Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Programme of Requirements part 3g: Certificate Policy Authenticity and Confidentiality certificates- Private Services domain

Datum	27 July 2015

Private Services (G1) Domain:

Services - Authenticity	2.16.528.1.1003.1.2.8.4
Services - Confidentiality	2.16.528.1.1003.1.2.8.5

Publisher's imprint

Version number	4.1
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 (CSPs) to the PKI for the government and preparing the administration;
- supervising and monitoring the activities of CSPs 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

1 Introduction to the Certificate Policy

1.1 Overview

This is part 3g 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 Certification Service Provider (CSP) within the PKI for the government. Within the PKI for the government , a distinction is made between various root certificates and underlying domains. This document only relates to the services certificates issued by CSPs in the Private Services domain.

Certificates which are issued under the private root certificate are not publicly trusted by browsers or other applications. The scope of these certificates is primarily a closed usergroup within which an agreement has been reached regarding the use of the PKIoverheid Private Root.

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 TS 102 042 standard where the policy NCP+ is applicable, so that a SUD is used (ETSI CP OID 0.4.0.2042.1.2);
- 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[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.

[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.*

This CP also includes a number of provisions that are not formulated as PKIo requirements. These provisions do not make any demands on the CSPs 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 status information certificate are listed in appendix A.

Based on chapters 1 to 9 inclusive, a reference matrix is included in appendix B. In accordance with the RFC 3647 structure, the matrix contains a reference to the applicable requirements within the PKI for the government. A distinction is made between the requirements originating from Dutch law, requirements from ETSI EN 319 411-3 and the PKIo requirements.

1.1.2 Status

This is version 4.1 of part 3g of the PoR. The current version has been updated up to and including July 2015.

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 multiple root certificates are in use for the regular – publicly trusted – root, the TRAIL root, the EV root and the private – not publicly trusted – root. Each of these root certificates contains a hierarchy consisting of differen domains. Each domain has its own specific domain structure.
Furthermore these root certificates often have multiple active generations or versions (g1, g2, g3). In addition the different PKI for the government structures or roots are based both on the SHA-1 algorithm (regular root G1) and the SHA-256 algorithm (regular root G2 and G3).

Each type of certificate within PKIoverheid is uniquely identified by an OID. The OIDs of the Certificate Policies of this part of the Programme of Requirements are in accordance with the following schedule.

Private Services Domain:	
OID	**CP**
2.16.528.1.1003.1.2.8.4	for the authenticity certificate for services within the Private Services domain, that contains the public key for identification and authentication.
2.16.528.1.1003.1.2.8.5	for the confidentiality certificate for services within the Private Services domain, that contains the public key for confidentiality.

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). private services domain (8). 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 Private Services domain, 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 natural or legal personality who enters into an agreement with a CSP 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:
    - a device or a system (a non-natural person), operated by or on behalf of an organizational entity; or
    - 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 2.16.528.1.1003.1.2.8.4]
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, which 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.

[OID 2.16.528.1.1003.1.2.8.5]
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.

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 CSP Information

RFC 3647	2.2 Publication of CSP information
Number	2.2-pkio8

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-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	3.2.5 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

RFC 3647	5.3.2 Background checks procedures
Number	5.3.2-pkio79

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 CSP 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	6.1.2 Pivate key and SUD delivery to the certificate holder
Number	6.1.2-pkio95

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

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 CSPs 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

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 CSPs
Number	9.6.1-pkio127

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

RFC 3647	9.6.1 CA Representations and Warranties by CSPs
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 Miscellaneous provisions

RFC 3647	9.17 Miscellaneous 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 authenticity and confidentiality certificates for the Private 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.
- N : Not allowed; indicates that the use of the attribute in the PKI for the government is not allowed.

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	This certificate MUST at least contain a 2048 bit RSA key.
Issuer	V	MUST contain a Distinguished Name (DN). The field contains the following attributes:	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 CSP 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 CSPs located in the Netherlands.

Field / Attribute	Criteria	Description	Standard reference	Type	Explanation
Issuer.stateOrProvinceName	N	Use is not allowed.	PKIo	UTF8String	-
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 entity. This field MUST NOT include a function indication or similar. It may include, if applicable, the types of certificates that are supported.	ETSI TS 102280	UTF8String	Several instances of this attribute MAY be used.
Issuer.localityName	N	Use is not allowed.	PKIo	UTF8String	-
Issuer.serialNumber	O	MUST be used in accordance with RFC 3739 if required for unambiguous naming	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 needed to identify the issuing government body (no part of the Distinguished Name, requirement from RFC 3739)

Field / Attribute	Criteria	Description	Standard reference	Type	Explanation
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 CSP 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 service, device or system is known. This MAY be a local domain name or host name.

Field / Attribute	Criteria	Description	Standard reference	Type	Explanation
Subject.Surname	N	Is not used for services certificates.			Services certificates are not personal. The use of this attribute is therefore not allowed, to avoid confusion.
Subject.givenName	N	Is not used for services certificates.			Services certificates are not personal. The use of this attribute is therefore not allowed, to avoid confusion.
Subject.pseudonym	N	Pseudonyms may not be used.	ETSI TS 102 280, RFC 3739, PKIo		
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 CSP has entered into an agreement and on behalf of which the certificate holder (service/server) communicates or acts.
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	PKIo, RFC 3739	UTF8String	Name of the province MUST correspond with the address of the subscriber in accordance with the accepted document or registry.

Field / Attribute	Criteria	Description	Standard reference	Type	Explanation
		accordance with an accepted document or Basic 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.
Subject.emailAddress	N	Use is not allowed.	RFC 5280	IA5String	This field MUST NOT be used in new certificates.
Subject.serialNumber	O	The CSP 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	RFC 3739, X 520, PKIo	Printable String	The number is determined by the CSP and/or the government. The number can differ for each domain and can be used for several applications.

Field / Attribute	Criteria	Description	Standard reference	Type	Explanation
		Logius.			
Subject.title	N	The use of the title attribute is not allowed for services certificates.	ETSI TS 102 280, RFC 3739, RFC 5280		This attribute is only used in personal certificates and therefore not in services certificates.
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.
IssuerUniqueIdentifier	N	Is not used.	RFC 5280		The use of this is not allowed (RFC 5280)
subjectUniqueIdentifier	N	Is not used.	RFC 5280		The use of this is not allowed (RFC 5280)

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 CSP/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.	RFC 3739, RFC 5280, ETSI TS 102 280	BitString	

Field / Attribute	Criteria	Critical?	Description	Standard reference	Type	Explanation
			In confidentiality certificates, keyEncipherment and dataEncipherment bits MUST be incorporated and marked as being essential. Optionally, this MAY be combined with the keyAgreement bit. Another keyUsage MUST NOT be combined with this.			
privateKeyUsagePeriod	N		Is not used.	RFC 5280		
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.	RFC 3739	OID, String, String	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).
PolicyMappings	N		Is not used.			This extension is not used in end user certificates

Field / Attribute	**Criteria**	**Critical?**	**Description**	**Standard reference**	**Type**	**Explanation**
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 dnsName for server certificates or the othername attribute for services certificates. Attributes other than those mentioned below MUST NOT be used.
SubjectAltName.dNSName[3]	V/N		Name that identifies the server. In services authentication and confidentiality certificates this field MUST NOT be used.	RFC2818, RFC5280	IA5String	The subscriber MUST prove that the organization is eliable to use the FQDN
SubjectAltName.iPAddress	N	No	The public IP address that identifies the service. MUST NOT be used in services certificates	RFC 5280, RFC 791, RFC 2460	Octet string	
SubjectAltName.otherName	O		MAY be used containing a unique identification number that identifies the certificate holder.	PKIo	IA5String, Microsoft UPN, IBM Principal-	Includes the OID of the CSP and a number that always uniquely identifies the subject (service), separated by a point or hyphen ('-'). It is recommended that an existing registration number from

[3] This field/attribute has to be included in certificates that are issued as from 1-7-2011.

Field / Attribute	Criteria	Critical?	Description	Standard reference	Type	Explanation
			In addition, in the authentication certificate, as othername a PrincipalName (UPN) MAY be included for use with SSO (Single Sign On).		Name or Permanent-Identifier	back office systems is used, along with a code for the organization. In combination with the CSP's OID number, this identifier is unique throughout the world. This number MUST be persistent. If an othername for Single Sign On is also included in the certificate, the SSO othername MUST be the first in the SubjectAltName, before the PKIoverheid format othername described above, in order to guarantee effective functioning of the SSO mechanism.
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.
IssuerAltName	N		Is not used.	RFC 5280		
subjectDirectoryAttributes	N		Is not used.	RFC 5280; RFC 3739		This use of this extension is not allowed.
BasicConstraints	O	Yes	The "CA" field MUST be set at "FALSE", or	RFC 5280		A (Dutch language) browser can then be seen:

Field / Attribute	**Criteria**	**Critical?**	**Description**	**Standard reference**	**Type**	**Explanation**
			be omitted (default value is then "FALSE").			Subjecttype = Eindentiteit", "Beperking voor padlengte = Geen ("Subjecttype = End Entity", "Path length constraint = None")
NameConstraints	N		Is not used.	RFC 5280		Is not used in end user certificates.
PolicyConstraints	N		Is not used.	RFC 5280		Is not used in end user certificates.
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.

Field / Attribute	Criteria	Critical?	Description	Standard reference	Type	Explanation
ExtKeyUsage	O	No	Is only used if needed for the specific service.	RFC 5280	KeyPurposeId's	Service certificates MAY use ExtendedKeyUsage, in which case the KeyPurposeId id-kp-serverAuth MUST NOT be included, that the KeyPurposeId id-kp-codeSigning MUST NOT be included, that the KeyPurposeId AnyextendedKeyusage MUST NOT be included, that every KeyPurposeId that is only intended for identification of a service based on its FDQN MUST NOT be included but the following MAY be included: every other KeyPurposeId defined in an open or accepted standard that corresponds with the key use shown in the KeyUsage extension.
InhibitAnyPolicy	N		Is not used.	RFC 5280		Is not used in end user certificates.
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 CSP 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 CSP.
SubjectInfoAccess	O	No		RFC 5280	OID, Generalname	This field can be used to reference additional information about the subject.
BiometricInfo	N		Are not used in services certificates.	PKIo		Biometric information is not advisable in non-personal certificates, such as services certificates.
QcStatement	N	No		RFC 3739, ETSI TS 102 280, ETSI TS 101 862	OID	This attribute is only used in personal certificates and is not allowed in services certificates.

10 Revisions

10.1 Amendments from version 4.0 to 4.1

10.1.1 New

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

10.1.2 Modifications

Not applicable

10.1.3 Editorial

- Small editorial modification to the following requirement:
    - Requirement 5.7.4-pkio86.