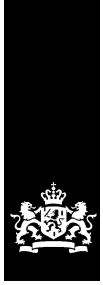

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Programme of Requirements part 3e: Certificate Policy Server certificates – Organization Services Domain (G3)

Appendix to CP Government/Companies (G1) and Organization (G2) domains

Datum 27 July 2015

Government/Companies Domain (G1):
Services - Server 2.16.528.1.1003.1.2.2.6

Organization (G2) / Organization Services (g3) Domains:
Services - Server 2.16.528.1.1003.1.2.5.6

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**
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

1 Introduction to the Certificate Policy

1.1 Overview

This is part 3e 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 domains. This document only relates to the server certificates issued by CSPs 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 TS 102 042 standard
    - where policy NCP in combination with OVCP, PTC-BR and Netsec are applicable for server certificates (extendedKeyUsage client and server authentication). Netsec requirements 1h, 3a, 3e, 4c.i and 4f are not normative (ETSI CP OID 0.4.0.2042.1.7).;
- 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 actualPKIoverheid 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

[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.*

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 TS 102 042 and the PKIo requirements.

1.1.2 Status

This is version 4.1 of part 3e 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 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 a 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.

Government/Companies Domain:	
OID	**CP**
2.16.528.1.1003.1.2.2.6	for the server certificate within the Government/Companies domain, that contains the public key for authenticity and 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). government and companies domains (2). server (6). version number}.

Organization Domain:	
OID	**CP**
2.16.528.1.1003.1.2.5.6	for the server certificate for services within the Organization domain, that contains the public key for authenticity and 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). organization domain (5). server (6). 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 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 person 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 2.16.528.1.1003.1.2.2.6 and 2.16.528.1.1003.1.2.5.6]
Server certificates that are issued under this CP, can be used to secure a connection between a specific client and a server that is part of the organizational entity 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 CSP Information

Contains no additional requirements.

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

RFC 3647	3.2.5 Authorization of the certificate holder
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

Contains no additional requirements.

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

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

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 CSP sub CA
Number	6.1.1-pkio89

RFC 3647	6.1.1 Key pair generation for the certificate holders
Number	6.1.1-pkio91

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

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	6.2.11 Cryptographic module rating
Number	6.2.11-pkio125

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-pkio107

6.3 Other Aspects of Key Pair Management

Contains no additional requirements.

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

Contains no additional requirements.

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-pkio128

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	9.8pkio133

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 of server certificates for the Government/Companies, Organization and Organisation Services domains

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'.

Server certificates

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 under the G1 root certificate, only sha-1WithRSAEncryption is allowed. As from 01-01-2011 the CSP MAY only issue certificates based on sha-1WithRSAEncryption under the G1 root certificate in very exceptional situations. This certificate MUST contain a 2048 bit RSA key. This certificate MAY only be valid until no later than 31-12-2011. For certificates under the G2 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. The attributes that are used MUST be the same as the corresponding

Field / Attribute	Criteria	Description	Standard reference	Type	Explanation
					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.
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	

Field / Attribute	Criteria	Description	Standard reference	Type	Explanation
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)
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.

Field / Attribute	Criteria	Description	Standard reference	Type	Explanation
Subject.commonName	A	Name that identifies the server. In server certificates the use of this field is advised against. If this field is used, this MUST contain no more than 1 "fully-qualified domain name (FQDN)" (see the definition in part 4). This FQDN MUST also be included in the SubjectAltName.dNSName field.	RFC 3739, ETSI TS 102 280, PKIo	UTF8String	If the subject.commonname is used for server certificates, a FQDN has to be incorporated here. In this attribute wildcard FQDNs, local domain names, private IP addresses, only a host name, internationalized domain names (IDNs) and null characters \0 MUST NOT be used. The subscriber MUST prove that the organization can use this name. In server certificates the CSP MUST check recognized registers (Stichting Internet Domeinregistratie Nederland (SIDN) or Internet Assigned Numbers Authority (IANA)) to find out whether the subscriber is the domain name owner or whether the subscriber is exclusively authorized by the registered domain name owner to use the domain name on behalf of the registered domain name owner. In exceptional situations, the CSP MAY issue another server certificate without FQDN. The following additional requirements apply: with effect from 1 July 2012, the CSP MUST inform the subscriber that the use of server certificates without FQDN is advised against and that by no later than 1 October 2016, all server certificates that are still valid without

Field / Attribute	Criteria	Description	Standard reference	Type	Explanation
					FQDN will be revoked. If a CSP issues a server certificate on or after 1 July 2012 without FQDN, 1 November 2015 at the latest MUST be used as "date of validity up to". The CSP MUST keep records of the issuance of a server certificate without FQDN and hands these records over to the PA on a monthly basis. The non-FQDN MUST not contain a new generic Top Level Domain (gTLD's) which have been taken under consideration by ICANN (https://gtldresult.icann.org/application-result/applicationstatus/viewstatus). Upon approval of a new gTLD the CSP will revoke within 120 days all certificates that contain a non-FQDN where the gTLD is a part of, unless the Subscriber is the owner of the domain name of has been exclusively authorised by the owner to use the domain name. Approval of new gTLD is published on the ICANN mailing list on https://mm.icann.org/mailman/listinfo/gtldnotification.
Subject.Surname	N	Is not used for server certificates.			Server certificates are not personal. The use of this attribute is therefore not allowed, to avoid confusion.

Field / Attribute	Criteria	Description	Standard reference	Type	Explanation
Subject.givenName	N	Is not used for server certificates.			Server 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 (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	MUST include the province of the subscriber's branch, in accordance with the 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	V/A	MUST include the location of the	PKIo, RFC 3739	UTF8String	Name of the location MUST correspond with the address of the subscriber

Field / Attribute	Criteria	Description	Standard reference	Type	Explanation
		subscriber, in accordance with the accepted document or Basic registry.			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 Logius.	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.
Subject.title	N	The use of the title attribute is not allowed for server certificates.	ETSI TS 102 280, RFC 3739,		This attribute is only used in personal certificates and therefore not in services certificates.

Field / Attribute	Criteria	Description	Standard reference	Type	Explanation
			RFC 5280		
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 server certificates the digitalSignature, keyEncipherment and keyAgreement bits 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
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	For server certificates in the Government/Companies domain the OID is: 2.16.528.1.1003.1.2.2.6. For server certificates in the Organization and Organization Services domains the OID is: 2.16.528.1.1003.1.2.5.6 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
SubjectAltName	V	No	MUST be used and given a worldwide unique number that identifies the server.	RFC 4043, RFC 5280, PKIo, ETSI 102 280		MUST include a unique identifier in the dnsName attribute for server certificates. Attributes other than those mentioned below MUST NOT be used.

Field / Attribute	Criteria	Critical?	Description	Standard reference	Type	Explanation
SubjectAltName.dNSName[3]	V		Name that identifies the server. In server certificates this field MUST include at least 1 "fully-qualified domain name (FQDN)" (see the definition in part 4). A server certificate MAY contain multiple FQDNs of multiple domains on the condition that these domains are registered to the name of the same subscriber or an authorization of the subscriber is present. It therefore is NOT permitted to combine multiple FQDNs in one certificate that are both from multiple domains and are registered to the name of multiple owners.	RFC2818, RFC5280	IA5String	The subscriber MUST prove that the organization can use this name. For server certificates additional wildcard FQDNs, local domain names, private IP addresses, only a host name, internationalized domain names (IDNs) and null characters \0 MUST NOT be used. In server certificates the CSP MUST check recognized registers (Stichting Internet Domeinregistratie Nederland (SIDN) or Internet Assigned Numbers Authority (IANA)) to find out whether the subscriber is the domain name owner or whether the subscriber is exclusively authorized by the registered domain name owner to use the domain name on behalf of the registered domain name owner. In exceptional situations, the CSP MAY issue another server certificate without FQDN. The following additional requirements apply: with effect from 1 July 2012, the CSP MUST inform the subscriber that the use of server certificates without FQDN is advised against and that by no later than 1 October 2016, all

[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
						server certificates that are still valid without FQDN will be revoked. If a CSP issues a server certificate on or after 1 July 2012 without FQDN, 1 November 2015 at the latest MUST be used as "date of validity up to". The CSP MUST keep records of the issuance of a server certificate without FQDN and hands these records over to the PA on a monthly basis. The non-FQDN MUST not contain a new generic Top Level Domain (gTLD's) which have been taken under consideration by ICANN (https://gtldresult.icann.org/application-result/applicationstatus/viewstatus). Upon approval of a new gTLD the CSP will revoke within 120 days all certificates that contain a non-FQDN where the gTLD is a part of, unless the Subscriber is the owner of the domain name of has been exclusively authorised by the owner to use the domain name. Approval of new gTLD is published on the ICANN mailing list on https://mm.icann.org/mailman/listinfo/gtldnotification.
SubjectAltName.iPAddress	A	No	MAY include the public IP address of the	RFC 5280, RFC	Octet string	The CSP MUST verify that the subscriber is the owner of the public

Field / Attribute	Criteria	Critical?	Description	Standard reference	Type	Explanation
			server of which the subscriber is the owner or that is hosted by a supplier at the instruction of the subscriber.	791, RFC 2460		IP address or that a supplier may use the public IP address at the instruction of the subscriber. Private IP addresses MUST NOT be included in this attribute.
SubjectAltName.otherName	N			PKIo		This attribute MUST NOT be used as a result of the Baseline Requirements by the CA/B Forum.
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 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")

Field / Attribute	Criteria	Critical?	Description	Standard reference	Type	Explanation
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.
ExtKeyUsage	V	Yes / No	Extension that indicates for which applications the certificate may be used.	RFC 5280	KeyPurposeId's	In server certificates this extension MUST be included, this extension MUST NOT be labelled “critical”, this extension MUST include the KeyPurposIds id-kp-serverAuth and id-kp-clientAuth, additionally the KeyPurposeId id-kp-emailProtection MAY be included, MAY additionally also include every other KeyPurposeId defined in an open or accepted standard that is used to identify a service based on its FQDN and other KeyPurposeIds MUST NOT be included.

Field / Attribute	Criteria	Critical?	Description	Standard reference	Type	Explanation
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	V	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 server certificates.

10 Revisions

10.1 Amendments from version 4.0 to 4.1

10.1.1 New

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

10.1.2 Modifications

- None

10.1.3 Editorial

None

10.2 Amendments from version 3.7 to 4.0

10.2.1 New

- None

10.2.2 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.

10.2.3 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.