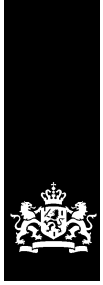

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Programme of Requirements part 3i: Certificate Policy - Private Persons Domain.

Datum 27 July 2015

Private Persons Domain (G1)

Authenticity	2.16.528.1.1003.1.2.8.1
Non repudiation	2.16.528.1.1003.1.2.8.2
Confidentiality	2.16.528.1.1003.1.2.8.3

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 3i of the Programme of Requirements (PoR) of the PKI for the government and is called 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 personal certificates issued by CSPs in the Private Persons 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 EN 319 411-2 standard, QCP public + SSCD (ETSI CP OID 0.4.0.1456.1.1) for non-repudiation certificates;
- that ensue from the latest version of the ETSI TS 102 042 standard, where policy NCP+ is applicable to authenticity and encryption certificates.;
- 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

[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 PKIo requirement applies.*

	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 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 end user certificates and certificate status information 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, a reference to the applicable requirements within the PKI for the government is included in the matrix. A distinction is made between requirements originating from Dutch law, requirements from ETSI EN 319 411-2 and the PKIo requirements.

1.1.2 Status

This is version 4.1 of part 3 of the Programme of Requirements. 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 Persons domain:	
OID	**CP**
2.16.528.1.1003.1.2.8.1	for the authenticity certificate within the Private Persons domain, that contains the public key for identification and authentication
2.16.528.1.1003.1.2.8.2	for the signature certificate within the Private Personsdomain, that

	contains the public key for the qualified electronic signature/irrefutability
2.16.528.1.1003.1.2.8.3	for the confidentiality certificate within the Private Personsdomain, 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 persons domain (8). authenticity (1)/non repudiation (2)/confidentiality (3). 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 Persons domain, the user community consists of subscribers who are organizational entities within the government and business community (see PKIo 3.2.2-pkio14) and of certificate holders, who also belong to these subscribers. There are also individuals working in a recognized profession who are both subscriber and certificate holder. 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 holders. certificate managers 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 subscriber can also be a certificate holder.
- 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 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 either a part of an organizational entity for which a subscriber is the contracting party (organization-linked certificate holder), or the practitioner of a recognized occupation and, in that capacity, is a subscriber and therefore the contracting party (profession-linked certificate holder).
- 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.

1.4 Certificate Usage

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

[OID 2.16.528.1.1003.1.2.8.1]
Authenticity certificates, which are issued under this CP, can be used to reliably identify and authenticate persons, organizations and resources electronically. This concerns both the mutual identification of people and identification between people and computerized devices.

[OID 2.16.528.1.1003.1.2.8.2]
Signature certificates, which are issued under this CP, can be used to verify electronic signatures, that have "the same legal consequences as a handwritten signature", as stated in article 15a, first and second paragraphs, in Title 1 of Book 3 of the Dutch Civil Code (Burgerlijk Wetboek) under section 1A and are qualified certificates as referred to in article 1.1, paragraph ss of the Telecommunications Act (Telecomwet).

[OID 2.16.528.1.1003.1.2.8.3]
Confidentiality certificates, which are issued under this CP, can be used to protect the confidentiality of data that is exchanged and/or stored in an electronic form. This concerns both the mutual exchange between people and exchange between people and computerized devices.

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

RFC 3647	3.1.3 Anonymity or pseudonimity of certificate holders
Number	3.1.3-pkio11

3.2 Initial Identity Validation

RFC 3647	3.2.2 Authentication of organizational entity
Number	3.2.2-pkio14

RFC 3647	3.2.2 Authentication of organizational entity
Number	3.2.2-pkio16

RFC 3647	3.2.3 Authentication of individual identity
Number	3.2.3-pkio21

RFC 3647	3.2.5 Validation of authority
Number	3.2.5-pkio29

RFC 3647	3.2.5 Validation of authority
Number	3.2.5-pkio32

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 Certificate Revocation and Suspension

RFC 3647	4.9.1 Circumstances for revocation
Number	4.9.1-pkio52

RFC 3647	4.9.3 Procedure 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	4.9.9-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-pkio68

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 check procedures
Number	5.3.2-pkio79

5.4 Audit Logging 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 records archived
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	6.1.2 Private key and SSCD delivery to certificate holder
Number	6.1.2-pkio94

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	6.2.3 Private key escrow of certificate holder key
Number	6.2.3-pkio101

RFC 3647	6.2.11 Cryptographic module rating
Number	6.2.1-pkio104

RFC 3647	6.2.11 Cryptographic module rating
Number	6.2.1-pkio105

RFC 3647	6.2.11 Cryptographic module rating
Number	6.2.1-pkio106

6.3 Other Aspects of Key Pair Management

RFC 3647	6.3.1 Public key archival
Number	6.3.2-pkio108

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-pkio131

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 Provisions

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-pkio139

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 profiles

Profile of the personal certificates for the Private Persons 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.

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

Naming convention Subject.commonName
The following requirements apply to the CommonName of the Subject field. The main principle is that the CSP is responsible for correct entry of the CommonName. For a correct implementation this entails that the CSP has to be able to check each part that is entered. The CommonName has the following format[3]:

[aristocratic designation] **[Full first forename]** [*initials other forenames OR full other forenames*] [surname prefixes + surname partner '-'] [aristocratic title] **[surname prefixes + surname at birth]**

whereby:
text in bold = compulsory part, style in accordance with Compulsory Identification Act document or presented Local Council Personal Records Database extract
Italic = compulsory part, choice from two options (full forenames or initials)
normal = optional part; if present, the style has to be the same as the Compulsory Identification Act document or the presented Local Council Personal Records Database extract

In principle, the CSP decides whether or not optional parts are allowed. If it prefers, the CSP can leave the choice for an option to the subscriber or the party requesting the certificate. If the CommonName becomes too long for the number of characters that are allowed, optional parts have to be omitted (starting with the replacement of other forenames by initials from the last to the first position) until the name fits in the maximum field length.

[3] *The presented order is not compulsory, the surname can also be given first followed by forenames/initials.*

Personal certificates – Private Persons Domain

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 set 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 only sha-1WithRSAEncryption is allowed for certificates under the G1 root certificate. 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 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	ETSI TS 102280	UTF8String	

Field / Attribute	Criteria	Description	Standard reference	Type	Explanation
		document or basic registry			
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: 5.2.4	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, optionally including the Domain indication and/or the types of certificates that are supported	PKIo, RFC 3739	UTF8String	The commonName attribute MUST NOT be necessary in order 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 (end user) MUST mention the subject in a unique manner and include information about the subscriber. 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	RFC 3739, X520, ISO 3166, PKIo	Printable String	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
		the user-assigned code XX.			
Subject.commonName	V	The commonName attribute MUST be entered in accordance with the paragraph *Naming convention Subject.commonName* above.	RFC 3739, ETSI TS 102 280, PKIo	UTF8String	See the naming convention of Subject.commonName.
Subject.Surname	A	A correct reproduction of the element of the name laid down in the CN. Based on the Compulsory Identification Act document.	RFC 3739	UTF8String	The use of this field is advised against. If this field is used, it MUST show the subject's surname including surname prefixes correctly. The surname MUST NOT be in conflict with the information in the commonname
Subject.givenName	A	A correct reproduction of the element of the name laid down in the CN. Based on the Compulsory Identification Act document.	RFC 3739	UTF8String	The use of this field is advised against. If this field is used, it MUST show the subject's forename(s) correctly. The givenName MUST NOT be in conflict with the information in the commonname
Subject.pseudonym	N	Pseudonyms may not be used.	ETSI TS 102 280, RFC 3739, PKIo		
Subject.organizationName	V	Full name of the subscriber in accordance with the accepted document or Basic Registry	PKIo	UTF8String	The subscriber is the entity with which the CSP has entered into an agreement and on behalf of which or pursuant to which the certificate holder acts when using the certificate.
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 in organization-linked certificate holders. The field MUST contain a valid name of an organizational entity of the subscriber in accordance with an accepted document or registry In occupational-linked certificate holders, this attribute MUST NOT be incorporated.

Field / Attribute	Criteria	Description	Standard reference	Type	Explanation
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.
Subject.emailAddress	N	Use is not allowed.	RFC 5280	IA5String	This field MUST NOT be used in new certificates.
Subject.serialNumber	V	Number to be determined by the CSP. The combination of CommonName, OrganizationName and Serialnumber MUST be unique within the context of the CSP.	RFC 3739, X 520, PKIo	Printable String	The serialnumber is intended to distinguish between subjects with the same commonName and the same OrganizationName. To avoid susceptibilities a serial Number attribute MUST be allocated to every subject.
Subject.title	O	Includes the position/function/profession/professional group of a subject.	ETSI TS 102 280, RFC 3739, RFC 5280		This attribute preferably gives static, verifiable professional titles (doctor, pharmacist, etc.), NOT the term of address (Mr, Mrs, etc.).
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)

Field / Attribute	Criteria	Description	Standard reference	Type	Explanation
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 critical. Another keyUsage MUST NOT be combined with this. In confidentiality certificates, keyEncipherment and dataEncipherment bits MUST be incorporated and marked as critical. Optionally, this MAY be combined with the keyAgreement bit. Another keyUsage MUST NOT be combined with this. In certificates for the electronic signature the non-repudiation bit MUST be	RFC 3739, RFC 5280, ETSI TS 102 280	BitString	

Field / Attribute	Criteria	Critical?	Description	Standard reference	Type	Explanation
			incorporated and marked as critical. 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	For the Private Persons domain, the OIDs are: 2.16.528.1.1003.1.2.8.1, 2.16.528.1.1003.1.2.8.2 and 2.16.528.1.1003.1.2.8.3. 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). If this concerns a profession-linked certificate, it is preferable to make a note of the fact in the user notice that the certificate holder is acting in the capacity of his/her profession.
PolicyMappings	N		Is not used.			This extension is not used in end user certificates
SubjectAltName	V	No	MUST be used and given a personal worldwide unique identification number.	RFC 4043, RFC 5280, PKIo, ETSI 102 280		MUST include a unique identifier in the othername attribute. Attributes other than those mentioned below MUST NOT be used.
SubjectAltName.otherName	V		MUST be used containing a unique identification number that identifies the certificate holder. In addition, in the authentication certificate,	PKIo	IA5String, Microsoft UPN, IBM Principal-Name, Kerberos PrincipalName or	Includes an *OID* of the CSP awarded by PKIoverheid to the CSP 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*]

Field / Attribute	Criteria	Critical?	Description	Standard reference	Type	Explanation
			an 'othername' MAY be included for use with Single Sign On (SSO).		Permanent-Identifier	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 operation of the SSO mechanism. It is recommended that an existing registration number from back office systems is used, such as a staff number in combination with a code for the organization. In combination with the CSP OID, this identifier is internationally unique. This number MUST be persistent.
SubjectAltName.rfc822Name	A		MAY be used for the certificate holder's e-mail address, for applications that need the e-mail address to be able to function properly.	RFC 5280	IA5String	For PKIoverheid certificates in the Government/Companies and Organization domains, the use of e-mail addresses is advised again, because e-mail addresses of certificate holders often change and furthermore are privacy sensitive (spam). If the e-mail address is included in the certificate, the CSP MUST: • have the subscriber sign his/her approval for these and; • check that the e-mail address belongs to the subscriber's domain, or; • check that the e-mail address belongs to the subscriber (e.g. the professional) and that this person has access to the e-mail address (for example by performing a challenge response).
IssuerAltName	N		Is not used.	RFC 5280		

Field / Attribute	Criteria	Critical?	Description	Standard reference	Type	Explanation
subjectDirectoryAttributes	O	No		RFC 5280; RFC 3739		The use of this extension is allowed. These attributes MAY NOT contain personal data that can impair the subject's privacy.
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" ("Subject type = 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.
ExtKeyUsage	O / N	No	ExtKeyUsage MUST NOT be used in certificates for the electronic signature. In other certificates, the use of ExtKeyUsage is allowed to support certain applications.	RFC 5280	KeyPurposeId's	If used, the following conditions all apply. An ExtKeyUsage: • MUST NOT be incorporated in certificates for the electronic signature [OID 2.16.528.1.1003.1.2.2.2 and 2.16.528.1.1003.1.2.5.2]; • MAY be incorporated in every other certificate; • MUST NOT be listed as critical; • MUST include at least one (1) KeyPurposeId. Each KeyPurpose Id incorporated in an ExtKeyUsage: • MUST NOT conflict with the KeyUsage extension; • MUST be appropriate for the type of certificate holder; • MUST be defined in an internationally recognized standard, such as an RFC.

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	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, provided that the information that is offered does not infringe the privacy of the subject.
BiometricInfo	O	No	Contains the hash of a biometric template and optionally a URI that references a file with the biometric template itself.	RFC 3739		
QcStatement	V/N	No	Certificates for the electronic signature MUST indicate that they are issued as qualified certificates complying with annex I and annex II of the European Directive This compliance is indicated by including the *id-etsi-qcs-QcCompliance* statement in this extension. Certificates for the electronic signature MAY indicate that the private key that is part of the public key in the certificate is saved on a secure signature creation device (SSCD) complying with annex III of the European Directive. This compliance is indicated by including the *id-etsi-qcs-QcSSCD* statement in this extension. The certificates for authenticity and the certificates for confidentiality MUST NOT use this extension.	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-qcs-QcSSCD { id-etsi-qcs 4 } 0.4.0.1862.1.4

10 Revisions

10.1 Amendments between version 4.0 and 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 editiorial changes to the following requirements:
  - 3.1.3-pkio11;
  - 3.2.5-pkio32;
  - 5.7.4-pkio86;
  - 9.6.1-pkio131.