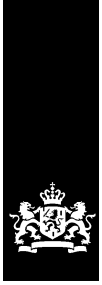

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Programme of Requirements part 3f: Certificate Policy - Extended Validation

Datum 1 February 2017

Extended Validation policy OID 2.16.528.1.1003.1.2.7

Publisher's imprint

Version number 4.4
Contact person Policy Authority of PKIoverheid

Organization Logius

Street address
Wilhelmina van Pruisenweg 52

Postal address
P.O. Box 96810
2509 JE THE HAGUE

T 0900 - 555 4555
servicecentrum@logius.nl

Contents

The Policy Authority (PA) of the PKI for the government supports the Minister of the Interior and Kingdom Relations in managing the PKI for the government.

The PKI for the government is an agreements system. This system enables generic and large-scale use of the electronic signature, and it also facilitates remote identification and confidential communication.
The tasks of the PA of PKIoverheid are:

- contributing towards the development and the maintenance of the framework of standards that underlies the PKI for the government, the Programme of Requirements (PoR);
- assisting in the process of admittance by Trust Service Providers (TSPs) to the PKI for the government and preparing the administration;
- supervising and monitoring the activities of TSPs that issue certificates under the root of the PKI for the government.

The purpose of the Policy Authority is:
Enforcement of a practicable and reliable framework of standards for PKI services that provides an established level of security for the government's communication needs that is transparent to users.

Revision control

Version	**Date**	**Description**
1.0	09-11-2005	Ratified by the Ministry of the Interior and Kingdom Relations November 2005
1.1	25-01-2008	Ratified by the Ministry of the Interior and Kingdom Relations January 2008
1.2	13-01-2009	Ratified by the Ministry of the Interior and Kingdom Relations January 2009
2.0	09-10-2009	Ratified by the Ministry of the Interior and Kingdom Relations October 2009
2.1	11-01-2010	Ratified by the Ministry of the Interior and Kingdom Relations January 2010
3.0	25-01-2011	Ratified by the Ministry of the Interior and Kingdom Relations January 2011
3.1	01-07-2011	Ratified by the Ministry of the Interior and Kingdom Relations June 2011
3.2	27-01-2012	Ratified by the Ministry of the Interior and Kingdom Relations January 2012
3.3	01-07-2012	Ratified by the Ministry of the Interior and Kingdom Relations June 2012
3.4	04-02-2013	Ratified by the Ministry of the Interior and Kingdom Relations 2012

3.5	06-07-2013	Ratified by the Ministry of the Interior and Kingdom Relations July 2013
3.6	01-2014	Ratified by the Ministry of the Interior and Kingdom Relations January 2014
3.7	06-2014	Ratified by the Ministry of the Interior and Kingdom Relations June 2014
4.0	12-2014	Ratified by the Ministry of the Interior and Kingdom Relations December 2014
4.1	07-2015	Ratified by the Ministry of the Interior and Kingdom Relations July 2015
4.1	08-2015	Correction to faulty modification of requirement 3.2.2-pkio147
4.2	01-2016	Ratified by the Ministry of the Interior and Kingdom Relations January 2015
4.3	07-2016	Ratified by the Ministry of the Interior and Kingdom Relations July 2016
4.4	02-2017	Ratified by the Ministry of the Interior and Kingdom Relations February 2017

1 Introduction to the Certificate Policy

1.1 Overview

This is part 3f of the Programme of Requirements (PoR) for the PKI for the government and is known as the Certificate Policy (CP) Extended Validation. Set out in the PoR are the standards for the PKI for the government. This section relates to the requirements laid down for the services of a Trust Service Provider (TSP) within the PKI for the government. This document only relates to the Extended Validation (EV) SSL certificates and EV issuing subordinate certificates issued by TSPs under the Staat der Nederlanden EV Root CA.

This chapter includes a brief explanation of the CP. A more detailed explanation regarding the background and structure of the PKI for the government, as well as the cohesion between the various parts within the PoR is included in part 1 of the PoR.

For a list of the definitions and abbreviations used in this section, please refer to part 4 of the PoR.

1.1.1 Design of the Certificate Policy

As stated in part 1 of the PoR, the requirements that form part of the CP consist of requirements [1]:

- that ensue from the Dutch legal framework in relation to the electronic signature;
- that ensue from the latest version of the ETSI EN 319 411-1 standard, combined with PTC BR and Netsec. **The Netsec requirements 1h, 3a, 3e, 4c.i and 4f are not normative** (ETSI CP OID 0.4.0.2042.1.4);
- that are specifically drawn up by and for the PKIoverheid Extended Validation.

Incorporated in chapters 2 to 9 inclusive are references to the specific PKIoverheid requirements in the Additional Requirements. The table below shows the structure of the reference to the actual PKIoverheid requirement (PKIo requirement).

RFC 3647	Reference to the paragraph from the RFC 3647 structure to which the PKIo requirement relates. RFC 3647 is a PKIX framework of the Internet Engineering Task Force (IETF) and is the de facto standard for the structure of Certificate Policies and Certification Practice Statements[2].
Number	Unique number of the PKIo requirement. In each paragraph, consecutive numbering is used for the PKIo requirements. In combination with the RFC 3647 paragraph number, this forms a unique label for the PKIo requirement.

This CP also includes a number of provisions that are not formulated as PKIo requirements. These provisions do not make any demands on the TSPs within the PKI for the government, but do apply as a policy to the

[1] *For an explanation regarding the positioning of the requirements applicable within the PKI for the government, please refer to part 1 of the PoR.*

[2] *Chapters 2 to 9 inclusive only include those paragraphs from RFC 3647 to which a PKIorequirement applies.*

PKI for the government. This concerns provisions from paragraphs 1.1, 1.1.1, 1.1.2, 1.2, 1.3, 1.4, 1.5, 8, 9.12.1, 9.12.2, 9.14 and 9.17.

The profiles used within PKIoverheid relating to the EV SSL certificates are listed in appendix A. The status information is listed in the basic requirements.

1.1.2 Relationship between CP and CPS

This CP describes the minimum requirements stipulated in respect of services, in terms of EV SSL certificates, of a Trust Service Provider (TSP) within the PKI for the government. The Certification Practice Statement for EV certificates within the PKI for the government states how these services should be interpreted, insofar as this falls under the direct responsibility of the PA.

1.1.3 Status

This is version 4.4 of part 3f of the PoR. The current version has been updated up to and including 1 February 2017.

The PA has devoted the utmost attention and care to the data and information incorporated in this CP. Nevertheless, it is possible that there are inaccuracies and imperfections. The PA accepts no liability for damage resulting from these inaccuracies or imperfections, nor is any liability assumed for damage caused by the use or distribution of this CP, if this CP is used for purposes other than for the use of certificates described in paragraph 1.4 of this CP.

1.2 References to this CP

Each CP is uniquely identified by an OID.
The following OID is registered by PKIoverheid for inclusion in all EV certificates:

EV policy OID **2.16.528.1.1003.1.2.7**

The OID is structured as follows: {joint-iso-itu-t (2). country (16). the Netherlands (528). Dutch organization (1). Dutch government (1003). PKI for the government (1). CP (2). ev (7).

1.3 User Community

The user community consists of subscribers located in The Netherlands who are organizational entities within the government and business community (see PKIo 3.2.2-pkio15) and of certificate holders, who also belong to these subscribers. In addition there are relying parties, who act with a reliance on certificates of the relevant certificate holders.

The parties within the user community are subscribers, certificate managers, certificate holders and relying parties.

- A subscriber is a natural or legal personality who enters into an agreement with a TSP on behalf of one or more certificate holders for the certification of public keys.
- A certificate holder is an entity, characterized in a certificate as the holder of the private key that is linked to the public key provided in the certificate. The certificate holder is part of an organizational entity, for which a subscriber is the contracting party.

Within the Certificate Policy Extended Validation, the term certificate holder means:

- a device or a system (a non-natural person), operated by or on behalf of an organizational entity.

In this CP we use the name "service" for the foregoing certificate holders. To perform the actions in respect of the lifecycle of the certificate holder's certificate, intervention by a party other than the certificate holder is required. The subscriber is responsible for this and has to appoint a certificate manager to perform these actions.

- A certificate manager is a natural personality who performs actions on behalf of the subscriber in respect of the certificate holder's certificate. The subscriber instructs the certificate manager to perform the relevant actions and records these in a certificate manager's testimony.
- A relying party is every natural or legal personality who is a recipient of a certificate and who acts with a reliance on that certificate. Other than for personal certificates, relying parties mainly derive security from the connection of a service (device or feature) to the organizational entity to which the service belongs. The CP Extended Validation therefore places the emphasis on providing certainty about the connection of a message sent by or a web service provided by a device, system or (staff) position with the relevant organization. In view of this, establishing the identity of the certificate holder (device or feature) is less important than establishing the certificate holder's connection to the organizational entity.

1.4 Certificate Usage

The use of certificates issued under this CP relates to communication from certificate holders who act on behalf of the subscriber.

[OID 2.16.528.1.1003.1.2.7]
EV SSL certificates that are issued under this CP, can be used to safeguard a connection between a specific client and a server, via the TLS/SSL protocol, that is part of the organizational entity that is listed as the subscriber in the relevant certificate.

1.5 Contact Information Policy Authority

The PA is responsible for this CP. Questions relating to this CP can be put to the PA; the address can be found at: http://www.logius.nl/pkioverheid.

2 Publication and Repository Responsibilities

2.1 Electronic Repository

Contains no additional requirements.

2.2 Publication of TSP Information

RFC 3647	2.2 Publication of TSP information
Number	2.2-pkio9

2.4 Access to Published Information

Contains no additional requirements.

3 Identification and Authentication

3.1 Naming

Contains no additional requirements.

3.2 Initial Identity Validation

RFC 3647	3.2.1. Method to prove possession of the private key
Number	3.2.1-pkio13

RFC 3647	3.2.2 Authentication of organizational entity
Number	3.2.2-pkio147

RFC 3647	3.2.3 Authentication of individual identity
Number	3.2.3-pkio27

RFC 3647	3.2.5 Validation of authority
Number	3.2.5-pkio30

RFC 3647	3.2.5 Validation of authority
Number	3.2.5-pkio33

RFC 3647	3.2.5 Validation of authority
Number	3.2.5-pkio35

RFC 3647	3.2.5 Validation of authority
Number	3.2.5-pkio146

3.3 Identification and Authentication for Re-key Requests

Contains no additional requirements.

4 Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

RFC 3647	4.1 Certificate Application
Number	4.1-pkio48

4.4 Certificate Acceptance

Contains no additional requirements.

4.5 Key Pair and Certificate Usage

RFC 3647	4.5.2 Relying party public key and certificate usage
Number	4.5.2-pkio145

4.9 Revocation and Suspension of Certificates

RFC 3647	4.9.3 Procedures for revocation request
Number	4.9.3-pkio57

RFC 3647	4.9.3 Procedures for revocation request
Number	4.9.3-pkio60

RFC 3647	4.9.5 Time within which CA must process the revocation request
Number	4.9.3-pkio62

RFC 3647	4.9.9 On-line revocation/status checking availability
Number	4.9.9-pkio152

4.10 Certificate Status Services

Contains no additional requirements.

5 Facility, Management and Operational Controls

5.2 Procedural Controls

Contains no additional requirements.

5.3 Personnel Controls

Contains no additional requirements.

5.4 Audit Logging Procedures

Contains no additional requirements.

5.5 Records Archival

RFC 3647	5.5.1 Types of events recorded
Number	5.5.1-pkio82

5.7 Compromise and Disaster Recovery

Contains no additional requirements.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

RFC 3647	6.1.1 Key pair generation for the TSP sub CA
Number	6.1.1-pkio87

RFC 3647	6.1.1 Key pair generation for the certificate holders
Number	6.1.1-pkio90

RFC 3647	6.1.1 Key pair generation for the certificate holders
Number	6.1.1-pkio92

6.2 Private Key Protection and Cryptographic Module Engineering Controls

RFC 3647	6.2.11 Cryptographic module rating
Number	6.2.11-pkio107

6.3 Other Aspects of Key Pair Management

Contains no additional requirements.

6.4 Activation data

Contains no additional requirements.

6.5 Computer Security Controls

Contains no additional requirements.

6.6 Life Cycle Technical Controls

Contains no additional requirements.

6.7 Network Security Controls

Contains no additional requirements.

7 Certificate, CRL and OSCP profiles

7.1 Certificate Profile

Contains no additional requirements.

7.2 CRL Profile

Contains no additional requirements.

7.3 OCSP Profile

RFC 3647	7.3 OCSP profile
Number	7.3-pkio123

8 Compliance Audit and Other Assessments

All subjects relating to the conformity assessment of the TSPs within the PKI for the government are covered in PoR part 2: Admittance to and Supervision within the PKI for the government.

9 Other Business and Legal Matters

9.2 Financial Responsibility

Contains no additional requirements.

9.5 Intellectual Property Rights

Contains no additional requirements.

9.6 Representations and Warranties

RFC 3647	9.6.1 CA Representations and Warranties by TSPs
Number	9.6.1-pkio128

9.8 Limitations of Liability

RFC 3647	9.8 Limitations of liability
Number	9.8-pkio134

9.12 Amendments

Contains no additional requirements.

9.13 Dispute Resolution Procedures

Contains no additional requirements.

9.14 Governing Law

Contains no additional requirements.

9.17 Miscellaneous provisions

Contains no additional requirements.

If by judicial decision one or more provisions of this CP are declared to be invalid or not applicable, this does not affect the validity and applicability of all other provisions.

Appendix A Certificate profile

Profile of Extended Validation certificates of the EV root certificate

Criteria
When defining the fields and attributes within a certificate, the following codes are used:

- V : Compulsory; indicates that the attribute is compulsory and MUST be used in the certificate.
- O : Optional; indicates that the attribute is optional and MAY be used in the certificate.
- A : Advised against; indicates that the attribute is advised against and SHOULD NOT be used in the certificate.

It is not allowed to use fields that are not specified in the certificate profiles .

For the extensions, fields/attributes are used that, in accordance with international standards, are critical, are marked in the 'Critical' column with 'yes' to show that the relevant attribute MUST be checked using a process by means of which a certificate is evaluated. Other fields/attributes are shown with 'no'.

Services certificates for authenticity and confidentiality

Basic attributes

Field / Attribute	Criteria	Description	Standard reference	Type	Explanation
Version	V	MUST be set at 2 (X.509v3).	RFC 5280	Integer	Describes the version of the certificate, the value 2 stands for X.509 version 3.
SerialNumber	V	A serial number that MUST uniquely identify the certificate within the publishing CA domain.	RFC 5280	Integer	All end user certificates have to contain at least 8 bytes of unpredictable random data in the certificate's serial number (SerialNumber).
Signature	V	MUST be created on the algorithm, as stipulated by the PA.	RFC 5280, ETSI TS 102176	OID	MUST be the same as the field signatureAlgorithm. For maximum interoperability, for certificates issued under this CP, only sha-256WithRSAEncryption is allowed. For the key lengths, see the PKIoverheid CPS EV certificates.
Issuer	V	MUST contain a Distinguished Name (DN). The field has the attributes listed below:	PKIo, RFC3739, ETSI TS 102280		Attributes other than those mentioned below MUST NOT be used. The attributes that are used MUST be the same as the corresponding attributes in the Subject field of the TSP certificate (for validation).
Issuer.countryName	V	MUST contain the country code of the country where the issuing organization of the certificate is located.	ETSI TS101862, X520, ISO 3166	Printable String	C = NL for TSPs located in the Netherlands.
Issuer.OrganizationName	V	Full name in accordance with the accepted document or basic registry	ETSI TS 102280	UTF8String	
Issuer. organizationalUnitName	O	Optional specification of an organizational	ETSI TS 102280	UTF8String	Several instances of this attribute MAY be used.

Field / Attribute	Criteria	Description	Standard reference	Type	Explanation
		entity. This field MUST NOT include a function indication or similar. It may include, if applicable, the types of certificates that are supported.			
Issuer.serialNumber	O	MUST be used in accordance with RFC 3739 IF unambiguous naming requires this	RFC 3739	Printable String	
Issuer.commonName	V	MUST include the name of the CA in accordance with accepted document or basic registry, MAY include the Domain label and/or the types of certificates that are supported	PKIo, RFC 3739	UTF8String	The commonName attribute MUST NOT be necessary to identify the issuing government body (no part of the Distinguished Name, requirement from RFC 3739)
Issuer.organizationIdentifier	V	The organizationIdentifier field contains an identification of the issuing CA. This field MUST be present when the subject.organizationIdentifier field is present in the TSP certificate and MUST NOT be present when this field is not part of the corresponding TSP certificate.	EN 319 412-1	String	The syntax of the identification string is specified in paragraph 5.1.4 van ETSI EN 319 412-1 and contains: • 3 character legal person identity type reference; • 2 character ISO 3166 [2] country code; • hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8)); and • identifier (according to country and identity type reference).
Validity	V	MUST define the period of validity of the certificate according to RFC 5280.	RFC 5280	UTCTime	MUST include the start and end date for validity of the certificate in accordance with the applicable policy laid down in the EV CPS.
subject	V	The attributes that are used to describe the subject (service) MUST mention the subject	PKIo, RFC3739, ETSI TS 102 280		MUST contain a Distinguished Name (DN). Attributes other than those mentioned below MUST NOT be used.

Field / Attribute	Criteria	Description	Standard reference	Type	Explanation
		in a unique way and include information about the subscriber organization. The field has the following attributes:			
Subject.businessCategory	V	MUST include one of the following values: 2.5.4.15 = Private Organization 2.5.4.15 = Government Entity 2.5.4.15 = Business Entity 2.5.4.15 = Non-Commercial Entity	PKIo		▪ Private Organization applies to organizations governed by private law with a legal personality; ▪ Government Entity applies to government organizations; ▪ Business Entity applies to organizations governed by private law without a legal personality; Formal collaborative ventures between companies also fall under this category; ▪ Non-Commercial Entity applies in international organizations that do not belong to one country or government (e.g. the NATO (http://www.nato.int) or the United Nations (http://www.un.int)). NO PKIoverheid EV SSL certificates MAY be issued to these types of organizations.
Subject.countryName	V	complete C with two-letter country code in accordance with ISO 3166-1. If an official alpha-2 code is missing, the TSP MAY use the user-assigned code XX.	RFC 3739, X520, ISO 3166, PKIo	PrintableString	The country code that is used in Subject.countryName MUST correspond with the subscriber's address in accordance with the accepted document or registry.
Subject.commonName	A	Name that identifies the server. 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	RFC 3739, ETSI TS 102 280, PKIo	UTF8String	In this attribute, wildcards, private IP addresses and/or host names, internationalized domain names (IDNs) and null characters \0 may not be used.

Field / Attribute	Criteria	Description	Standard reference	Type	Explanation
		FQDN MUST also be included in the SubjectAltName.dNSName field.			
Subject.organizationName	V	MUST include the full name of the subscriber organization in accordance with the accepted document (State Almanac) or Basic Registry (Trade Register).	PKIo	UTF8String	The subscriber organization is the organization with which the TSP has entered into an agreement and on behalf of which the certificate holder (service/server) communicates or acts. The TSP MAY modify the full name of the subscriber organization if this has more than 64 positions. The TSP MUST consult the subscriber about this. The modification MUST take place in such a way that the relying parties do not think that they are dealing with a different organization. If this type of modification is not possible, then TSP MAY NOT issue the EV SSL certificate.
Subject.organizationalUnitName	O/ V	Optional specification of an organizational entity. This attribute MUST NOT include a function indication or similar. Compulsory labelling of a government organization.	PKIo		This attribute MAY appear several times. The field MUST contain a valid name of an organizational entity of the subscriber in accordance with an accepted document or registry. Only in those cases in which a government organization entity is not yet listed in the Trade Register, in this field the TSP MUST include the words “government organization”.
Subject.stateOrProvinceName	V	MUST include the province of the subscriber's branch, in accordance with the accepted document (State Almanac) or Basic registry (Trade Register).	PKIo, RFC 3739	UTF8String	

Field / Attribute	Criteria	Description	Standard reference	Type	Explanation
Subject.localityName	V	MUST include the subscriber's location in accordance with the accepted document (State Almanac) or Basic registry (Trade Register).	PKIo, RFC 3739	UTF8String	.
Subject.streetAddress	O	If present, this field MUST contain the subscriber's street name in accordance with an accepted document (State Almanac) or Basic registry (Trade Register).	PKIo, RFC 3739	UTF8String	
Subject.postalCode	O	If present, this field MUST contain the postcode related to the subscriber's street name in accordance with an accepted document (State Almanac) or Basic registry (Trade Register).	PKIo, RFC 3739	UTF8String	
Subject:jurisdictionOfIncorporationCountryName	V	Fixed value: 1.3.6.1.4.1.311.60.2.1.3 = NL	RFC 5280, ISO 3166	OID	
Subject.postalAddress	A	The use is advised against. If available, this field MUST contain the postal address of the subscriber in accordance with an accepted document or Basic registry.	PKIo, RFC 3739	UTF8String	The address MUST correspond with the address of the subscriber in accordance with the accepted document or registry.
Subject.serialNumber	V	The TSP is responsible for safeguarding the uniqueness of the subject (service). The Subject.serialNumber MUST be used to	RFC 3739, X 520, PKIo	Printable String	The Chamber of Commerce number MUST be included in this field. In those cases where an organizational entity within the government is

Field / Attribute	Criteria	Description	Standard reference	Type	Explanation
		identify the subject uniquely.			not yet listed in the Trade Register the TSP MUST determine the number itself with which the uniqueness of the subject (service) is safeguarded. The TSP MUST then also include in the field Subject.organizationalUnitName the word "government organisation".
subjectPublicKeyInfo	V	Contains, among other things, the public key.	ETSI TS 102 280, RFC 3279		Contains the public key, identifies the algorithm with which the key can be used.

Standard extensions

Field / Attribute	Criteria	Critical?	Description	Standard reference	Type	Explanation
authorityKeyIdentifier	V	No	The algorithm to generate the AuthorityKey MUST be created on an algorithm determined by the PA.	ETSI TS 102 280, RFC 5280	BitString	The value MUST contain the SHA-1 hash from the authorityKey (public key of the TSP/CA).
SubjectKeyIdentifier	V	No	The algorithm to generate the subjectKey MUST be created on an algorithm determined by the PA.	RFC 5280	BitString	The value MUST contain the SHA-1 hash from the subjectKey (public key of the certificate holder).
KeyUsage	V	Yes	In EV subordinate CA certificates that are issued under an EV TSP CA certificate the keyCertSign and cRLSign MUST be included and marked as essential. Another keyUsage MUST NOT be combined with this. In EV SSL certificates the digitalSignature and keyEncipherment bits MUST be incorporated and marked as critical. Another keyUsage MUST NOT be combined with this.	RFC 3739, RFC 5280, ETSI TS 102 280	BitString	
CertificatePolicies	V/ O	No	MUST include the OID of this EV certificate policy (CP) and the EV OID of the CA/B forum. When the certificate is also issued as Qualified Web Certificate the QCP-w policy id MUST be included.	RFC 3739 RFC 5280	OID, String, UTF8String or IA5 String	The following OIDs apply: • 2.16.528.1.1003.1.2.7 and • 2.23.140.1.1 This OID MUST be included in EV SSL certificates and in EV subordinate CA certificates that are issued under an EV TSP CA

Field / Attribute	Criteria	Critical?	Description	Standard reference	Type	Explanation
			policyIdentifier ▪ EV policy identifier policyQualifiers:policyQualifierId ▪ id-qt 1 [RFC 5280] In EV subordinate CA certificates that are issued under an EV TSP CA certificate the HTTP URL of the EV Certification Practice Statement of the PA of PKIoverheid MUST be incorporated. policyQualifiers:qualifier:cPSuri ▪ HTTP URL of the Certification Practice Statement of the PA of PKIoverheid In EV SSL certificates, the HTTP URL of the certification practice statement (CPS) of the TSP MUST be incorporated policyQualifiers:qualifier:cPSuri ▪ HTTP URL of the Certification Practice Statement of the TSP In EV SSL certificates a user notice MUST be incorporated. The TSP SHOULD use UTF8String in the userNotice, but MAY use IA5String.			certificate. The QCP-w policy OID is 0.4.0.194112.1.4 The HTTP URL of the EV Certification Practice Statement of the PA of PKIoverheid is: http://www.logius.nl/producten/toegang/pkioverheid/documentatie/cps/

Field / Attribute	Criteria	Critical?	Description	Standard reference	Type	Explanation
PolicyMappings	N		Is not used.			This extension is not used in EV SSL certificates
QcStatement	V/ N	No	Qualified Web Certificates MUST indicate that they are issued as qualified certificates complying with annex IV of EU regulation 920/2014. This compliance is indicated by including the *id-etsi-qcs-QcCompliance* statement in this extension. Qualified Web Certificates MUST indicate that they are issued as type of certificate complying with annex IV of EU regulation 920/2014. This compliance is indicated by including the *id-etsi-qct-web* statement in this extension. Qualified Web Certificates MAY indicate that the private key that is part of the public key in the certificate is saved on a qualified signature creation device (QSCD) complying with annex II of EU regulation 920/2014. This compliance is indicated by including the *id-etsi-qcs-QcSSCD* statement in this extension. If a QSCD is used this statement MUST be included. Qualified Web Certificates MUST contain a	RFC 3739, ETSI TS 102 280, ETSI TS 101 862	OID	The aforementioned QcStatement identifiers relate to the following OIDs: • id-etsi-qcs-QcCompliance { id-etsi-qcs 1 } 0.4.0.1862.1.1 • id-etsi-qct-web { id-etsi-qcs-QcType 3 } 0.4.0.1862.1.6.3 • id-etsi-qcs-QcSSCD { id-etsi-qcs 4 } 0.4.0.1862.1.4 • id-etsi-qcs-QcPDS { id-etsi-qcs 5 } 0.4.0.1862.1.5

Field / Attribute	Criteria	Critical?	Description	Standard reference	Type	Explanation
			reference to the location of the PKI Disclosure Statement (PDS). This URL must present in the *id-etsi-qcs-QcPDS* statement in this extension.			
SubjectAltName	V	No	MUST be used and given a worldwide unique number that identifies the service.	RFC 4043, RFC 5280, PKIo, ETSI 102 280		MUST include a unique identifier in the othername attribute. Attributes other than those mentioned below MUST NOT be used.
SubjectAltName.dNSName	V		Name that identifies the server. This field MUST include at least 1 "fully-qualified domain name (FQDN)" (see the definition in part 4). Several FQDNs MAY be used in this field. These FQDNs MUST come from the same domain name range. (e.g. www.logius.nl, applicatie.logius.nl, secure.logius.nl etc. etc.).	RFC2818, RFC5280	IA5String	In this attribute, wildcards, private IP addresses and/or host names, internationalized domain names (IDNs) and null characters \0 may not be used.
SubjectAltName.rfc822Name	A		MAY be used for a service's e-mail address, for applications that need the e-mail address in order to be able to function properly.	RFC 5280	IA5String	For EV SSL certificates, the use of e-mail addresses is advised against, because e-mail addresses of certificate holders often change and are susceptible to spam.
SignedCertificate-TimestampList	V	No	The Signed Certificate Timestamp List	RFC 6962	OCTET STRING	See requirement 4.4.3-pkio154 for the usage of the

Field / Attribute	Criteria	Critical?	Description	Standard reference	Type	Explanation
(OID 1.3.6.1.4.1.11129.2.4.2)			contains one or more Signed Certificate Timestamps.			SignedCertificateTimestampList
BasicConstraints	O	Yes	The "CA" field must be omitted (default value is then "FALSE").	RFC 5280		In a (Dutch language) browser, the following will be visable: Subjecttype = Eindentiteit", "Beperking voor padlengte = Geen ("Subjecttype = End Entity", "Restriction for the path length = None")
CRLDistributionPoints	V	No	MUST include the HTTP URI of a CRL distribution point.	RFC 5280, ETSI TS 102 280		
ExtKeyUsage	V	No	Extension that indicates for which applications the certificate can be used.	RFC 5280	KeyPurposeId's	In EV SSL certificates, the attributes id-kp-serverAuth (Verification of the server) and id-kp-clientAuth (Client verification) MUST be included.
FreshestCRL	O	No	MUST contain the URI of a Delta CRL distribution point, if Delta CRLs are used.	RFC 5280, PKIo		Delta-CRLs are an optional extension. In order to fulfil the requirements of PKIoverheid a TSP MUST also publish full CRLs at the required release frequency.

Private extensions

Field / Attribute	Criteria	Critical?	Description	Standard reference	Type	Explanation
authorityInfoAccess	V	No	This attribute MUST include the HTTP URI of an OCSP responder such as Online Certificate Status Protocol (OCSP).			The EV CA certificate (EV TSP CA or EV subordinate CA certificate) MAY also include the HTTP URL of the State of the Netherlands EV Root CA certificate. The EV SSL certificate MAY also include the HTTP URL of the issuing EV CA certificate (EV TSP CA or EV subordinate CA certificate).
SubjectInfoAccess	O	No		RFC 5280	OID, Generalname	This field can be used to reference additional information about the subject.

10 Revisions

10.1 Amendments from version 4.3 to 4.4

10.1.1 New

- Added requirement 4.4.3-pkio154 and modified certificate profile accordingly (mandatory use of Certificate Transparency, effective date 1-7-2017)

10.1.2 Modifications

- Clarification of issuer.organizationIdentifier field (effective date 1-2-2017)
- Tightening of use optional EKUs that conflict with the parent TSP CA certificate (effective date 1-2-2017)

10.1.3 Editorial

- Replaced CSP (Certificate Service Provider) with TSP (Trust Service Provider) in accordance with eIDAS directive.

10.2 Amendments from version 4.2 to 4.3

10.2.1 New

- Addition of qualified website certificates (effective date 1-7-2016)
- Addition of issuer.organizationalIdentifier in the certificate profile (effective date 1-7-2016)

10.2.2 Modifications

- Description with attribute CertificatePolicies (effective date 1-7-2016)
- ETSI TS 102 042 replaced by ETSI EN 319 411-1 (effective date 1-7-2016 or when the accreditation to the certifying body has been granted with a final date of 30 June 2017)
- Use of values in BasicConstraints field no longer permitted in end entity certificates (effective date 1-7-2016)
- ETSI TS 102 176-1 replaced by ETSI TS 119 312 (effective date no later than 4 weeks after publication of PoR 4.3)

10.2.3 Editorial

None

10.3 Amendments from version 4.1 to 4.2

10.3.1 New

- Requirement 7.1-pkio152 (effective date 1 july 2016)

10.3.2 Modifications

- Addition of OID to Certificate Profiles (effective date 1 april 2016)

10.3.3 Editorial

None

10.4 Amendments from version 4.0 to 4.1

10.4.1 New

- Requirement 3.2.5-pkio146 (effective date no later than 31-12-2015);

10.4.2 Modifications

- Requirement 3.2.5-pkio35
- The following requirements have been deleted:
    - Requirement 3.2.0-pkio12;
    - Requirement 3.2.2-pkio15 (combined with requirement 3.2.3-pkio23 under new requirement 3.2.2-pkio147);
    - Requirement 3.2.2-pkio17;
    - Requirement 3.2.2-pkio18;
    - Requirement 3.2.2-pkio19;
    - Requirement 3.2.2-pkio20;
    - Requirement 3.2.3-pkio23 (combined with requirement 3.2.3-pkio23 under new requirement 3.2.2-pkio147);
    - Requirement 3.2.3-pkio25;
    - Requirement 3.2.3-pkio28;
    - Requirement 4.4.1-pkio50;
    - Requirement 4.9.3-pkio59;
    - Requirement 9.6.1-pkio130.
- Ban on the use of SubjectAltName.otherName (effective date no later than 4 weeks after publication of PoR 4.1)

10.4.3 Editorial

- Small editorial modification to the following requirement:
    - Requirement 3.2.3-pkio27.

10.5 Amendments from version 3.7 to 4.0

10.5.1 New

- Requirement 2.2-pkio9
- Requirement 4.5.2-pkio145
- Requirement 5.2.4-pkio77

10.5.2 Modifications

- PoR requirements have been renumbered according to a new naming convention;
- The creation of a document containing the baseline and additional requirements;
- Changes to requirements can be found in the baseline and additional requirements documents respectively.

10.5.3 Editorial

Editorial changes to requirements can be found in the baseline and additional requirements documents respectively. These changes have no effect on the content of the information.