EV Domain ownership/control	The requirements in the Programme of Requirements(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."
Sub-CA verification requirements EV Domain ownership/control	The requirements in the EV CP (PoR_EN_part3e_v3.6.pdf) regarding the validation of Domain ownership/control are as follows: 3.2.5-3: Validation of authority "The CSP has to verify that the subscriber is the registered owner of the domain name listed in the request (FQDN) or that the subscriber is exclusively authorized by the registered domain name owner to use the domain name on behalf of the registered domain name owner. This verification may not be contracted out by the CSP to Registration Authorities or other parties. If the subscriber states that he/she is the registered owner of the domain name listed in the request, the CSP has to: - verify that the domain name is registered with a registrar or domain manager, such as SIDN (The Netherlands Internet Domain Registration Foundation), affiliated with the Internet Corporation for Assigned Names and Numbers (ICANN) or an organization that is a member of the Internet Assigned Numbers Authority (IANA), and; - use a WHOIS service, of an organization affiliated with or that is a member of ICANN or IANA, that offers the information via HTTPS or the de CSP must use a command line programme if a WHOIS service is used that offers information via HTTP, and; - in the WHOIS service, verify the name, the residential address and the administrative contact person of the organization and compare this information to the verified subscriber information and establish that there are no inconsistencies between the two sets of information, and; - The CSP must verify that the domain name does not appear on a spam list and/or phishing black list. Use, to this end, at least

	http://www.phishtank.com. If the domain name is mentioned on phish tank or a different black list that is consulted, during the verification process the CSP has to deal particularly carefully with the request for the relevant services server certificate. The information that the CSP uses to verify that the subscriber is the registered owner of the domain name (FQDN) listed in the application may not be older than 13 months, otherwise the information has to be requested and verified again. If the subscriber states that it is exclusively authorized by the registered domain name owner to use the domain name on behalf of the registered domain name owner, as well as the checks listed above, the CSP has to: - request a declaration from the registered domain name owner (e.g. by e-mail or telephone) in which the registered domain name owner has to confirm that the subscriber has the exclusive right to use the domain name (FQDN), and; - request and verify a written and signed declaration from a notary or external accountant which must state for which domain name (FQDN) the subscriber has been given the exclusive user right on behalf of the registered domain name owner, and; - verify that the domain name (FQDN) is not a generic TopLevelDomein (gTLD) or country code TopLevelDomein (ccTLD). For these domain names, only the subscriber, as registered domain name owner, is allowed to submit an application. A declaration from the registered domain name owner or notary or external accountant may not be older than 13 months."
Sub-CA verification requirements 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 (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
Sub-CA verification requirements Digitally signing code	Not applicable. PKIoverheid does not intend to issue Code Signing certificates within the G3 hierarchy. PKIoverheid does not allow the issuance of Code Signing certificates under the EV CP.
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

The other CSPs in the PKIoverheid ecosystem have not yet been issued with subroots under the G3 or EV hierarchy.

More information on the other CSPs can be found here: https://bugzilla.mozilla.org/show_bug.cgi?id=551399

Subordinate CA	KPN Corporate Market CSP CA	QuoVadis CSP
Company name	KPN Corporate Market	QuoVadis
Corporate URL	http://certificaat.kpn.com	https://www.quovadisglobal.com
Sub-CA certificate	see attachment to bug	http://cert.pkioverheid.nl/QuoVadis_CSP_-_PKI_Overheid_EV_CA.cer

URL to test website	https://roottest-g3.pkioverheid.nl	https://pkioevssl-v.quovadisglobal.com
General CA hierarchy under the sub-CA	No sub-CAs have been issued under this 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	https://www.quovadisglobal.com/~/media/Files/Repository/QV_CPS_PKI_Overheid_EV_V1_0.ashx
Domain ownership/control	Section 3.2.3.2.2 of KPN PKIoverheid 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)." 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. ") "	Section 3.2.5.3 of QuoVadis EV PKIoverheid CPS (QV_CPS_PKI_Overheid_EV_V1_0.ashx) states that: Translation: "QuoVadis verifies that the subscriber is the registered owner of the domain name listed in the request (FQDN) or that the subscriber is exclusively authorized by the registered domain name owner to use the domain name on behalf of the registered domain name owner. This verification shall not be contracted out by QuoVadis to Registration Authorities or other parties. If the subscriber states that he/she is the registered owner of the domain name listed in the request, QuoVadis shall: - verify that the domain name is registered with a registrar or domain manager, such as SIDN (The Netherlands Internet Domain Registration Foundation), affiliated with the Internet Corporation for Assigned Names and Numbers (ICANN) or an organization that is a member of the Internet Assigned Numbers Authority (IANA), and; - use a WHOIS service, of an organization affiliated with or that is a member of ICANN or IANA, that offers the information via HTTPS or the de CSP must use a command line programme if a WHOIS service is used that offers information via HTTP, and; - in the WHOIS service, verify the name, the residential address and the administrative contact person of the organization and compare this information to the verified subscriber information and establish that there are no inconsistencies between the two sets of information, and; - verify that the domain name does not appear on a spam list and/or phishing black list. Use, to this end, at least http://www.phishtank.com. If the domain name is mentioned on phish tank or a different black list that is consulted, during the verification process QuoVadis shall handle the request for the relevant services server certificate with particular care. The information that the CSP uses to verify that the subscriber is the registered owner of the domain name (FQDN) listed in the application may not be older than 13 months, otherwise the information has to be requested and verified again."

Email address ownership/control	Section 4.2.2.1 of KPN PKIoverheid 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."	
Code Signing	N/A	N/A
SSL Category	OV	EV
Potentially Problematic Practices	None. KPN does not use PKCS#12 objects for distribution of key material.	None. Please see the Potentially Problematic Practices section at the bottom of this document for a detailed review.
Audit report	Certificate of Registration: https://certificaat.kpn.com/files/ETSI/Getronics%20-%20ETSI%20certificate%20by%20BSI.pdf Comment #6: More specific: the CSPs will be audited against the NCP- combined with OVCP- and PTC-BR requirements as stated in ETSI TS 102 042. ... The ETSI 102 042 certificate from our CSP KPN will be publicly available coming October.	Auditor: BSI Group https://bugzilla.mozilla.org/attachment.cgi?id=8472145 -- ETSI TS 102042 v2.4.1 NCP+, OVCP, PTC-BR (2014.04.08)

Verification Policies and Practices

Policy Documentation	Document Repository (Dutch): https://www.logius.nl/ondersteuning/pkioverheid/aansluiten-als-csp/programma-van-eisen/ Document Repository (English): https://www.logius.nl/languages/english/pkioverheid/ Staat der Nederlanden Root and Domain CAs (Tier 1 and 2) CP (English): · Part 3a: Certificate policy Government, Companies and Organizations (https://www.logius.nl/fileadmin/logius/ns/diensten/pkioverheid/programma-van-eisen/PoR_EN_part3a_v3.6.pdf) · Part 3b: Certificate policy Services (https://www.logius.nl/fileadmin/logius/ns/diensten/pkioverheid/programma-van-eisen/PoR_EN_part3b_v3.6.pdf) · Part 3c: Certificate policy Citizen (https://www.logius.nl/fileadmin/logius/ns/diensten/pkioverheid/programma-van-eisen/PoR_EN_part3c_v3.6.pdf) · Part 3d: Certificate policy Autonomous Devices (https://www.logius.nl/fileadmin/logius/ns/diensten/pkioverheid/programma-van-eisen/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) EV CP: https://www.logius.nl/fileadmin/logius/ns/diensten/pkioverheid/programma-van-eisen/PoR_EN_part3e_v3.6.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 QuoVadis CSP - PKI Overheid EV CA (Tier3) CPS (Dutch): https://www.quovadisglobal.com/~/media/Files/Repository/QV_CPS_PKI_Overheid_V1_1_4.ashx Relying Party Agreement (English): https://www.quovadisglobal.com/~/media/Files/Repository/QV_RPA_v1%201.ashx **The other CSPs in the PKIoverheid ecosystem have not yet been issued with subroots under the G3 or EV hierarchy.** **More information on the other CSPs can be found here: https://bugzilla.mozilla.org/show_bug.cgi?id=551399**
Audits	Staat der Nederlanden Root and Domain CAs (Tier 1 and 2) Audit Type: WebTrust CA and WebTrust BR 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 (2014.03.20) With regard to the Extended Validation root a point-in-time audit has been executed by KPMG. Audit Statement: https://bugzilla.mozilla.org/attachment.cgi?id=8429540 (2013.11.19) KPN Corporate Market CSP CA (Tier3) Audit Type: ETSI TS 101 456 **-- The ETSI 102 042 certificate from our CSP KPN will be publicly available coming October.** Auditor: BSI, http://www.bsigroup.com/ URL to Certificate of Registration: https://certificaat.kpn.com/files/ETSI/Getronics%20-%20ETSI%20certificate%20by%20BSI.pdf QuoVadis CSP (Tier3) - Auditor: BSI Group - https://bugzilla.mozilla.org/attachment.cgi?id=8472145 -- ETSI TS 102042 v2.4.1 NCP+, OVCP, PTC-BR (2014.04.08) **The other CSPs in the PKIoverheid ecosystem have not yet been issued with subroots under the G3 or EV hierarchy.** **More information on the other CSPs can be found here: https://bugzilla.mozilla.org/show_bug.cgi?id=551399** Comment #6: At this moment we are in the midst of a migration process were we will phase out the BR requirements in our CP part 3b and require from our CSPs, if they issue PKIoverheid SSL certs, that they are audited against ETSI TS 102 042 (http://www.etsi.org/deliver/etsi_ts/102000_102099/102042/02.04.01_60/ts_102042v020401p.pdf) by an independent auditor (BSI Management). More specific: the CSPs will be audited against the NCP- combined with OVCP- and PTC-BR requirements as stated in ETSI TS 102 042. Our CSP QuoVadis will be the first CSP who will be audited against these requirements. The ETSI TS 102 042 certificate (including a reference to the NCP, OVCP and PTC-BR requirements) from QuoVadis will be publicly available coming august. The ETSI 102 042 certificate from our CSP KPN will be publicly available coming October. The ETSI TS 102 042 certification form our other CSPs, if they issue PKIoverheid SSL certs, will follow end this year or early 2015.
Baseline	Staat der Nederlanden Root and Domain CAs (Tier 1 and 2)

Requirements (SSL)	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. The "Commitment to Comply" with the CA/Browser Forum Baseline Requirements is regulated by requirement 2.2-4 of the EV CP (PoR_EN_part3e_v3.6.pdf): "The following clause has to be incorporated in the CPS and in all agreements with parties that are involved in the issue of the EV SSL certificates of the CSP (such as, for example, the Registration Authority): "CSP [name] conforms to the current version of the CA/Browser Forum Guidelines for Issuance and Management of Extended Validation Certificates as published at http://www.cabforum.org. In the event of an inconsistency between the PKIoverheid Programme of Requirements part 3e and the relevant Requirements, because of which it is not possible to (at the very least) fulfil the minimum requirements, which is at the discretion of the PA, the provisions in the Requirements shall prevail." " This commitment is incorporated in the QuoVadis EV CPS in section 2.2.4 (QV_CPS_PKI_Overheid_EV_V1_0.ashx) Translation: "QuoVadis conforms to the current version of the CA/Browser Forum Guidelines for Issuance and Management of Extended Validation Certificates as published at http://www.cabforum.org. In the event of an inconsistency between the PKIoverheid Programme of Requirements part 3e and the relevant Requirements, because of which it is not possible to (at the very least) fulfil the minimum requirements, which is at the discretion of the PA, the provisions in the Requirements shall prevail."
Non-EV SSL Verification Procedures	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 (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)." 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. ") "
Non-EV	The Certificate Policies of PKIoverheid require the following regarding Organization verification:

Organization Verification Procedures	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. (PoR_EN_part3a_v3.6.pdf and PoR_EN_part3b_v3.6.pdf) Section 3.2.2. of the KPN PKIoverheid 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.”
EV SSL Verification Procedures	The validation of authority must adhere to section 3.2.5 of the Requirement 3.2.5-3 “The CSP has to verify that the subscriber is the registered owner of the domain name listed in the request (FQDN) or that the subscriber is exclusively authorized by the registered domain name owner to use the domain name on behalf of the registered domain name owner. This verification may not be contracted out by the CSP to Registration Authorities or other parties. If the subscriber states that he/she is the registered owner of the domain name listed in the request, the CSP has to: - verify that the domain name is registered with a registrar or domain manager, such as SIDN (The Netherlands Internet Domain Registration Foundation), affiliated with the Internet Corporation for Assigned Names and Numbers (ICANN) or an organization that is a member of the Internet Assigned Numbers Authority (IANA), and; - use a WHOIS service, of an organization affiliated with or that is a member of ICANN or IANA, that offers the information via HTTPS or the de CSP must use a command line programme if a WHOIS service is used that offers information via HTTP, and; - in the WHOIS service, verify the name, the residential address and the administrative contact person of the organization and compare this information to the verified subscriber information and establish that there are no inconsistencies between the two sets

	of information, and; - The CSP must verify that the domain name does not appear on a spam list and/or phishing black list. Use, to this end, at least http://www.phishtank.com. If the domain name is mentioned on phish tank or a different black list that is consulted, during the verification process the CSP has to deal particularly carefully with the request for the relevant services server certificate. The information that the CSP uses to verify that the subscriber is the registered owner of the domain name (FQDN) listed in the application may not be older than 13 months, otherwise the information has to be requested and verified again. If the subscriber states that it is exclusively authorized by the registered domain name owner to use the domain name on behalf of the registered domain name owner, as well as the checks listed above, the CSP has to: - request a declaration from the registered domain name owner (e.g. by e-mail or telephone) in which the registered domain name owner has to confirm that the subscriber has the exclusive right to use the domain name (FQDN), and; - request and verify a written and signed declaration from a notary or external accountant which must state for which domain name (FQDN) the subscriber has been given the exclusive user right on behalf of the registered domain name owner, and; - verify that the domain name (FQDN) is not a generic TopLevelDomein (gTLD) or country code TopLevelDomein (ccTLD). For these domain names, only the subscriber, as registered domain name owner, is allowed to submit an application. A declaration from the registered domain name owner or notary or external accountant may not be older than 13 months." QuoVadis satisfies these requirements through section 3.2.5.3 (Verification ownership domain name (FQDN)) of their EV CPS (https://www.quovadisglobal.com/~/media/Files/Repository/QV_CPS_PKI_Overheid_EV_V1_0.ashx). QuoVadis has chosen to use the wording from the requirements in the corresponding sections of the QuoVadis EV CPS.
EV Organization Verification Procedures	The verification of the organization applying for an Extended Validation certificate is governed by section 3.2.2 of the PKIoverheid EV CP (http://www.logius.nl/fileadmin/logius/product/pkioverheid/documenten/PoR_EN_part3e_v3.6.pdf). Requirement 3.2.2-1 "The CSP has to verify that the subscriber is an existing and legal organization. As evidence that it is an existing and legal organization, the CSP has to request and verify at least the following supporting documents: - For government organizations, a recently certified excerpt (no more than 1 month old) from the Chamber of Commerce's Trade Register or a law, deed of incorporation or a general governmental decree; - For bodies governed by private law with and without a legal personality with a recently certified excerpt (maximum 1 month old) from the Chamber of Commerce's Trade Register. As proof that it is a legal organization, the CSP has to find out whether this appears on the latest EU list of prohibited terrorists and terrorist organizations, published by the European Council These lists can be found on the web page: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32001E0931:NL:NOT These are decisions concerning updating the list of people, groups and entities referred to in articles 2, 3 and 4 of Common Position 2001/931/GBVB concerning the use of specific measures to combat terrorism." Requirement 3.2.2-2 "The CSP has to verify that the organization name shown on the certificate is correct and complete and corresponds with the organization name provided by the subscriber. As proof of the correctness of the official organizational name that has been provided the CSP has to request and verify, at the very least, the following supporting documents: - For government organizations, a recently certified excerpt (maximum 1 month old) from the Chamber of Commerce's Trade Register or, if registration in the Trade Register has not yet taken place, a copy of the relevant page from the latest version of the State Almanac in which the address of the relevant government organization is given;

	- For bodies governed by private law with and without a legal personality with a recently certified excerpt (maximum 1 month old) from the Chamber of Commerce's Trade Register. Furthermore it applies that the supporting document that has been provided has to distinguish the organizational entity from any other organizations with the same name. In general, in an excerpt from the Chamber of Commerce's Trade Register, the official name of the organization is also given." QuoVadis satisfies these requirements through section 3.2.2.1 (Verification status organization) and 3.2.2.2 (Verification name organisation) of their EV CPS (https://www.quovadisglobal.com/~/media/Files/Repository/QV_CPS_PKI_Overheid_EV_V1_0.ashx). QuoVadis has chosen to use the wording from the requirements in the corresponding sections of the QuoVadis EV CPS.
Email Address Verification Procedures	PKIoverheid does not allow the issuance Email certificates under the EV CP. The requirements on the SubjectAltName.rfc822Name attribute in part 3a of the PoR (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 (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." 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. Not requesting the Code Signing trust bit for either root.
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	See above
CA Hierarchy	See above
Audit Criteria	See above
Document Handling of IDNs in CP/CPS	Internationalized Domain Names (IDNs) are not allowed as described in the requirements regarding the subject.commonName (page 60) and subjectAltName.dNSName (page 67) in the EV CP (PoR_EN_part3e_v3.6.pdf), and as described in the requirements regarding the subject.commonName (page 56) and subjectAltName.dNSName (page 64) in the Programme of Requirements (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 EV CP (PoR_EN_part3e_v3.6.pdf). The circumstances for the revocation of certificates are laid down in requirement 4.9.1.1 of the Programme of Requirements (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	See above
Verifying Email Address Control	See above
Verifying Identity of Code Signing Certificate Subscriber	N/A
DNS names go in SAN	The requirements in the Programme of Requirements(PoR_EN_part3b_v3.6.pdf) and the EV CP (PoR_EN_part3e_v3.6.pdf) state the following. 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	See above

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 (PoR_EN_part3b_v3.6.pdf) and section 3.2 of the EV CP (PoR_EN_part3e_v3.6.pdf).
Wildcard DV SSL certificates	N/A
Email Address Prefixes for DV Certs	N/A
Delegation of Domain / Email validation to third parties	Within the PKIoverheid system the CSPs are responsible for the validation of information they include in the end entity 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.

	Requirement 3.2.5-3 (PoR_EN_part3e_v3.6.pdf) states: "The CSP has to verify that the subscriber is the registered owner of the domain name listed in the request (FQDN) or that the subscriber is exclusively authorized by the registered domain name owner to use the domain name on behalf of the registered domain name owner. This verification may not be contracted out by the CSP to Registration Authorities or other parties."
Issuing end entity certificates directly from roots	N/A. See above.
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 TS 102 042 in accordance with the TTP.NL scheme and/or the "WebTrust for CA Extended Validation criteria". 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 (PoR_EN_part3b_v3.6.pdf) Requirement 6.1.1-3 of the EV CP (PoR_EN_part3e_v3.6.pdf) states the following: "The generation of the certificate holder's key, where the CSP also generates the private key (PKCS#12) is not allowed."
Certificates referencing hostnames or private IP addresses	Programme of Requirements (PoR_EN_part3b_v3.6.pdf) regarding the subject.commonName (page 56) and subjectAltName.dNSName (page 64) and EV CP (PoR_EN_part3e_v3.6.pdf) regarding the subject.commonName (page 58) and subjectAltName.dNSName (page 67) state that FQDNs must be used. Furthermore "wildcards, private IP addresses and/or host names, internationalized domain names (IDNs) and null characters \0 may not be used."
Issuing SSL Certificates for Internal Domains	Issuing SSL Certificates for Internal Domains is not allowed under PKIoverheid.
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
CRL with critical CIDP Extension	The CIDP extension is not part of the CRL profile used by PKIoverheid. The use of Delta CRLs is optional in the PKIoverheid Extended Validation hierarchy. If the CIDP extension is used it must however be critical in order to satisfy the CRL profile in the EV CP (page 75 of http://www.logius.nl/fileadmin/logius/product/pkioverheid/documenten/PoR_EN_part3e_v3.6.pdf). At present the CIDP extension is not used in any CRL published in the PKIoverheid Extended Validation hierarchy.
Generic names for CAs	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 (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 supplies the CN, O and C fields they want to include in the CA certificate. This information is then vetted.
Lack of Communication	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

With End Users	the Programme of Requirements (PoR_EN_part3b_v3.6.pdf) or requirement 2.4.1 of the EV CP (PoR_EN_part3e_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.