Logius
*Ministerie van Binnenlandse Zaken en Koninkrijksrelaties*

# Programme of Requirements part 3e: Certificate Policy – Extended Validation

Date 28 January 2014

EV policy OID 2.16.528.1.1003.1.2.7

Publisher's imprint

| | |
|---|---|
| Version number | 3.6 |
| 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

**Contents** 3

**1 Introduction to the Certificate Policy** 7

*1.1 Overview* 7

1.1.1 Design of the Certificate Policy 7

1.1.2 Relationship between CP and CPS 8

1.1.3 Status 8

*1.2 References to this CP* 8

*1.3 User community* 8

*1.4 Certificate Usage* 9

*1.5 Contact information Policy Authority* 9

**2 Publication and Repository Responsibilities** 10

*2.1 Electronic Repository* 10

*2.2 Publication of CSP Information* 10

*2.4 Access to Published Information* 12

**3 Identification and Authentication** 14

*3.1 Naming* 14

*3.2 Initial identity validation* 14

*3.3 Identification and Authentication for Re-key Requests* 22

**4 Certificate Life-Cycle Operational Requirements** 24

*4.1 Certificate Application* 24

*4.4 Certificate Acceptance* 25

*4.5 Key Pair and Certificate Usage* 26

*4.9 Certificate Revocation and Suspension* 26

*4.10 Certificate Status Services* 32

**5 Facility, Management and Operational Controls** 34

*5.2 Procedural Controls* 34

*5.3 Personnel Controls* 35

*5.4 Audit Loggin Procedures* 37

*5.5 Records archival* 38

*5.7 Compromise and Disaster Recovery* 39

**6 Technical Security Controls** 42

*6.1 Key Pair Generation and Installation* 42

*6.2 Private Key Protection and Cryptographic Module Engineering Controls* 43

*6.3 Other Aspects of Key Pair Management* ..... *45*
*6.4 Activation data* ..... *45*
*6.5 Computer Security Controls* ..... *46*
*6.6 Life Cycle Technical Controls* ..... *47*
*6.7 Network Security Controls* ..... *47*

**7 Certificate, CRL and OSCP profiles ..... 49**
*7.1 Certificate Profile* ..... *49*
*7.2 CRL Profile* ..... *49*
*7.3 OCSP Profile* ..... *49*

**8 Compliance Audit and Other Assessments ..... 50**

**9 Other Business and Legal Matters ..... 51**
*9.2 Financial Responsibility* ..... *51*
*9.5 Intellectual Property Rights* ..... *52*
*9.6 Representations and Warranties* ..... *52*
*9.8 Limitations of Liability* ..... *53*
*9.12 Amendments* ..... *53*
9.12.1 Amendment procedure ..... 53
*9.13 Dispute Resolution Provisions* ..... *54*
*9.14 Governing Law* ..... *54*
*9.17 Miscellaneous provisions* ..... *54*

**Appendix A Profiles certificates and certificate status information ..... 55**

**Appendix B Reference matrix ..... 79**

**10 Revisions ..... 105**
*10.1 Amendments from version 3.5 to 3.6* ..... *105*
10.1.1 New ..... 105
*10.2 Amendments from version 3.4 to 3.5* ..... *105*
10.2.1 New ..... 105
10.2.2 Modifications ..... 105
*10.3 Amendments from version 3.3 to 3.4* ..... *105*
10.3.1 New ..... 105
10.3.2 Modifications ..... 105
10.3.3 Editorial ..... 105
*10.4 Amendments from version 3.2 to 3.3* ..... *106*
10.4.1 New ..... 106
10.4.2 Modifications ..... 106
10.4.3 Editorial ..... 106
*10.5 Amendments from version 3.1 to 3.2* ..... *106*
10.5.1 New ..... 106
10.5.2 Modifications ..... 106

10.5.3 Editorial ........ 106

*10.6 Amendments from version 3.0 to 3.1 ........ 106*

10.6.1 New ........ 106

10.6.2 Modifications ........ 107

10.6.3 Editorial ........ 107

*10.7 Version 3.0 ........ 107*

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

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

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

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

*Revision control*

| **Version** | **Date** | **Description** |
|---|---|---|
| 1.0 | 07-12-2010 | Definitive version |
| 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 January 2013 |
| 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 |

# 1 Introduction to the Certificate Policy

## 1.1 Overview

This is part 3e of the Programme of Requirements (PoR) for the PKI for the government and is known as the Certificate Policy (CP) Extended Validation (EV). 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. This document only relates to the Extended Validation (EV) SSL certificates and EV issuing subordinate CA certificates issued by CSPs under the State of the Netherlands EV Root CA.

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 current version of the standard ETSI TS 102 042 EVCP+, combined with the PTC-BR and Netsec (ETSI CP OID 0.4.0.2042.1.4);
- that are specifically drawn up by and for the PKIoverheid Extended Validation.

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[2]. |
| **Number** | Unique number of the PKIo requirement. In each paragraph, consecutive numbering is used for the PKIo requirements. In combination with the RFC 3647 paragraph number, this forms a unique label for the PKIo requirement. |
| **ETSI** | Reference to the requirement(s) from ETSI TS 102 042 from which the PKIo requirement is derived or which provides further detail. |
| **PKIo** | The PKIo Extended Validation requirement that applies within the PKI for the government. |

[1] *For clarification of positioning of the requirements applicable within the PKI for the government, reference is made 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*

| | |
|---|---|
| **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. |

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 EV SSL certificates and certifcate 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, the matrix contains a reference to the applicable requirements within the PKI for the government. A distinction is made between requirements originating from Dutch law, requirements from ETSI TS 102 042 V2.2.1 (2011-12) and the PKIo requirements.

### *1.1.2 Relationship between CP and CPS*

This CP describes the minimum requirements stipulated in respect of services, in terms of EV SSL certificates, of a Certification Service Provider (CSP) within the PKI for the government. The Certification Practice Statement for EV certificates within the PKI for the government states how these services should be interpreted, insofar as this falls under the direct responsibility of the PA.

### *1.1.3 Status*

This is version 3.6 of part 3e of the PoR. The current version has been updated up to January 2014 inclusive.

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

Each CP is uniquely identified by an OID. The following OID is registered by PKIoverheid for inclusion in all EV certificates:

EV policy OID **2.16.528.1.1003.1.2.7**

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). ev (7).

## 1.3 User community

The user community consists of subscribers located in the Netherlands, that are organizational entities within the government and business world (see PKIo 3.2.2) and of certificate holders that belong to these subscribers. In addition there are relying parties, who act with a reliance on certificates of the relevant certificate holders.

The parties within the user community are subscribers, certificate managers, certificate holders and relying parties.

- A subscriber is a natural or legal personality who enters into an agreement with a CSP on behalf of one or more certificate holders for the certification of public keys.
- A certificate holder is an entity, characterized in a certificate as the holder of the private key that is linked to the public key provided in the certificate. The certificate holder is part of an organizational entity, for which a subscriber is the contracting party.

  Within the Certificate Policy Extended Validation, the term certificate holder means:
  a device or a system (a non-natural person), operated by or on behalf of an organizational entity;

  In this CP we use the name "service" for the foregoing certificate holders. To perform the actions in respect of the lifecycle of the certificate holder's certificate, intervention by a party other than the certificate holder is required. The subscriber is responsible for this and has to appoint a certificate manager to perform these actions.
- A certificate manager is a natural person who performs actions on behalf of the subscriber in respect of the certificate holder's certificate. The subscriber instructs the certificate manager to perform the relevant actions and records these in a certificate manager's testimony.
- A relying party is every natural or legal personality who is a recipient of a certificate and who acts with a reliance on that certificate. Differently than with personal certificates, relying parties mainly derive security from the connectedness of a service (device or feature) to the organizational entity to which the service belongs. The CP Extended Validation therefore place the emphasis on offering security regarding the connectedness of a message sent by or a web service provided by a device, system or (staff) position with the relevant organization. In view of this, establishing the identity of the certificate holder (device or feature) is less important than establishing the certificate holder's connectedness to the organizational entity.

## 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 2.16.528.1.1003.1.2.7 ] EV SSL certificates that are issued under this CP, can be used to safeguard a connection between a specific client and a server, via the TLS/SSL protocol, that is part of the organizational entity that is listed as the subscriber in the relevant certificate.

## 1.5 Contact information Policy Authority

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

# 2 Publication and Repository Responsibilities

## 2.1 Electronic Repository

| | |
|---|---|
| **RFC 3647** | 2.1 Electronic repository |
| **Number** | 1 |
| **ETSI** | 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 |
| **ETSI** | 7.3.1.c<br>7.3.4.b<br>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 102 042. 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** | 1 |
| **ETSI** | 7.1.b<br>7.3.1.c |
| **PKIo** | The CPS only has to relate to the issue of EV SSL certificates and has to be drawn up in Dutch. The layout of this CPS has, as far as possible, to be set up in accordance with the RFC3647[3] standard. |

| | |
|---|---|
| **RFC 3647** | 2.2 Publication of CSP information |

[3] http://www.ietf.org/rfc/rfc3647.txt?number=3647

| | |
|---|---|
| **Number** | 2 |
| **ETSI** | 5.2.b |
| **PKIo** | The CSP has to include the Extended Validation OID of this CP in its CPS. |

| | |
|---|---|
| **RFC 3647** | 2.2 Publication of CSP information |
| **Number** | 3 |
| **ETSI** | 7.3.1.c |
| **PKIo** | All information has to be available in Dutch. |

| | |
|---|---|
| **RFC 3647** | 2.2 Publication of CSP information |
| **Number** | 4 |
| **ETSI** | 7.1.b<br>7.1.d.2 |
| **PKIo** | The following clause has to be incorporated in the CPS and in all agreements with parties that are involved in the issue of the EV SSL certificates of the CSP (such as, for example, the Registration Authority): "CSP [name] conforms to the current version of the CA/Browser Forum Guidelines for Issuance and Management of Extended Validation Certificates as published at http://www.cabforum.org. In the event of an inconsistency between the PKIoverheid Programme of Requirements part 3e and the relevant Requirements, because of which it is not possible to (at the very least) fulfil the minimum requirements, which is at the discretion of the PA, the provisions in the Requirements shall prevail." |

| | |
|---|---|
| **RFC 3647** | 2.2 Publication of CSP information |
| **Number** | 5 |
| **ETSI** | 7.3.1.h.iii |
| **PKIo** | In its CPS the CSP has to state that during the time that an EV SSL certificate is valid it guarantees when issuing an EV SSL certificate that it has followed the requirements in the CA/Browser Forum Guidelines for Issuance and Management of Extended Validation Certificates and this CP and that it has checked the information as incorporated in the EV SSL certificate for correctness and completeness.<br>In its CPS, at the very least the CSP has to define that it guarantees that:<br>• the subscriber is an existing and legal organization, and; |

| | |
|---|---|
| | • the name of the subscriber corresponds with the name given in a recently certified excerpt (maximum 1 month old) from the Chamber of Commerce's Trade Register or, with regard to government organizations, if registration in the Trade Register has not yet taken place, corresponds with the entry in the most recent version of the State Almanac;<br>• if it has reasonably taken all necessary verification steps to verify that the subscriber is the registered owner of the domain name as stated in the EV SSL certificate, and;<br>• if it has reasonably taken all necessary verification steps to verify that the subscriber has authorized the issue of the EV SSL certificate, and;<br>• if it has reasonably taken all necessary verification steps to verify that all other information in the EV SSL certificate is correct effective from the date of issue of the EV SSL certificate, and;<br>• it enters into a legally enforceable agreement with a subscriber that is based on the requirements described in this CP, and;<br>• it offers revocation information that is available online 24x7 with information about the status of an EV SSL certificate, and;<br>• when issuing EV SSL certificates, it will comply with and execute all requirements described in this CP and will revoke an EV SSL certificate if necessary. |

| | |
|---|---|
| **RFC 3647** | 2.2 Publication of CSP information |
| **Number** | 6 |
| **ETSI** | 4.5.1 |
| **PKIo** | The CSP has to describe the primary and secondary purpose of EV SSL certificates in the CPS. In addition, the CSP has to describe in detail in the CPS what the EV SSL certificates are not intended for. |

| | |
|---|---|
| **RFC 3647** | 2.2 Publication of CSP information |
| **Number** | 7 |
| **ETSI** | 7.1.d.3 |
| **PKIo** | The certificate policy statement of the CSP has to be structured in accordance with RFC 2527, RFC 3647 or the Programme of Requirements of PKIoverheid that is based on RFC 3647 and has to include all relevant chapters described in RFC 2527, RFC 3647 or the PoR of PKIoverheid. |

## 2.4 Access to Published Information

| | |
|---|---|
| **RFC 3647** | 2.4 Access to published information |
| **Number** | 1 |

| | |
|---|---|
| **ETSI** | 7.1.b<br>7.1.d.1 |
| **PKIo** | It has to be possible for anyone to consult the CPS of a Certification Service Provider within PKIoverheid. |
| **Comment** | 'Anyone' means that, in addition to the subscribers, certificate holders and manager s, every potential relying party has to be able to consult the CPS. |

# 3 Identification and Authentication

## 3.1 Naming

| | |
|---|---|
| **RFC 3647** | 3.1.1 Types of names |
| **Number** | 1 |
| **ETSI** | 7.3.3.a<br>7.3.6.i |
| **PKIo** | The CSP has to fulfil the requirements laid down for name formats in the Programme of Requirements, part 3 – appendix A Certificate, CRL and OCSP profiles. |
| **Comment** | Appendix A provides clarification of the various profiles. |

## 3.2 Initial identity validation

| | |
|---|---|
| **RFC 3647** | 3.2.0 Initial identity validation |
| **Number** | 1 |
| **ETSI** | 7.3.3.a.x |
| **PKIo** | The information used by the CSP to verify:<br>▪ whether the subscriber is an existing and legal organization;<br>▪ whether the organization name in the certificate is correct and complete and corresponds with the organization name registered by the subscriber.<br>▪ whether the address of the organization provided by the subscriber is correct and complete and that it is also the address where it performs its activities;<br>▪ whether the organization's general telephone number provided by the subscriber is correct and complete;<br>▪ or, if it is found that the subscriber's organization has existed for less than three years, that the subscriber has an active current account;<br>may not be older than 13 months, otherwise the information has to once again be requested and verified. In those cases where the sources of information have not be updated or modified for the past 13 months, the most recent version must be assumed. |

| | |
|---|---|
| **RFC 3647** | 3.2.1. Method to prove possession of  private key |
| **Number** | 1 |
| **ETSI** | 7.3.1 |
| **PKIo** | The CSP is responsible for ensuring that the subscriber supplies the certificate signing request (CSR) securely. To supply this securely, the following has to be taken into account: |

| | |
|---|---|
| | • the entry of the CSR on the CSP's application especially developed for that purpose, where an SSL connection is used, which uses a PKIoverheid SSL certificate or similar or;<br>• the entry of the CSR on the HTTPS website of the CSP that uses a PKIoverheid SSL certificate or similar or;<br>• sending the CSR by e-mail, along with a qualified electronic signature of the certificate manager that uses a PKIoverheid qualified certificate or similar or;<br>• the entry of or sending a CSR in a way that is at least equivalent to the aforementioned ways. |

| | |
|---|---|
| **RFC 3647** | 3.2.2 Authentication of organizational entity |
| **Number** | 1 |
| **ETSI** | 7.3.1.d<br>7.3.1.h.i<br>7.3.1.r<br>7.3.1.t |
| **PKIo** | The CSP has to verify that the subscriber is an existing and legal organization.<br><br>As evidence that it is an existing and legal organization, the CSP has to request and verify at least the following supporting documents:<br>▪ For government organizations, a recently certified excerpt (no more than 1 month old) from the Chamber of Commerce's Trade Register or a law, deed of incorporation or a general governmental decree;<br>▪ For bodies governed by private law with and without a legal personality with a recently certified excerpt (maximum 1 month old) from the Chamber of Commerce's Trade Register.<br><br>As proof that it is a legal organization, the CSP has to find out whether this appears on the latest EU list of prohibited terrorists and terrorist organizations, published by the European Council<br>These lists can be found on the web page:<br>http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32001E0931:NL:NOT<br>These are decisions concerning updating the list of people, groups and entities referred to in articles 2, 3 and 4 of Common Position 2001/931/GBVB concerning the use of specific measures to combat terrorism. |

| | |
|---|---|
| **RFC 3647** | 3.2.2 Authentication of organizational entity |
| **Number** | 2 |
| **ETSI** | 7.3.1.d<br>7.3.1.h.i |

| | |
|---|---|
| **PKIo** | The CSP has to verify that the organization name shown on the certificate is correct and complete and corresponds with the organization name provided by the subscriber.<br><br>As proof of the correctness of the official organizational name that has been provided<br>the CSP has to request and verify, at the very least, the following supporting documents:<br>▪ For government organizations, a recently certified excerpt (maximum 1 month old) from the Chamber of Commerce's Trade Register or, if registration in the Trade Register has not yet taken place, a copy of the relevant page from the latest version of the State Almanac in which the address of the relevant government organization is given;<br>▪ For bodies governed by private law with and without a legal personality with a recently certified excerpt (maximum 1 month old) from the Chamber of Commerce's Trade Register. Furthermore it applies that the supporting document that has been provided has to distinguish the organizational entity from any other organizations with the same name. In general, in an excerpt from the Chamber of Commerce's Trade Register, the official name of the organization is also given. |

| | |
|---|---|
| **RFC 3647** | 3.2.2 Authentication of organizational entity |
| **Number** | 3 |
| **ETSI** | 7.3.1.d<br>7.3.1.h.i<br>7.3.1.l |

| | |
|---|---|
| **PKIo** | The CSP has to verify whether the address of the organization provided by the subscriber is correct and complete and that it is also the address where it performs its activities;<br>Understood to be meant by address is only the street name, house number (if applicable with addition) postcode and town/city.<br>As proof of the correctness and the existence of the address that is given and that it is also the address where the organization performs its activities, at the very least the CSP has to request and verify the following supporting documents:<br>▪ For government organizations, a recently certified excerpt (maximum 1 month old) from the Chamber of Commerce's Trade Register or, if registration in the Trade Register has not yet taken place, a copy of the relevant page from the latest version of the State Almanac in which the address of the relevant government organization is given;<br>▪ For bodies governed by private law with and without a legal personality with a recently certified excerpt (maximum 1 month old) from the Chamber of Commerce's Trade Register.<br>If the address in the supporting documents corresponds with the address of the request, the CSP can consider this to be sufficient proof that this is also the address where the organization performs its activities.<br>If the address in the supporting documents does not correspond, then the CSP has to visit the location given by the subscriber and record its findings in a report. This report has to include, at the very least, the following:<br>▪ Whether the address of the subscriber's location corresponds exactly with the address provided in the application;<br>▪ The type of accommodation of the subscriber and whether this is the location where the organization in all probability performs its activities;<br>▪ Whether permanent signs are present that identify the subscriber's location;<br>▪ One or more photos of (i) the outside of the subscriber's accommodation (which shows the signs, if present, and the street (address) sign) and (ii) the reception desk or office space of the subscriber.<br>As an alternative, the CSP may also accept a declaration from an external accountant or notary in which the address that has been provided is confirmed and also that this is the address where the organization performs its activities. |

| | |
|---|---|
| **RFC 3647** | 3.2.2 Authentication of organizational entity |
| **Number** | 4 |
| **ETSI** | 7.3.1.d<br>7.3.1.h.i |

| | |
|---|---|
| **PKIo** | The CSP has to verify that the organization's general telephone number provided by the subscriber is correct and complete.<br>As proof of correctness and the existence of the organization's general telephone number that has been provided, the CSP has to:<br>▪ dial the relevant telephone number and verify that the subscriber can indeed be reached on the telephone number provided, and;<br>▪ verify the organization's general telephone number in the latest version of the (online) Telephone Directory or by means of an authorized excerpt (no more than 1 month old) from the Chamber of Commerce's Trade Register, or;<br>▪ receive a declaration from an external accountant or notary in which the subscriber's general telephone number that has been provided is confirmed. |

| | |
|---|---|
| **RFC 3647** | 3.2.2 Authentication of organizational entity |
| **Number** | 5 |
| **ETSI** | 7.3.1.d<br>7.3.1.h.i |
| **PKIo** | If, based on the information that is requested, it is found that the subscriber's organization has existed for less than three years (counting from the date of registration in the Trade Register or the date of publication of a law or general governmental decree until the date on which the EV SSL certificate application was signed) then the CSP has to verify that the subscriber is able to take part in the business because it has an active current account.<br>As proof of correctness and the existence of the current account that is provided, the CSP has to request and verify at least one of the following supporting documents:<br>▪ A declaration from a financial establishment that has a licence from The Dutch Bank in the Netherlands and is covered by the Dutch deposit guarantee scheme, which shows that the subscriber has an active current account;<br>▪ A declaration from an external accountant that the subscriber has a current account at a financial establishment that has a licence from The Dutch Bank in the Netherlands and is covered by the Dutch deposit guarantee scheme; |

| | |
|---|---|
| **RFC 3647** | 3.2.3 Authentication of individual identity |
| **Number** | 1 |
| **ETSI** | 6.2 Note 2<br>7.3.1.r |

|  |  |
|---|---|
| **PKIo** | The CSP has to verify who the Authorized Representative (or Representation) of the subscriber is.<br>As proof of the accuracy and the existence of the Authorized Representative (or Representation) provided by the subscriber, at the very least, the CSP has to request and verify the following supporting documents:<br>• For governmental organizations, a recently certified excerpt (maximum 1 month old) from the Chamber of Commerce's Trade Register or, if registration in the Trade Register has not yet taken place, a copy of the relevant page from the latest version of the State Almanac[4] in which the Authorized Representative (or Representation) is listed;<br>• For organizational entities within the business world, a recently certified excerpt (maximum 1 month old) from the Chamber of Commerce's Trade Register which lists the Authorized Representative (or Representation).<br>The CSP must also find out whether the Authorized Representative appears on the latest EU list of prohibited terrorists and terrorist organizations:<br>http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:028:0057:0059:EN:PDF<br>The CSP may not issue an EV SSL certificate to an organization or its Authorized Representative on this list. |

|  |  |
|---|---|
| **RFC 3647** | 3.2.3 Authentication of individual identity |
| **Number** | 2 |
| **ETSI** | 7.3.1.d<br>7.3.1.k<br>7.3.3.a.x |
| **PKIo** | In accordance with Dutch legislation and regulations, the CSP has to check the identity and, if applicable, specific properties of the certificate manager. Proof of the identity has to be checked based on the physical appearance of the person himself.<br>This check has to be repeated every 13 months, unless this is explicitly deviated from in the agreement with the subscriber by, for example, stating that the certificate manager retains his or her role until this is reviewed by the subscriber or until the agreement expires or is terminated. |

|  |  |
|---|---|
| **RFC 3647** | 3.2.3 Authentication of individual identity |
| **Number** | 3 |
| **ETSI** | 7.3.1.d<br>7.3.1.k<br>7.3.1.r |

[4] http://staatsalmanak.sdu.nl/do/welkom

| | |
|---|---|
| **PKIo** | To detail the provisions in 3.2.3-2, the identity of the certificate manager can only be established using the valid documents referred to in article 1 of the Compulsory Identification Act. The CSP has to check the validity and authenticity of these documents.<br><br>The CSP must also find out whether the certificate manager appears on the latest EU list of prohibited terrorists and terrorist organizations:<br>http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:028:0057:0059:EN:PDF<br>The CSP may not issue an EV SSL certificate to an organization or its certificate manager that is included on this list |

| | |
|---|---|
| **RFC 3647** | 3.2.3 Authentication of individual identity |
| **Number** | 4 |
| **ETSI** | 7.3.1.g<br>7.3.1.k<br>7.3.3.a.x |
| **PKIo** | The certificate manager is a person whose identity has to be established in conjunction with an organizational entity. Proof has to be submitted of:<br>▪ full name, including surname, first name, initials or other first (names) (if applicable) and surname prefixes (if applicable);<br>▪ date of birth and place of birth, a nationally applicable registration number, or other characteristics of the certificate manager that can be used in order to, as far as possible, distinguish this person from other persons with the same name;<br>▪ proof that the certificate manager is entitled to receive a certificate for a certificate holder on behalf of the legal personality or other organizational entity. This proof may not be older than 13 months, otherwise the information has to be requested and verified again, unless in the agreement with the subscriber, it explicitly states that the certificate manager retains his or her authorization until the time at which this is reviewed by the subscriber or until the agreement expires or is terminated. |

| | |
|---|---|
| **RFC 3647** | 3.2.5 Validation of authority |
| **Number** | 1 |
| **ETSI** | 7.3.1.d<br>7.3.1.k<br>7.3.1.m.vi |
| **PKIo** | The CSP has to check that:<br>▪ the proof that the certificate holder, authorized to request and receive a certificate on behalf of the subscriber, is authentic;<br>▪ or the certificate manager has received permission from the subscriber to perform the actions that he has been asked to perform (if the certificate manager performs the registration process). |

| | |
|---|---|
| **Comment** | The "certificate manager" who takes over those actions from the certificate holder does not necessarily have to be the same person as the systems manger or personnel officer. Also the knowledge of the activation data of the key material (for example PIN) can be shared by various people if the organization of the management requires that. However, it is recommended that as few people as possible should be aware of the PIN. It would also be wise to take measures that restrict access to the PIN. An example of this is placing the PIN in a safe to which only authorized persons can gain access in certain situations. |

| | |
|---|---|
| **RFC 3647** | 3.2.5 Validation of authority |
| **Number** | 2 |
| **ETSI** | 6.2.h |
| **PKIo** | The agreement that the CSP enters into with the subscriber should include the fact that the subscriber is responsible for immediately informing the CSP when relevant changes are made to the relationship between the subscriber and certificate manager and/or service. When the service no longer exists, this has to take place by means of a revocation request. |

| | |
|---|---|
| **RFC 3647** | 3.2.5 Validation of authority |
| **Number** | 3 |
| **ETSI** | 7.3.1.i.i<br>7.3.1.r<br>7.3.3.a.x |
| **PKIo** | The CSP has to verify that the subscriber is the registered owner of the domain name listed in the request (FQDN) or that the subscriber is exclusively authorized by the registered domain name owner to use the domain name on behalf of the registered domain name owner.<br>This verification may not be contracted out by the CSP to Registration Authorities or other parties.<br>If the subscriber states that he/she is the registered owner of the domain name listed in the request, the CSP has to:<br>▪ verify that the domain name is registered with a registrar or domain manager, such as SIDN (The Netherlands Internet Domain Registration Foundation), affiliated with the Internet Corporation for Assigned Names and Numbers (ICANN) or an organization that is a member of the Internet Assigned Numbers Authority (IANA), and;<br>▪ use a WHOIS service, of an organization affiliated with or that is a member of ICANN or IANA, that offers the information via HTTPS or the de CSP must use a command line programme if a WHOIS service is used that offers information via HTTP, and;<br>▪ in the WHOIS service, verify the name, the residential address and the administrative contact person of the organization and compare this |

| | |
|---|---|
| | information to the verified subscriber information and establish that there are no inconsistencies between the two sets of information, and;<br>▪ The CSP must verify that the domain name does not appear on a spam list and/or phishing black list. Use, to this end, at least http://www.phishtank.com.<br>If the domain name is mentioned on phish tank or a different black list that is consulted, during the verification process the CSP has to deal particularly carefully with the request for the relevant services server certificate.<br><br>The information that the CSP uses to verify that the subscriber is the registered owner of the domain name (FQDN) listed in the application may not be older than 13 months, otherwise the information has to be requested and verified again.<br><br>If the subscriber states that it is exclusively authorized by the registered domain name owner to use the domain name on behalf of the registered domain name owner, as well as the checks listed above, the CSP has to:<br>▪ request a declaration from the registered domain name owner (e.g. by e-mail or telephone) in which the registered domain name owner has to confirm that the subscriber has the exclusive right to use the domain name (FQDN), and;<br>▪ request and verify a written and signed declaration from a notary or external accountant which must state for which domain name (FQDN) the subscriber has been given the exclusive user right on behalf of the registered domain name owner, and;<br>▪ verify that the domain name (FQDN) is not a generic TopLevelDomein (gTLD) or country code TopLevelDomein (ccTLD). For these domain names, only the subscriber, as registered domain name owner, is allowed to submit an application.<br><br>A declaration from the registered domain name owner or notary or external accountant may not be older than 13 months. |

## 3.3 Identification and Authentication for Re-key Requests

| | |
|---|---|
| **RFC 3647** | 3.3.1 Identification and authentication for routine re-key |
| **Number** | 1 |
| **ETSI** | 7.3.2.d |
| **PKIo** | 7.3.2.d does not apply. |
| **Comment** | The requirement means that certificates CANNOT be renewed without a re-key for the EV SSL certificate. |

| | |
|---|---|
| **RFC 3647** | 3.3.1 Identification and authentication for routine re-key |
| **Number** | 2 |
| **ETSI** | 7.3.2.c |

| | |
|---|---|
| **PKIo** | Before EV SSL certificates are renewed, it must be verified whether all requirements stated under [3.1] and ]3.2] have been fulfilled. |
| **Comment** | The relevant articles in which the requirements are specified can be found in the reference matrix in appendix B. |

| | |
|---|---|
| **RFC 3647** | 3.3.2 Identification and authentication for re-key after revocation |
| **Number** | 1 |
| **ETSI** | 7.3.2.d |
| **PKIo** | After revocation of the certificate, the relevant keys cannot be recertified.<br>7.3.2.d does not apply. |

# 4 Certificate Life-Cycle Operational Requirements

## 4.1 Certificate Application

| | |
|---|---|
| **RFC 3647** | 4.1 Certificate Application |
| **Number** | 1 |
| **ETSI** | 6.2 Note 2<br>7.3.6 Note 2 |
| **PKIo** | Before an EV SSL certificate is issued, the CSP must enter into an agreement with the subscriber and receive a certificate request signed by the certificate manager.<br>At the very least, the agreement has to fulfil the following conditions:<br>• the agreement has to be signed by the subscriber's Authorized Representative or Representation;<br>• the subscriber must declare that the information that is provided in the context of an EV SSL certificate application process, is complete and correct;<br>• the subscriber must declare that appropriate measures will be taken to ensure that the private key (and the corresponding access information, e.g. a PIN code), belonging to the public key in the relevant EV SSL certificate, is kept under his control and secret and to protect this;<br>• the subscriber must declare that the EV SSL certificate will not be installed and used until the correctness and completeness have been verified;<br>• If the domain name (FQDN) listed in a services server certificate is identifiable and addressable through the Internet, the subscriber has to declare that the services server certificate is only placed on a server that, at the very least, can be reached using one of the FQDNs in this services server certificate;<br>• the subscriber must declare that the EV SSL certificate will only be used in line with the regulation that applies to its business operations and only in relation to the subscriber's activities and in line with the provisions of this agreement;<br>• the subscriber must declare that it will immediately discontinue use of the EV SSL certificate if it becomes clear that the information in the EV SSL certificate is incorrect or incomplete or if there are signs that the private key, belonging to the public key of the relevant EV SSL certificate, has been compromised;<br>• the subscriber must declare that it will immediately discontinue use of the private key, belonging to the public key of the relevant EV SSL certificate, if the validity of the EV SSL certificate has expired or if the EV SSL certificate has been revoked;<br>• The subscriber has to state that it will respond to instructions from the CSP within the period of time stipulated by the CSP in the event of infringement of the private key or certificate misuse;<br>• The subscriber must accept that the CSP is entitled to revoke the EV SSL certificate if the subscriber has violated the user agreement or if the CSP has discovered that the EV SSL certificate is being used for criminal activities, such as phishing, fraud or the dissemination of malware. |
| **RFC 3647** | 4.1 Certificate Application |

| | |
|---|---|
| **Number** | 2 |
| **ETSI** | 7.3.1.u |
| **PKIo** | Before issuing an EV SSL certificate, the CSP has to have received a fully completed application, signed by the certificate manager on behalf of the subscriber. The application must contain the following information:<br>▪ the name of the organization;<br>▪ the domain name (FQDN);<br>▪ Chamber of Commerce number or Government Identification Number;<br>▪ subscriber's address consisting of:<br>o street name and house number;<br>o town or city;<br>o province;<br>o country;<br>o postcode and<br>o general telephone number.<br>▪ certificate manager's name. |

## 4.4 Certificate Acceptance

| | |
|---|---|
| **RFC 3647** | 4.4.1 Conduct constituting acceptance of certificates |
| **Number** | 1 |
| **ETSI** | 7.3.1.m.vi |
| **PKIo** | The CSP has to verify the signature of the Authorized Representative on the subscriber agreement.<br>To verify this, the CSP has to use one of the following methods:<br>▪ if the Authorized Representative has signed the agreement with his or her qualified electronic signature, the CSP has to check the content and the status of the certificate;<br>▪ the CSP can dial the subscriber's general telephone number and ask for the Authorized Representative. The Authorized Representative then has to confirm, by telephone, that it is his or her signature on the agreement;<br>▪ the CSP can send a letter to the subscriber, for the attention of the Authorized Representative. The Authorized Representative then has to confirm by telephone or by e-mail that it is his or her signature on the agreement; |

| | |
|---|---|
| **RFC 3647** | 4.4.1 Conduct constituting acceptance of certificates |
| **Number** | 2 |
| **ETSI** | 7.3.1.m |
| **PKIo** | After a certificate is issued, the certificate holder or certificate manager has to |

| | |
|---|---|
| | specifically confirm the delivery to the CSP of the key material that is part of the certificate. |
| **Comment** | If software-protected keys are used (see [6.2.11-3]), whereby the private key is generated by the certificate manager and not by the CSP, transfer of the key material and receipt confirmation do not apply. The information that is requested in 7.3.1.m still has to be recorded. |

## 4.5 Key Pair and Certificate Usage

| | |
|---|---|
| **RFC 3647** | 4.5.2 Relying party public key and certificate usage |
| **Number** | 1 |
| **ETSI** | 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.<br>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 should not be confused with the authority of the certificate holder to perform a specific transaction on behalf of an organization. The PKI for the government does not arrange authorization; a relying party has to convince itself of that in a different manner. |

| | |
|---|---|
| **RFC 3647** | 4.5.2 Relying party public key and certificate usage |
| **Number** | 2 |
| **ETSI** | 6.3 NOTE 2 |
| **PKIo** | In addition to 4.9.1-1, the CSP has to clearly instruct the subscriber, relying parties and other third parties how they have to report a problem with a certificate. The CSP has to be able to accept and to confirm registered incidents of this nature 24x7. |

## 4.9 Certificate Revocation and Suspension

| | |
|---|---|
| **RFC 3647** | 4.9.1 Circumstances for revocation |
| **Number** | 1 |
| **ETSI** | 7.4.5 NOTE 2<br>7.3.6.a |

| | |
|---|---|
| **PKIo** | Certificates must be revoked when:<br>• the subscriber states that the original request for a certificate was not allowed and the subscriber does not provide consent with retrospective force;<br>• the CSP has sufficient proof that the subscriber's private key (that corresponds with the public key in the certificate) is compromised or if compromise is suspected, or if there is inherent security vulnerability, or if the certificate has been misused in any other way. A key is considered to be compromised in the event of unauthorized access or suspected unauthorized access to the private key, if the private key or SUD is lost or suspected to be lost, if the key or SUD is stolen or suspected to be stolen, or if the key or SUD is destroyed;<br>• a subscriber does not fulfil its obligations outlined in this CP or the corresponding CPS of the CSP or the agreement that the CSP has entered into with the subscriber;<br>• the CSP is informed, or otherwise becomes aware that the use of the domain name in the certificate is no longer legally permitted (e.g. by a judgement of a court);<br>• the CSP is informed or otherwise becomes aware of a substantial change in the information that is provided in the certificate. An example of that is: a change in the name of the certificate holder (service);<br>• the CSP determines that the certificate has not been issued in line with this CP or the corresponding CPS of the CSP or the agreement that the CSP has entered into with the subscriber;<br>• the CSP determines that information in the certificate is incorrect or misleading;<br>• the CSP ceases its work and the CRL and OCSP services are not taken over by a different CSP.<br>• the technical content of the certificate entails an irresponsible risk for subscribers, relying parties and third parties (e.g. browser parties). |
| **Comment** | In addition, certificates can be revoked as a measure to prevent or to combat an emergency. Considered to be an emergency is definitely the compromise or suspected compromise of the private key of the CSP used to sign certificates. |

| | |
|---|---|
| **RFC 3647** | 4.9.2 Who can request revocation |
| **Number** | 1 |
| **ETSI** | 7.3.6.a |
| **PKIo** | The following parties can request revocation of an end user certificate:<br>▪ the certificate manager;<br>▪ the subscriber;<br>▪ the CSP;<br>▪ any other party or person that has an interest, at the discretion of the CSP. |

| | |
|---|---|
| **RFC 3647** | 4.9.3 Procedures for revocation request |
| **Number** | 1 |

| | |
|---|---|
| **ETSI** | 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 Procedures for revocation request |
| **Number** | 2 |
| **ETSI** | 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 Procedures for revocation request |
| **Number** | 3 |
| **ETSI** | 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** | 4.9.3 Procedures for revocation request |
| **Number** | 4 |
| **ETSI** | 6.3 Note 1<br>7.3.6.h.iii<br>7.3.6.j.iii (and Electronic Signature Directive article 2 paragraph 1l)<br>7.3.6.k |
| **PKIo** | The CSP has to use an OCSP and a CRL to make the certificate status information available. 7.3.6.l does not apply. |

| | |
|---|---|
| **RFC 3647** | 4.9.3 Procedures for revocation request |
| **Number** | 5 |
| **ETSI** | 6.3 Note 1<br>7.3.6.h.iii<br>7.3.6.j.iii<br>7.3.6.k |
| **PKIo** | The revocation management services have to be available 24 hours a day, 7 |

| | |
|---|---|
| | days a week. |

| | |
|---|---|
| **RFC 3647** | 4.9.3 Procedures for revocation request |
| **Number** | 6 |
| **ETSI** | 6.3 Note 1<br>7.3.6.h.iii<br>7.3.6.j.iii<br>7.3.6.k |
| **PKIo** | A CRL is valid for no more than 48 hours. |

| | |
|---|---|
| **RFC 3647** | 4.9.3 Procedures for revocation request |
| **Number** | 7 |
| **ETSI** | 6.3 Note 1<br>7.3.6.h.iii<br>7.3.6.j.iii<br>7.3.6.k |
| **PKIo** | If there is an issuing subordinate CA under a CSP CA then:<br>▪ the CSP has to use an OCSP and a CRL to make available the certificate status information, relating to the issuing subordinate CA;<br>▪ the CSP has to record the reason for the revocation of the issuing subordinate CA certificate;<br>▪ the validity of the CRL, with regard to the certificate status information of the issuing subordinate CA, is no more than 7 days. |

| | |
|---|---|
| **RFC 3647** | 4.9.5 Time within which CA must process the revocation request |
| **Number** | 1 |
| **ETSI** | 6.3 Note 1<br>7.3.6.h.iii<br>7.3.6.j.iii<br>7.3.6.k |
| **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** | 4.9.5 Time within which CA must process the revocation request |
| **Number** | 2 |
| **ETSI** | 6.3 Note 1<br>7.3.6.h.iii<br>7.3.6.j.iii<br>7.3.6.k |
| **PKIo** | In the case of an issuing subordinate CA, the maximum delay between the time at which the decision is taken to revoke an issuing subordinate CA (recorded in a report) and the amendment of the revocation status information, that is available to all relying parties, is 72 hours. |

| | |
|---|---|
| **RFC 3647** | 4.9.5 Time within which CA must process the revocation request |
| **Number** | 3 |
| **ETSI** | 7.3.6.m |
| **PKIo** | With regard to its OCSP and CRL services, the CSP has to retain appropriate server capacity with which a commercially acceptable response time can be achieved based on queries from all outstanding EV SSL certificates of the CSP. |

| | |
|---|---|
| **RFC 3647** | 4.9.6 Revocation checking requirement for relying parties |
| **Number** | 1 |
| **ETSI** | 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** | 2 |
| **ETSI** | 6.3.a |
| **PKIo** | The obligation mentioned in [4.9.6-1] has to be included by the CSP in the terms and conditions for users that are made available to the relying parties. |

| | |
|---|---|
| **RFC 3647** | 4.9.7 CRL issuance frequency |
| **Number** | 1 |

| | |
|---|---|
| **ETSI** | 7.3.6 |
| **PKIo** | The CSP has to update and reissue the CRL for end user certificates at least once every 7 calendar days and the date of the “ Next update” field may not exceed the date of the “Effective date” field by 10 calendar days. |

| | |
|---|---|
| **RFC 3647** | 4.9.9 On-line revocation/status verification |
| **Number** | 1 |
| **ETSI** | 7.3.6.j |
| **PKIo** | Support with the Online Certificate Status Protocol (OCSP) has to be in line with {16} IETF RFC 162560. |

| | |
|---|---|
| **RFC 3647** | 4.9.9 On-line revocation/status verification |
| **Number** | 2 |
| **ETSI** | 7.3.6.j |
| **PKIo** | To detail the provisions of {16} IETF RFC 2560, OCSP responses have to be signed digitally by either:<br>• the private (CA) key with which the certificate is signed of which the status is requested;<br>• the private key of a responder appointed by the CSP that holds an OCSP Signing Certificate that is signed for this purpose by the private (CA) key with which the certificate is also signed, the status of which has to be requested;<br><br>If a CSP chooses the second option, the OCSP Signing certificate which the responder holds MUST fulfil the following additional condition (see RFC2560 and the requirement PoR part 3e, 4.9.9.4):<br>• The OCSP Signing Certificate is given the extension id-pkix-ocsp-nocheck that is not marked as “critical” and is given the value “NULL”. |

| | |
|---|---|
| **RFC 3647** | 4.9.9 On-line revocation/status verification |
| **Number** | 3 |
| **ETSI** | 7.3.6.j |
| **PKIo** | To detail the provisions of {16} IETF RFC 2560, the use of the precomputed OCSP responses (precomputed responses) is not allowed. |

| | |
|---|---|
| **RFC 3647** | 4.9.9 On-line revocation/status verification |

| | |
|---|---|
| **Number** | 4 |
| **ETSI** | 7.3.6.j |
| **PKIo** | The CSP must update the OCSP service at least once every 4 calendar days. The maximum expiry term of the OCSP responses is 10 calendar days. |

| | |
|---|---|
| **RFC 3647** | 4.9.9 On-line revocation/status verification |
| **Number** | 5 |
| **ETSI** | 7.3.6.h.iv |
| **PKIo** | The CSP MUST support the GET method when offering OCSP responses in accordance with RFC5019. |
| **Comment** | Http based OCSP requests can use either the GET or the POST method to submit a request. To enable http caching, the CSP has to support the GET method. |

| | |
|---|---|
| **RFC 3647** | 4.9.9 On-line revocation/status verification |
| **Number** | 6 |
| **ETSI** | 7.3.6.h.iv |
| **PKIo** | If the OCSP responder of the CSP receives a status request from a certificate that has not been issued, the responder may not answer with the status "good". The CSP must register such requests to the responder as part of the security procedures and, if necessary, take action on these. |

| | |
|---|---|
| **RFC 3647** | 4.9.13 Circumstances for suspension |
| **Number** | 1 |
| **ETSI** | 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** | 1 |
| **ETSI** | 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. |

# 5 Facility, Management and Operational Controls

## 5.2 Procedural Controls

| | |
|---|---|
| **RFC 3647** | 5.2.4 Roles requiring separation of duties |
| **Number** | 1 |
| **ETSI** | 7.3.1.s<br>7.4.3.d and 7.4.3.h |
| **PKIo** | The CSP has to enforce segregation of functions between members of staff with decision-making, operational and monitoring tasks.<br>The CSP has to enforce segregation of functions between at least the following functions:<br>▪ Security officer<br>The security officer is responsible for the implementation of and compliance with the stipulated security guidelines.<br>▪ System auditor<br>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.<br>▪ Systems administrator<br>The systems manager maintains the CSP systems, which includes installing, configuring and maintaining the systems.<br>▪ CSP operator<br>The CSP operators are responsible for the everyday operation of the CSP systems, for registration, the generation of certificates 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** | 2 |
| **ETSI** | 7.3.1.s<br>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 an EV SSL certificate and staff who approve the issuance of an EV SSL certificate. |

| | |
|---|---|
| **RFC 3647** | 5.2.5 Maintenance and security |

| | |
|---|---|
| **Number** | 1 |
| **ETSI** | 7.4.1.a<br>7.4.1 NOTE 1<br>7.4.1.h<br>7.4.4.i<br>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.<br><br>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** | 5.2.5 Maintenance and security |
| **Number** | 2 |
| **ETSI** | 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.<br><br>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.<br><br>The CSP is also entitled to view the underlying evidentiary material, such as audit files and other documentation including system documentation.<br><br>Of course the foregoing is limited to the CSP processes, systems and infrastructure hosted by the suppliers for PKIo core services. |

## 5.3 Personnel Controls

| | |
|---|---|
| **RFC 3647** | 5.3 Employee responsible for verifying and screening identity |
| **Number** | 1 |
| **ETSI** | 7.4.3 Note 4<br>7.4.3.j |

| | |
|---|---|
| **PKIo** | The CSP has to establish the identity and trustworthiness of staff members directly involved in issuing, revoking, renewing or replacing EV SSL certificates, before he or she enters the employment of the CSP.<br>The identity of the staff member has to be established by an HR or information security staff member from the CSP face to face, using a valid passport, a valid identity card or a valid driving licence.<br>When establishing the trustworthiness of the staff member, the CSP has to perform, at the very least, the following actions:<br>▪ verification of the accuracy and completeness of the employment history provided by the staff member;<br>▪ verification of the accuracy of the references provided by the staff member;<br>▪ verification of the accuracy of the highest level of, or most relevant, education provided by the staff member;<br>▪ Request a Certificate of Good Character from the staff member.<br>For members of staff who are already in the employment of the CSP and for whom the aforementioned checks have not yet taken place, these checks have to take place within 3 months of the CSP starting to issue EV certificates based on this CP. |

| | |
|---|---|
| **RFC 3647** | 5.3 Declaration of confidentiality |
| **Number** | 2 |
| **ETSI** | 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. |

| | |
|---|---|
| **RFC 3647** | 5.3.1 Qualifications, experience and clearance requirements |
| **Number** | 1 |
| **ETSI** | 7.4.3.l |
| **PKIo** | Before services server certificates can be issued the CSP has to:<br>▪ ensure that all staff who will be involved in verifying and approving services server certificates undergo training, which covers general knowledge about PKI, authentication and verification policies and procedures with regard to the verification and the approvals process and threats, including phishing and other social engineering tactics;<br>▪ ensure that all staff take an internal exam, which must be successfully completed; |

| | |
|---|---|
| | ▪ keep records of the training course(s) and the exam and make sure that the skills of the relevant staff remain at the required level. |

| | |
|---|---|
| **RFC 3647** | 5.3.2 Background checks procedures |
| **Number** | 1 |
| **ETSI** | 7.4.3-l |
| **PKIo** | Before engaging the services of someone to work on one or more PKIoverheid core services, the CSP or external supplier that performs part of this work MUST verify the identity and the security of this employee. |

## 5.4 Audit Loggin Procedures

| | |
|---|---|
| **RFC 3647** | 5.4.1 Types of events recorded |
| **Number** | 1 |
| **ETSI** | 7.4.6 Note 3<br>7.4.6.h<br>7.4.5.j |
| **PKIo** | Logging has to take place on at least:<br>• Routers, firewalls and network system components;<br>• Database activities and events;<br>• Transactions;<br>• Operating systems;<br>• Access control systems;<br>• Mail servers.<br><br>At the very least, the CSP has to log the following events:<br>• CA key life cycle management;<br>• Certificate life cycle management;<br>• Threats and risks such as:<br>  • Successful and unsuccessful attacks on the PKI system;<br>  • Activities of staff on the PKI system;<br>  • Reading, writing and deleting data;<br>  • Profile changes (Access Management);<br>  • System failure, hardware failure and other abnormalities;<br>  • Firewall and router activities;<br>  • Entering and leaving the CA space.<br><br>At the very least, the log files have to register the following:<br>• Source addresses (IP addresses if available);<br>• Target addresses (IP addresses if available);<br>• Time and date;<br>• User IDs (if available);<br>• Name of the incident;<br>• Description of the incident. |
| **Comment** | Based on a risk analysis the CSP determines which data it should save. |

| **RFC 3647** | 5.4.3 Retention period for audit log |
|---|---|
| **Number** | 1 |
| **ETSI** | 7.4.11.e |
| **PKIo** | The CSP has to store log files for incidents relating to:<br>• CA key life cycle management and;<br>• Certificate life cycle management;<br>These log files must be retained for 7 years and then deleted.<br><br>The CSP has to store log files for incidents relating to:<br>• Threats and risks;<br>These log files must be retained for 18 months and then deleted.<br><br>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** | 5.5.1 Types of events recorded |
|---|---|
| **Number** | 1 |
| **ETSI** | 7.3.1.j<br>7.3.1.n<br>7.4.11 Note 2 |
| **PKIo** | The CSP has to save all information that is used for verifying the identity of the subscriber and certificate manager, including reference numbers of the documentation that is used for verification, as well as restrictions in respect of the validity. |

| **RFC 3647** | 5.5.1 Types of events recorded |
|---|---|
| **Number** | 2 |
| **ETSI** | 7.3.1.n<br>7.4.11 Note 2 |
| **PKIo** | The CSP has to maintain a register of all revoked EV SSL certificates and all rejected requests for an EV SSL certificate, in connection with the suspicion of phishing or other possible misuse, which will be at the discretion of the CSP and has to report these to http://www.phishtank.com. |

| **RFC 3647** | 5.5.2 Retention period for archive |
|---|---|

| | |
|---|---|
| **Number** | 1 |
| **ETSI** | 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. |

| | |
|---|---|
| **RFC 3647** | 5.5.2 Retention period for archive |
| **Number** | 2 |
| **ETSI** | 7.4.11.e<br>7.3.1.n<br>7.4.11 Note 2 |
| **PKIo** | Once the validity of the EV SSL certificate has expired, the CSP has to save all information relating to applying for and revocation, if applicable, of the EV SSL certificate and all information that it used to verify the identity of the subscriber, the Authorized Representative and the certificate manager, for at least 7 years. |

## 5.7 Compromise and Disaster Recovery

| | |
|---|---|
| **RFC 3647** | 5.7.1 Incident and compromise handling procedures. |
| **Number** | 1 |
| **ETSI** | 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:<br>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:<br>• unauthorized inactivation of a core service or rendering this core service inaccessible;<br>• unauthorized access to a core service in order to eavesdrop on, intercept and/or change electronic messaging;<br>• 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** | 2 |
| **ETSI** | 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. |

| | |
|---|---|
| **RFC 3647** | 5.7.1 Incident and compromise handling procedures. |
| **Number** | 3 |
| **ETSI** | 6.3 Note 2 |
| **PKIo** | Within 24 hours of receiving notification of a certificate-related registered incident (requirement 4.5.2-2), the CSP has to decide whether the EV SSL certificate will be revoked or whether different action is needed. This decision has to be taken, taking into consideration the following criteria:<br>▪ the nature of the incident;<br>▪ the number of registered incidents reported regarding the specific EV SSL certificate or website;<br>▪ who has submitted the certificate-related registered incident;<br>▪ applicable laws |

| | |
|---|---|
| **RFC 3647** | 5.7.1 Incident and compromise handling procedures. |
| **Number** | 4 |
| **ETSI** | 6.3 Note 2<br>7.4.5 NOTE 2<br>7.3.6.c<br>7.4.5 Note 2 |
| **PKIo** | The CSP has to have an availability of 24x7 in order to:<br>▪ be able to respond internally to high priority incidents, including but not limited to the circumstances listed under 4.9.1-1, that relate to EV SSL certificates and;<br>▪ if necessary, revoke the EV SSL certificate in relation to which the high priority problem has occurred. |

| | |
|---|---|
| **RFC 3647** | 5.7.4 Business continuity capabilities after a disaster. |
| **Number** | 1 |

| | |
|---|---|
| **ETSI** | 7.4.8.a |
| **PKIo** | The CSP has to draw up a business continuity plan (BCP) for, at the very least, the core services dissemination service, revocation management service and revocation status service, the aim being, in the event of a security breach or emergency, to inform, reasonably protect and to continue the CSP services for subscribers, relying parties and third parties (including browser parties). The CSP has to test, assess and update the BCP annually. At the very least, the BCP has to describe the following processes:<br>▪ Requirements relating to entry into force;<br>▪ Emergency procedure/fall-back procedure;<br>▪ Requirements relating to restarting CSP services;<br>▪ Maintenance schedule and test plan that cover the annual testing, assessment and update of the BCP;<br>▪ Provisions in respect of highlighting the importance of business continuity;<br>▪ Tasks, responsibilities and competences of the involved agents;<br>▪ Intended Recovery Time or Recovery Time Objective (RTO);<br>▪ Recording the frequency of back-ups of critical business information and software;<br>▪ Recording the distance of the fall-back facility to the CSP's main site; and<br>▪ Recording the procedures for securing the facility during the period following a security breach or emergency and for the organization of a secure environment at the main site or fall-back facility. |

# 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** | 1 |
| **ETSI** | 7.2.8.b<br>7.2.1.c and 7.2.1.d |
| **PKIo** | The algorithm and the length of the cryptographic keys that are used for generating the keys for the CSP sub CA have to fulfil the requirements laid down in that respect in the list of recommended 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** | 6.1.1 Key pair generation for the certificate holders |
| **Number** | 2 |
| **ETSI** | 7.2.8.c |
| **PKIo** | Certificate holders' keys have to be generated in a device that fulfils the requirements outlined in {7} CWA 14169 Secure signature creation devices "EAL 4+" or similar security criteria. |
| **Comment** | See paragraph 6.2.11 for the options for software-based generation and storage of the key material of the certificate holders. |

| | |
|---|---|
| **RFC 3647** | 6.1.1 Key pair generation for the certificate holders |
| **Number** | 3 |
| **ETSI** | 7.2.8.d |
| **PKIo** | The generation of the certificate holder's key, where the CSP also generates the private key (PKCS#12) is not allowed |

| | |
|---|---|
| **RFC 3647** | 6.1.1 Key pair generation for the certificate holders |
| **Number** | 4 |

| | |
|---|---|
| **ETSI** | 7.2.8.d |
| **PKIo** | A CSP of PKIoverheid is not allowed to issue code siging certificates under this Certificate Policy. |

| | |
|---|---|
| **RFC 3647** | 6.1.5 Key sizes |
| **Number** | 1 |
| **ETSI** | 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** | 1 |
| **ETSI** | 7.2.5 |
| **PKIo** | The key usage extension (key usage) in X.509 v3 certificates (RFC5280 Internet X.509 Public Key Infrastructure Certificate and CRL Profile) defines the objective of the use of the key embodied 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 'Certificate and CRL and OCSP profiles' of this CP. |

## 6.2 Private Key Protection and Cryptographic Module Engineering Controls

| | |
|---|---|
| **RFC 3647** | 6.2.3 Private key escrow of certificate holder key |
| **Number** | 1 |
| **ETSI** | 7.2.4.a |
| **PKIo** | Escrow by the CSP is not allowed for the private keys of the EV SSL certificate. |

| | |
|---|---|
| **RFC 3647** | 6.2.4 Private key backup of certificate holder key |
| **Number** | 1 |

| | |
|---|---|
| **ETSI** | 7.2.4.a and 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** | 1 |
| **ETSI** | 7.2.4.a and 7.2.8.e |
| **PKIo** | Archiving by the CSP of the certificate holders' private keys is not allowed. |

| | |
|---|---|
| **RFC 3647** | 6.2.11 Cryptographic module rating |
| **Number** | 1 |
| **ETSI** | 3.1 |
| **PKIo** | Secure devices issued or recommended by the CSP for the storage of keys (SUDs) have to fulfil the requirements laid down in document {7} CWA 14169 Secure signature-creation devices "EAL 4+". |

| | |
|---|---|
| **RFC 3647** | 6.2.11 Cryptographic module rating |
| **Number** | 2 |
| **ETSI** | 3.1 |
| **PKIo** | Instead of demonstrating compliance with CWA 14169, CSPs can issue or recommend SUDs that are certified in line with a different protection profile against the Common Criteria (ISO/IEC 15408) at level EAL4+ or that have a comparable trust level. This has to be established by a test laboratory that is accredited for performing Common Criteria evaluations. |

| | |
|---|---|
| **RFC 3647** | 6.2.11 Cryptographic module rating |
| **Number** | 3 |
| **ETSI** | 3.1 |
| **PKIo** | Instead of using a hardware-based SUD, the keys of an EV SSL certificate can be protected by software if compensating measures are taken in the system's environment that contains the keys. The compensating measures have to be of such a quality that it is practically impossible to steal or copy the key unnoticed |

| | |
|---|---|
| | When registering, the manager of the EV SSL certificates that uses this option for software-based storage has, at the very least, to submit a written declaration to state that compensating measures have been taken that fulfil the condition stipulated to this end. The agreement between the subscriber and CSP must state that the CSP is entitled to verify the measures that have been taken. |
| **Comment** | For example, for compensating measures, thought should be given to a combination of physical access security, logical access security, logging and audit and segregation of functions. |

## 6.3 Other Aspects of Key Pair Management

| | |
|---|---|
| **RFC 3647** | 6.3.2 Certificate operational periods and key pair usage periods |
| **Number** | 1 |
| **ETSI** | 7.3.3.a.x |
| **PKIo** | Private keys that are used by a certificate holder and issued under the responsibility of this CP must not be used for more than 27 months. The certificates, that are issued under the responsibility of this CP, have to be valid for no more than 27 months. |

| | |
|---|---|
| **RFC 3647** | 6.3.2 Certificate operational periods and key pair usage periods |
| **Number** | 2 |
| **ETSI** | 7.2.6 |
| **PKIo** | At the time that an end user certificate is issued, the remaining term of validity of the overall CSP certificate and/or subordinate certificate has to exceed the intended term of validity of the end user certificate. |

## 6.4 Activation data

| | |
|---|---|
| **RFC 3647** | 6.4.1 Activation data generation and installation |
| **Number** | 1 |
| **ETSI** | 7.2.9.d |
| **PKIo** | The CSP attaches activation data to the use of an SUD, to protect the private keys of the certificate holders. |
| **Comment** | The requirements that the activation data (for example the PIN code) have to fulfil, can be determined by the CSPs themselves based on, for example, a risk analysis. Requirements that could be considered are the length of the PIN code and use of special characters. |

| **RFC 3647** | 6.4.1 Activation data generation and installation |
|---|---|
| **Number** | 2 |
| **ETSI** | 7.2.9.d |
| **PKIo** | An unlocking code can only be used if the CSP can guarantee that, at the very least, the security requirements are fulfilled that are laid down in respect of the use of the activation data. |

## 6.5 Computer Security Controls

| **RFC 3647** | 6.5.1 Specific computer security technical requirements |
|---|---|
| **Number** | 1 |
| **ETSI** | 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** | 2 |
| **ETSI** | 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** | 3 |
| **ETSI** | 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, or the various core services will be implemented on separate network domains, where there has to be a unique authentication for each core service. If core services use the same network domains, the CSP enforces a unique authentication for each core service. The CSP documents 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** | 1 |
| **ETSI** | 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 NCP 7.4.7. and Electronic Signature Directive art. 2 paragraph 1c can be demonstrated by:<br>▪ an audit statement from the supplier of the products, which has had an independent EDP audit performed based on CWA 14167-1;<br>▪ an audit statement from an internal auditor from the CSP based on CWA 14167-1;<br>▪ 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** | 1 |
| **ETSI** | 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:<br>• are equipped with the latest updates and;<br>• the web application controls and filters all input by users and;<br>• the web application codes the dynamic output and;<br>• the web application maintains a secure session with the user and;<br>• the web application uses a database securely. |

| | |
|---|---|
| **Comment** | The CSP has to use the NCSC's "Checklist beveiliging webapplicaties (Security of Web Applications Checklist)[5]" 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** | 2 |
| **ETSI** | 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** | 3 |
| **ETSI** | 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, external supplier. The CSP has to document the findings from the pen test and the measures that will be taken in this respect, or to arrange for these to be documented. |
| **Comment** | 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[6]" (how to perform penetration testing) published by the NCSC.<br>If necessary, the PA can instruct the CSP to perform additional pen tests. |

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

[6] *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** | 1 |
| **ETSI** | 7.3.3.a |
| **PKIo** | The CSP has to issue certificates in accordance with the requirements stipulated in that respect in appendix A of this document, "Certificate, CRL and OCSP profiles". |

## 7.2 CRL Profile

| | |
|---|---|
| **RFC 3647** | 7.2 CRL profile |
| **Number** | 1 |
| **ETSI** | 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, "Certificate, CRL and OCSP profiles". |

## 7.3 OCSP Profile

| | |
|---|---|
| **RFC 3647** | 7.3 OCSP profile |
| **Number** | 1 |
| **ETSI** | OCSP is not covered in ETSI. |
| **PKIo** | The CSP has to use the OCSP certificates and responses in accordance with the requirements stipulated in that respect in appendix A of this document, which are "Certificate, CRL and OCSP profiles". |

# 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, 9.2.2 Other resources |
| **Number** | 1 |
| **ETSI** | 6.4<br>7.1.k<br>7.5.d |
| **PKIo** | The CSP has to take out business liability insurance (including cover for product liability) amounting to at least EUR 2,500,000 or US $ 5,000,000 per year.<br><br>At the very least, the insurance has to cover the following:<br>1. claims for compensation that ensue from an activity, error or omission or an unintentional violation of the contract, or neglecting to issue or enforce EV certificates by the CSP and;<br>2. claims for compensation that ensue from breach of a third party's right of ownership (with the exception of the copyright, and violation of the trademark) or claims that ensue from violation of the privacy or defamation of a third party by the CSP. |

| | |
|---|---|
| **RFC 3647** | 9.2.1 Insurance coverage, 9.2.2 Other resources |
| **Number** | 2 |
| **ETSI** | EVSP+ 6.4<br>7.1.k<br>7.5.d |
| **PKIo** | The business liability insurance (including cover for product liability) has to be taken out with an insurance company that has at least an “A‟ rating from a recognized rating agency. |

| | |
|---|---|
| **RFC 3647** | 9.2.1 Insurance coverage, 9.2.2 Other resources |
| **Number** | 3 |
| **ETSI** | EVSP+ 6.4<br>7.1.k<br>7.5.d |
| **PKIo** | The CSP is not obliged to take out business liability insurance (including cover |

| | |
|---|---|
| | for product liability). The CSP may also guarantee the liability with its own assets in relation to the issue and the maintenance of EV SSL certificates based on the requirements described in this CP. These own assets then have to consist of, at least EUR 250,000,000 or US $ 500,000,000 in liquid assets · |

## 9.5 Intellectual Property Rights

| | |
|---|---|
| **RFC 3647** | 9.5 Intellectual property rights |
| **Number** | 1 |
| **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. |

## 9.6 Representations and Warranties

| | |
|---|---|
| **RFC 3647** | 9.6.1 CA Representations and Warranties by CSPs |
| **Number** | 1 |
| **ETSI** | 6.4 |
| **PKIo** | In the agreement between the CSP and the subscriber, a clause (a clause as specified in article 6:253 of the Civil Code) will be included in which the CSP champions a relying third party on the certificate. This clause addresses a liability of the CSP in accordance with article 6:196b, first up to and including third paragraph, of the Civil Code, with the proviso that:<br>a. for "a qualified certificate specified in article 1.1, division ss Telecommunications Act": "an EV SSL certificate";<br>b. for "signatory": "certificate holder" is read;<br>c. for "creation of electronic signatures": "verification of authenticity features and creating encrypted data";<br>d. For "verification of electronic signatures": "deciphering authentication features and encrypted data". |

| | |
|---|---|
| **RFC 3647** | 9.6.1 CA Representations and Warranties by CSPs |
| **Number** | 2 |
| **ETSI** | 6.4<br>7.1.k |
| **PKIo** | In its CPS the CSP has to state that it cannot be held liable for damage suffered by subscribers, relying parties or other parties if the EV SSL certificate is improperly used and/or trusted. |
| **Comment** | 'Improperly' means that subscribers, relying parties or other parties have not strictly adhered to the provisions as described in the CPS of the CSP, with |

| | |
|---|---|
| | regard to the use of and/or trust in an EV SSL certificate. |

## 9.8 Limitations of Liability

| | |
|---|---|
| **RFC 3647** | 9.8 Limitations of liability |
| **Number** | 1 |
| **ETSI** | 6.4 |
| **PKIo** | The CSP is not allowed to place restrictions on the use of certificates within the scope of EV SSL certificates as mentioned in paragraph 1.4 in this CP. |

| | |
|---|---|
| **RFC 3647** | 9.8 Limitations of liability |
| **Number** | 2 |
| **ETSI** | 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

### *9.12.1 Amendment procedure*

The procedures relating to managing changes in the PoR of PKIoverheid are incorporated in the Certificate Policy Statement of PKIoverheid. 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** | 1 |
| **ETSI** | This subject is not covered in ETSI. |
| **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** | 2 |

| | |
|---|---|
| **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** | 1 |
| **ETSI** | 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

Dutch law applies to this CP.

## 9.17 Miscellaneous provisions

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 Profiles certificates and certificate status information

Profile of services certificates for the Government/Companies and Organisation domains

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

- V : Compulsory; indicates that the attribute is compulsory and MUST be used in the certificate.
- O : Optional; indicates that the attribute is optional and MAY be used in the certificate.
- A : Advised against; indicates that the attribute is advised against and SHOULD NOT be used in the certificate.
- N : Not allowed; indicates that the use of the attribute in the PKI for the government is not allowed.

For the extensions, fields/attributes are used that, in accordance with international standards, are critical, are marked in the 'Critical' column with 'yes' to show that the relevant attribute MUST be verified using a process by means of 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. Guidelines for The Issuance and Management of Extended Validation Certificates, CA Browser Forum, 20 November 2010, Version 1.3.
5. Guidelines Version 1.3 Errata.
6. RFC 2818: "HTTP about TLS".
7. RFC 2560: "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP".
8. RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and CRL Profile".
9. RFC 3739: "Internet X.509 Public Key Infrastructure Qualified Certificates Profile".
10. OID RA management_PKI overheid – OID scheme.
11. ETSI TS 101 862: "Qualified certificate profile", version 1.3.3 (2006-01).
12. ETSI TS 102 280 : "X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons", version 1.1.1 (2004-03).
13. ETSI TS 102176-1 : "Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms", version 2.0.0 (2007-11).
14. 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 included 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, Optional or Advised Against may be used.

# Extended Validation certificates

## Basic attributes

| Field / Attribute | Criteria | Description | Standard reference | Type | Explanation |
|---|---|---|---|---|---|
| Version | V | MUST be set at 2 (X.509v3). | RFC 5280 | Integer | Describes the version of the certificate, the value 2 stands for X.509 version 3. |
| SerialNumber | V | A serial number that MUST uniquely identify the certificate within the publishing CA domain. | RFC 5280 | Integer | All end user certificates have to contain at least 8 bytes of unpredictable random data in the certificate's serial number (SerialNumber). |
| Signature | V | MUST be created on the algorithm, as stipulated by the PA. | RFC 5280, ETSI TS 102176 | OID | MUST be the same as the field signatureAlgorithm. For maximum interoperability, for certificates issued under this CP, only sha-256WithRSAEncryption is allowed.<br>For the key lengths, see the PKIoverheid CPS EV certificates. |
| 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 CSP certificate (for validation). |
| Issuer.countryName | V | MUST contain the country code of the country where the issuing organization of | ETSI TS101862, X520, ISO 3166 | Printable String | C = NL for CSPs located in the Netherlands. |

| Field / Attribute | Criteria | Description | Standard reference | Type | Explanation |
|---|---|---|---|---|---|
| | | the certificate is located. | | | |
| Issuer.stateOrProvinceName | N | Use is not allowed. | PKIo | UTF8String | - |
| Issuer.OrganizationName | V | Full name in accordance with the accepted document or basic registry | ETSI TS 102280 | UTF8String | |
| Issuer. organizationalUnitName | O | Optional specification of an organizational entity. This field MUST NOT include a function indication or similar. It may include, if applicable, the types of certificates that are supported. | ETSI TS 102280 | UTF8String | Several instances of this attribute MAY be used. |
| Issuer.localityName | N | Use is not allowed. | PKIo | UTF8String | - |
| Issuer.serialNumber | O | MUST be used in accordance with RFC 3739 IF unambiguous naming requires this | RFC 3739 | Printable String | |
| Issuer.commonName | V | MUST include the name of the CA in accordance with accepted document or basic registry, MAY include the Domain | PKIo, 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) |

| Field / Attribute | Criteria | Description | Standard reference | Type | Explanation |
|---|---|---|---|---|---|
| | | label and/or the types of certificates that are supported | | | |
| 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 EV CPS. |
| subject | V | The attributes that are used to describe the subject (service) MUST mention the subject in a unique way and include information about the subscriber organization. The field has the following attributes: | PKIo, RFC3739, ETSI TS 102 280 | | MUST contain a Distinguished Name (DN). Attributes other than those mentioned below MUST NOT be used. |
| Subject.businessCategory | V | MUST include one of the following values:<br>2.5.4.15 = Private Organization<br>2.5.4.15 = Government Entity<br>2.5.4.15 = Business Entity<br>2.5.4.15 = Non-Commercial Entity | PKIo | | ▪ Private Organization applies to organizations governed by private law with a legal personality;<br>▪ Government Entity applies to government organizations;<br>▪ Business Entity applies to organizations governed by private law without a legal personality; Formal collaborative ventures between companies also fall under this category;<br>▪ Non-Commercial Entity applies in international organizations that do not belong to one country or government (e.g. the NATO (http://www.nato.int) or the United Nations (http://www.un.int)). |

| Field / Attribute | Criteria | Description | Standard reference | Type | Explanation |
|---|---|---|---|---|---|
| | | | | | NO PKIoverheid EV SSL certificates MAY be issued to these types of organizations. |
| Subject.countryName | V | complete C with two-letter country code in accordance with ISO 3166-1. If an official alpha-2 code is missing, the CSP MAY use the user-assigned code XX. | RFC 3739, X520, ISO 3166, PKIo | PrintableString | The country code that is used in Subject.countryName MUST correspond with the subscriber's address in accordance with the accepted document or registry. |
| Subject.commonName | A | Name that identifies the server.<br>The use of this field is advised against. If this field is used, this MUST contain no more than 1 "fully-qualified domain name (FQDN)" (see the definition in part 4). This FQDN MUST also be included in the SubjectAltName.dNSName field. | RFC 3739, ETSI TS 102 280, PKIo | UTF8String | In this attribute, wildcards, private IP addresses and/or host names, internationalized domain names (IDNs) and null characters \0 may not be used. |
| Subject.Surname | N | Is not used for EV SSL certificates. | | | EV SSL certificates are not personal. The use of this attribute is therefore not allowed, to avoid confusion. |
| Subject.givenName | N | Is not used for EV SSL certificates. | | | EV SSL certificates are not personal. The use of this attribute is therefore |

| **Field / Attribute** | **Criteria** | **Description** | **Standard reference** | **Type** | **Explanation** |
|---|---|---|---|---|---|
| | | | | | not allowed, to avoid confusion. |
| Subject.pseudonym | N | Pseudonyms may not be used. | ETSI TS 102 280, RFC 3739, PKIo | | |
| Subject.organizationName | V | MUST include the full name of the subscriber organization in accordance with the accepted document (State Almanac) or Basic Registry (Trade Register). | PKIo | UTF8String | The subscriber organization is the organization with which the CSP has entered into an agreement and on behalf of which the certificate holder (service/server) communicates or acts.<br>The CSP MAY modify the full name of the subscriber organization if this has more than 64 positions. The CSP MUST consult the subscriber about this. The modification MUST take place in such a way that the relying parties do not think that they are dealing with a different organization. If this type of modification is not possible, then CSP MAY NOT issue the EV SSL certificate. |
| Subject.organizationalUnitName | O/V | Optional specification of an organizational entity. This attribute MUST NOT include a function indication or similar. | PKIo | | This attribute MAY appear several times. The field MUST contain a valid name of an organizational entity of the subscriber in accordance with an accepted document or registry. |

| Field / Attribute | Criteria | Description | Standard reference | Type | Explanation |
|---|---|---|---|---|---|
| | | Compulsory labelling of a government organization. | | | Only in those cases in which a government organization entity is not yet listed in the Trade Register, in this field the CSP MUST include the words “government organization”. |
| Subject.stateOrProvinceName | V | MUST include the province of the subscriber's branch, in accordance with the accepted document (State Almanac) or Basic registry (Trade Register). | PKIo, RFC 3739 | UTF8String | |
| Subject.localityName | V | MUST include the subscriber's location in accordance with the accepted document (State Almanac) or Basic registry (Trade Register). | PKIo, RFC 3739 | UTF8String | . |
| Subject.streetAddress | O | If present, this field MUST contain the subscriber's street name in accordance with an accepted document (State Almanac) or Basic registry (Trade Register). | PKIo, RFC 3739 | UTF8String | |
| Subject.postalCode | O | If present, this field MUST contain the postcode related to the subscriber's street | PKIo, RFC 3739 | UTF8String | |

| Field / Attribute | Criteria | Description | Standard reference | Type | Explanation |
|---|---|---|---|---|---|
| | | name in accordance with an accepted document (State Almanac) or Basic registry (Trade Register). | | | |
| Subject:jurisdictionOfIncorporationLocalityName | N | 1.3.6.1.4.1.311.60.2.1.1<br>LocalityName as specified in RFC 5280 | PKIo,<br>RFC 5280 | | |
| Subject:jurisdictionOfIncorporationStateOrProvinceName | N | 1.3.6.1.4.1.311.60.2.1.2<br>StateOrProvinceName as specified in RFC 5280 | PKIo,<br>RFC 5280 | | |
| Subject:jurisdictionOfIncorporationCountryName | V | Fixed value:<br>1.3.6.1.4.1.311.60.2.1.3 = NL | RFC 5280,<br>ISO 3166 | OID | |
| Subject.postalAddress | A | The use is advised against. If available, 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 EV SSL certificates. |

| **Field / Attribute** | **Criteria** | **Description** | **Standard reference** | **Type** | **Explanation** |
|---|---|---|---|---|---|
| Subject.serialNumber | V | The CSP is responsible for safeguarding the uniqueness of the subject (service). The Subject.serialNumber MUST be used to identify the subject uniquely. | RFC 3739, X 520, PKIo | Printable String | The Chamber of Commerce number MUST be included in this field.<br>In those cases where an organizational entity within the government is not yet listed in the Trade Register the CSP MUST determine the number itself with which the uniqueness of the subject (service) is safeguarded. The CSP MUST then also include in the field Subject.organizationalUnitName the word "government organisation". |
| Subject.title | N | The use of the title attribute is not allowed for EV SSL certificates. | ETSI TS 102 280, RFC 3739, RFC 5280 | | This attribute is only used in personal certificates and therefore not in EV SSL certificates. |
| subjectPublicKeyInfo | V | Contains, among other things, the public key. | ETSI TS 102 280, RFC 3279 | | Contains the public key, identifies the algorithm with which the key can be used. |
| IssuerUniqueIdentifier | N | Is not used. | RFC 5280 | | The use of this is not allowed (RFC 5280) |
| subjectUniqueIdentifier | N | Is not used. | RFC 5280 | | The use of this is not allowed (RFC 5280) |

## Standard extensions

| Field / Attribute | Criteria | Critical? | Description | Standard reference | Type | Explanation |
|---|---|---|---|---|---|---|
| authorityKeyIdentifier | V | No | The algorithm to generate the AuthorityKey MUST be created on an algorithm determined by the PA. | ETSI TS 102 280, RFC 5280 | BitString | The value MUST contain the SHA-1 hash from the authorityKey (public key of the CSP/CA). |
| SubjectKeyIdentifier | V | No | The algorithm to generate the subjectKey MUST be created on an algorithm determined by the PA. | RFC 5280 | BitString | The value MUST contain the SHA-1 hash from the subjectKey (public key of the certificate holder). |
| KeyUsage | V | Yes | In EV subordinate CA certificates that are issued under an EV CSP CA certificate the keyCertSign and cRLSign MUST be included and marked as essential. Another keyUsage MUST NOT be combined with this.<br>In EV SSL certificates the digitalSignature and keyEncipherment bits MUST be incorporated and marked as critical. Another keyUsage MUST NOT be combined with this. | RFC 3739, RFC 5280, ETSI TS 102 280 | BitString | |

| Field / Attribute | Criteria | Critical? | Description | Standard reference | Type | Explanation |
|---|---|---|---|---|---|---|
| privateKeyUsagePeriod | N |  | Is not used. | RFC 5280 |  |  |
| CertificatePolicies | V | No | MUST include the OID of this EV certificate policy (CP).<br>policyIdentifier<br>▪ EV policy identifier<br>policyQualifiers:policyQualifierId<br>▪ id-qt 1 [RFC 5280]<br>In EV subordinate CA certificates that are issued under an EV CSP CA certificate the HTTP URL of the EV Certification Practice Statement of the PA of PKIoverheid MUST be incorporated.<br>policyQualifiers:qualifier:cPSuri<br>▪ HTTP URL of the Certification Practice Statement of the PA of PKIoverheid<br>In EV SSL certificates, the HTTP URL of the certification practice statement (CPS) of the | RFC 3739<br>RFC 5280 | OID, String, String | The following OID applies: 2.16.528.1.1003.1.2.7<br>This OID MUST be included in EV SSL certificates and in EV subordinate CA certificates that are issued under an EV CSP CA certificate.<br>The HTTP URL of the EV Certification Practice Statement of the PA of PKIoverheid is: http://www.logius.nl/producten/toegang/pkioverheid/documentatie/cps/ |

| Field / Attribute | Criteria | Critical? | Description | Standard reference | Type | Explanation |
|---|---|---|---|---|---|---|
| | | | CSP MUST be incorporated<br>policyQualifiers:qualifier:cPSuri<br>▪ HTTP URL of the Certification Practice Statement of the CSP<br>In EV SSL certificates a user notice MUST be incorporated. | | | |
| PolicyMappings | N | | Is not used. | | | This extension is not used in EV SSL certificates |
| SubjectAltName | V | No | MUST be used and given a worldwide unique number that identifies the service. | RFC 4043, RFC 5280, PKIo, ETSI 102 280 | | MUST include a unique identifier in the othername attribute. Attributes other than those mentioned below MUST NOT be used. |
| SubjectAltName.dNSName | V | | Name that identifies the server.<br>This field MUST include at least 1 "fully-qualified domain name (FQDN)" (see the definition in part 4). | RFC2818, RFC5280 | IA5String | In this attribute, wildcards, private IP addresses and/or host names, internationalized domain names (IDNs) and null characters \0 may not be used. |

| Field / Attribute | Criteria | Critical? | Description | Standard reference | Type | Explanation |
|---|---|---|---|---|---|---|
| | | | Several FQDNs MAY be used in this field. These FQDNs MUST come from the same domain name range. (e.g. www.logius.nl, applicatie.logius.nl, secure.logius.nl etc. etc.). | | | |
| SubjectAltName.otherName | V | | MUST be used containing a unique identification number that identifies the certificate holder. | PKIo | IA5String, Microsoft UPN, IBM Principal-Name or Permanent-Identifier | Includes the OID of the CPS and a number that permanently and uniquely identifies the subject (service), separated by a point or hyphen ('-'). It is recommended that an existing registration number from back office systems is used, along with a code for the organization. In combination with the CSP's OID number, this identifier is unique throughout the world. This number MUST be persistent. |
| SubjectAltName.rfc822Name | A | | MAY be used for a 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 EV SSL certificates, the use of e-mail addresses is advised against, because e-mail addresses of certificate holders often change and are susceptible to spam. |
| IssuerAltName | N | | Is not used. | RFC 5280 | | |

| Field / Attribute | Criteria | Critical? | Description | Standard reference | Type | Explanation |
|---|---|---|---|---|---|---|
| subjectDirectoryAttributes | N | | Is not used. | RFC 5280; RFC 3739 | | This extension may not be used. |
| BasicConstraints | V | Yes | In EV SSL certificates, the "CA" field must show "FALSE" or be omitted (default value is then "FALSE").<br>In EV subordinate CA certificates that are issued under an EV CSP CA certificate, the "CA" field must show "TRUE". The field pathLenConstraint MAY be present. | RFC 5280 | | In a (Dutch language) browser, the following will be seen for EV SSL certificates: Subjecttype = Eindentiteit", "Beperking voor padlengte = Geen ("Subjecttype = End Entity", "Restriction for the path length = None")<br>In EV subordinate CA certificates that are issued under an EV CSP CA certificate, the following will be seen: Subjecttype = CA", Beperking voor padlengte = Geen ("Subjecttype = CA", "Path length constraint= None") |
| NameConstraints | N | | Is not used. | RFC 5280 | | Is not used in EV SSL certificates. |
| PolicyConstraints | N | | Is not used. | RFC 5280 | | Is not used in EV SSL certificates. |
| CRLDistributionPoints | V | No | MUST include the HTTP URI of a CRL distribution point. | RFC 5280, ETSI TS 102 280 | | |
| ExtKeyUsage | V | No | In EV SSL certificates, the attributes id-kp- | RFC 5280 | KeyPurposeId's | |

| Field / Attribute | Criteria | Critical? | Description | Standard reference | Type | Explanation |
|---|---|---|---|---|---|---|
| | | | serverAuth (Verification of the server) and id-kp-clientAuth (Client verification) MUST be included. The value id-kp-emailProtection MAY be combined with this. Other extKeyUsage MUST NOT be combined with this. | | | |
| InhibitAnyPolicy | N | | Is not used. | RFC 5280 | | Is not used in EV SSL certificates. |
| FreshestCRL | O | No | MUST contain the URI of a Delta CRL distribution point, if Delta CRLs are used. | RFC 5280, PKIo | | Delta-CRLs are an optional extension. In order to fulfil the requirements of PKIoverheid a CSP MUST also publish full CRLs at the required release frequency. |

## Private extensions

| Field / Attribute | Criteria | Critical? | Description | Standard reference | Type | Explanation |
|---|---|---|---|---|---|---|
| authorityInfoAccess | V | No | This attribute MUST include the HTTP URI of an OCSP responder such as Online Certificate Status Protocol (OCSP). | | | The EV CA certificate (EV CSP CA or EV subordinate CA certificate) MAY also include the HTTP URL of the State of the Netherlands EV Root CA certificate.<br>The EV SSL certificate MAY also include the HTTP URL of the issuing EV CA certificate (EV CSP CA or EV subordinate CA certificate). |
| SubjectInfoAccess | O | No | | RFC 5280 | OID, Generalname | This field can be used to reference additional information about the subject. |
| BiometricInfo | N | | Is not used in EV SSL certificates. | PKIo | | Biometric information is not advisable in non-personal certificates, such as EV SSL certificates. |
| QcStatement | N | No | | RFC 3739, ETSI TS 102 280, ETSI TS 101 862 | OID | This attribute is only used in personal certificates and not allowed in EV SSL certificates. |

# 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 reference1** | **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 created on the algorithm, as stipulated by the PA. | RFC 5280 | OID | MUST be the same as the field signatureAlgorithm. For maximum interoperability, 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 | ISO3166, X.520 | Printable String | C = NL for CSPs located in the Netherlands. |

| Field / Attribute | Criteria | Description | Standard reference1 | Type | Explanation |
|---|---|---|---|---|---|
| | | the certificate is located. | | | |
| 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 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 | 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 | PKIo, RFC 5280 | UTF8String | |

| Field / Attribute | Criteria | Description | Standard reference1 | Type | Explanation |
|---|---|---|---|---|---|
| | | Domain label and/or the types of certificates that are supported | | | |
| ThisUpdate | V | MUST indicate the date and time on which the CRL is amended. | RFC 5280 | UTCTime | MUST include the issue 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 reference1 | 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 | RFC 5280 | | If used, this field MUST fulfil the specifications in RFC 5280 |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | additional information (such as a limited set of reason codes why the certificate has been revoked). | | | |
| 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. |
| 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 can be used to identify the original issuer of the certificate. | RFC 5280 | GeneralNames | |

# Profile OCSP

### General requirements in respect of OCSP

- OCSP responses and OCSPSigning certificates MUST fulfil the requirements laid down in this respect in IETF RFC 2560.
- OCSPSigning certificates MUST correspond with the X.509v3 standard for public key certificates. General requirements in relation to certificates 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.
- OCSPSigning certificates must fulfil the profile for services certificates indicated above, with the following exceptions:

### OCSP Signing certificate attributes

| **Field / Attribute** | **Criteria** | **Description** | **Standard reference1** | **Type** | **Explanation** |
|---|---|---|---|---|---|
| Issuer | V | MUST contain a Distinguished Name (DN). | PKIo | | An OCSPSigning certificate MUST be issued under the hierarchy of the State of the Netherlands EV Root CA. |

| **Field / Attribute** | **Criteria** | **Critical?** | **Description** | **Standard reference** | **Type** | **Explanation** |
|---|---|---|---|---|---|---|

| 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.<br>In OCSPSigning certificates, the digitalSignature bit MUST be incorporated and the extension marked as being critical. Another keyUsage MUST NOT be combined with this. | RFC 5280, RFC 2560 | BitString | |
| CertificatePolicies | V | No | MUST include the OID of this EV certificate policy (CP). | RFC 3739 | OID, String, String | The following OID applies: 2.16.528.1.1003.1.2.7 |
| ExtKeyUsage | V | Yes | MUST be used with the value id-kp-OCSPSigning. | RFC 5280 | | |
| ocspNoCheck | O | | | RFC 2560 | | |

# Appendix B Reference matrix

Based on chapters 1 to 9 inclusive, a reference matrix is included in appendix B. In accordance with the RFC 3647 structure, the matrix contains a reference to the applicable requirements within the PKI for the government. Here a distinction is made between the Dutch legislation, ETSI TS 102 042 EVCP and the PKIo requirements.

In the table below, the first and second column correspond with the chapter and paragraph division used in RFC 3647. Subsequently, the column 'ETSI requirement' outlines which requirements from ETSI apply to the relevant paragraph from the Certificate Policy applied within PKIoverheid. When an ETSI requirement applies to several paragraphs from RFC 3647, the reference to the relevant ETSI requirement is included once.

In addition, the table states which requirements from the legal framework are not covered by ETSI and on which parts in the CP these legal requirements apply. Harmonization is sought with the Electronic Signature Regulation, which states which requirements from the Electronic Signature Regulation are not covered by ETSI. Also included in the table below are the articles from the Electronic Signature Act that relate to liability. This has been done because these articles are detailed further in PKIo requirements.

In the final column, for the PKIo requirements it is stated to which paragraph from the CP these requirements apply. The ETSI requirements written in italics have been detailed further in PKIo requirements. In the table, a PKIo requirement may be included without an ETSI requirement being linked to this. This is caused by the fact that a PKIo requirement is sometimes based on a part of an ETSI requirement, whilst that ETSI requirement as a whole fits in better with a different RFC paragraph. Also, several PKIo requirements can sometimes use the same ETSI requirement as a source, whilst every ETSI requirement is only mentioned once.

For a number of RFC paragraphs no requirements have been included. This means that no requirements apply to the relevant RFC paragraph or that the requirements are already incorporated in another RFC paragraph[7]. The PA has specifically decided to include all requirements just once.

[7] *This is partially caused by the fact that ETSI TS 102 042 is not constructed in accordance with the RFC 3647 structure.*

| **No.** | **CP reference** | **ETSI requirement** | **Legal requirement** | **PKIo requirement** |
|---|---|---|---|---|
| **1** | **Introduction to the Certificate Policy** | | | |
| **1.1** | **Overview** | | | 1.1 |
| 1.1.1 | Design of the Certificate Policy | | | 1.1.1 |
| 1.1.2 | Relationship between CP and CPS | | | 1.1.2 |
| 1.1.3 | Status | | | 1.1.3 |
| **1.2** | **References to this CP** | | | 1.2 |
| **1.3** | **User community** | | | 1.3 |
| **1.4** | **Certificate usage** | | | 1.4 |
| **1.5** | **Contact information Policy Authority** | | | 1.5 |
| **2** | **Publication and Repository Responsibilities** | | | |
| **2.1** | **Electronic Repository** | *7.3.1.c*<br>*7.3.4.b*<br>*7.3.5.e.ii* | | 2.1-1<br>2.1-2 |

| No. | CP reference | ETSI requirement | Legal requirement | PKIo requirement |
|---|---|---|---|---|
| | | *7.3.5.f* | | |
| **2.2** | **Publication of CSP Information** | *4.5.1*<br>*5.2.b*<br>7.1.a<br>*7.1.b*<br>7.1.c<br>*7.1.d.2*<br>7.1.e<br>*7.3.1.h.iii*<br>7.3.2.b<br>7.3.4<br>7.3.4.a<br>7.3.5<br>7.3.5.c<br>7.3.5.d<br>7.3.6.a | | 2.2-1<br>2.2-2<br>2.2-3<br>2.2-4<br>2.2-5<br>2.2-6<br>2.2-7 |
| **2.3** | **Frequency of Publication** | | | |
| **2.4** | **Access to Published Information** | *7.1.d.1*<br>7.3.6.o | | 2.4-1 |
| **3** | **Identification and Authentication** | | | |

| No. | CP reference | ETSI requirement | Legal requirement | PKIo requirement |
|---|---|---|---|---|
| **3.1** | **Naming** | | | |
| 3.1.1 | Types of names | | | 3.1.1-1 |
| 3.1.2 | Need for names to be meaningful | | | |
| 3.1.3 | Anonymity or pseudonimity of certificate holders | | | |
| 3.1.4 | Rules for interpreting various name forms | | | |
| 3.1.5 | Uniqueness of names | 7.3.3.e | | |
| 3.1.6 | Recognition, authentication and role of trademarks | | | |
| **3.2** | **Initial identity validation** | *7.3.3.a.x* | | 3.2.0-1 |
| 3.2.1 | Method to prove possession of private key | 7.3.1.o | | 3.2.1-1 |
| 3.2.2 | Authentication of organization identity | *7.3.1.d*<br>7.3.1.h<br>*7.3.1.h.i*<br>*7.3.1.l*<br>*7.3.1.r*<br>*7.3.1.t* | | 3.2.2-1<br>3.2.2-2<br>3.2.2-3<br>3.2.2-4<br>3.2.2-5 |

| **No.** | **CP reference** | **ETSI requirement** | **Legal requirement** | **PKIo requirement** |
|---|---|---|---|---|
| 3.2.3 | Authentication of individual identity | 6.2<br>6.2.a<br>7.3.1<br>7.3.1.a<br><br>7.3.1.e<br>*7.3.1.g*<br>*7.3.1.k* | | 3.2.3-1<br>3.2.3-2<br>3.2.3-3<br>3.2.3-4 |
| 3.2.4 | Non-verified subscriber information | | | |
| 3.2.5 | Validation of authority | 7.3.1.i<br>*7.3.1.i.i*<br>*6.2.h* | | 3.2.5-1<br>3.2.5-2<br>3.2.5-3 |
| 3.2.6 | Criteria for interoperation | | | |
| **3.3** | **Identification and Authentication for Re-key Requests** | | | |
| 3.3.1 | Identification and authentication for routine re-key | 7.3.2<br><br>*7.3.2.c*<br>*7.3.2.d* | | 3.3.1-1<br>3.3.1-2 |

| **No.** | **CP reference** | **ETSI requirement** | **Legal requirement** | **PKIo requirement** |
|---|---|---|---|---|
| 3.3.2 | Identification and authentication for re-key after revocation | | | 3.3.2-1 |
| **3.4** | **Identification and Authentication Revocation Requests** | 7.3.6.d | | |
| **4** | **Certificate Life-Cycle Operational Requirements** | | | |
| **4.1** | **Certificate Application** | *7.3.1.u* | | 4.1-1<br>4.1-2 |
| **4.2** | **Certificate Application Processing** | | | |
| **4.3** | **Certificate Issuance** | | | |
| 4.3.1 | CA actions during certificate issuance | 7.3.3<br>*7.3.3.a*<br>7.3.3.b<br>7.3.3.c<br>7.3.3.d | | |
| 4.3.2 | Notification to  subscriber by the CA of the issuance of the certificate | 7.3.5.a | | |
| **4.4** | **Certificate Acceptance** | | | |
| 4.4.1 | Conduct constituting certificate acceptance | *6.2 Note 2* | | 4.4.1-1 |

| No. | CP reference | ETSI requirement | Legal requirement | PKIo requirement |
|---|---|---|---|---|
| | | *7.3.1.m.vi* | | 4.4.1-2 |
| 4.4.2 | Publication of the certificate by CSP | | | |
| 4.4.3 | Notification of certificate issuance by the CSP to other entities | | | |
| **4.5** | **Key Pair and Certificate Usage** | | | |
| 4.5.1 | Subscriber private key and certificate usage | 6.2<br>6.2.b<br>6.2.c<br>6.2.f<br>6.2.g<br>6.2.i<br>6.2.j | | |
| 4.5.2 | Relying party public key and certificate usage | 6.3<br>*6.3.a*<br>*6.3 NOTE 2*<br>6.3.b<br>6.3.c | | 4.5.2-1<br>4.5.2-2 |
| **4.6** | **Certificate Renewal** | | | |

| **No.** | **CP reference** | **ETSI requirement** | **Legal requirement** | **PKIo requirement** |
|---|---|---|---|---|
| **4.7** | **Certificate Re-key** | | | |
| **4.8** | **Certificate Modification** | | | |
| **4.9** | **Certificate Revocation and Suspension** | *7.3.6*<br>7.3.6.g | | |
| 4.9.1 | Circumstances for revocation | | | 4.9.1-1 |
| 4.9.2 | Who can request revocation | | | 4.9.2-1 |
| 4.9.3 | Procedures for revocation request | 7.3.6.f<br>*6.3 Note 1*<br>*7.3.6.h.iii*<br>*7.3.6.j.iii*<br>*7.3.6.k* | Electronic Signature Regulation (BEH)[8] article 2 paragraph 1l | 4.9.3-1<br>4.9.3-2<br>4.9.3-3<br>4.9.3-4<br>4.9.3-5<br>4.9.3-6<br>4.9.3-7 |
| 4.9.4 | Revocation request grace period | | | |
| 4.9.5 | Time within which CSP must process the revocation request | *7.3.6.a*<br>7.3.6.b | | 4.9.5-1<br>4.9.5-2 |

[8] *BEH stands for Electronic Signature Regulation.*

| No. | CP reference | ETSI requirement | Legal requirement | PKIo requirement |
|---|---|---|---|---|
| | | *7.3.6.m* | | 4.9.5-3 |
| 4.9.6 | Revocation checking requirement for relying parties | | | 4.9.6-1<br>4.9.6-2 |
| 4.9.7 | CRL issuance frequency | 7.3.6.h<br>*7.3.6.i* | | 4.9.7-1 |
| 4.9.8 | Maximum latency for CRLs | | | |
| 4.9.9 | On-line revocation/status checking availability | | | 4.9.9-1<br>4.9.9-2<br>4.9.9-3<br>4.9.9-4<br>4.9.9-5<br>4.9.9-6 |
| 4.9.10 | On-line revocation checking requirements | | | |
| 4.9.11 | Other forms of revocation advertisements available | | | |
| 4.9.12 | Special requirements re key compromise | | | |
| 4.9.13 | Circumstances for suspension | *7.3.6.e* | | 4.9.13-1 |

| No. | CP reference | ETSI requirement | Legal requirement | PKIo requirement |
|---|---|---|---|---|
| **4.10** | **Certificate Status Service** | | | |
| 4.10.1 | Operational characteristics | 7.3.6.n<br>7.3.6.p | | |
| 4.10.2 | Service availability | *7.3.6.j* | | 4.10.2-1 |
| 4.10.3 | Optional features | | | |
| **4.11** | **End of Subscription** | | | |
| **4.12** | **Key Escrow and Recovery** | See par. 6.2.3 | | |
| **5** | **Facility, Management and Operational Controls** | 7.4.1<br>7.4.1.a<br>7.4.1.b<br>7.4.1.c<br>7.4.1.d<br>7.4.1.e<br>7.4.1.f<br>7.4.1.g | | |
| **5.1** | **Physical Security Controls** | 7.4.4 | | |

| No. | CP reference | ETSI requirement | Legal requirement | PKIo requirement |
|---|---|---|---|---|
| 5.1.1 | Site location and construction | 7.4.4.d<br>7.4.4.f | | |
| 5.1.2 | Physical access | 7.4.4.a<br>7.4.4.b<br>7.4.4.c<br>7.4.4.e<br>7.4.4.h | | |
| 5.1.3 | Power and air conditioning | 7.4.4.g | | |
| 5.1.4 | Water exposures | | | |
| 5.1.5 | Fire prevention and protection | | | |
| 5.1.6 | Media storage | 7.4.5.c<br>7.4.5.d<br>7.4.5.f | | |
| 5.1.7 | Waste disposal | | | |
| 5.1.8 | Off-site backup | | | |
| **5.2** | **Procedural Controls** | 7.4.5 | | |

| No. | CP reference | ETSI requirement | Legal requirement | PKIo requirement |
|---|---|---|---|---|
| 5.2.1 | Trusted roles | 7.4.3.g<br>*7.4.3.h*<br>7.4.3.i | | |
| 5.2.2 | Number of persons required for each task | | | |
| 5.2.3 | Identification and authentication for each role | | | |
| 5.2.4 | Roles that require separation of duties | *7.3.1.s*<br>7.4.5.k | | 5.2.4-1<br>5.2.4-2 |
| 5.2.5 | Maintenance and security | 7.4.5.a<br>7.4.5.b<br>7.4.5.g<br>7.4.5.h | | 5.2.5-1<br>5.2.5-2 |
| **5.3** | **Personnel Controls** | | | |
| 5.3 | Personnel controls | *7.4.3*<br>7.4.3.c<br>7.4.3.d<br>*7.4.3.e*<br>7.4.5.e<br>7.5.h | | 5.3-1<br>5.3-2 |

| No. | CP reference | ETSI requirement | Legal requirement | PKIo requirement |
|---|---|---|---|---|
| | | 7.5.i | | |
| 5.3.1 | Qualifications, experience, and clearance requirements | 7.4.3.a<br>7.4.3.f<br>7.4.3.k | | 5.3.1-1 |
| 5.3.2 | Background checks procedures | *7.4.3.j* | Electronic Signature Regulation art.2, paragraph 1s<br>Electronic Signature Regulation art.2, paragraph 2<br>Electronic Signature Regulation art.2, paragraph 3 | 5.3.2-1 |
| 5.3.3 | Training requirements | | | |
| 5.3.4 | Retraining frequency and requirements | | | |
| 5.3.5 | Job rotation frequency and sequence | | | |
| 5.3.6 | Sanctions for unauthorized actions | 7.4.3.b | | |
| 5.3.7 | Independent contractor requirements | | | |
| 5.3.8 | Documentation supplied to personnel | | | |

| **No.** | **CP reference** | **ETSI requirement** | **Legal requirement** | **PKIo requirement** |
|---|---|---|---|---|
| **5.4** | **Audit Logging Procedures** | | | |
| 5.4.1 | Types of events recorded | 7.4.5.i<br>7.4.11.g<br>7.4.11.h<br>7.4.11.d<br>7.4.11.k<br>7.4.11.l<br>7.4.11.m<br>7.4.11.n<br>7.4.11.o | | 5.4.1-1 |
| 5.4.2 | Frequency processing log | 7.4.5.j | | |
| 5.4.3 | Retention period for audit log | See 5.5.2 | | 5.4.3-1 |
| 5.4.4 | Protection of audit logs | 7.4.11.a<br>7.4.11.f | | |
| 5.4.5 | Audit log backup procedures | | | |
| 5.4.6 | Audit collection system (internal vs. External) | | | |
| 5.4.7 | Notification to event-causing subject | | | |

| No. | CP reference | ETSI requirement | Legal requirement | PKIo requirement |
|---|---|---|---|---|
| 5.4.8 | Vulnerability assessments | | | |
| **5.5** | **Records Archival** | | | |
| 5.5.1 | Types of records archived | 7.4.11<br>*7.4.11 Note 2*<br>7.4.11.i<br>*7.3.1.j*<br>*7.3.1.m* | | 5.5.1-1<br>5.5.1-2 |
| 5.5.2 | Retention period for archive | 7.4.11.e<br>*7.3.1.n* | | 5.5.2-1<br>5.5.2-2 |
| 5.5.3 | Protection of archive | 7.4.10.a<br>7.4.11.b | | |
| 5.5.4 | Archive backup procedures | | | |
| 5.5.5 | Requirements for time-stamping of records | | | |
| 5.5.6 | Archive collection system (internal or external) | | | |
| 5.5.7 | Procedures to obtain and verify archive information | | | |

| No. | CP reference | ETSI requirement | Legal requirement | PKIo requirement |
|---|---|---|---|---|
| **5.6** | **Key Changeover** | | | |
| **5.7** | **Compromise and Disaster Recovery** | | | |
| 5.7.1 | Incident and compromise handling procedures | *7.3.6.c*<br>*7.4.8.e*<br>*7.4.8.f*<br>*7.4.5 Note 2* | | 5.7.1-1<br>5.7.1-2<br>5.7.1-3<br>5.7.1-4 |
| 5.7.2 | Computing resources, software, and/or data are corrupted | | | |
| 5.7.3 | Entity private key compromise procedures | 7.4.8.d<br>7.4.8.g | | |
| 5.7.4 | Business continuity capabilities after a disaster | 7.4.8<br>7.4.8.a<br>7.4.8.b<br>7.4.8.c | | 5.7.4-1 |
| **5.8** | **CSP Termination** | 7.4.9<br>7.4.9.a<br>7.4.9.b<br>7.4.9.c | Electronic Signature Regulation art.2, paragraph 1p<br>Electronic Signature Regulation art.2, paragraph 1q | |

| No. | CP reference | ETSI requirement | Legal requirement | PKIo requirement |
|---|---|---|---|---|
| **6** | **Technical Security Controls** | | | |
| **6.1** | **Key Pair Generation and Installation** | | | |
| 6.1.1 | Key pair generation for the CSP sub CA | 7.2.1<br>7.2.1.a<br>*7.2.1.c*<br>*7.2.1.d* | | 6.1.1-1<br>6.1.1-4 |
| | Key pair generation of the certificate holders | 6.2.d<br>6.2.e<br>7.2.8<br>*7.2.8.a* | | 6.1.1-2<br>6.1.1-3 |
| 6.1.2 | Private key and SSCD delivery to certificate holder | *7.2.8.c*<br>*7.2.8.d*<br>*7.2.8.e*<br>7.2.9<br>7.2.9.a<br>7.2.9.b<br>7.2.9.c | | |
| 6.1.3 | Public key delivery to certificate issuer | | | |

| **No.** | **CP reference** | **ETSI requirement** | **Legal requirement** | **PKIo requirement** |
|---|---|---|---|---|
| 6.1.4 | / | 7.2.3<br>7.2.3.a | | |
| 6.1.5 | Key sizes | *7.2.8.b* | | 6.1.5-1 |
| 6.1.6 | Public key parameters generation and quality checking | | | |
| 6.1.7 | Key usage purposes (as per X.509 v3 key usage field) | *7.2.5*<br>7.2.5.a<br>7.2.5.b | | 6.1.7-1 |
| **6.2** | **Private Key Protection and Cryptographic Module Engineering Controls** | | | |
| 6.2.1 | Cryptographic module standards and controls | 7.2.1.b<br>7.2.2<br>7.2.2.a<br>7.2.2.b | | |
| 6.2.2 | Private CSP key (n out of m) multi-person control | | | |
| 6.2.3 | Private key escrow of certificate holder key | 7.2.4<br>*7.2.4.a*<br>7.2.4.b | | 6.2.3-1 |

| **No.** | **CP reference** | **ETSI requirement** | **Legal requirement** | **PKIo requirement** |
|---|---|---|---|---|
| 6.2.4 | Private key backup | | | |
| 6.2.4.1 | Private key backup of the CSP key | 7.2.2.c<br>7.2.2.d | | |
| 6.2.4.2 | Private key backup of certificate holder key | | | 6.2.4.2-1 |
| 6.2.5 | Private key archival of certificate holders key | | | 6.2.5-1 |
| 6.2.6 | Private key transfer into or from a cryptographic module | 7.2.2.e | | |
| 6.2.7 | Private key storage on cryptographic module | | | |
| 6.2.8 | Method of activating private key | | | |
| 6.2.9 | Method of deactivating private key | | | |
| 6.2.10 | Method of destroying private key | 7.2.6.b | | |
| 6.2.11 | Cryptographic Module Rating | *3.1* | | 6.2.11-1<br>6.2.11-2<br>6.2.11-3 |
| **6.3** | **Other Aspects of Key Pair Management** | | | |

| No. | CP reference | ETSI requirement | Legal requirement | PKIo requirement |
|---|---|---|---|---|
| 6.3.1 | Public key archival | | | |
| 6.3.2 | Certificate operational periods and key pair usage periods | 7.2.1.e<br>*7.2.6* | | 6.3.2-1<br>6.3.2-2 |
| **6.4** | **Activation data** | | | |
| 6.4.1 | Activation data generation and installation | *7.2.9.d* | | 6.4.1-1<br>6.4.1-2 |
| 6.4.2 | Activation data protection | | | |
| 6.4.3 | Other aspects of activation data | | | |
| **6.5** | **Computer Security Controls** | | | |
| 6.5.1 | Specific computer security technical requirements | 7.4.6<br>7.4.6.c<br>7.4.6.d<br>7.4.6.e<br>7.4.6.f<br>7.4.6.j<br>7.4.6.l | | 6.5.1-1<br>6.5.1-2<br>6.5.1-3 |

| No. | CP reference | ETSI requirement | Legal requirement | PKIo requirement |
|---|---|---|---|---|
| 6.5.2 | Computer security rating | 7.4.2<br>7.4.2.a | | |
| **6.6** | **Life Cycle Technical Controls** | | | |
| 6.6.1 | System development controls | *7.4.7*<br>7.4.7.a<br>7.4.7.b | Electronic Signature Directive art.2, paragraph 1c | 6.6.1-1 |
| 6.6.2 | Security Management Controls | | | |
| 6.6.3 | Life cycle security classification | | | |
| 6.6.4 | Life cycle of cryptographic hardware for signing certificates | 7.2.7<br>7.2.7.a<br>7.2.7.b<br>7.2.7.c<br>7.2.7.d<br>7.2.7.e | | |
| **6.7** | **Network Security Controls** | 7.4.6.a<br>7.4.6.b<br>7.4.6.g<br>7.4.6.h | | 6.7.1-1<br>6.7.1-2<br>6.7.1-3 |

| **No.** | **CP reference** | **ETSI requirement** | **Legal requirement** | **PKIo requirement** |
|---|---|---|---|---|
| | | 7.4.6.i<br>7.4.6.k<br>7.3.3.f<br>7.3.3.g | | |
| **6.8** | **Time-stamping** | | | |
| **7** | **Certificate, CRL and OSCP Profiles** | | | |
| **7.1** | **Certificate Profile** | | | 7.1-1 |
| **7.2** | **CRL Profile** | | | 7.2-1 |
| **7.3** | **OCSP Profile** | | | 7.3-1 |
| **8** | **Complicance Audit and Other Assessments** | | | See chapter 8 |
| **9** | **Other Business and Legal Matters** | | | |
| **9.1** | **Fees** | | | |
| **9.2** | **Financial Responsibility** | | | |
| 9.2.1 | Insurance cover | *7.1.k* | | 9.2.1-1 |

| No. | CP reference | ETSI requirement | Legal requirement | PKIo requirement |
|---|---|---|---|---|
| | | *7.5.d* | | 9.2.1-2<br>9.2.1-3 |
| 9.2.2 | Other assets | | | 9.2.2-1 |
| **9.3** | **Confidentiality of Business Information** | | | |
| **9.4** | **Privacy of Personal Information** | | | |
| 9.4.1 | Privacy plan | | | |
| 9.4.2 | Information treated as private | 7.4.11.j | | |
| 9.4.3 | Information not deemed private | | | |
| 9.4.4 | Responsibility to protect private information | 7.4.10.c | | |
| 9.4.5 | Notice and consent to use private information | 7.3.5.b<br>7.4.10.b<br>7.4.10.d | | |
| 9.4.6 | Disclosure pursuant to judicial or administrative process | 7.4.11.c | | |
| 9.4.7 | Other information disclosure circumstances | | | |

| **No.** | **CP reference** | **ETSI requirement** | **Legal requirement** | **PKIo requirement** |
|---|---|---|---|---|
| **9.5** | **Intellectual Property Rights** | | | 9.5-1 |
| **9.6** | **Representations and Warranties** | | | |
| 9.6.1 | CSP representations and warranties | *6.4* | | 9.6.1-1<br>9.6.1-2 |
| 9.6.2 to 9.6.5 | Various articles concerning liability | | | |
| **9.7** | **Disclaimers of Warranties** | | | |
| **9.8** | **Limitations of Liability** | | | 9.8-1<br>9.8-2 |
| **9.9** | **Indemnities** | | | |
| **9.10** | **Term and Termination** | | | |
| **9.11** | **Individual notices and communications with participants** | | | |
| **9.12** | **Amendments** | | | |
| 9.12.1 | Procedure for amendment | | | 9.12.1 |

| **No.** | **CP reference** | **ETSI requirement** | **Legal requirement** | **PKIo requirement** |
|---|---|---|---|---|
| 9.12.2 | Notification mechanism and period | | | 9.12.2-1<br>9.12.2-2 |
| 9.12.3 | Circumstances under which OID must be changed | | | |
| **9.13** | **Dispute Resolution Provisions** | *7.5.f* | Electronic Signature Regulation art.2, paragraph 1n | 9.13-1 |
| **9.14** | **Governing Law** | | | 9.14 |
| **9.15** | **Compliance with Applicable Law** | 7.4.10 | | |
| **9.16** | **Miscellaneous Provisions** | | | |
| **9.17** | **Other provisions** | 6.1<br>7.1.f<br>7.1.g<br>7.1.j<br>7.5<br>7.5.a<br>7.5.b<br>7.5.c<br>7.5.e<br>7.5.g | | 9.17 |

# 10 Revisions

## 10.1 Amendments from version 3.5 to 3.6

### *10.1.1 New*

- Requirement 6.1.1-4 (effective date 4 weeks after publication of PoR 3.6);
- Certification against ETSI TS 102 042 including PTC-BR in pararagraph.1.1.1 4 (effective date 1 June 2014);
- Certification against ETSI TS 102 042 including PTC-BR and Netsec in paragraph.1.1.1 4 (effective date 1 December 2014);

## 10.2 Amendments from version 3.4 to 3.5

### *10.2.1 New*

- Requirement 4.9.9-6 (effective date no later than 4 weeks after publication of PoR 3.5 );

### *10.2.2 Modifications*

- Explanation of attribute SerialNumber (effective date no later than 4 weeks after publication of PoR 3.5 );
- Requirement 3.2.2-1 (effective date no later than 4 weeks after publication of PoR 3.5 );

## 10.3 Amendments from version 3.3 to 3.4

### *10.3.1 New*

- Requirement 2.2-7 (effective date no later than 4 weeks after publication of PoR 3.4 );
- Requirement 5.2.5-2 (effective date no later than 4 weeks after publication of PoR 3.4 );
- Requirement 5.3.2-1 (effective date no later than 4 weeks after publication of PoR 3.4 );

### *10.3.2 Modifications*

- Requirement 4.1-1 (effective date no later than 4 weeks after publication of PoR 3.4 );
- Requirement 4.9.9-5 (effective date no later than 4 weeks after publication of PoR 3.4 );
- Requirement 5.3.1-1 (effective date no later than 4 weeks after publication of PoR 3.4 );
- Description and explanation in respect of subject.Countryname (already effective by means of accelerated amendment procedure on 1-10-2012);
- Paragraph 9.12.1 relating to the change procedure

### *10.3.3 Editorial*

- Requirement 5.4.1-1 (effective date no later than 4 weeks after publication of PoR 3.4 );

## 10.4 Amendments from version 3.2 to 3.3

### *10.4.1 New*

- Requirement 4.1-1 and 4.4.1-1;
- Requirement 4.1-2
- Requirement 4.5.2-2
- Requirement 5.2.5-1 (effective date no later than 1-12-2012)
- Requirement 5.3.1-1
- Requirement 5.4.3-1
- Requirement 5.5.2-2
- Requirement 5.7.1-3
- Requirement 5.7.4-1 (effective date no later than 1-12-2012).

### *10.4.2 Modifications*

- Requirement 2.2-4
- Requirement 3.2.5-3
- Requirement 4.9.9-3
- Requirement 5.4.1-1
- Requirement 5.5.1-1
- Requirement 5.5.1-2
- Requirement 5.7.1-1 (effective date no later than 1-10-2012)
- Requirement 5.7.1-2 (effective date no later than 1-10-2012)
- Requirement 6.5.1-3
- Requirement 6.7.1-1
- Explanation in respect of attributes Subject.commonName, SubjectAltName.iPAddress, SubjectAltName.dNSName and Extkeyusage.

### *10.4.3 Editorial*

A number of editorial changes have been made but these do not affect the content of the information.

## 10.5 Amendments from version 3.1 to 3.2

### *10.5.1 New*

- Requirement 5.4.1-1 (effective date no later than 1-6-2012)
- Requirement 6.5.1-3 (effective date no later than 1-7-2012)
- Requirement 6.7.1-1 (effective date no later than 1-7-2012)
- Requirement 6.7.1-2 (effective date no later than 1-7-2012)
- Requirement 6.7.1-3

### *10.5.2 Modifications*

- Requirement 3.2.1-1
- Requirement 4.5.2-1 (effective date no later than 1-2-2012)
- Requirement 5.2.4-2
- Requirement 5.7.1-2

### *10.5.3 Editorial*

A number of editorial changes have been made but these do not affect the content of the information.

## 10.6 Amendments from version 3.0 to 3.1

### *10.6.1 New*

- Requirement 4.9.73.2.1-1-1, 4.9.9-4, 6.5.1-1 and 6.5.1-2.

### *10.6.2 Modifications*

- Requirement 4.9.1-1;
- Explanation of attribute SerialNumber.

### *10.6.3 Editorial*

A number of editorial changes have been made but these do not affect the content of the information.

## 10.7 Version 3.0

First version.