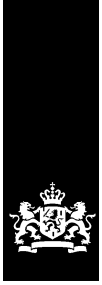


Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Programme of Requirements part 3: Basic Requirements PKIoverheid

Datum 27 July 2015

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

1.1 Overview

This is part 3 Basic Requirements of the Programme of Requirements (PoR) of the PKI for the government and is called the Basic Requirements Pkioverheid. Set out in the PoR are the standards for the PKI for the government. This section of part 3 relates to the basic 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. These basic requirements relate to all types of certificate issued under these domains.

A 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 Policies

Part 3 of the Programme of Requirements of PKIoverheid consitis of the following elements:

- *Part 3 Basic Requirements:* The basic requirements are applicable to all Certificate Policies in part 3 of the Programme of Requirements;
- *Part 3 Additional Requirements:* Contains all additional requirements that are applicable to one or more CPs, but not all CPs;
- *Part 3 Reference matrix PKIoverheid and ETSI:* An overview of PKIoverheid requirements with a reference to the applicable ETSI norm(s);
- *Part 3a through 3i:* The Certificate Policies for the different PKIoverheid certificates. These CP's govern the issueance of end entity certificates under the regular root, the private root and the Extended Validation root. These root certificates are broken down into different versions or generations.

The CPs in part 3 of the PoR are structured as follows:

- *Part 3a:* Personal certificates in the Organization domain;
- *Part 3b:* Services authentication and encryption certificates in the Organization domain;
- *Part 3c:* Personal certificates in the Citizen domain;
- *Part 3d:* Services certificates in the Autonomous Devices domain;
- *Part 3e:* Website and server certificates in the Organization domain;
- *Part 3f:* Extended Validation certificates under the Extended Validation root;
- *Part 3g:* Services authentication and encryption certificates in the Private Services domain;
- *Part 3h:* Server certificates in the Private Services domain;
- *Part 3i:* Personal certificates in the Private Services domain.

All PKIoverheid requirements have an unique and persistant number which also contains a reference to RFC 3647. Furthermore each PKIoverheid requirement is an addition to one or more ETSI requirements

for the issueance of PKI certificates and is thus reference to the ETSI norm(s) in question. These references are listed in a separate Excel sheet named *Reference Matrix PKIoverheid and ETSI*.

The PKIoverheid requirements are devided into the *Basic Requirements* and the *Additonal Requirements*. The *Basic Requirements* are applicable to all CPs. Additionally, each CP contains references to the *Additional Requirments* that are applicable to that specific CP. The CPs do not contain reference to the *Basic Requirements* or relevant ETSI standard, as these are automatically applicable.

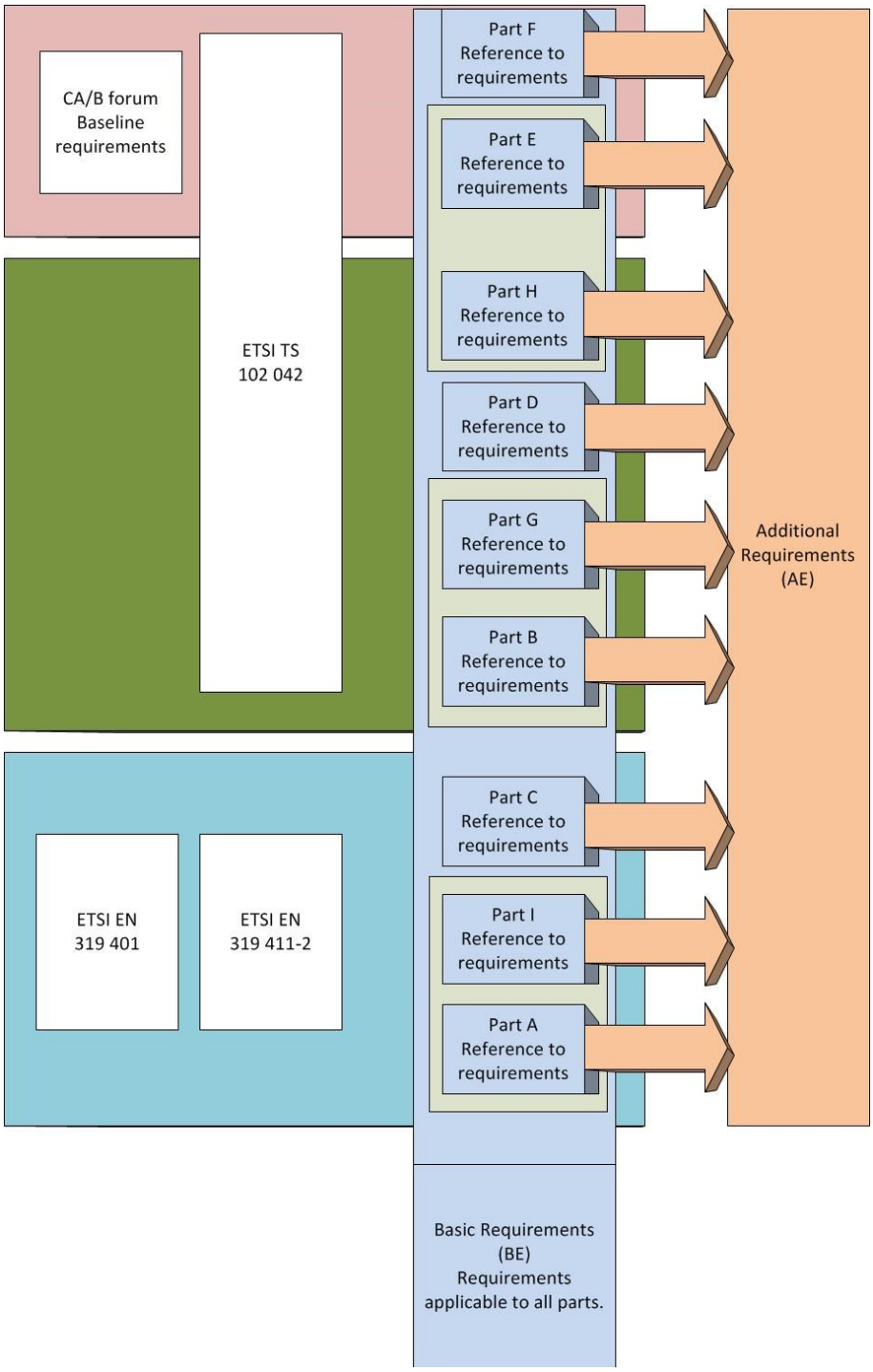
To comply with a specific CP the applicable ETSI standard, the *Basic Requirements* and part of the *Additional Requirements* of PKIoverheid must be met.

Incorporated in chapters 2 to 9 inclusive are the specific PKIoverheid requirements. The table below shows the structure within which all PKIoverheid requirements (PKIo requirement) are specified individually.

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[1].
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.
ETSI	Reference to the applicable ETSI requirement(s) from which the PKIo requirement is derived or to which it provides further detail.
PKIo	The PKIo requirement that applies to this domain of the PKI for the government.
Comment	To provide a better understanding of the context in which the requirement has to be placed a comment has been added to a number of PKIo requirements.

The following figure gives a graphical overview of the structure of part 3 of the Programme of Requirements:

[1] *Chapters 2 to 9 inclusive only include those paragraphs from RFC 3647 to which a PKIo requirement applies.*



1.1.2 Status

This is version 4.1 of part 3 Basic Requirements 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 these Basic Requirements of the PoR. 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 these Basic Requirements, if these Basic Requirements

are used for purposes other than for the use of certificates described in paragraph 1.4 of the individual PoR parts.

1.2 Contact information Policy Authority

The PA is responsible for these Basic Requirements. Questions relating to the Basic Requirements can be directed to the PA; the address can be found at: http://www.logius.nl/pkioverheid.

2 Publication and Repository Responsibilities

2.1 Electronic Repository

RFC 3647	2.1 Electronic repository	
Number	2.1-pkio1	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- 7.3.5.e 7.3.5.e.ii
PKIo	The maximum period of time within which the availability of the dissemination service has to be restored is set at 24 hours.	

RFC 3647	2.1 Electronic repository	
Number	2.1-pkio2	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	6.2 7.3.1.b and 7.3.5.f 7.3.1.c, 7.3.4.b and 7.3.5.f
PKIo	There MUST be an electronic repository where the information referred to in [2.2] is published. This repository can be managed by the CSP or by an independent organisation.	
Comment	The information that has to be published is included in ETSI TS 101 456. The relevant articles in which the information is specified can be found in the reference matrix in appendix B.	

2.2 Publication of CSP Information

RFC 3647	2.2 Publication of CSP information	
Number	2.2-pkio3	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- 7.3.1.b 7.3.1.c
PKIo	The CPS has to be written in Dutch.	

RFC 3647	2.2 Publication of CSP information
Number	2.2-pkio5

ETSI	EN 319 401 EN 319 411-2 TS 102 042	- 7.3.1.b 7.3.1.c
PKIo	The CSP has to include the OIDs of the CPs that are used in the CPS.	

RFC 3647	2.2 Publication of CSP information	
Number	2.2-pkio6	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- 7.3.1.b 7.3.1.c
PKIo	All information has to be available in Dutch.	

3 Identification and Authentication

3.1 Naming

RFC 3647	3.1.1 Types of names	
Number	3.1.1-pkio10	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	QCP - 7.3.3.a QCP and 7.3.6.g 7.3.3.a and 7.3.6.i
PKIo	The CSP has to fulfil the requirements laid down for name formats in the Certificate, CRL and OCSP profiles.	
Comment	Included in appendix A of the Basic Requirements are the CRL and OCSP profiles. The PoR part for a certain type of certificate contains the certificate profile in appendix A.	

3.2 Initial Identity Validation

Contains no Basic Requirements.

3.3 Identification and Authentication for Re-key Requests

RFC 3647	3.3.1 Identification and authentication for routine re-key	
Number	3.3.1-pkio36	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- 7.3.2.d 7.3.2.d
PKIo	7.3.2.d only applies to encryption certificates. For all other types of PKIoverheid certificates a re-key MUST take place when renewing a certificate.	
Comment	7.3.2.d. states under which conditions recertification of the keys of encryption certificates is permitted. The requirement means that certificates CANNOT be renewed without a re-key for the authenticity, signature and server certificates.	

RFC 3647	3.3.1 Identification and authentication for routine re-key	
Number	3.3.1-pkio45	
ETSI	EN 319 401 EN 319 411-2	- 7.3.2.a and 7.3.2c

	TS 102 042	7.3.2.a and 7.3.2c
PKIo	Before certificates are renewed, it must be checked that both requirement 3.1.1-pkio and all requirements stated under [3.1] and [3.2] of the CP for that type of certificate have been fulfilled.	
Comment	The relevant articles in which the requirements are specified can be found in part 3 Reference matrix PKIoverheid and ETSI. When replacing a personal certificate at the end of its lifetime the qualified signature of the non-repudiation certificate can be used during registration and identification, instead of the physical presence of the certificate holder. This is subject to a number of conditions: • The non-repudiation certificate must be valid at the time of renewal; • The file must be current and complete, including a copy of a valid ID document (WID); • Subject details of the applicant of the new personal certificate are the same as the details in the valid non-repudiation certificate, e.g. organization field; • The single renewal of the certificate without physical appearance is only possible through the CSP that issued the non-repudiation certificate based on physical identification. All personal certificates under PoR parts 3a, 3c and 3i can be renewed once in this manner.	

RFC 3647	3.3.2 Identification and authentication for re-key after revocation	
Number	3.3.2-pkio46	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- 7.3.2.d 7.3.2.d
PKIo	After revocation of the certificate, the relevant keys cannot be recertified. 7.3.2.d does not apply.	

4 Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

Contains no Basic Requirements.

4.4 Certificate Acceptance

RFC 3647	4.4.1 Conduct constituting acceptance of certificates	
Number	4.4.1-pkio49	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- 7.3.1.i 7.3.1.m
PKIo	After issuance of a certificate, the certificate holder of a personal certificate or the certificate manager of the other types of certificate has to specifically confirm to the CSP the delivery of the key material that is part of the certificate.	
Comment	When keys protected by software are used (see [6.2.11-pkio106 and 6.2.11-pkio107]) where the private key is generated by the certificate manager rather than the CSP, the delivery of key material is not applicable. However, the data required in 7.3.1.i and 7.3.1.m must be logged. This stipulation is applicable to CP parts E, F and H.	

4.5 Key Pair and Certificate Usage

RFC 3647	4.5.2 Relying party public key and certificate usage	
Number	4.5.2-pkio51	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- 6.3.a 6.3.a
PKIo	The terms and conditions for users that are made available to the relying parties have to state that the relying party has to check the validity of the full chain of certificates up to the source (root certificate) that is relied on. The terms and conditions must also state that the subscriber is personally responsible for prompt replacement in the event of an approaching expiry of validity, and for emergency replacement in the event of a private key compromise and/or other types of emergencies relating to the certificate or the higher level certificates. The subscriber is expected to take adequate measures in order to safeguard the continuity of the use of certificates.	
Comment	The validity of a certificate does not indicate the certificate holder's authority to perform a specific transaction on behalf of an organization or pursuant to his or	

	her profession. The PKI for the government does not arrange authorization; a relying party has to convince itself of that in a different manner. It is advisable to inform the subscriber to take into account the "ICT beveiligingsrichtlijnen voor de transport layer security (TLS)" of the NCSC when using PKIoverheid server certificates. This advice can be obtained online via the website of the NCSC.

4.9 Certificate Revocation and Suspension

RFC 3647	4.9.2 Who can request revocation	
Number	4.9.2-pkio53	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- 7.3.6.a 7.3.6.a
PKIo-OO	The following parties can request revocation of an end user certificate: • the certificate manager; • the certificate holder; • the subscriber; • the CSP; • any other party or person that has an interest, at the discretion of the CSP.	

RFC 3647	4.9.3 Procedure for revocation request	
Number	14.9.3-pkio54	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- 7.3.6.a 7.3.6.a
PKIo	The CSP is entitled to lay down additional requirements in respect of a request for revocation. These additional requirements have to be included in the CPS of the CSP.	

RFC 3647	4.9.3 Procedure for revocation request	
Number	4.9.3-pkio55	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- 7.3.6.h 7.3.6
PKIo	The maximum period of time within which the availability of the revocation management services have to be restored is set at four hours.	

RFC 3647	4.9.3 Procedure for revocation request	
Number	4.9.3-pkio56	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- 7.3.6.a 7.3.6.a
PKIo	The CSP has to record the reasons for revocation of a certificate if the revocation is initiated by the CSP.	

RFC 3647	4.9.5 Time within which CA must process the revocation request	
Number	4.9.5-pkio61	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- 7.3.6.a 7.3.6.a
PKIo	The maximum delay between receiving a revocation request or revocation report and the amendment of the revocation status information, that is available to all relying parties, is set at four hours.	
Comment	This requirement applies to all types of certificate status information (CRL and OCSP)	

RFC 3647	4.9.6 Revocation checking requirement for relying parties	
Number	4.9.5-pkio63	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- 6.3.a 6.3.a
PKIo	An end-user who consults the certificate status information has to verify the authenticity of this information using the electronic signature with which the information has been signed and the corresponding certification path.	

RFC 3647	4.9.6 Revocation checking requirement for relying parties	
Number	4.9.5-pkio64	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- 6.3.a 6.3.a
PKIo	The obligation mentioned in [4.9.6-pkio63] has to be included by the CSP in	

	the terms and conditions for users that are made available to the relying parties.

RFC 3647	4.9.9 On-line revocation/status checking availability	
Number	4.9.9-pkio694	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- 7.3.6.i 7.3.6.j
PKIo	To detail the provisions in {16} IETF RFC 2560, the use of precomputed OCSP responses is not allowed.	

RFC 3647	4.9.13 Circumstances for suspension	
Number	4.9.13-pkio72	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- 7.3.6.d 7.3.6.e
PKIo	Suspension of a certificate CANNOT be supported.	

4.10 Certificate Status Services

RFC 3647	4.10.2 Service availability	
Number	4.10.2-pkio73	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- 7.3.6.i 7.3.6.j
PKIo	The maximum period of time within which the availability of the revocation status information has to be restored is set at four hours.	
Comment	This requirement only applies to the CRL and not to other mechanisms, such as OCSP.	

5 Facility, Management and Operational Controls

5.2 Procedural Controls

RFC 3647	5.2 Procedural Controls	
Number	5.2-pkio74	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	6.4.1.a and 6.4.5 - 7.4.1.a and 7.4.5
PKIo	The CSP has to reperform the risk analysis at least every year, or if the PA provides an instruction to that end, or the NCSC provides advice to that end. The risk analysis has to cover all PKIoverheid processes that fall under the responsibility of the CSP. Based on the risk analysis, the CSP has to develop, implement, maintain, enforce and evaluate an information security plan. This plan describes a cohesive framework of appropriate administrative, organizational, technical and physical measures and procedures with which the CSP can safeguard the availability, exclusivity and integrity of all PKIoverheid processes, requests and the information that is used to this end.	

RFC 3647	5.2 Procedural Controls	
Number	5.2-pkio75	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	6.4.1.b - 7.4.1.b
PKIo	In addition to an audit performed by an accredited auditor, the CSP MAY perform an audit of the external suppliers of PKIoverheid core services, in order to satisfy itself that these suppliers have implemented and operationalized the relevant requirements from the PoR of PKIoverheid, in accordance with the requirements of the CSP and taking into account its business objectives, processes and infrastructure. The CSP is entirely free to choose to perform its own audit, or to arrange for this to be performed, or to use existing audit results such as those from the formal certification audits, the various internal and external audits, Third Party Notifications and (foreign) compliancy reports. The CSP is also entitled to view the underlying evidentiary material, such as audit files and other documentation including system documentation. Of course the foregoing is limited to the CSP processes, systems and infrastructure hosted by the suppliers for PKIo core services.	

RFC 3647	5.2.4 Roles requiring separation of duties	
Number	5.2.4-pkio76	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	6.4.3.d and 6.4.3.h - 7.4.3.d and 7.4.3.h
PKIo	The CSP has to enforce separation of duties between at least the following roles: • Security officer The security officer is responsible for the implementation of and compliance with the stipulated security guidelines. • System auditor The system auditor fulfils a supervisory role and provides an independent opinion on the manner in which the business processes are arranged and on the manner in which the requirements relating to security are fulfilled. • Systems administrator The systems manager maintains the CSP systems, which includes installing, configuring and maintaining the systems. • CSP operators The CSP operators are responsible for the everyday operation of the CSP systems for, among other things, registration, the generation of certificates, the delivery of an SSCD to the certificate holder and revocation management.	
Comment	The aforementioned job descriptions are not limitative and the CSP is free to extend the description within the requirements of segregation of functions, or to divide the functions further still, or to share these between other trusted officials.	

RFC 3647	5.2.4 Roles requiring separation of duties	
Number	5.2.4-pkio77	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	6.4.3.d and 6.4.3.h - 7.4.3.d and 7.4.3.h
PKIo	The CSP has to enforce separation of duties between staff who monitor the issuance of a certificate and staff who approve the issuance of a certificate.	

5.3 Personnel Controls

RFC 3647	5.3 Declaration of confidentiality	
Number	5.3-pkio78	
ETSI	EN 319 401 EN 319 411-2	6.4.3.e -

	TS 102 042	7.4.3.e
PKIo	Because publication of confidential information can have significant consequences (among other things, for the trustworthiness) the CSP has to make every effort to make sure that confidential information is dealt with confidentially and that it remains confidential. One important aspect is to ensure that declarations of confidentiality are signed by staff members and contracted third parties.	

5.4 Audit Logging Procedures

RFC 3647	5.4.3 Retention period for audit log	
Number	5.4.3-pkio81	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	6.4.11.e - 7.4.11.e
PKIo	The CSP has to store log files for incidents relating to: • CA key life cycle management and; • Certificate life cycle management; These log files must be retained for 7 years and then deleted. The CSP has to store log files for incidents relating to: • Threats and risks; These log files must be retained for 18 months and then deleted. The log files have to be retained in such a way that the integrity and accessibility of the data is safeguarded.	

5.5 Records Archival

RFC 3647	5.5.2 Retention period for archive	
Number	5.5.2-pkio83	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	6.4.11.e - 7.4.11.e
PKIo	No PKIo requirement applies, only a comment.	
Comment	At the request of the entitled party, it can be agreed that the required information is stored for longer by the CSP. This is, however, not mandatory for the CSP.	

5.7 Compromise and Disaster Recovery

RFC 3647	5.7.1 Incident and compromise handling procedures.	
Number	5.7.1-pkio84	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- 7.4.8.ed 7.4.8.f
PKIo	After analysis and establishment of a security breach and/or emergency the CSP has to immediately inform the PA, the NCSC and the auditor, and has to keep the PA, the NCSC and the auditor informed about how the incident is progressing.	
Comment	Understood to be meant by security breach in the PKIoverheid context is: An infringement of the CSP core services: registration service, certificate generation service, subject device provisioning service, dissemination service, revocation management service and revocation status service. This is including, but not limited to: • unauthorized elimination of a core service or rendering this core service inaccessible; • unauthorized access to a core service in order to eavesdrop on, intercept and/or change electronic messaging; • unauthorized access to a core service for unauthorized removal, amendment or alteration of computer data.	

RFC 3647	5.7.1 Incident and compromise handling procedures.	
Number	5.7.1-pkio85	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- 7.4.8.d 7.4.8.e
PKIo	The CSP will inform the PA immediately about the risks, dangers or events that can in any way threaten or influence the security of the services and/or the image of the PKI for the government. This is including, but not limited to, security breaches and/or emergencies relating to other PKI services performed by the CSP, which are not PKIoverheid services.	

6 Technical Security Controls

6.1 Key Pair Generation and Installation

RFC 3647	6.1.5 Key sizes	
Number	6.1.5-pkio96	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- 7.2.8.b 7.2.8.b
PKIo	The length of the certificate holders' cryptographic keys have to fulfil the requirements laid down in that respect in the list of cryptographic algorithms and key lengths as defined in ETSI TS 102 176-1.	
Comment	Although ETSI TS 102 176 outlines the recommended algorithms and key lengths, these are compulsory within the PKI for the government. Requests relating to the use of other algorithms have to be submitted, along with the reasoning behind this, to the PA of the PKI for the government.	

RFC 3647	6.1.7 Key usage purposes (as per X.509 v3 key usage field)	
Number	6.1.7-pkio97	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- 7.2.5 7.2.5
PKIo	The key usage extension in X.509 v3 certificates (RFC 5280 Internet X.509 Public Key Infrastructure Certificate and CRL Profile) defines the purpose of the use of the key contained in the certificate. The CSP has to indicate the use of keys in the certificate, in accordance with the requirements laid down in that respect in appendix A of this document, namely 'CRL and OCSP profiles' and appendix A of the applicable PoR part for that type of certificate.	

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-pkio98	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- 7.2.4 7.2.4.a
PKIo	Escrow by the CSP is not allowed for the private keys of PKIoverheid certificates, with the exception of encryption certificates.	

RFC 3647	6.2.4 Private key backup of certificate holder key	
Number	6.2.4-pkio102	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- 7.2.4 en 7.2.8.e 7.2.4 en 7.2.8.e
PKIo	Back-up of the certificate holders' private keys by the CSP is not allowed.	

RFC 3647	6.2.5 Private key archival of certificate holder key	
Number	6.2.5-pkio103	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- 7.2.4 en 7.2.8.e 7.2.4.a en 7.2.8.e
PKIo	Archiving of the certificate holders' private keys by the CSP is not allowed.	

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-pkio110	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	QCP - 7.2.6 7.2.6
PKIo	At the time that an end user certificate is issued, the remaining term of validity of the higher level CSP certificate has to exceed the intended term of	

	validity of the end user certificate.

6.4 Activation data

Contains no basic requirements.

6.5 Computer Security Controls

RFC 3647	6.5.1 Specific computer security technical requirements	
Number	6.5.1-pkio114	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	6.4.6 7.4.6 7.4.6
PKIo	The CSP has to use multi-factor authentication (e.g. smartcard with personal certificates and a personal password or biometry and a personal password) for the system or the user accounts which are used to issue or approve certificates.	
Comment	Multi-factor authentication tokens cannot be connected permanently or semi-permanently to the system (e.g. a permanently activated smartcard). That is because this would enable certificates to be issued or approved (semi) automatically, or for non-authorized staff to issue or approve certificates.	

RFC 3647	6.5.1 Specific computer security technical requirements	
Number	6.5.1-pkio115	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	6.4.6 7.4.6 7.4.6
PKIo	The staff of external Registration Authorities (RA) or Resellers may not have access to the system or the user accounts of the CSP which enables issuance or approval of certificates. This function is restricted to authorized staff of the CSP. If an RA or a Reseller does have this access, the RA or the Reseller will be seen as part of the CSP and it/they have to comply with the PKI for the government Programme of Requirements fully and demonstrably.	

RFC 3647	6.5.1 Specific computer security technical requirements	
Number	6.5.1-pkio116	
ETSI	EN 319 401 EN 319 411-2	6.4.6.a -

	TS 102 042	7.4.6.a
PKIo	The CSP prevents unauthorized access to the following core services: registration service, certificate generation service, subject device provision service, dissemination service, revocation management service and revocation status service. To this end, these core services are separated either physically or logically from the non-PKI network domains and PKI network domains that do not meet the Network Security Guidelines of the Cabforum and network related PKIoverheid requirements from RFC3647 paragraph 6, "Technical Security Controls". The CSP enforces a unique authentication for each core service mentioned above. When the physical or logical separation of the network domains described above is not feasible, the various core services must be implemented on separate network domains, where there has to be a unique authentication for each core service mentioned above. The CSP must document the organization of the network domains, at least in a graphical manner.	
Comment	This requirement applies to both the production environment and the fall-back environment. This requirement does not apply to other environments, such as acceptance and test.	

6.6 Life Cycle Technical Controls

RFC 3647	6.6.1 System development controls	
Number	6.6.1-pkio117	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	6.4.7 7.4.7 7.4.7
PKIo	In relation to this ETSI requirement, the PKIoverheid have only formulated a comment and no specific PKIo requirement applies.	
Comment	Compliance with 6.4.7, 7.4.7 and Electronic Signature Regulation art. 2 paragraph 1c can be demonstrated by: • an audit statement from the supplier of the products, which has had an independent EDP audit performed based on CWA 14167-1; • an audit statement from an internal auditor from the CSP based on CWA 14167-1; • an audit statement from an external auditor based on CWA 14167-1.	

6.7 Network Security Controls

RFC 3647	6.7.1 Network security controls
Number	6.7.1-pkio118

ETSI	EN 319 401 EN 319 411-2 TS 102 042	6.4.6 7.4.6 7.4.6
PKIo	The CSP has to ensure that all PKIoverheid ICT systems relating to the registration service, certificate generation service, subject device provision service, dissemination service, revocation management service and revocation status service: • are equipped with the latest updates and; • the web application controls and filters all input by users and; • the web application codes the dynamic output and; • the web application maintains a secure session with the user and; • the web application uses a database securely.	
Comment	The CSP has to use the NCSC's "Checklist beveiliging webapplicaties (Security of Web Applications Checklist)[2]" as guidance for this. In addition it is recommended that the CSP implements all other recommendations from the latest version of the white paper "Raamwerk Beveiliging Webapplicaties (The Framework for Web Application Security)" by the NCSC.	

RFC 3647	6.7.1 Network security controls	
Number	6.7.1-pkio119	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	6.4.6 7.4.6 7.4.6
PKIo	Using an audit tool, at least each month the CSP performs a security scan on its PKIoverheid infrastructure. The CSP documents the result of every security scan and the measures that were taken in relation to this scan.	
Comment	Some examples of commercial and non-commercial audit tools are GFI LanGuard, Nessus, Nmap, OpenVAS and Retina.	

RFC 3647	6.7.1 Network security controls	
Number	6.7.1-pkio120	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	6.4.6 7.4.6 7.4.6
PKIo	At least once a year, the CSP arranges for a pen test to be performed on the PKIoverheid internet facing environment, by an independent, experienced, and competent external supplier.	

[2] *http://www.govcert.nl/binaries/live/govcert/hst%3Acontent/dienstverlening/kennis-en-publicaties/factsheets/checklist-webapplicatie-beveiliging/checklist-webapplicatie-beveiliging/govcert%3AdocumentResource/govcert%3Aresource*

	In addition a CSP is obliged to arrange a pen test to be performed when substantial changes to the internet facing environment have occurred, - The assessment if substantial changes have occurred takes place by means of a documented risk analysis. - The pen test is performed by an independent, experienced, and competent pen tester. - The pen test must take place no later than one month after the release, but preferably before going to production. The CSP has to document the findings from the pen tests mentioned above and the measures that will be taken in this respect, or to arrange for these to be documented. If necessary, the PA can instruct the CSP to perform additional pen tests.
Comment	CLARIFICATION Substantial changes include: • New software; • New version of existing software, excluding patches; • Changes in infrastructuur. As guidance for the selection of suppliers, the CSP can use the recommendation in chapter 4 ("Supplier Selection") as described in the latest version of the whitepaper entitled "Pentesten doe je zo[3]" (how to perform penetration testing) published by the NCSC.

[3] *http://www.govcert.nl/binaries/live/govcert/hst%3Acontent/dienstverlening/kennis-en-publicaties/whitepapers/pentesten-doe-je-zo/pentesten-doe-je-zo/govcert%3AdocumentResource/govcert%3Aresource*

7 Certificate, CRL and OSCP profiles

7.1 Certificate Profile

RFC 3647	7.1 Certificate profile	
Number	7.1-pkio121	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- 7.3.3.a 7.3.3.a
PKIo	The CSP has to issue certificates in accordance with the requirements stipulated in that respect in appendix A of the applicable PoR part for that type of certificate, namely "Certificate profiles".	

7.2 CRL Profile

RFC 3647	7.2 CRL profile	
Number	7.2-pkio122	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- 7.3.6.g 7.3.6.i
PKIo	The CSP has to issue CRLs in accordance with the requirements stipulated in that respect in appendix A of this document, "CRL and OCSP profiles".	

7.3 OCSP Profile

Contains no basic 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

Contains no basic requirements.

9.5 Intellectual Property Rights

RFC 3647	9.5 Intellectual property rights
Number	9.5-pkio126
ETSI	ETSI does not cover a violation of intellectual property rights
PKIo	The CSP indemnifies the subscriber in respect of claims by third parties due to violations of intellectual property rights by the CSP.

9.8 Limitations of Liability

RFC 3647	9.8 Limitations of liability	
Number	9.8-pkio135	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- 6.4 6.4
PKIo	Within the scope of certificates, as mentioned in paragraph 1.4 in this CP the CSP is not allowed to place restrictions on the value of the transactions for which certificates can be used.	

9.12 Amendments

The change procedure for the PoR of the PKIoverheid is incorporated in PKIoverheid's Certificate Practice Statement. The CPS can be obtained in an electronic format on the PA's website:

https://www.logius.nl/producten/toegang/pkioverheid/documentatie/cps/

RFC 3647	9.12.2 Notification mechanism and period	
Number	9.12.2-pkio136	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	- 7.1.a 7.1.a

PKIo	If a published amendment of the CP can have consequences for the end users, the CSPs will announce the amendment to the subscribers and/or certificate holders registered with them in accordance with their CPS.

RFC 3647	9.12.2 Notification mechanism and period
Number	9.12.2-pkio137
ETSI	This subject is not covered in ETSI.
PKIo	The CSP has to provide the PA with information about the intention to amend the CA structure. Consider, for example, the creation of a sub-CA.

This CP and the approved amendments made to it can be obtained in an electronic format through the Internet on the PA's website. The address of this is: http://www.logius.nl/pkioverheid.

9.13 Dispute Resolution Provisions

RFC 3647	9.13 Dispute resolution provisions	
Number	9.13-pkio138	
ETSI	EN 319 401 EN 319 411-2 TS 102 042	6.5.e - 7.5.f
PKIo	The complaints handling process and dispute resolution procedures applied by the CSP may not prevent proceedings being instituted with the ordinary court.	

9.14 Governing Law

Contains no basic requirements.

Appendix A CRL and OCSP certificate Profiles for certificate status information

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'.

References

1. Guideline 1999/93/EC of the European Parliament and of the European Council of Ministers dated 13 December 1999 concerning a European framework for electronic signatures
2. ITU-T Recommendation X.509 (1997) | ISO/IEC 9594-8: "Information Technology – Open Systems Interconnection – The directory: Public key and attribute certificate frameworks".
3. ITU-T Recommendation X.520 (2001) ISO/IEC 9594-6: "Information Technology – Open Systems Interconnection – The directory: Selected Attribute Types".
4. RFC 2560: "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP".
5. RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and CRL Profile".
6. RFC 3739: "Internet X.509 Public Key Infrastructure Qualified Certificates Profile".
7. OID RA management_PKI overheid – OID scheme.
8. ETSI TS 101 862: "Qualified certificate profile", version 1.3.3 (2006-01).
9. ETSI TS 102 280 : "X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons", version 1.1.1 (2004-03).
10. ETSI TS 102 176-1 : "Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms", version 2.0.0 (2007-11).
11. ISO 3166 "English country names and code elements".

General requirements

- End user certificates MUST correspond with the X.509v3 standard for public key certificates. General requirements in relation to certificates are listed in RFC 5280.
- The [X.509] standard allows unlimited extension of the attributes within a certificate. In connection with interoperability requirements, this may not be used within the PKI for the government. Only

attributes indicated in this appendix as Compulsory, Optional or Advised Against may be used.

- The certificate for the electronic signature MUST correspond with the EESSI Qualified Certificate profile (ETSI TS 101 862). If there are any differences between TS 101 862 and RFC 3739, TS 101 862 prevails.
- Personal certificates MUST correspond with the standard ETSI TS 102 280 as far as the certificate profile is concerned. If there are any differences between TS 102 280 and TS 101 862, RFC 5280, TS 102 280 prevails.

Profile of the CRL

General requirements in relation to the CRL

- The CRLs have to fulfil the X.509v3 standard for public key certificates and CRLs.
- A CRL contains information about revoked certificates that fall within the current period of validity or of which the period of validity expired less than 6 months ago (in accordance with the Electronic Signatures Act).

CRL attributes

Field / Attribute	Criteria	Description	Standard reference[1]	Type	Explanation
Version	V	MUST be set to 1 (X.509v2 CRL profile).	RFC 5280	Integer	Describes the version of the CRL profile, the value 1 stands for X.509 version 2.
Signature	V	MUST be set to the algorithm, as stipulated by the PA.	RFC 5280	OID	MUST be the same as the field signatureAlgorithm. For maximum interoperability, for certificates under the G1 root certificate, only sha-1WithRSAEncryption is allowed. For certificates under the G2 root certificate, only sha-256WithRSAEncryption is allowed.
Issuer	V	MUST contain a Distinguished Name (DN). The field has attributes as described in the following rows.	PKIo, RFC 5280		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.	ISO3166, X.520	Printable String	C = NL for CSPs located in the Netherlands.
Issuer.stateOrProvinceName	N	Is not used.	PKIo	UTF8String	-
Issuer.OrganizationName	V	Full name in accordance with the accepted document or basic registry	ETSI TS 102280: 5.2.4	UTF8String	
Issuer. organizationalUnitName	O	Optional specification of an organizational entity. This field MUST NOT include a	ETSI TS 102280: 5.2.4	UTF8String	Several instances of this attribute MAY be used.

Field / Attribute	Criteria	Description	Standard reference[1]	Type	Explanation
		function indication or similar. It may include, if applicable, the types of certificates that are supported.			
Issuer.localityName	N	Is not used.	PKIo	UTF8String	-
Issuer.serialNumber	O	MUST be used 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 5280	UTF8String	
ThisUpdate	V	MUST indicate the date and time on which the CRL is amended.	RFC 5280	UTCTime	MUST include the issuance date of the CRL in accordance with the applicable policy set out in the CPS.
NextUpdate	V	MUST indicate the date and time of the next version of the CRL (when it can be expected).	PKIo, RFC 5280	UTCTime	This is the latest date on which an update can be expected, however an earlier update is possible. MUST be completed in accordance with the applicable policy set out in the CPS.
revokedCertificates	V	MUST include the date and time of revocation and *serialNumber* of the revoked certificates.	RFC 5280	SerialNumbers, UTCTime	If there are no revoked certificates, the revoked certificates list MUST NOT be present.

CRL extensions

Field / Attribute	Criteria	Critical?	Description	Standard reference[1]	Type	Explanation
authorityKeyIdentifier	O	No	This attribute is interesting if a CSP 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 CSP/CA).
IssuerAltName	A	No	This attribute allows alternative names to be used for the CSP (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.
CRLNumber	V	No	This attribute MUST contain an incremental number that provides support when determining the order of CRLs (the CSP 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.

Field / Attribute	Criteria	Critical?	Description	Standard reference[1]	Type	Explanation
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.
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 CSP 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	

Profile OCSP

General requirements in respect of OCSP

- If the CSP supports the Online Certificate Status Protocol (OCSP), OCSP responses and OCSPSigning certificates MUST fulfil the requirements relating to this stipulated in IETF RFC 2560.
- OCSPSigning certificates MUST correspond with the X.509v3 standard for public key certificates. General requirements in relation to certificates are listed in RFC5280
- The [X.509] standard allows unlimited extension of the attributes within a certificate. In connection with interoperability requirements, this may not be used within the PKI for the government. Only attributes indicated in this appendix as Compulsory (V), Optional (O) or Advised Against (A) may be used.
- OCSPSigning certificates must fulfil the profile for services certificates indicated above, with the following exceptions:

OCSP Signing certificate attributes

Field / Attribute	Criteria	Critical?	Description	Standard reference	Type	Explanation
Issuer	V		MUST contain a Distinguished Name (DN).	PKIo		An OCSPSigning certificate MUST be issued under the hierarchy of the PKI for the government.

Field / Attribute	Criteria	Critical?	Description	Standard reference	Type	Explanation
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 OCSPSigning certificates, the digitalSignature bit MUST be incorporated and the extension marked as being critical. The non-Repudiation bit MUST NOT be included.	RFC 5280, RFC 2560	BitString	
CertificatePolicies	V	No	MUST contain the OID of the PKIoverheid certificate policy (CP) for authenticity certificates, the URI of the CPS, and a user notice. The OID schedule to be used in the PKI for the government is described in the CP - Services.	RFC 3739	OID, String, String	For services authentication certificates in the Government/Companies domain the OID is: 2.16.528.1.1003.1.2.2.4. For services authentication certificates in the Organization domain the OID is: 2.16.528.1.1003.1.2.5.4.
ExtKeyUsage	V	Yes	MUST be used with the value id-kp-OCSPSigning.	RFC 5280		
ocspNoCheck	V/O		The CA/B Forum Baseline Requirements require the use of the ocspNoCheck for publicly trusted server and EV certificates. For the other PKIoverheid certificates the use is optional.	RFC 2560		The CA/B Forum Baseline Requirements require the use of the ocspNoCheck. It is therefore not clear how browsers are to react on OCSP responder certificates without a ocspNoCheck extension. Browsers will most probably not check the status of an ocsp signing certificate without the extension.

10 Revisions

10.1 Amendments between version 4.0 and 4.1

10.1.1 New

None.

10.1.2 Modifications

- Requirement 6.7.1-pkio120 (effective date no later than 01-09-2015)

10.1.3 Editorial

- Small editiorial changes to the following requirements:
  - 2.2-pkio5;
  - 5.3-pkio78;
  - 6.2.5-pkio103;
  - 6.7.1-pkio118;
  - 6.7.1-pkio119;
  - 6.7.1-pkio120;
  - 9.12.2-pkio136.

10.2 Amendments between version 3.7 and 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 basic and additional requirements;
- Requirement 3.3.1-pkio45;
- Requirement 6.5.1-pkio116;
- Requirement 4.5.2-pkio52.

10.2.3 Editorial

None