

Bugzilla ID:**Bugzilla Summary: Staat der Nederlanden 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	http://www.logius.nl/producten/toegang/pkioverheid/ (Dutch Language) http://www.logius.nl/english/products/access/pkioverheid/ (English language)
Organisational 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 Extended Validation Root is to enable CSPs to issue certificates to their customers. The CSPs (commercial and governmental organisations) will issue Extended Validation certificates 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: <ul style="list-style-type: none"> • 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 EV Root CA
Certificate Issuer Field	CN = Staat der Nederlanden EV Root CA O = Staat der Nederlanden C = NL
Certificate Summary	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 URL	http://cert.pkioverheid.nl/EVRootCA.cer
SHA1 Fingerprint	76 e2 7e c1 4f db 82 c1 c0 a6 75 b5 05 be 3d 29 b4 ed db bb
Valid From	2010-12-08
Valid To	2022-12-08
Certificate Version	v3
Certificate Signature Algorithm	sha256RSA
Signing Key Parameters	RSA modulus length 4096 bits.
Test Website URL (SSL)	https://pkioevssl-v.quovadisglobal.com/
CRL URL	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

	<p>can be found here: https://bugzilla.mozilla.org/show_bug.cgi?id=551399</p> <p>The following CRLs for the EV root are presently available:</p> <p>Validation of Staat der Nederlanden Intermediar CA (subordinate CA) certificate: http://crl.pkioverheid.nl/EVRootLatestCRL.crl</p> <p>Validation of Extended Validation CSP (subordinate CA) certificates: http://crl.pkioverheid.nl/EVIntermediarLatestCRL.crl</p> <p>Validation of end-entity certificates issued by QuoVadis CSP: http://crl.quovadisglobal.com/pkioevca.crl</p> <p>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).</p> <p>This is in conformance with requirement 4.9.7.1 of the Extended Validation CP (Part 3e of the Programme of Requirements: http://www.logius.nl/fileadmin/logius/product/pkioverheid/documenten/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.”</p> <p>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.</p>
OCSP URL	<p>The following OCSP URLs are in use within the PKIoverheid Extended Validation hierarchy:</p> <p>Validation of Staat der Nederlanden Intermediar CA (subordinate CA) certificates: http://evrootocsp.pkioverheid.nl</p> <p>Validation of Extended Validation CSP (subordinate CA) certificates: http://ocsp.pkioverheid.nl</p> <p>Validation of end-entity certificates issued by QuoVadis CSP: http://ocsp.quovadisglobal.com</p>

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:

http://www.logius.nl/fileadmin/logius/product/pkioverheid/documenten/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:

http://www.logius.nl/fileadmin/logius/product/pkioverheid/documenten/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.”.

Extended Validation Treatment Test:

Per the instructions on https://wiki.mozilla.org/PSM:EV_Testing_Easy_Version the Extended Validation treatment of the PKIoverheid EV hierarchy was tested. The publicly available test website on <https://pkioevssl-v.quovadisglobal.com/> was requested, resulting in the following successful test:

	
Requested Trust Bits	Websites (SSL/TLS)
SSL Validation Type	EV
EV Policy OID	2.16.528.1.1003.1.2.7
Non-sequential serial numbers and entropy in cert	<p>On page 57 of the PKIoverheid EV CP (Part 3e of the Programme of Requirements: http://www.logius.nl/fileadmin/logius/product/pkioverheid/documenten/PoR_EN_part3e_v3.6.pdf) states the following regarding serial numbers and allowed hashing algorithms:</p> <p>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).</p>

	<p>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.</p>
--	--

CA Hierarchy information for each root certificate

CA Hierarchy	<p>The PKIoverheid EV hierarchy consists of three tiers; Root CA, Intermediate Subroot CA and CSP Subroot CA. This hierarchy is described in further detail below:</p> <p>Tier 1: Root CA</p> <ul style="list-style-type: none"> • 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. <p>Tier 2: Intermediate Subroot CA</p> <ul style="list-style-type: none"> • Staat der Nederlanden EV Intermediair CA This internally operated offline Intermediate Subroot CA is used to sign CSP Subroot CAs. <p>Tier 3: CSP Subroot CA</p> <ul style="list-style-type: none"> • 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	<p>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:</p> <ul style="list-style-type: none"> - 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.

While issuing Extended Validation certificates CSPs have to follow the Certificate Policy stated below

- 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 the EV CP in paragraph 9.12.2.2. 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 EV CP

(http://www.logius.nl/fileadmin/logius/product/pkioverheid/documenten/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.”

Email address ownership/control :

Not applicable. PKIoverheid does not allow the issuance of Email certificates under the EV CP.

Digitally signing code:

Not applicable. PKIoverheid does not allow the issuance of Code Signing certificates under the EV CP.

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

QuoVadis CSP

Company name	QuoVadis
Corporate URL	https://www.quovadisglobal.com
Sub-CA certificate	http://cert.pkioverheid.nl/QuoVadis_CSP_-_PKI_Overheid_EV_CA.cer
URL to test website	https://pkioevssl-v.quovadisglobal.com
General CA hierarchy under the sub-CA	No sub-CAs have been issued under this sub-CA
CPS (Dutch)	https://www.quovadisglobal.com/~media/Files/Repository/QV_CPS_PKI_Overheid_EV_V1_0.ashx
Ownership verification	<p><i>Domain ownership/control:</i> Section 3.2.5.3 of QuoVadis EV PKIoverheid CPS (https://www.quovadisglobal.com/~media/Files/Repository/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:</p> <ul style="list-style-type: none">- 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;

		<ul style="list-style-type: none"> - 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. <p>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.”</p> <p>(Original text: “QuoVadis verifiëert dat de abonnee de geregistreerde eigenaar is van de in de aanvraag vermelde domeinnaam (FQDN) of dat de abonnee exclusief geautoriseerd is door de geregistreerde domeinnaam eigenaar om, namens de geregistreerde domeinnaam eigenaar, de domeinnaam te gebruiken. Deze verificatie zal door QuoVadis niet worden uitbesteed aan Registration Authorities of andere partijen. Als de abonnee aangeeft de geregistreerde eigenaar te zijn van de in de aanvraag vermelde domeinnaam dan zal QuoVadis:</p> <ul style="list-style-type: none"> - verifiëren dat de domeinnaam is geregistreerd bij een registrar of domeinbeheerder, zoals SIDN (Stichting Internet Domeinregistratie Nederland), verbonden aan Internet Corporation for Assigned Names and Numbers (ICANN) of een organisatie die onderdeel is van Internet Assigned Numbers Authority (IANA) én; - gebruik maken van een WHOIS service, van een organisatie verbonden aan- of onderdeel van ICANN of IANA, die de gegevens aanbiedt via HTTPS of de CSP
--	--	--

		<p>moet gebruik maken van een command line-programma, indien gebruik wordt gemaakt van een WHOIS service die gegevens aanbiedt via HTTP én;</p> <ul style="list-style-type: none"> - in de WHOIS service, de naam, het woonadres en de administratieve contactpersoon van de organisatie verifiëren en deze gegevens vergelijken met de geverifieerde abonnee gegevens en vastleggen dat er geen inconsistentie is tussen beide gegevens én; - verifiëren dat de domeinnaam niet voorkomt op een spam- en/of phishing blacklist. Gebruik hiervoor tenminste http://www.phishtank.com. <p>Als de domeinnaam voorkomt op phishtank of eventueel een andere blacklist die is geraadpleegd, zal QuoVadis tijdens het verificatieproces extra zorgvuldig om te gaan met de aanvraag van het betreffende services server certificaat.</p> <p>De gegevens die de CSP gebruikt om te verifiëren dat de abonnee de geregistreerde eigenaar is van de in de aanvraag vermelde domeinnaam (FQDN) mogen niet ouder zijn dan 13 maanden anders moeten de gegevens opnieuw worden opgevraagd en geverifieerd.”)</p> <p><i>Email address ownership/control:</i> Not applicable. PKIoverheid does not allow the issuance of Email certificates under the EV CP.</p> <p><i>Digitally signing code objects:</i> Not applicable. PKIoverheid does not allow the issuance of Code Signing certificates under the EV CP.</p>
	SSL category	EV
	Problematic Practices	None. Please see the Problematic Practices section at the bottom of this document for a review of the problematic practices.
	Audit report	Webtrust for Certification Authorities https://cert.webtrust.org/ViewSeal?id=1503 Webtrust for Extended Validation https://cert.webtrust.org/ViewSeal?id=1508 Webtrust for Baseline Requirements

	https://cert.webtrust.org/ViewSeal?id=1520 ETSI 101 456 http://www.quovadisglobal.com/~media/Files/Files_Global/ETS%20010%20eCertificate.ashx
Cross Signing	Not applicable. At present no cross signing has been performed in the PKIoverheid EV hierarchy.
Technical Constraints on Third-party Issuers	<p>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.</p> <p>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).</p>

Verification Policies and Practices

Policy Documentation	<p>Staat der Nederlanden EV Root and Intermediair CAs (Tier 1 and 2) CP (English): 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/Programma_en_eisen/CPS_PA_PKIoverheid_Extended_Validation_v1.2.pdf</p> <p>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</p>
Audits	<p>Staat der Nederlanden Root and Domain CAs (Tier 1 and 2) Audit Type:</p> <ul style="list-style-type: none"> • Trust Service Principles and Criteria for Certification Authorities • WebTrust® for Certification Authorities – SSL Baseline Requirements Audit Criteria, Version 1.1 – January 2013 <p>Auditor: KPMG Advisory N.V.</p>

	<p>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</p> <p>With regard to the Extended Validation root a point-in-time audit has been executed by KPMG. The Management Assertion and Independent Auditor’s Report of this audit have been attached to the bug of this submission request.</p> <p>QuoVadis CSP (Tier3) Audit Type:</p> <ul style="list-style-type: none"> - Webtrust for Certification Authorities (https://cert.webtrust.org/ViewSeal?id=1503) - Webtrust for Extended Validation (https://cert.webtrust.org/ViewSeal?id=1508) - Webtrust for Baseline Requirements (https://cert.webtrust.org/ViewSeal?id=1520) <p>Auditor: Ernst & Young Auditor Website: http://www.ey.com</p> <ul style="list-style-type: none"> - ETSI 101 456 (http://www.quovadisglobal.com/~media/Files/Files_Global/ETS%2010%20eCertificate.ashx) <p>Auditor: BSI Auditor Website: http://www.bsigroup.com</p>
Baseline Requirements (SSL)	<p>The "Commitment to Comply" with the CA/Browser Forum Baseline Requirements is regulated by requirement 2.2-4 of the EV CP (http://www.logius.nl/fileadmin/logius/product/pkioverheid/documenten/PoR_EN_part3e_v3.6.pdf):</p> <p>“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.” “</p> <p>This commitment is incorporated in the QuoVadis EV CPS in section 2.2.4 (https://www.quovadisglobal.com/~media/Files/Repository/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</p>

	<p>inconsistency between the PKI-overheid 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.”</p> <p>(Original text: “QuoVadis conformeert zich aan de huidige versie van de CA/Browser Forum Guidelines for Issuance and Management of Extended Validation Certificates zoals gepubliceerd op http://www.cabforum.org. Mocht er een inconsistentie aanwezig zijn tussen het PKI-overheid Programma van Eisen deel 3e en de betreffende Requirements, waardoor niet tenminste tegemoet wordt gekomen aan de hierin beschreven minimale eisen, dit ter beoordeling door de PA, dan prevaleert het gestelde in de Requirements.”</p>
SSL Verification Procedures	<p>The validation of authority must adhere to section 3.2.5 of the</p> <p><i>Requirement 3.2.5-3</i></p> <p>“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.</p> <p>This verification may not be contracted out by the CSP to Registration Authorities or other parties.</p> <p>If the subscriber states that he/she is the registered owner of the domain name listed in the request, the CSP has to:</p> <ul style="list-style-type: none"> - 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 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. <p>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</p>

	<p>server certificate.</p> <p>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.</p> <p>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:</p> <ul style="list-style-type: none"> - 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. <p>A declaration from the registered domain name owner or notary or external accountant may not be older than 13 months.”</p> <p>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.</p>
<p>Organization Verification Procedures</p>	<p>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).</p> <p><i>Requirement 3.2.2-1</i></p> <p>“The CSP has to verify that the subscriber is an existing and legal organization.</p> <p>As evidence that it is an existing and legal organization, the CSP has to request and verify at least the following supporting documents:</p> <ul style="list-style-type: none"> - 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;

	<ul style="list-style-type: none"> - 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. <p>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.”</p> <p><i>Requirement 3.2.2-2</i> “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:</p> <ul style="list-style-type: none"> - 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.” <p>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.</p>
Email Address Verification Procedures	Not applicable, PKIoverheid does not allow the issuance Email certificates under the EV CP.
Code Signing Subscriber Verification Procedures	Not applicable, PKIoverheid does not allow the issuance Code Signing certificates under the EV CP.
Multi-factor Authentication	The PKIoverheid EV CP (http://www.logius.nl/fileadmin/logius/product/pkioverheid/documenten/PoR_EN_part3e_v3.6.pdf) stipulates the

	<p>following regarding multi-factor authentication:</p> <p><i>Requirement 6.5.1.1:</i> 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.</p> <p>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. “</p> <p><i>Requirement 6.5.1.2</i> “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.”</p> <p><i>Requirement 6.5.1.3</i> “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.”</p> <p>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.</p>
Network Security	<p>The PKIoverheid EV CP (http://www.logius.nl/fileadmin/logius/product/pkioverheid/documenten/PoR_EN_part3e_v3.6.pdf) requires the following regarding Network Security:</p>

	<p><i>Requirement 6.5.1.3</i> “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.”</p> <p><i>Requirement 6.7.1.1</i> “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.”</p> <p><i>Requirement 6.7.1.2</i> “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.”</p> <p><i>Requirement 6.7.1.3</i> “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.”</p>
--	---

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

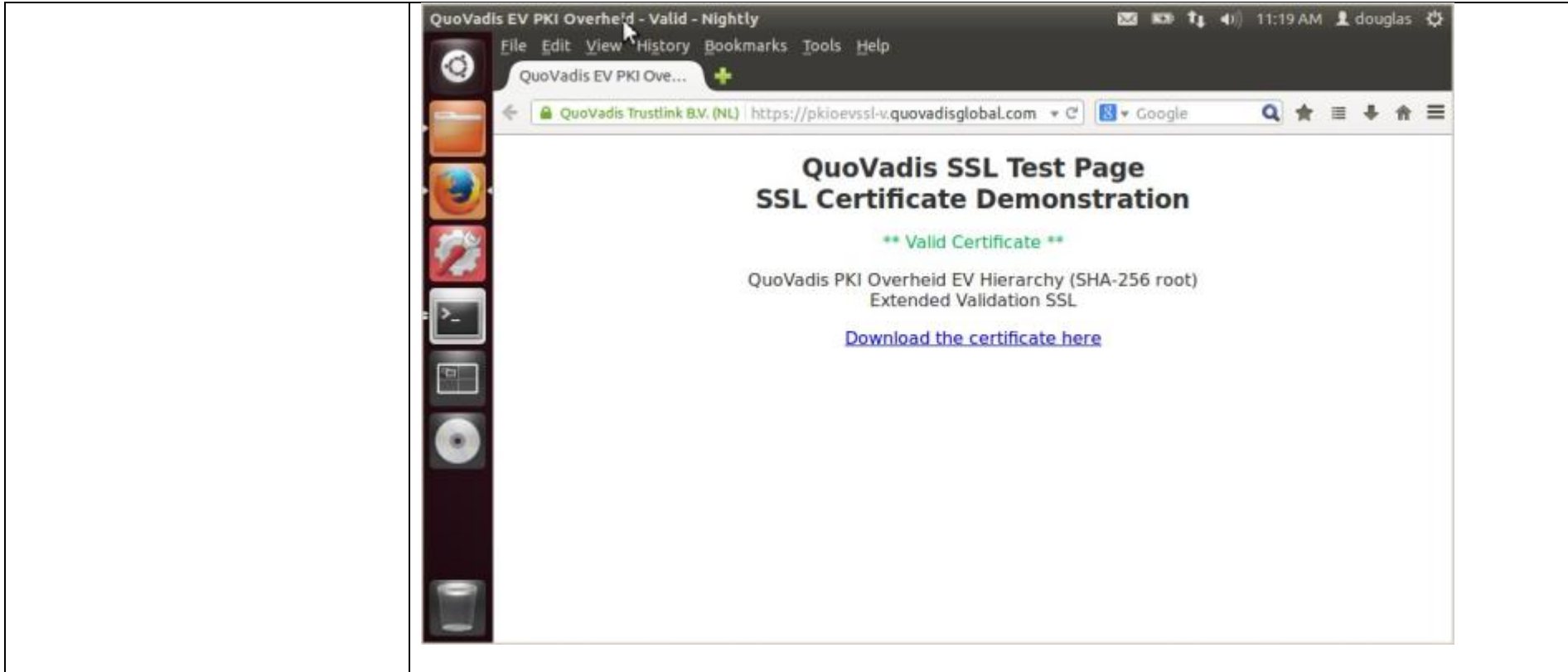
Publicly available CP and CPS	The Extended Validation Certificate Policies is part of the PKIoverheid Programme of Requirements. The full Programme is available in PDF format. The Dutch language version can be obtained here: http://www.logius.nl/producten/toegang/pkioverheid/aansluiten-als-csp/programma-van-eisen/
-------------------------------	--

	<p>The English language version can be obtained here: http://www.logius.nl/english/products/access/pkioverheid/</p> <p>The EV CP is part 3e of the Programme of Requirements and is available as a direct download here: http://www.logius.nl/fileadmin/logius/product/pkioverheid/documenten/PoR_EN_part3e_v3.6.pdf</p> <p>At present one CSP acts as subCA within the Extended Validation hierarchy of PKIoverheid. The Certificate Practice Statement of QuoVadis CSP is available in PDF format. The Dutch language version can be obtained here: https://www.quovadisglobal.com/~media/Files/Repository/QV_CPS_PKI_Overheid_V1_1_4.ashx</p>
CA Hierarchy	<p>The PKIoverheid EV hierarchy consists of three tiers; Root CA, Intermediate Subroot CA and CSP Subroot CA. This hierarchy is described in further detail below:</p> <p>Tier 1: Root CA</p> <ul style="list-style-type: none"> • 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. <p>Tier 2: Intermediate Subroot CA</p> <ul style="list-style-type: none"> • Staat der Nederlanden EV Intermediair CA This internally operated offline Intermediate Subroot CA is used to sign CSP Subroot CAs. <p>Tier 3: CSP Subroot CA</p> <ul style="list-style-type: none"> • 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.
Audit Criteria	<p>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.</p> <p>Section 3.2.1 of part 2 of the PoR stipulates that CSPs have to submit the following documents annually:</p> <ul style="list-style-type: none"> - Proof of compliance with ETSI TS 102 042 or TTP.NL certification for non-personal certificates issued under PoR parts 3b, 3d and 3e;

	<ul style="list-style-type: none"> - 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 PKI 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	<p>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 http://www.logius.nl/fileadmin/logius/product/pkioverheid/documenten/PoR_EN_part3e_v3.6.pdf</p>
Revocation of Compromised Certificates	<p>The circumstances for the revocation of certificates are laid down in requirement 4.9.1.1 of the EV CP http://www.logius.nl/fileadmin/logius/product/pkioverheid/documenten/PoR_EN_part3e_v3.6.pdf.</p> <p>“Certificates must be revoked when:</p> <ul style="list-style-type: none"> - 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 becomes 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 technical content of the certificate entails an irresponsible risk for subscribers, relying parties and third parties (e.g. browser parties).”

<p>Verifying Domain Name Ownership</p>	<p>The requirements in the EV CP (http://www.logius.nl/fileadmin/logius/product/pkioverheid/documenten/PoR_EN_part3e_v3.6.pdf) regarding the validation of Domain ownership/control are as follows:</p> <p>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:</p> <ul style="list-style-type: none"> - 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. <p>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.</p> <p>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:</p>
--	--

	<ul style="list-style-type: none"> - 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. <p>A declaration from the registered domain name owner or notary or external accountant may not be older than 13 months.”</p>
Verifying Email Address Control	Not applicable, PKIoverheid does not allow the issuance Email certificates under the EV CP.
Verifying Identity of Code Signing Certificate Subscriber	Not applicable, PKIoverheid does not allow the issuance Code Signing certificates under the EV CP.
DNS names go in SAN	<p>The requirements in the Extended Validation Certificate Policy (http://www.logius.nl/fileadmin/logius/product/pkioverheid/documenten/PoR_EN_part3e_v3.6.pdf) state the following regarding the subject.commonName (page 60) and subjectAltName.dNSName (page 67).</p> <p>subject.commonName “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.”</p> <p>subjectAltName.dNSName. “This field MUST include at least 1 "fully-qualified domain name (FQDN)" (see the definition in part 4).”</p>
Domain owned by a Natural Person	Not applicable. PKIoverheid does not allow issuance of Extended Validation certificates to natural persons.
OCSP	Per the instructions on https://wiki.mozilla.org/PSM:EV_Testing_Easy_Version the Extended Validation treatment of the PKIoverheid EV hierarchy was tested. The publicly available test website on https://pkioevssl-v.quovadisglobal.com/ 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	Not applicable under the PKIoverheid Extended Validation hierarchy. The organizational identity of the subscriber must be verified as per section 3.2 of the EV CP (part 3e of the Programme of Requirements (http://www.logius.nl/fileadmin/logius/product/pkioverheid/documenten/PoR_EN_part3e_v3.6.pdf))
Wildcard DV SSL certificates	Not applicable under the PKIoverheid Extended Validation hierarchy. The organizational identity of the subscriber must be verified as per section 3.2 of the EV CP (part 3e of the Programme of Requirements (http://www.logius.nl/fileadmin/logius/product/pkioverheid/documenten/PoR_EN_part3e_v3.6.pdf))
Email Address Prefixes for DV Certs	Not applicable under the PKIoverheid Extended Validation hierarchy. The organizational identity of the subscriber must be verified as per section 3.2 of the EV CP (part 3e of the Programme of Requirements)

	http://www.logius.nl/fileadmin/logius/product/pkioverheid/documenten/PoR_EN_part3e_v3.6.pdf
Delegation of Domain / Email validation to third parties	Delegation of domain validation under the EV CP is not allowed. Requirement 3.2.5-3 (http://www.logius.nl/fileadmin/logius/product/pkioverheid/documenten/PoR_EN_part3e_v3.6.pdf) states that “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 form 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 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	Requirement 6.1.1-3 of the EV CP (part 3e of the Programme of Requirements (http://www.logius.nl/fileadmin/logius/product/pkioverheid/documenten/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	The requirements stipulated in the EV CP (http://www.logius.nl/fileadmin/logius/product/pkioverheid/documenten/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 EV CP (http://www.logius.nl/fileadmin/logius/product/pkioverheid/documenten/PoR_EN_part3e_v3.6.pdf). Requirement 3.2.5-3 of the EV CP states that “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), ...”
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 4.9.9-2 of the EV CP (http://www.logius.nl/fileadmin/logius/product/pkioverheid/documenten/PoR_EN_part3e_v3.6.pdf)
CRL with critical CIDP Extension	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 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 supplies 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 requirement 2.4.1 of the EV CP (http://www.logius.nl/fileadmin/logius/product/pkioverheid/documenten/PoR_EN_part3e_v3.6.pdf). These CSPs must conform to RFC3647 to satisfy requirement 2.2.5 of the EV CP. 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.