Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Programme of Requirements part 3b:
Certificate Policy authenticity, confidentiality
and non-reputiation certificates –
Organisation Services (G3)
Appendix to CP Organization (G2)

Date   8 February 2019

Organization (G2) / Organization Services (G3) Domains:
Services - Authenticity   2.16.528.1.1003.1.2.5.4
Services - Confidentiality   2.16.528.1.1003.1.2.5.5
Services – Non-repudiation   2.16.528.1.1003.1.2.5.7

Publisher's imprint

Version number   4.7
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 Certification 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
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
4.2	01-2016	Ratified by the Ministry of the Interior and Kingdom Relations January 2016
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
4.5	07-2017	Ratified by the Ministry of the Interior and Kingdom Relations July 2016
4.6	01-2018	Ratified by the Ministry of the Interior and Kingdom Relations January 2017
4.7	01-2019	Ratified by the Ministry of the Interior and Kingdom Relations Februari 2019

1   Introduction to the Certificate Policy

1.1   Overview

This is part 3b of the Programme of Requirements (PoR) for the PKI for the government and is known as the Certificate Policy (CP). 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. Within the PKI for the government , a distinction is made between various domains. This document only relates to the services certificates issued by TSPs in the Government/Companies and Organization domains.

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
    - where policy NCP+ is applicable, so that a SUD is used (ETSI CP OID 0.4.0.2042.1.2)[2];
- that ensue from the latest version of the ETSI EN 319 411-2 standard, QCP-l-qcsd (ETSI CP OID 0.4.0.194112.3) for seal certificates (*eSeals*);
- that are specifically drawn up by and for the PKIoverheid.

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[3].
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.

---

[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] *The CP services are based on an underlying standard different to that of the CPs for ersonal certificates. Because services certificates are not personal and are not qualified certificates in accordance to the "Wet Elektronische Handtekeningen" (Electronic Signature Act), the requirements for services certificates differ on certain points from the requirements for other types of certificates*

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

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 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 services certificates and are listed in appendix A. The status information is listed in the basic requirements.

1.1.2   *Status*
This is version 4.7 of part 3b of the PoR. The current version has been updated up to and including 8 February 2019.

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
Within the PKI for the government different structures or roots are used based both on the SHA-1 algorithm (G1) and the SHA-256 algorithm (G2 and G3). Furthermore these structures are devided into different domains. For the G1 root this division consists of the Government/Companies domains (these two domains have merged over time) and Citizen domain. The G2 root is devided into an Organization, a Citizen and an Autonomous Devices domain.
Under the G3 root there are domains for Organization Person, Organization Services, Citizen, and Autonomous Devices.

Each CP is uniquely identified by an OID, in accordance with the following schedule.

Organization / Organization Services Domains:	
OID	**CP**
2.16.528.1.1003.1.2.5.4	for the authenticity certificate for services within the Organization domain, that contains the public key for identification and authentication. Under this OID OCSP certificates may be issued for use within the context of this CP part.
2.16.528.1.1003.1.2.5.5	for the confidentiality certificate for services within the Organization domain, that contains the public key for confidentiality.
2.16.528.1.1003.1.2.5.7	for the seal Certificate for services within the Organization domain, that contains the public key for the qualified electronic seal/non-repudiation.

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). organization domain (5). authenticity (4)/ confidentiality (5). version number}.

If requirements only apply to one or two types of certificates, this is expressly specified by stating the Object Identifier (OID) referencing the applicable CP or CPs.

1.3   **User Community**

Within the Government/Companies and Organization domains, the user community consists of subscribers who are organizational entities within the government and business community (see PKIo 3.2.2-pkio4) 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 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 Services, the term certificate holder means:
  - o   a device or a system (a non-natural person), operated by or on behalf of an organizational entity; or
  - o   a function 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 Services 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 2.16.528.1.1003.1.2.5.4]
Authenticity certificates, issued under this CP, can be used to identify and authenticate, by electronic means, the service that is part of the organizational entity, that is responsible for the relevant service. Issuance of code signing certificates by means of which the integrity and authenticity of software can be safeguarded by a digital signature being placed are NOT allowed under this CP.

Under this OID OCSP responder certificates may be issued for use within the domain Organisation Services. Said certificates can be used to sign OCSP responses for use in the verification of the validity of the end user certificate. More information can be obtained in appendix A of the base requirements.

[OID 2.16.528.1.1003.1.2.5.5]
Confidentiality certificates, issued under this CP, can be used to protect the confidentiality of data that is exchanged and/or stored in an electronic format.

[OID 2.16.528.1.1003.1.2.5.7]
Seal certificates, issued under this CP, can be used to verify electronic seals.

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-pkio3

RFC 3647	2.2 Publication of TSP information
Number	2.2-pkio8

RFC 3647	2.2 Publication of TSP information
Number	2.2-pkio156

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-pkio4

RFC 3647	3.2.2 Authentication of organizational entity
Number	3.2.2-pkio144

RFC 3647	3.2.3 Authentication of individual identity
Number	3.2.3-pkio22

RFC 3647	3.2.3 Authentication of individual identity
Number	3.2.3-pkio24

RFC 3647	3.2.3 Authentication of individual identity
Number	3.2.3-pkio26

RFC 3647	3.2.3 Authentication of individual identity
Number	3.2.3-pkio169

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

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-pkio47

4.4 Certificate Acceptance

Contains no additional requirements.

4.5 Key Pair and Certificate Usage

Contains no additional requirements.

4.9 Revocation and Suspension of Certificates

RFC 3647	4.9.1 Circumstances for revocation
Number	4.9.1-pkio52

RFC 3647	4.9.3 Procedures for revocation request
Number	4.9.3-pkio57

RFC 3647	4.9.7 CRL issuance frequency
Number	4.9.7-pkio65

RFC 3647	4.9.9 On-line revocation/status checking availability
Number	4.9.7-pkio66

RFC 3647	4.9.9 On-line revocation/status checking availability
Number	4.9.9-pkio67

RFC 3647	4.9.9 On-line revocation/status checking availability
Number	4.9.9-pkio70

RFC 3647	4.9.9 On-line revocation/status checking availability
Number	4.9.9-pkio71

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 Loggin Procedures

RFC 3647	5.4.1 Types of events recorded
Number	5.4.1-pkio80

5.5 Records Archival

RFC 3647	5.5.1 Types of events recorded
Number	5.5.1-pkio82

5.7 Compromise and Disaster Recovery

RFC 3647	5.7.4 Business continuity capabilities after a disaster.
Number	5.7.4-pkio86

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-pkio88

RFC 3647	6.1.1 Key pair generation for the certificate holders
Number	6.1.1-pkio89

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

RFC 3647	6.1.1 Key pair generation for the certificate holders
Number	6.1.1-pkio93

RFC 3647	6.1.1 Key pair generation for the certificate holders
Number	6.1.1-pkio153

6.2 Private Key Protection and Cryptographic Module Engineering Controls

RFC 3647	6.2.3 Private key escrow of certificate holder key
Number	6.2.3-pkio99

RFC 3647	6.2.3 Private key escrow of certificate holder key
Number	6.2.3-pkio100

RFC 3647	6.2.11 Cryptographic module rating
Number	6.2.11-pkio105

RFC 3647	6.2.11 Cryptographic module rating
Number	6.2.11-pkio125

6.3 Other Aspects of Key Pair Management

RFC 3647	6.3.2 Certificate operational periods and key pair usage periods
Number	6.3.2-pkio109

6.4 Activation data

RFC 3647	6.4.1 Activation data generation and installation
Number	6.4.1-pkio112

RFC 3647	6.4.1 Activation data generation and installation
Number	6.4.1-pkio113

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

RFC 3647	7.1 Certificate Profile
Number	7.1-pkio150

RFC 3647	7.1 Certificate Profile
Number	7.1-pkio177

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 and the basic requirements.

9 Other Business and Legal Matters

9.2 Financial Responsibility

RFC 3647	9.2.1 Insurance coverage
Number	9.2.1-pkio124

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-pkio127

RFC 3647	9.6.1 CA Representations and Warranties by TSPs
Number	9.6.1-pkio129

RFC 3647	9.6.1 CA Representations and Warranties by TSPs
Number	9.6.1-pkio132

9.8 Limitations of Liability

RFC 3647	9.8 Limitations of liability
Number	9.8-pkio133

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   Other provisions

RFC 3647	9.17 Other provisions
Number	9.17-pkio140

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 services certificates for the Organisation Services domain

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 certificates under the G2 and G3 root certificate, only sha-256WithRSAEncryption is allowed.
Issuer	V	MUST contain a Distinguished Name (DN). The field has the following attributes:	PKIo, RFC3739, ETSI TS 102280		Attributes other than those mentioned below MUST NOT be used.
Issuer.countryName	V	See requirement 7.1-pkio174	ETSI TS101862, X520, ISO 3166	Printable String	
Issuer.OrganizationName	V	See requirement 7.1-pkio174	ETSI TS 102280	UTF8String	
Issuer. organizationalUnitName	O	See requirement 7.1-pkio174	ETSI TS 102280	UTF8String	
Issuer.serialNumber	O	See requirement 7.1-pkio174	RFC 3739	Printable String	
Issuer.commonName	V	See requirement 7.1-pkio174	PKIo, RFC 3739	UTF8String	The commonName attribute MUST NOT be needed 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	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:

Field / Attribute	Criteria	Description	Standard reference	Type	Explanation
		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.			• 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 CPS.
Subject	V	The attributes that are used to describe the subject (service) MUST mention the subject in a unique way and include information about the subscriber organization. The field has the following attributes:	PKIo, RFC3739, ETSI TS 102 280		MUST contain a Distinguished Name (DN). Attributes other than those mentioned below MUST NOT be used.
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	V	Name that identifies the service. In services certificates this field is compulsory	RFC 3739, ETSI TS 102 280, PKIo	UTF8String	Incorporated in the subject.commonname is the function of an organizational entity or the name by which the device or system is known.
Subject.pseudonym	N	Pseudonyms may not be used.	ETSI TS 102 280, RFC 3739, PKIo		

Field / Attribute	Criteria	Description	Standard reference	Type	Explanation
Subject.organizationName	V	The full name of the subscriber's organization in accordance with the accepted document or Basic Registry.	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) communicates or acts.
Subject.organizationIdentifier	V	The organizationIdentifier field contains an identification of the subject.	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).
Subject.organizationalUnitName	O	Optional specification of an organizational entity. This attribute MUST NOT include a function indication or similar.	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.
Subject.stateOrProvinceName	A	The use is advised against. If present, this field MUST contain the province in which the subscriber is established in accordance with an accepted document or Basic registry.	PKIo, RFC 3739	UTF8String	Name of the province MUST correspond with the address of the subscriber in accordance with the accepted document or registry.
Subject.localityName	A	The use is advised against. If present, this field MUST contain the location of the subscriber in accordance with an accepted document or Basic registry.	PKIo, RFC 3739	UTF8String	Name of the location MUST correspond with the address of the subscriber in accordance with the accepted document or registry.
Subject.postalAddress	A	The use is advised against. If present, 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.

Field / Attribute	Criteria	Description	Standard reference	Type	Explanation
Subject.serialNumber	O	The TSP is responsible for safeguarding the uniqueness of the subject (service). The Subject.serialNumber MUST be used to identify the subject uniquely. The use of 20 positions is only allowed for OIN and HRN after additional arrangements with Logius.	RFC 3739, X 520, PKIo	Printable String	The number is determined by the TSP and/or the government. The number can differ for each domain and can be used for several applications.
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	The attribute extension specifies the intended purpose of the key incorporated in the certificate. In the PKI for the government, for each certificate type various bits are incorporated in the keyUsage extension. In authenticity certificates the digitalSignature bit MUST be incorporated and marked as being essential. Another keyUsage MUST NOT be combined with this. In confidentiality certificates, keyEncipherment and dataEncipherment bits MUST be incorporated and marked as being essential. Another keyUsage MUST NOT be combined with this. In seal certificates the nonRepudiation bit MUST be incorporated and marked as being essential. Another keyUsage MUST NOT be combined with this.	RFC 3739, RFC 5280, ETSI TS 102 280	BitString	

Field / Attribute	Criteria	Critical?	Description	Standard reference	Type	Explanation
CertificatePolicies	V	No	MUST contain the OID of the certificate policy (CP), the URI of the certification practice statement (CPS), and a user notice. The applicable PKI for the government OID scheme is described in the CP. The TSP SHOULD use UTF8String in the userNotice, but MAY use IA5String.	RFC 3739	OID, String, UTF8String or IA5String	For services certificates in the Government/Companies domain the OIDs are: 2.16.528.1.1003.1.2.2.4 and 2.16.528.1.1003.1.2.2.5 For services certificates in the Organization domain the OIDs are: 2.16.528.1.1003.1.2.5.4 2.16.528.1.1003.1.2.5.5 2.16.528.1.1003.1.2.5.7. Reference to the paragraph numbers of the PoR/CP in the user notice is advised against because the persistency of this cannot be guaranteed (unlike the OID number of the CP).
SubjectAltName	O	No	MAY be used and given a worldwide unique number that identifies the service.	RFC 4043, RFC 5280, PKIo, ETSI 102 280		

SubjectAltName.otherName	O		MUST be used containing a unique identification number that identifies the certificate holder.
			
			An additional othername entry MAY be included in the authentication certificate for use with SSO (Single Sign On).
				PKIo	IA5String, Microsoft UPN, IBM Principal-Name or Permanent-Identifier	Includes an OID of the TSP awarded by the PA to the TSP and a number that is unique within the namespace of that OID that permanently identifies the subject, in one of the following ways:
						
						1. MS UPN: [number]@[OID]
						2. MS UPN: [OID].[number]
						3. IA5String: [OID]-[number]
						4. Permanent Identifier:
						        Identifiervalue = [number]
						        Assigner = [OID]
						
						Alternative 1. is also suitable for SSO. If a second othername for SSO is given in the certificate, the SSO othername MUST be given first in the SubjectAltName, before the PKIoverheid format othername described above, in order to ensure the proper

Field / Attribute	Criteria	Critical?	Description	Standard reference	Type	Explanation
						operation of the SSO mechanism. It is recommended that an existing registration number from back office systems is used, in combination with a code for the organization. In combination with the TSP OID, this identifier is internationally unique. This number MUST be persistent.
SubjectAltName.rfc822Name	A		MAY be used for the 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 PKIoverheid certificates, the use of e-mail addresses is advised against, because e-mail addresses of certificate holders often change and are susceptible to spam.
BasicConstraints	O	Yes	The "CA" field MUST be be omitted (default value is then "FALSE").	RFC 5280		A (Dutch language) browser can then be seen: Subjecttype = Eindentiteit", "Beperking voor padlengte = Geen ("Subjecttype = End Entity", "Path length constraint = None")
CRLDistributionPoints	V	No	MUST include the URI of a CRL distribution point.	RFC 5280, ETSI TS 102 280		The reference MUST be accessible through the http or LDAP protocol. The attribute Reason MUST NOT be used, reference MUST be made to 1 CRL for all types of reasons for revocation. In addition to CRL, other types of certificate status information service MAY be supported.
ExtKeyUsage	V	No		RFC 5280	KeyPurposeId's	See requirement 7.1-pkio150
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	O	No	This attribute MUST include the URI of an OCSP responder if Online Certificate Status Protocol (OCSP) plays a role.			This field can optionally be used to reference other additional information about the TSP.
SubjectInfoAccess	O	No		RFC 5280	OID, Generalname	This field can be used to reference additional information about the subject.
QcStatement	V/N	No	Certificates for the electronic seals MUST indicate that they are issued as qualified certificates complying with annex III of EU regulation 920/2014. This compliance is indicated by including the *id-etsi-qcs-QcCompliance* statement in this extension. Certificates for the electronic seals MUST indicate that they are issued as type of certificate complying with annex I of EU regulation 920/2014. This compliance is indicated by including the *id-etsi-qct-eseal* statement in this extension. Certificates for the electronic seals MUST 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. Certificates for the electronic signature MUST contain a reference to the location of	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-eseal { id-etsi-qcs-QcType 2 } 0.4.0.1862.1.6.2 • 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
			the PKI Disclosure Statement (PDS). This URL must present in the *id-etsi-qcs-QcPDS* statement in this extension.			
QcStatement-2	V	No	This extension munst contain an *id-etsi-qcs-SemanticsId-Legal* statement. This semantics identifier indicates that the organizationalIdentifier in the subject adheres to the prescribed layout.	ETSI EN 319 412-1	OID	Said QcStatement identifiers are the following OIDs: id-etsi-qcs-SemanticsId-Legal { id-etsi-qcs-semantics-identifiers 2 } 0.4.0.194121.1.2

10 Revisions

10.1 Amendments from version 4.6 to 4.7

10.1.1 New
- Requirement 7.1-pkio177 (effective date immediately after publication PoR 4.7)
- Requirement 3.2.3-pkio169 (effective date 4 weeks after publication of PoR 4.7)

10.1.2 Modifications
- Description of a number of certificate attributes replaced by reference to requirement 7.1-pkio174 (effective date 8 weeks after publication PoR 4.7)
- Reference to CWA 14 169 amended to EN 419 211 for QSCDs. This also sets requirements for the issue of QSCDs for requirements 6.1.1-pkio88, 6.1.1-pkio93, 6.1.1-pkio153, 6.2.11-pkio105, 6.4.1-pkio112 and 4.9.1-pkio52 (effective date immediately after publication PoR 4.7)
- Requirement 6.3.2-pkio148 expired and is replaced by requirement 6.3.2-pkio109 (effective date immediately after publication of PoR 4.7)

10.2 Amendments from version 4.5 to 4.6

10.2.1 Modifications
- Added subject.organizationIdentifier in the certificate profile to fix an ommission (effective date directly after publication of PoR 4.6)
- Modified reference to ETSI certificate profiles (effective date directly after publication of PoR 4.6)
- Corrected subjectAltName.othername field (effective date directly after publication of PoR 4.6)

10.3 Amendments from version 4.4 to 4.5

10.3.1 New
- Mandatory English CPS (requirement 2.2-pkio3, effective date 1-10-2017)
- Mandatory yearly renewal CPS (requirement 2.2-pkio156, effective date 1-1-2017)

10.3.2 Modifications
- Requirement 4.9.9-pkio67 now references RFC6960 instead of RFC2560 (effective date 31-12-2016)
- Allow/require EKU emailProtection in authenticity and non-repudiation certificates in requirement 7.1-pkio149 (effectrive date1-4-2017)
- Change in OID 2.16.528.1.1003.1.2.5.4 to also cover OCSP responder certificates (effective date 1-7-2017)
- Mandatory use of field "NextUpdate" in OCSP responses (requirement 4.9.9-pkio71, effective date 1-7-2017)

10.3.3 Editorial
- Removed typos from certificate profile.

10.4 Amendments from version 4.3 to 4.4

10.4.1 Modifications
- Removal of requirement 5.3.2-pkio79 (effective date 1-2-2017)

- 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)

10.4.2 Editorial
- Moved QCStatements from Public to Private Extensions
- Replaced CSP (Certificate Service Provider) with TSP (Trust Service Provider) in accordance with eIDAS directive.

10.5 Amendments from version 4.2 to 4.3

10.5.1 New
- Pkio153: additional requirements on the use of qualified seals (effective date 1-7-2016)
- New policyidentifier and profile modifications for the use of qualified seals (effective date 1-7-2016)
- Addition of Issuer.organizationalIdentifier in the certificate profile (effective date 1-7-2016)

10.5.2 Modifications
- Description with attribute CertificatePolicies (effective date 1-7-2016)
- Removal of optional use KeyAgreement with Key Usage (effective date no later than 4 weeks after publication of PoR 4.3)
- ETSI TS 102 176-1 replaced by ETSI TS 119 312 (effective date no later than 4 weeks after publication of PoR 4.3)
- Dropped requirement pkio95 because of i.v.m. duplicate requirement in ETSI EN 319 411-1
- Use of values in the BasicConstraints field no longer permitted in end entity certificates (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)
- Requirement 7.1-pkio150 modified (removed not permitted EKU) (effective date 1-11-2016).

10.5.3 Editorial
- Removed references to G1 (expired) and clarified reference to G3 (domains).

10.6 Amendments from version 4.1 to 4.2

10.6.1 New
- Requirement 6.3.2-pkio148 (effective date no later than 4 weeks after publication of PoR)
- Requirement 7.1-pkio150 (effective date 1 juli 2016)

10.6.2 Modifications
- Certificate profile: changed use of subjectAltName from "prohibited toegestaan" to "optional".
- Ban on issuance of 5 year services certificates to 3 year: removed requirements 6.3.2.-pkio109 and added 6.3.2-pkio148.

10.6.3   Editorial
- None

10.7   Amendments from version 4.0 to 4.1

10.7.1   New
- Certification against ETSI TS 102 042 (effective date no later than 4 weeks after publication of PoR 4.1);

10.7.2   Modifications
- Requirement 6.3.2-pkio109 (effective date no later than 4 weeks after publication of PoR 4.1);

10.7.3   Editorial
- Small editiorial change to the following requirements:
  - Requirement 5.7.4-pkio86.

10.8   Amendments from version 3.7 to 4.0

10.8.1   New
- None

10.8.2   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.

10.8.3   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.