Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Programme of Requirements part 3d: Certificate Policy – Autonomous Devices domain

Datum 1 February 2017

Autonomous Devices Domain:	
Autonomous Devices - Authenticity	2.16.528.1.1003.1.2.6.1
Autonomous Devices – Confidentiality	2.16.528.1.1003.1.2.6.2
Autonomous Devices - Combination	2.16.528.1.1003.1.2.6.3

Publisher's imprint

Version number 4.4
Contact person Policy Authority of PKIoverheid

Organization Logius

Street address
Wilhelmina van Pruisenweg 52

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

T 0900 - 555 4555
servicecentrum@logius.nl

Contents

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

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

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

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

Revision control

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

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

1 Introduction to the Certificate Policy

1.1 Overview

This is part 3d of the Programme of Requirements (PoR) for the PKI for the government and is known as the Certificate Policy (CP). Set out in the PoR are the standards for the PKI for the government. This section relates to the requirements laid down for the services of a Trust Service Provider (TSP) within the PKI for the government. Within the PKI for the government , a distinction is made between various domains. This document only relates to the device-linked certificates issued by TSPs in the Autonomous Devices domain.

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

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

1.1.1 Design of the Certificate Policy

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

- that ensue from the Dutch legal framework in relation to the electronic signature;
- that ensue from the latest version of the ETSI EN 319 411-1 standard where policy NCP+ is applicable, so that a SUD is used (ETSI CP OID 0.4.0.2042.1.2)[2];
- that are specifically drawn up by and for the PKIoverheid.

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

RFC 3647	Reference to the paragraph from the RFC 3647 structure to which the PKIo requirement relates. RFC 3647 is a PKIX framework of the Internet Engineering Task Force (IETF) and is the de facto standard for the structure of Certificate Policies and Certification Practice Statements[3].
Number	Unique number of the PKIo requirement. In each paragraph, consecutive numbering is used for the PKIo requirements. In combination with the RFC 3647 paragraph number, this forms a unique label for the PKIo requirement.

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

[2] The CP Autonomous Devices is based on an underlying standard different to that of the CPs for ersonal certificates. Because device-linked certificates are not personal and are not qualified certificates in accordance to the "Wet Elektronische Handtekeningen" (Electronic Signature Act), the requirements for device-linked certificates differ on certain points from the requirements for other types of certificates. For certificates with an ExtkeyUsage client authentication and server authentication the policies NCP in combination with OVCP, PTC and Netsec are applicable. This is due to the fact that these certificates are deemed to be SSL certificates according to the CABforum. The Netsec requirements 1h, 3a, 3e 4c.i and 4f are not normative (ETSI CP OID 0.4.0.2042.1.7).

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

This CP also includes a number of provisions that are not formulated as PKIo requirements. These provisions do not make any demands on the TSPs within the PKI for the government, but do apply as a policy to the PKI for the government. This concerns provisions from paragraphs 1.1, 1.1.1, 1.1.2, 1.2, 1.3, 1.4, 1.5, 8, 9.12.1, 9.12.2, 9.14 and 9.17.

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

1.1.2 Status

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

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

1.2 References to this CP

Within the PKI for the government different structures or roots are used based on the SHA-256 algorithm (G2 and G3). Furthermore these structures are devided into different domains.
The G2 root is devided into an Organization, a Citizen and an Autonomous Devices domain.
Under the G3 root there are domains for Organization Person, Organization Services, Citizen, and Autonomous Devices.

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

Autonomous Devices Domain:	
OID	**CP**
2.16.528.1.1003.1.2.6.1	for the authenticity certificate for services within the Autonomous Devices domain, that contains the public key for identification and authentication.
2.16.528.1.1003.1.2.6.2	for the confidentiality certificate for services within the Autonomous Devicesdomain, that contains the public key for confidentiality.
2.16.528.1.1003.1.2.6.3	for the combination certificate for devices within the Autonomous Devices 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). autonomous devices domain (6). authenticity (1)/ confidentiality (2)/ combination (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 Autonomous Devices domain, the certificate holders are devices that, in their operational stage of life, independently safeguard the integrity and authenticity of (measurement) data for (a specific purpose within a core task of) a specific government agency. The relevant government agency publishes a framework of standards for the devices to be manufactured for the specified purpose and is therefore seen as the "party responsible for establishing the framework".

Based on the framework of standards, the party responsible for establishing the framework issues a conformity certificate to every manufacturer that, for every type of device that is to be produced by the manufacturer, conforms to the framework of standards (the party responsible for establishing the framework can appoint a regulator responsible for conducting conformity assessments and issuing conformity certificates). This enables (prospective) device manufacturers to market devices that conform to the framework of standards.
Before a device (that conforms with the framework of standards) is ready for operation, a certificate has to be assigned (linked) to that device from the Autonomous Devices domain. During the operational life of an autonomous device, the devices certificate can be replaced or revoked. The party responsible for establishing the framework has to authorize one or more organizations to perform these tasks. The aforementioned organization is considered in this CP to be a Subscriber.

A Subscriber can nominate one or more certificate managers for performing (on behalf of the Subscriber) one or more activities relating to certificates in the Autonomous Devices domain. There are two types of certificate managers:

- Natural personalities directly related to the Subscriber organization;
- Natural personalities related to one or more legal personalities who have an agreement with the Subscriber organization.

Taking into account the aforementioned, in the Autonomous Devices domain the user community consists of parties responsible for establishing frameworks, manufacturers, subscribers, certificate managers, certificate holders (the devices themselves) and relying parties (including the parties responsible for establishing the frameworks).

- A *Party responsible for establishing a framework* is a government agency that:
    - for a specific core task has a need for (measurement) data that originates from outside its immediate sphere of influence;
    - to safeguard the integrity and authenticity of that (measurement) data, wishes to use specific devices that operate autonomously;
    - to safeguard the trustworthiness of specimens of that type of device:

  - draws up a framework of standards for the production, activation, operation, maintenance, collection and use and formulates this in legislation and regulations;
  - based on that framework of standards, authorizes organizations to:
    - produce and distribute devices of a particular type;
    - link certificates to particular devices;
    - replace certificates on particular devices;
    - revoke certificates of particular types of devices.

- A *Manufacturer* is an organization recognized in the Netherlands, that demonstrably conforms to the Framework of standards for producing, and distributing in the Netherlands of specific types of Autonomous Devices and is authorized to do so by the Party responsible for establishing the framework.

- A *subscriber* is a natural or legal personality who enters into an agreement with a TSP on behalf of one or more certificate holders for certification of the public keys. Within the framework of the Autonomous Devices domain, a Subscriber is an organization recognized in the Netherlands, who demonstrably conforms to the admission requirements for mapping certificates (from the Autonomous Devices domain) to specific types of Autonomous Devices.

- A *certificate holder* is an entity, characterized in a protected link with a certificate as the holder of the private key that is linked to the public key provided in the certificate.

  A Certificate holder is a device of which the operation and the method of production demonstrably conform to the framework of standards of a specific type of autonomous device and that, in that capacity, is authorized by the party responsible for establishing the framework to use an Autonomous Devices certificate linked to that device.

  The linkage between certificate and device is made and protected by an organizational entity for which a subscriber is the contracting party.

- A *Certificate manager* is a natural person or a combination of a natural person and a legal personality who perform activities on behalf of the Subscriber (linking, replacement and/or revocation) with regard to the certificate holder's certificate. The subscriber instructs the certificate manager to perform the relevant actions and records these in a proof of certificate management.

- A *relying party* is every natural or legal personality who is a recipient of a certificate and who acts with a trust in that certificate. Unlike with other CPs, relying parties derive security from both the interconnectedness between an autonomous device and its certificate, and with the approval shown by that certificate of the operation of the autonomous device. The CP Autonomous Devices therefore places an equal emphasis on offering security about the interconnectedness of a message signed by an autonomous device with on the one hand the identity of the autonomous device and on the other hand its approved operation. Establishing the identity of the certificate holder (device) is, in light of this, as equally important as establishing the approval of its operation.

1.4 Certificate Usage

The use of certificates issued under this CP relates to communication from certificate holders who act in accordance with their certified operation.

[OID 2.16.528.1.1003.1.2.6.1] Authenticity certificates, which are issued under this CP, can be used for electronically reliably identifying and authenticating the Autonomous Device and its certified operation.

[OID 2.16.528.1.1003.1.2.6.2] Confidentiality certificates, issued under this CP, can be used to protect the confidentiality of data that is exchanged with the Autonomous Device and/or stored in that in its electronic form.

[OID 2.16.528.1.1003.1.2.6.3] Combination certificates that are issued under this CP can be used to safeguard a connection between a specific client and an Autonomous Device.

1.5 Contact Information Policy Authority

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

2 Publication and Repository Responsibilities

2.1 Electronic Repository

Contains no additional requirements.

2.2 Publication of TSP Information

Contains no additional requirements.

3 Identification and Authentication

3.1 Naming

Contains no additional requirements.

3.2 Initial Identity Validation

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-pkio31

RFC 3647	3.2.5 Validation of authority
Number	3.2.5-pkio34

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	4.9.1 Circumstances for revocation
Number	4.9.1-pkio52

RFC 3647	4.9.3 Procedures for revocation request
Number	4.9.3-pkio57

RFC 3647	4.9.3 Procedures for revocation request
Number	4.9.3-pkio58

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

4.10 Certificate Status Services

Contains no additional requirements.

5 Facility, Management and Operational Controls

5.2 Procedural Controls

Contains no additional requirements.

5.3 Personnel Controls

Contains no additional requirements.

5.4 Audit Loggin Procedures

RFC 3647	5.4.1 Types of events recorded
Number	5.4.1-pkio80

5.5 Records Archival

RFC 3647	5.5.1 Types of events recorded
Number	5.5.1-pkio82

5.7 Compromise and Disaster Recovery

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

6 Technical Security Controls

6.1 Key Pair Generation and Installation

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

RFC 3647	6.1.1 Key pair generation for the certificate holders
Number	6.1.1-pkio88

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

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

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-pkio111

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 and CRL profiles

7.1 Certificate Profile

RFC 3647	7.1 Certificate Profile
Number	7.1-pkio151

7.2 CRL Profile

Contains no additional requirements.

8 Compliance Audit and Other Assessments

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

9 Other Business and Legal Matters

9.2 Financial Responsibility

RFC 3647	9.2.1 Insurance coverage
Number	9.2.1-pkio124

9.5 Intellectual Property Rights

Contains no additional requirements.

9.6 Representations and Warranties

RFC 3647	9.6.1 CA Representations and Warranties by TSPs
Number	9.6.1-pkio127

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

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

RFC 3647	9.6.1 CA Representations and Warranties by TSPs
Number	9.6.1-pkio142

9.8 Limitations of Liability

RFC 3647	9.8 Limitations of liability
Number	9.8-pkio143

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-pkio141

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 device-linked certificates for the Autonomous Devices domain

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

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

It is not allowed to use fields that are not specified in the certificate profiles.
For the extensions, fields/attributes are used that, in accordance with international standards, are critical, are marked in the 'Critical' column with 'yes' to show that the relevant attribute MUST be checked using a process by means of which a certificate is evaluated. Other fields/attributes are shown with 'no'.

Device-linked 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 certificates under the G2 and G3 root certificate, only sha-256WithRSAEncryption is allowed.
Issuer	V	MUST contain a Distinguished Name (DN). The field has the attributes listed below:	PKIo, RFC3739, ETSI TS 102280		Attributes other than those mentioned below MUST NOT be used. The attributes that are used MUST be the same as the corresponding attributes in the Subject field of the TSP certificate (for validation).
Issuer.countryName	V	MUST contain the country code of the country where the issuing organization of the certificate is located.	ETSI TS101862, X520, ISO 3166	Printable String	C = NL for TSPs located in the Netherlands.
Issuer.OrganizationName	V	Full name in accordance with the accepted document or basic registry	ETSI TS 102280	UTF8String	
Issuer. organizationalUnitName	O	Optional specification of an organizational 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.

Field / Attribute	Criteria	Description	Standard reference	Type	Explanation
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 the accepted document or basic registry, MAY include the Domain label and/or the types of certificates that are supported	PKIo, RFC 5280, RFC 3739	UTF8String	The commonName attribute MUST NOT be necessary to identify the issuing government body (no part of the Distinguished Name, requirement from RFC 3739)
Issuer.organizationIdentifier	V/N	The organizationIdentifier field contains an identification of the issuing CA. This field MUST be present when the subject.organizationIdentifier field is present in the TSP certificate and MUST NOT be present when this field is not part of the corresponding TSP certificate.	EN 319 412-1	String	The syntax of the identification string is specified in paragraph 5.1.4 van ETSI EN 319 412-1 and contains: • 3 character legal person identity type reference; • 2 character ISO 3166 [2] country code; • hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8)); and • identifier (according to country and identity type reference).
Validity	V	MUST define the period of validity (validity) of the certificate.	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 (device) 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	Fixed value: C=NL, conform ISO 3166.	RFC 3739, X520, ISO 3166, PKIo	PrintableString	Country name specifies that the certificate is issued within the *context* of the (Dutch) PKI for the government.

Field / Attribute	Criteria	Description	Standard reference	Type	Explanation
Subject.commonName	V	MUST identify the framework of standards that the device conforms to OR MUST identify the framework of standards in accordance with the model/type of the device.	RFC 3739, ETSI TS 102 280, PKIo	UTF8String	The subscriber MUST prove that the organization can assign this name. Wildcards cannot be used in this attribute. Examples of a correct entry are: The type approval number of the relevant device; The (short) description of the specific type of Autonomous Devices
Subject.organizationName	V	The full name of the subscriber's organization in accordance with the accepted document or Basic Registry.	PKIo	UTF8String	The subscriber organization is the organization with which the TSP has entered into an agreement for the linkage/award of certificates to devices within the framework of standards drawn up by the party responsible for establishing the framework.
Subject.organizationalUnitName	O	Optional naming of part of an organization within the subscriber organization. MUST correspond with the name of a part of an organization documented by the subscriber organisation.	PKIo		This attribute MAY appear several times. The documentation that can be requested from the subscriber organization MUST show that the name used in this attribute mentions that part of the organization in which the certificate manager(s) of the subscriber organization work(s).
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	PKIo, RFC 3739	UTF8String	The address MUST correspond with the address of the subscriber in

Field / Attribute	**Criteria**	**Description**	**Standard reference**	**Type**	**Explanation**
		MUST contain the postal address of the subscriber in accordance with an accepted document or Basic registry.			accordance with the accepted document or registry.
Subject.serialNumber	O	The TSP is responsible for safeguarding the uniqueness of the subject (device). The Subject.serialNumber MUST be used to identify the subject uniquely.	RFC 3739, X 520, PKIo	Printable String	The number is determined by the TSP and/or the government. The number can differ for each domain and can be used for several applications. In addition to the definition in RFC 3739, the number MAY be added to, in order to identify as well as the subject, for example, the SUD.
Subject.title	O	Shows the applicable authorization of the (autonomous) device within the framework of standards.	ETSI TS 102 280, RFC 3739, RFC 5280		The party responsible for establishing the framework determines whether this attribute is used and establishes that usage in a framework of standards drawn up by this party.
subjectPublicKeyInfo	V	Contains, among other things, the public key.	ETSI TS 102 280, RFC 3279		Contains the public key, identifies the algorithm with which the key can be used.

Standard extensions

Field / Attribute	Criteria	Critical?	Description	Standard reference	Type	Explanation
authorityKeyIdentifier	V	No	The algorithm to generate the AuthorityKey MUST be created on an algorithm determined by the PA.	ETSI TS 102 280, RFC 5280	BitString	The value MUST contain the SHA-1 hash from the authorityKey (public key of the TSP/CA).
SubjectKeyIdentifier	V	No	The algorithm to generate the subjectKey MUST be created on an algorithm determined by the PA.	RFC 5280	BitString	The value MUST contain the SHA-1 hash from the subjectKey (public key of the certificate holder).
KeyUsage	V	Yes	The attribute extension specifies the intended purpose of the key incorporated in the certificate. In the PKI for the government, for each certificate type various bits are incorporated in the keyUsage extension. The digitalSignature bit MUST be included in authenticity certificates. Another keyUsage MAY NOT be combined with this. In confidentiality certificates, the keyEncipherment and dataEncipherment bits MUST be included. Another keyUsage MAY NOT be combined with this. In combination certificates the digitalSignature, keyEncipherment and keyAgreement bits MUST be incorporated and marked as critical. Another	RFC 3739, RFC 5280, ETSI TS 102 280	BitString	

			keyUsage MAY NOT be combined with this.			
CertificatePolicies	V	No	MUST contain the OID of the certificate policy (CP), the URI of the certification practice statement (CPS), and a user notice. The applicable PKI for the government OID scheme is described in the CP. The TSP SHOULD use UTF8String in the userNotice, but MAY use IA5String.	RFC 3739	OID, String, UTF8String or IA5 String	For devices certificates in the Autonomous Devices domain, the OIDs are: 2.16.528.1.1003.1.2.6.1, 2.16.528.1.1003.1.2.6.2 and 2.16.528.1.1003.1.2.6.3. A further restriction, if any, with regard to the use of the certificate MUST be included in the CPS which this extension references and are preferably also shown in the user note included for this extension. Reference to the paragraph numbers of the PoR/CP in the user note is advised against because the persistency of this cannot be guaranteed (unlike the OID number of the CP).
SubjectAltName	V	No	Contains one or more alternative names/identification numbers of the certificate holder	RFC 5280, PKIo, ETSI 102 280		Attributes other than those mentioned below MUST NOT be used.
SubjectAltName.otherName	V		MUST be used, containing a number that identifies the certificate holder (subject) globally. In addition, in the authenticity certificate, as othername a PrincipalName (UPN) MAY be included for use with SSO (Single Sign On).	RFC 4043, PKIo	IA5String, Microsoft UPN, IBM Principal-Name or Permanent-Identifier	Contains an OID assigned by PKIoverheid to the TSP (issuer) and a unique number within the namespace of that OID that will permanently identify the certificate holder (subject), in one of the following ways: 1. MS UPN: [number]@[OID] 2. IA5String: [OID].[number] 3. IA5String: [OID]-[number] 4. Permanent Identifier: Identifiervalue = [number] Assigner = [OID] Alternative 1. is also suitable for SSO (Single Sign On). 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.
SubjectAltName.rfc822Name	A		MAY be used for the service's e-mail address, for applications that need the e-mail address in order to be able to function properly.	RFC 5280	IA5String	For PKIoverheid certificates, the use of e-mail addresses is advised against, because e-mail addresses of certificate holders often change and are susceptible to spam.
BasicConstraints	O	Yes	The "CA" field MUST be omitted (default value is then "FALSE").	RFC 5280		A (Dutch language) browser can then be seen: Subjecttype = Eindentiteit", "Beperking voor padlengte = Geen ("Subjecttype = End Entity", "Path length constraint = None")
CRLDistributionPoints	V	No	MUST include the URI of a CRL distribution point.	RFC 5280, ETSI TS 102 280		The reference MUST be accessible through the http or LDAP protocol. The attribute Reason MUST NOT be used, reference MUST be made to 1 CRL for all types of reasons for revocation. In addition to CRL, other types of certificate status information service MAY be supported.
ExtKeyUsage	V	Yes / No		RFC 5280	KeyPurposeId's	See requirement 7.1-pkio151.
FreshestCRL	O	No	MUST contain the URI of a Delta CRL distribution point, if Delta CRLs are used.	RFC 5280, PKIo		Delta-CRLs are an optional extension. In order to fulfil the requirements of PKIoverheid a TSP MUST also publish full CRLs at the required release frequency.

Private extensions

Field / Attribute	Criteria	Critical?	Description	Standard reference	Type	Explanation
authorityInfoAccess accessMethod (id-ad-caIssuers)	O		An AccessDescription item with accessMethod id-ad-caIssuers references the online location where the certificate of the TSP CA that signed the current certificate (issue) is located.	RFC 5280	URI	This attribute MUST include the URI of the relevant certificate file/object. If this is an HTTP-URI, the file that is referenced: is preferably a DER-coded CA certificate file, that is seen by the relevant HTTP server as the type MIME "application/pkix-cert".
SubjectInfoAccess	O	No		RFC 5280	OID, Generalname	This field can be used to reference additional information about the subject.

CRL extensions

Field / Attribute	Criteria	Critical?	Description	Standard reference[1]	Type	Explanation
authorityKeyIdentifier	O	No	This attribute is interesting if a TSP has more signature certificates with which a CRL could be signed (using this attribute, it can then be ascertained which public key has to be used to verify the signature of the CRL).	RFC 5280	KeyIdentifier	The value MUST include the SHA-1 hash from the authorityKey (public key of the TSP/CA).
IssuerAltName	A	No	This attribute allows alternative names to be used for the TSP (as issuer of the CRL) (the use is advised against).	RFC 5280		The DNS name, IP address and URI could potentially be entered into this field. The use of a rfc822 name (e-mail address) is NOT allowed.

Field / Attribute	Criteria	Critical?	Description	Standard reference[1]	Type	Explanation
CRLNumber	V	No	This attribute MUST contain an incremental number that provides support when determining the order of CRLs (the TSP provides the numbering in the CRL).	RFC 5280	Integer	
DeltaCRLIndicator	O	Yes	If 'delta CRLs' are used, a value for this attribute MUST be entered.	RFC 5280	BaseCRLNumber	Contains the number of the baseCRL of which the Delta CRL is an extension.
issuingDistributionPoint	O	Yes	If this extension is used, this attribute identifies the CRL distribution point. It can also contain additional information (such as a limited set of reason codes why the certificate has been revoked).	RFC 5280		If used, this field MUST fulfil the specifications in RFC 5280
FreshestCRL	O	No	This attribute is also known by the name 'Delta CRL Distribution Point'. If used it MUST contain the URI of a Delta CRL distribution point. This is never present in a Delta CRL.	RFC 5280		This field is used in complete CRLs and indicates where Delta CRL information can be found that will update the complete CRL.
authorityInfoAccess	O	No	Optional reference to the certificate of the CRL.Issuer.	RFC 5280	id-ad-caIssuers (URI)	MUST conform to § 5.2.7 of RFC 5280.
CRLReason	O	No	If used, this gives the reason why a certificate has been revoked.	RFC 5280	reasonCode	If no reason is given, this field MUST be omitted
holdInstructionCode	N	No	Is not used.	RFC 5280	OID	The PKI for the government does not use the 'On hold' status.

Field / Attribute	Criteria	Critical?	Description	Standard reference[1]	Type	Explanation
invalidityDate	O	No	This attribute can be used to indicate a date and time on which the certificate has become compromised if it differs from the date and time on which the TSP processed the revocation.	RFC 5280	GeneralizedTime	
certificateIssuer	A	Yes	If an indirect CRL is used, this attribute MAY be used to identify the original issuer of the certificate.	RFC 5280	GeneralNames	

CRL entry

Field / Attribute	Criteria	Description	Standard reference	Type	Explanation
userCertificate	V	Identifies the (revoked) certificate	RFC 5280	Certificate-Serial-Number	Contains the (integer) serialnumber of the revoked certificate.
revocationDate	V	Specifies the time (date and time) when the Certificate was added to the CRL.	RFC 5280	UTCTime	Contains the same time as the field ThisUpdate of the first CRL generated after te revocation of the certificate.
crlEntryExtensions	O	Contains a series of CRL entry extensions.	RFC 5280	Extensions	This field contains a series of extensions that are exclusively applicable to this CRL entry. See the section "CRL entry extensions" below.

CRL entry extensions

Field / Attribute	Criteria	Critical?	Description	Standard reference[1]	Type	Explanation
CRLReason	O	No	If used contains the reason for the revocation of the certificate.	RFC 5280, PKIo	reasonCode	If no reason is give this extension MUST NOT be used. If this extension is used it MUS NOT appear more than once. The reasonCode used MUST be one of the following: keyCompromise (1); affiliationChanged (3); superseded (4); privilegeWithdrawn (9).
invalidityDate	O	No	This attribute can be used to indicate a date and time when the certificate was compromised if this deviates from (is earlier than) the date and time when the TSP processed the revocation.	RFC 5280	Generalized-Time	When a revocation request is presented to the TSP it is possible that the requestor indicates that the reason for revocation (for instance theft) happened some time previously. Additionally the validation of the request may take some time. This extension presents the possibility register the original time of revocation, even though the time of processing (and addition to the CRL) occurs later.
certificateIssuer	A	Yes	If an indirect CRL is used this attribute MUST contain the original issuer of the certificate.	RFC 5280	General-Names	The Distinguished Name (DN) of the issuer of the (revoked) certificate in question must be included in this extension in the exact same manner that this Issuer.DN is encoded in the (revoked) certificate.

10 Revisions

10.1 Amendments from version 4.3 to 4.4

10.1.1 New

None

10.1.2 Modifications

- Removal of requirement 5.3.2-pkio79 (effective date 1-2-2017)
- Modificaton of requirement 7.1-pkio151; use of EKUs broken down to the different certificate types (effective date 1-2-2017)
- Clarification of issuer.organizationIdentifier field (effective date 1-2-2017)
- Tightening of use optional EKUs that conflict with the parent TSP CA certificate (effective date 1-2-2017)

10.1.3 Editorial

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

10.2 Amendments from version 4.2 to 4.3

10.2.1 New

- Addition of Issuer.organizationalIdentifier in the certificate profile (effective date 1-7-2016)

10.2.2 Modifications

- Description with attribute CertificatePolicies (effective date 1-7-2016)
- Removal of optional use KeyAgreement with Key Usage (effective date no later than 4 weeks after publication of PoR 4.3)
- ETSI TS 102 176-1 replaced by ETSI TS 119 312 (effective date no later than 4 weeks after publication of PoR 4.3)
- Dropped requirement pkio95 because of duplicate requirement in ETSI EN 319 411-1
- Use of values in the BasicConstraints field no longer permitted in end entity certificates (effective date 1-7-2016)
- ETSI TS 102 042 replaced by ETSI EN 319 411-1 (effective date 1-7-2016)

10.2.3 Editorial

- Removed references to G1 Root (expired)

10.3 Amendments from version 4.1 to 4.2

10.3.1 New

- Requirement 7.1-pkio151 (effective date 1 juli 2016)

10.3.2 Modifications

None

10.3.3 Editorial

None

10.4 Amendments from version 4.0 to 4.1

10.4.1 New

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

10.4.2 Modifications

Not applicable.

10.4.3 Editorial

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

10.5 Amendments from version 3.7 to 4.0

10.5.1 New

- Requirement 4.9.9-pkio69

10.5.2 Modifications

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

10.5.3 Editorial

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