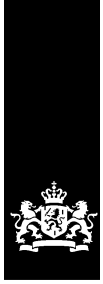

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Programme of Requirements part 1: Introduction

Date 28 January 2014

Publisher's imprint

Version number 3.6
Contact person Policy Authority PKIoverheid

Organization Logius

Street address
Wilhelmina van Pruisenweg 52

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

T 0900 - 555 4555
servicecentrum@logius.nl

Contents

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

The government's PKI 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 government's PKI, the Programme of Requirements (PoR);
- supervising and preparing for the process of admittance of Certification Service Providers (CSPs) to the government's PKI;
- regulating and monitoring the activities of CSPs that issue certificates under the root of the government's PKI.

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

Revision control

Version	**Date**	**Description**
1.0	09-11-2005	Ratified by the Ministry of the Interior and Kingdom Relations November 2005
1.1	25-01-2008	Ratified by the Ministry of the Interior and Kingdom Relations January 2008
1.2	13-01-2009	Ratified by the Ministry of the Interior and Kingdom Relations January 2009
2.0	09-10-2009	Ratified by the Ministry of the Interior and Kingdom Relations October 2009
2.1	11-01-2010	Amendments further to a change of name from GBO.Overheid to Logius
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

1.1 Aim of the Programme of Requirements

This is part 1 of the Programme of Requirements (PoR) for the PKI for the government. The purpose of the PoR is to lay down requirements for the use of the government's PKI and to inform the parties involved in the PKI for the government accordingly.

This part introduces the PoR. First of all, in chapter 1 the history of the PKI for the government is described and a short introduction to PKI (Public Key Infrastructure) is provided. Chapter 2 then outlines the design of the PKI for the government, in which the criteria and architecture are dealt with. Chapter 3 describes the requirements that apply within the PKI for the government and how these are positioned within the PKI for the government. The chapter also outlines how the trustworthiness of the services within the PKI for the government is safeguarded and can be verified. Finally, chapter 4 incorporates a summary, providing an explanation on all parts of the PoR.

1.2 History

The Dutch government has high ambitions in the area of electronic services; these are outlined in the "Andere Overheid (Different Government)" programme of action. This specifically expresses the goal that, by 2007 65% of public services have to be offered via the Internet. In late 2007 it was established that this goal had been achieved[1]. An essential condition for electronic services is the trustworthiness of the electronic communication. For example, an electronic grant application generally asks that the identity of the involved parties is established, for a declaration of intent that a public service is actually being requested and for confidentiality regarding the communication between the applicant and the government body providing the grant.

All of the foregoing can be made possible by using generic mechanisms, such as identification and an electronic signature based on Public Key Cryptography. Public Key Cryptography can be used in various ways to ensure trustworthy electronic communication, which is termed a Public Key Infrastructure (PKI). PKI is a very effective basis for the cryptographic part of information security.

Towards the end of 1999, following a decision by the Council of Ministers, the PKIoverheid Task Force was set up. The work of the PKIoverheid Task Force led to a top structure for the PKI for the government being established in 2002[2]. In 2003, the first Certification Service Provider (CSP) joined the PKI for the government and now several organizations are active as CSPs within the PKI for the government.

[1] *See report "Publieke dienstverlening 65% electronisch (65% of all public services electronic)" dated 5 December 2007*

[2] *Paragraph 2.4 details this top structure, plus the full design of the government's PKI .*

In 2003, the Policy Authority (PA) of the PKI for the government was established as an offshoot of the PKIoverheid Task Force. The PA manages the PKI for the government top structure and of the framework of standards (Programme of Requirements, PoR) that underlies the PKI for the government. In the PA's Certification Practice Statement (CPS), the activities performed by the PA, in terms of the management of the PKI for the government, are described in detail. This CPS can be found at www.logius.nl/pkioverheid.

1.3 Why PKI

1.3.1 Need for trust

The need for PKI cannot be seen separately from the growing need for electronic communication and services within society in general and the government in particular. There is an increasing demand for transactions to be dealt with electronically. The user does not have to physically visit his transaction partner and, in a user-friendly manner, can perform the transaction from his PC. Furthermore, the recipient of a transaction request can streamline his administrative organization with the new technology and, by doing so, organize his business process more efficiently. This meets the ever increasing demand for high-quality services in the 24-hour economy.

A precondition for a full and completely electronic service is a reliable mechanism that can ensure the same safeguards that currently apply in the "paper" world. This applies to all services, both government services and services within the ordinary economic traffic. Electronic transactions require the identity of the involved parties to be established, the declaration of intent of parties and the confidentiality of the communication between transaction partners.

1.3.2 Opportunities of PKI

The PKI for the government provides communicating parties with safeguards in relation to:

- the identity of a person who purchases a service or the service itself (identification and authenticity);
- the (legal) certainty that a message has been sent by a specific person or a document has been signed by a specific person and that this cannot be denied afterwards (electronic signature, non-repudiation);
- the ability to protect communication against unwanted access (confidentiality, privacy) or amendment (integrity) by third parties.

1.3.3 What is a PKI and how does it work

A PKI is an infrastructure comprising organizational and technical components, within which secure communication is possible. The foundation for PKI is formed by the asymmetric cryptographic algorithms that are used. With this system, the user receives a key pair, comprising a private key which is only known to him and a public key, which is accessible by everyone. A user's private and public keys are inextricably tied together. The public key can be distributed (for example in a database, cf. a telephone book); the private key has to be carefully kept secret by the user.

Using these key pairs, secure electronic communication can take place. To apply a digital signature and to achieve confidentiality and authentication, various transactions are performed with the keys.

What is the guarantee that a used key does in fact belong to the sender/recipient? The solution for the linkage between the user and the key pair is achieved by PKI. The user is given a digital identity, a certificate, which states that the public key belongs to him. A certificate is a small file containing the user's details, along with his public key. These details are then signed electronically by a Certification Service Provider. Using the certificate, the recipient, also known as the relying party, can check whether the sender is actually who he says he is. The relying party places trust in the CSP that certified the details in the certificate with its electronic signature. You can find a further explanation regarding the operation of PKI at www.logius.nl/pkioverheid.

1.3.4 Opting for PKI

In addition to PKI there are also other mechanisms for establishing identities electronically. Consider the use of passwords, PIN codes and tools that generate one-time codes. However, unlike PKI, these mechanisms do not offer support for confidentiality or the legal equivalence with the handwritten signature. Therefore, when there is a need to communicate information confidentially and/or for an electronic signature to be included that is legally equivalent to the handwritten signature, PKI is the perfect solution.

The support of multiple functions by PKI is often the reason for using PKI to ensure secure communication. PKIoverheid certificates are now used in various processes within the government and the business world. At www.logius.nl/pkioverheid there is an up-to-date list of organizations that act as CSPs with the PKI for the government.

1.4 Status

This is version 3.6 of part 1 of the Programme of Requirements. The current version has been updated up to January 2014 inclusive.

All parts of the PoR are version controlled. Change requests are dealt with in accordance with the procedure described in the document "Procedurebeschrijving wijzigingen in PvE (Procedural description amendments in PoR)". This document can be consulted at the following website www.logius.nl/pkioverheid.

1.5 Normative references

The standards, legislation and regulations referred to in this document are as follows:

[1] Wet Elektronische Handtekeningen (Electronic Signatures Act)
Act dated 8 May 2003 amending Book 3 and Book 6 of the Civil Code, the Telecommunications Act and the Law on Economic Crime concerning electronic signatures for implementation of Directive no. 1999/93/EC of the European Parliament and the Council of the European Union dated 13 December 1999 regarding a common framework for electronic signatures (PbEG L 13).

[2] Besluit Elektronische Handtekeningen (Electronic Signatures Decree)
Decree dated 8 May 2003, establishing the requirements for providing services for electronic signatures.

[3] Regeling Elektronische Handtekeningen (Electronic Signatures Regulation), 6 May 2003 no. WJZ/03/02263
Regulation of the Secretary of State for Economic Affairs establishing further rules with regard to electronic signatures.

[4] Beleidsregel aanwijzing certificatieaties elektronische handtekeningen (Policy rule instruction for certification organizations for electronic signatures), 6 May 2003 no. WJZ/03/02264
Policy rule of the Secretary of State for Economic Affairs with regard to the instruction of organizations that test certification service providers against compliance with the requirements laid down in or pursuant to the Telecommunications Act, under article 18.16 of the Telecommunications Act.

[5] ETSI EN 319 411-2 v.1.1.1 (2013-01), "Electronic Signatures and Infrastructures (ESI);Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Policy requirements for certification authorities issuing qualified certificates This European Norm contains the requirements for CSPs that issue qualified certificates for electronic signatures to the public. Within the PKI for the government, this standard is laid down for all of its CSPs for the issuance of personal certificates.

[6] ETSI TS 102 042 V2.3.1 (2012-11), "Policy requirements for certification authorities issuing public key certificates", ESI.
This Technical Specification contains the requirements for CSPs that issue public key certificates to the public. Within the PKI for the government, this standard is specifically laid down for CSPs that issue non-personal certificates.

[7] TTP.NL Scheme for management system certification of Service Providers issuing Qualified Certificates for Electronic Signatures, Public Key Certificates, and/or Time-stamp tokens, version 8.1_final
The aim of this scheme is to provide criteria and procedures for certification investigations being performed by independent institutions and certifying Certification Authorities (CAs) that issue qualified certificates.

[8] EN 45012:1998, General requirements for bodies operating assessment and certification/registration of quality systems.

[9] "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures", CEN/ISSS WS/E-Sign (CWA 14167-1).
This is an elaboration of the requirements for systems of certification service providers, as listed in Appendix II (sub f) of European Directive 1999/93/EC.

[10] ETSI TS 102 176-1 v2.0.0 (2007-11), "Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms.
This document describes which algorithms and key lengths are allowed within the PKI for the government.

[11] "Security Requirements For Cryptographic Modules", NIST (FIPS PUB 140-2).
This outlines the requirements of the American government for cryptographic products.

[12] "Secure Electronic Signature Devices, Version EAL 4+", CEN/ISSS WS/E-Sign (CWA 14169).
This outlines the requirements for the secure tool for creating electronic signatures, as mentioned in Appendix III of the guideline.

[13] "EESSI Conformity Assessment Guidance - Part 2: Certification Authority services and processes", CEN/ISSS WS/E-Sign (CWA 14172-2).
This provides clarification of the requirements for certification service providers.

[14] "Cryptographic module for CSP Signing Operations" – Protection Profile CEN/ISSS WS/E-Sign (CWA 14167-2).
This outlines the requirements for the cryptographic product specifically used by a certification service provider.

[15] "EESSI Conformity Assessment Guidance – Part 3: Trustworthy systems managing certificates for electronic signatures", CEN/ISSS WS/E-Sign (CWA 14172-3).
This provides clarification of the requirements for the systems used by a certification service provider.

[16] "Cryptographic module for CSP Signing Operations" – Protection Profile CEN/ISSS WS/E-Sign (CWA 14167-4).
This outlines the requirements for the cryptographic product specifically used by a certification service provider.

2 Overview of the PKI for the government

2.1 Introduction

This chapter first covers the strategic criteria that underlie the PKI for the government. It then deals with the certificate model that is used and finally an explanation is given about the design of the PKI for the government.

2.2 Strategic criteria

To execute PKI services within the PKI for the government, the following strategic criteria apply:

- Workable infrastructure. The PKI for the government facilitates the communication between government and government, between government and businesses, between businesses and businesses and between the government and citizen (communication domains).
- One established trust level. The trust level of the PKI for the government is based on the Electronic Signatures Act and international standards. This enables users to use the government's electronic services with one type of signature, which has the same legal consequences as a handwritten signature.
- Organizational interoperability. High demands are made on organizations that wish to issue certificates within the PKI for the government with regard to registering, producing, issuing, managing and monitoring certificates and key pairs. These demands are incorporated in the Certificate Policy (CP)[3], which is part of the PoR (part 3). These demands are placed on all parties within the PKI for the government.
- Technical interoperability. The PKI for the government is based on open standards by means of which interoperability is achieved. This enables various suppliers to offer products within the PKI for the government and means process owners are not dependent on one provider.
- Certificates for roles. Within the PKI for the government, certificates are issued in a number of domains, which are the Government/Companies, Organization, Citizen and Autonomous Devices domain. In the Government/Companies and Organization domains, certificates are issued to entities that are attached to an organization, or that act under a recognized profession. In the Citizen domain, certificates are issued to individuals. This provides transparency about the role that a person fulfils in the electronic communication. In the Autonomous Devices domain, certificates are issued to devices that, during their operational lives, independently safeguard the integrity and authenticity of (measurement) data for (a specific objective within a core task of) a specific government agency.
- The central part of the PKI for the government is the determinative factor for trust. The trustworthiness of the PKI for the government is determined by the trustworthiness of the central part. The PA's Certification Practice Statement describes which procedures and measures the PA has taken to safeguard the security of the central part.

[3] *A CP describes the requirements laid down for the issuance and use of a specific type of certificate. By contrast, a Certification Practice Statement (CPS) describes how a CSP meets these requirements. The CPs are compiled by the PA and apply to all CSPs in a domain. By contrast, the CPS is compiled by every individual CSP.*

2.3 Certificate model

The certificate plays a key role within a PKI (also see paragraph 1.3). That is because the certificate enables the certificate holder to obtain a digital identity. Within the PKI for the government, a distinction is made between certificates for people, certificates for services (for example systems and applications), Extended Validation SSL certificates and certificates for Autonomous Devices. In the paragraphs below, an explanation is given about the certificate model that is used within the PKI for the government.

2.3.1 Personal certificates

Certificates for individuals are linked to the person (or linked to the identity). People in different capacities can obtain different certificates: as a citizen, as an employee of a government organization or company or working in a recognized profession. The PKI for the government uses three separate certificates and keys for the electronic signature, authenticity and confidentiality. This is also known as the 3-certificate model.

The electronic signature certificate fulfils the legal requirements published in the European Directive 1999/93/EC and outlined in Dutch legislation[4], of a signature relating to electronic data, in the same way as a handwritten signature.

The authenticity certificate is suitable for reliable electronic identification and authentication of people.

The confidentiality certificates that are issued within the PKI for the government are suitable for protecting the confidentiality of data that is interchanged electronically.

The authentication and confidentiality certificates have the same trust level as the qualified certificate. This means that the requirements laid down in respect of the electronic signature certificate also apply to the authenticity certificate and the confidentiality certificate.

2.3.2 Services certificates

The services certificate is a certificate that is not linked to a specific person. This kind of certificate applies when the certificate holder is a device or a system (a non-natural person), operated by or on behalf of an organizational entity. But this also applies when a certificate, under the responsibility of an organizational entity, is not linked to one certificate holder. An example of this is a certificate that is linked to a position (job); when an employee leaves, a different person will take over the job, and the certificate can be given to this person.

The PKI for the government uses three separate services certificates and keys, which are an authenticity certificate, a confidentiality certificate and a server certificate. The authenticity and confidentiality certificates can be used in both of the categories described above. The server certificate only belongs to the first category (device or system). With services certificates it is particularly important that certainty is provided about the connection between the device, the system or the position and the organization listed in the certificate.

[4] *This concerns the Electronic Signatures Act and Decree and corresponding Regulations.*

The three types of services certificates have the same security level. This security level is based on the level of the personal certificates.

2.3.3 Extended Validation (EV) SSL certificates

EV SSL certificates are not personal certificates. These can be used to secure a connection, through the TLS/SSL protocol, between a specific client and a server that belongs to the organizational entity listed as subscriber in the relevant certificate.

One of the main properties of an EV SSL certificate is that this colours the address bar of the browser green. This means that the identity of the website's owner, which is given in the SSL certificate, is validated based on the extremely strict EV guidelines.

2.3.4 Autonomous device certificates

The autonomous device certificate is a non-personal certificate that is issued in the Autonomous Devices domain. This kind of certificate applies when the certificate holder is a device, where the operation and the method of production is demonstrable in accordance with the framework of standards of the specific type of autonomous devices and that, in that capacity, is authorized by the framework author to use the autonomous device certificate linked to (for example, the serial number of) that device.

The PKI for the government uses three separate autonomous devices certificates and keys, which are an authenticity certificate, a confidentiality certificate and a combination certificate.

Authenticity certificates can be used for the electronic identification and authentication of the Autonomous Device and its certified operation. Confidentiality certificates can be used to protect the confidentiality of data that is exchanged using the Autonomous Device and/or that is stored within that device in an electronic format. Combination certificates can be used to secure a connection between a specific client and an Autonomous Device.

2.4 Design of the PKI for the government

The government's Public Key Infrastructure (PKI) has a structure where a central and an operational or local part of PKIoverheid are defined. This is a structure or root (Staat der Nederlanden (State of the Netherlands) Root CA) based on the SHA-1 algorithm, a root (Staat der Nederlanden (State of the Netherlands) Root CA – G2) based on the SHA-256 algorithm and a root (Staat der Nederlanden Root CA – G3) also based on the SHA-256 algorithm.

The root and the domains based on the SHA-1 algorithm will be denoted as G1, where G stands for generation. The root and the domains based on the SHA-256 algorithm will be denoted as G2 and G3.

In addition, there is a separate structure or root (State of the Netherlands EV Root CA) for the issue of PKIoverheid EV SSL certificates.

For the G1 (SHA-1) root, there are the Government/Companies domains (these two domains have merged over time) and the Citizen domain.

The G2 (SHA-256) contains the following domains:

- Organisation

- Citizen
- Autonomous Devices

The G3 (SHA-256) bevat contains the following domains:
- Organisation Person
- Citizen
- Organisation Services
- Autonomous Devices

2.4.1 Description of the structure State of the Netherlands Root CA structure

Within the central part of the structure of the State of the Netherlands Root CA structure, a number of actors are distinguished. These actors are:

1. the Government (Ov)-PA, responsible at the highest level for laying down the policy and general standards that apply within the structure of the State of the Netherlands Root CA and the issue of certificates;
2. the Ov-CA, concerns a technical component that produces the highest (or Root) certificate within the structure of the State of the Netherlands Root CA and produces certificates for the underlying domain CAs;
3. the Domain (D)-PA, that is responsible for the domain-specific content of the Ov-PA standards, and determines the conditions of the issue of certificates within a domain;
4. the D-CA, concerns a technical component that performs the actual production of certificates for the CSPs.

The coordinating government level and the domain level form the PKI's policy structure. Within these levels, policy and standards are laid down and the regulation is organized.

The CSP level is the operational or local part of the State of the Netherlands Root CA structure, where the direct interaction with the users takes place. At CSP level, the CSP organization is ultimately responsible for issuing certificates.

The CSP level is the operational level where the direct interaction with the users of the State of the Netherlands Root CA structure takes place. At CSP level, the CSP organization is ultimately responsible for issuing certificates. The certificates of the CSPs are generated by the CAs domain. Further details are shown in figure 1 below. This figure also shows the certificates from the central infrastructure, which are the root certificate (1), the domain certificates (2) and the CSP certificates (3). As shown in the figure, the Policy Authority CPS describes the procedures followed by the PA when issuing and managing the certificates from the central infrastructure. In the following paragraphs, the various levels and components are described in more detail.

2.4.2 Coordinating Government level and Domain level

Maintenance of the entire agreements system and organization of the required supervision are tasks and responsibilities referred to in PKI terms as the PA (Policy Authority). The PA of PKIoverheid has a number of roles within the State of the Netherlands Root CA structure; a few of the important roles are mentioned below:

- to maintain the framework of standards (PoR), which lists the requirements for each domain;

- identifying consequences for and required adaptations of legislation and regulations;
- maintaining the central part of the State of the Netherlands Root CA structure and making sure that parties are included within the hierarchy of the State of the Netherlands Root CA structure;
- enforcing the supervision of the hierarchy (CSPs);
- making preparations in relation to admitting CSPs to the State of the Netherlands Root CA structure;
- executing the admission of CSPs including creation, issue and maintenance of CSP certificates;
- regular publication of the State of the Netherlands Root CA G1, G2, G3 and domain CRLs;
- following the international standardisation developments and, if necessary, taking the initiative in relation to these developments, as well as synchronising these with developments in respect of the PKI of foreign governments.

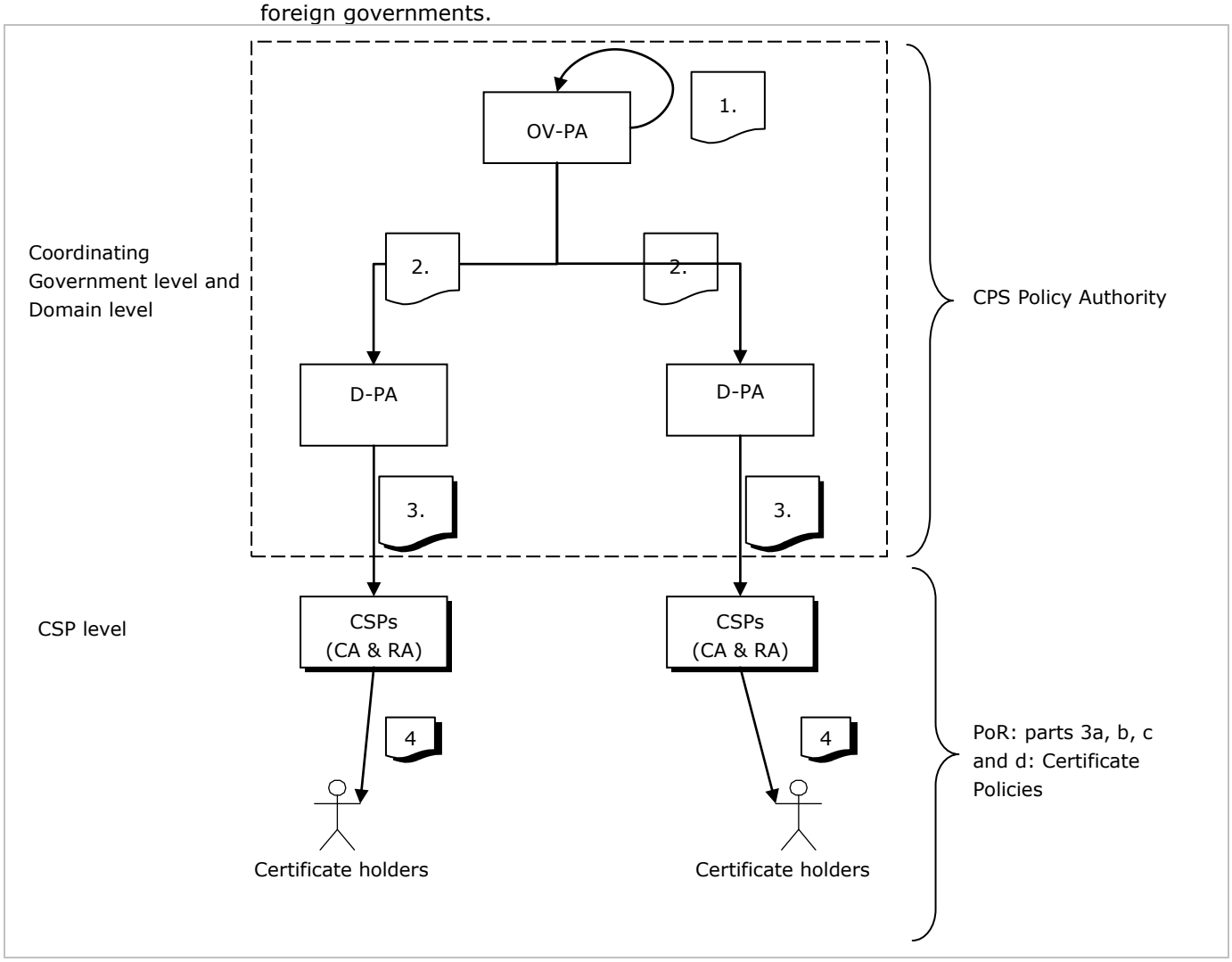

Figure 1

2.4.3 *Description of the structure State of the Netherlands EV Root CA*
The structure of the State of the Netherlands EV Root CA largely corresponds with the structure of the State of the Netherlands Root CA G1 and G2.

Within the central part of the structure of the State of the Netherlands EV CA a number of actors are distinguished. These actors are:

1. the Government (Ov)-PA, responsible at the highest level for laying down the policy and general standards that apply within the structure of the State of the Netherlands EV Root CA and the issue of certificates;
2. the Ov-CA, concerns a technical component that produces the highest (or Root) certificate within the State of the Netherlands EV CA and produces certificates for the underlying domain CAs;
3. the intermediary I-CA, concerns a technical component that actually produces certificates for the CSPs.

The coordination government level forms the policy structure of the State of the Netherlands EV Root CA structure. Within this level, policy and standards are laid down and the regulation is organized.

The CSP level is the operational or local part within the State of the Netherlands Root CA structure, where the direct interaction with the users takes place. At CSP level, the CSP organization is ultimately responsible for issuing EV SSL certificates.

The CSP level is the operational level where the direct interaction with the users takes place. At CSP level, the CSP organization is ultimately responsible for issuing EV SSL certificates. The certificates of the CSPs are generated by the State of the Netherlands EV Intermediary CA. Further details are provided in figure 2 below. This figure also shows the certificates in the central infrastructure, which are the State of the Netherlands EV Root CA (1), the State of the Netherlands EV Intermediary CA certificate (2) and the EV CSP certificates (3). As shown in the figure, the CPS Policy Authority describes the procedures that are used by the PA when issuing and managing the EV certificates from the central infrastructure. In the following paragraphs, the various levels and components are described in more detail.

2.4.4 Coordinating Government and Intermediate level

Maintenance of the entire agreements system and organization of the required regulation are tasks and responsibilities referred to in PKI terms as the PA (Policy Authority). The PA PKIoverheid has a number of tasks within the State of the Netherlands EV Root CA; a few of the important tasks are mentioned below:

- maintaining the framework of standards PoR part 3e;
- identifying consequences for and required adaptations of legislation and regulations;
- maintaining the central part of the State of the Netherlands EV Root CA structure and making sure that parties are included within the hierarchy of the State of the Netherlands EV Root CA structure;
- enforcing the supervision of the hierarchy (CSPs);
- making preparations in relation to admitting CSPs to the State of the Netherlands EV Root CA structure;
- implementation of the admission of CSPs including creation, issue and maintenance of EV CSP CA certificates;
- regular publication of the State of the Netherlands EV Root CA and the State of the Netherlands EV Intermediary CA CRLs;
- following the international standardisation developments and, if necessary, taking the initiative in relation to these developments, as

well as coordinating with developments in respect of the PKI of foreign governments.

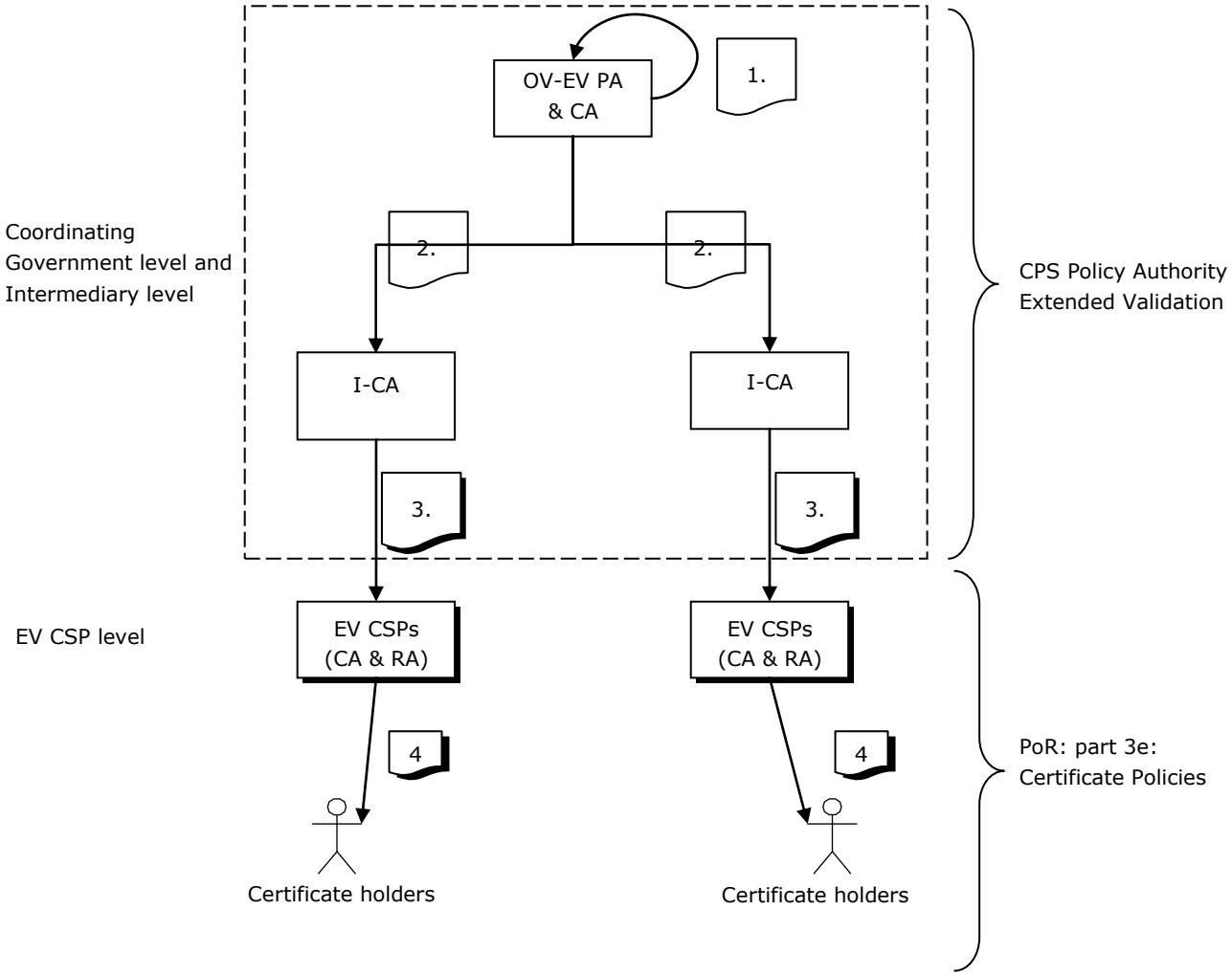

Figure 2

2.4.5 Operational level

CSP level
Below the central infrastructure is the layer where, in terms of the European Directive and the Dutch Law, the Certification Service Provider (CSP) resides. The CSP is responsible for issuing certificates to end users, both in the form of natural persons and other end entities. The organization that performs the CSP function is included in the certificate in the "issuer" field. Several CSPs are active within the PKI for the government based on the requirements laid down by the PA.

RA
The RA is a sub-activity that falls under the responsibility of the CSP. In the RA process, the identity of the applicant for a certificate is verified before the certificate is issued. The RA process consists of the registration of the request, the verification of the identity of the applicant and the issuance of the certificate. The RA has a clear relationship with one or more CAs (for example, for the various types of certificates): The RA instructs the CAs to produce certificates.

CA
The CA is a sub-activity that is performed under the responsibility of the CSP. After registration and successful verification, the certificate has to be produced. The RA instructs the CA to produce this certificate.

3 Trustworthiness of the services

3.1 Positioning of the PKI for the government requirements

3.1.1 *CSP services*

The requirements laid down by the PKI for the government relate to the services of CSPs within the PKI for the government. These requirements are based on national legislation and international standards. The positioning of the requirements within the PKI for the government is as follows:

A. The primary principle as far as the requirements that have to be fulfilled within the PKI for the government (by CSPs) is the Electronic Signatures Act and corresponding regulations (in particular the Decree on Electronic Signatures and the Regulation on Electronic Signatures). The Act only applies to the qualified certificate.

B. Under the auspices of the EESSI, in an international context a detailed system has been created of standards with substantive demands for CSPs that issue qualified certificates. The requirements under these standards provide further specifications for articles under the legal framework. This mainly concerns requirements from the standard ETSI EN 319 411-2 (" Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Policy requirements for certification authorities issuing qualified certificates"), which lists requirements for CSPs that issue qualified certificates and requirements from the standard ETSI TS 102 042 ("Policy requirements for certification authorities issuing public key certificates") which lists requirements for CSPs that issue Services, Autonomous Devices or EV SSL certificates. These requirements are also valid within the PKI for the government.

C. A number of points in the requirements formulated under A. and B. are not formulated sufficiently specific as far as the PKI for the government is concerned. That is why these requirements have been specified further. CSPs that wish to issue PKIoverheid certificates therefore also have to fulfil these requirements. In the CPs (PoR part 3) these are named [PKIo].

D. Although the Electronic Signatures Act, the ETSI EN 319411-2 standard and the PKIo requirements have been specifically developed for the qualified certificate, based on the principle of one security level for all personal certificates, within the State of the Netherlands Root CA structure, it has been decided to also declare this security level applicable to the confidentiality certificate and the authenticity certificate[5].

[5] *The services certificate and the autonomous devices certificate are not personal certificates. The requirements in this respect originate from the international standard ETSI TS 102 042.*

3.2 Establishing security

3.2.1 Admittance and regulation

To safeguard the security of the PKI for the government, CSPs within the PKI for the government have to be reliable organizations that fulfil high requirements in respect of their operational procedures, technical devices, security of information, expertise and reliability of staff and the provision of information to their target group. The specific requirements which a CSP has to fulfil in order to be able to issue certificates within the PKI for the government are listed in part 3 of the PoR.

To establish whether the CSP meets the stipulated requirements and all formalities, a formal admittance procedure has to be followed. This procedure describes the proof of conformity that has to be supplied and which quality criteria apply to the executive audit organizations, following previously developed, generally accepted standards and certification schemes.

To be able to continue to safeguard the trustworthiness of the PKI for the government, including after the admittance to the PKI for the government, the CSPs have to continue to fulfil the requirements stipulated in part 3. To determine this, the PA supervises the CSPs that have entered. Furthermore, the CSPs have to regularly supply proof of conformity.

The entire admittance procedure and the way in which the PA supervises is described in PoR part 2 "Admittance to and Supervision within the PKI for the government".

3.2.2 Chain of reliance

To enable relying parties to rely on an end user certificate, a number of checks have to be performed, walking the so-called 'chain of trust'. Shown as a diagram in figure 3 is the chain of trust for the PKI for the government. It then states which verification steps have to be followed.

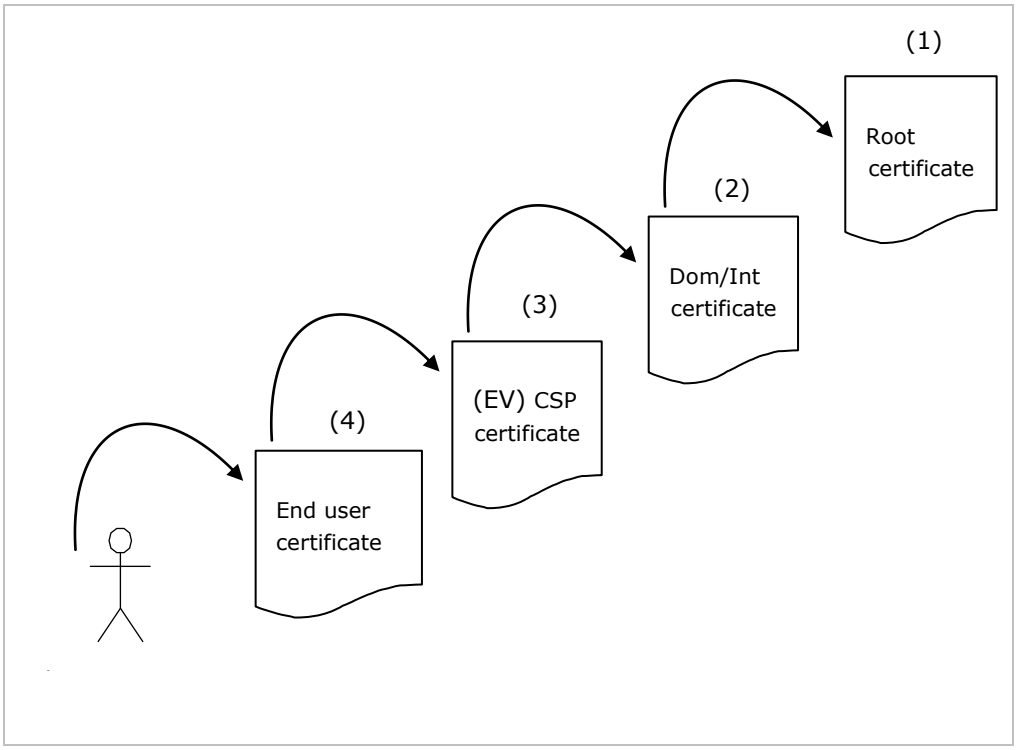

Figure 3

A relying party has a certificate from someone else (the certificate holder) and wants certainty in respect of the trustworthiness of this certificate. A certificate is verified by performing the following checks [6]:

- Has the message been changed whilst being sent, or is the integrity safeguarded?
- Has the certificate that has been used been revoked and included on a so-called "black list"?
- Is the certificate still valid?

The software then establishes whether the certificate has been issued by a trusted party. To be able to perform this latter check, the software has to have the State of the Netherlands Root CA G1, G2, G3 or the State of the Netherlands EV Root CA root certificate of the PKI for the government. If the root certificate is not available, the user receives an error message. That is why the PA has decided to include the root certificate in frequently used operating systems and Open Source browsers.

When software is used in which the root certificate is not included, the relying party can securely download the root certificate at www.logius.nl/pkioverheid.

The CSP certificate is issued by the PA and can be checked using the domain/intermediary certificate. This latter certificate is also issued by the PA and can be checked using the root certificate. At each level of the PKI for the government, the trust in a certificate therefore depends on the trust placed in the party that has issued the certificate. From the relying party's point of view, in the first verification step that is the CSP, in the second step the PA at the level of the domains or the Intermediary

[6] *These checks are usually performed automatically by the application that is used. The aforementioned checks have to be performed for every certificate in the chain of reliance.*

certificate and finally the PA at the highest level of the hierarchy. The root certificate is therefore the anchor point of trust in the hierarchy of the PKI for the government and establishes the trust that is placed in all other certificates that are issued within the State of the Netherlands CA structure or the State of the Netherlands EV Root CA structure. By expressing trust in the root certificate, all underlying domain or intermediary, CSP and end user certificates are trusted. The users only have to trust one certificate. An important aspect is determining the trustworthiness of the government body that issued the certificate.

3.2.3 Trustworthiness of the government body issuing the certificate

To be able to speak of a trustworthy hierarchy, it is extremely important that the PA functions in a trustworthy manner. The PA safeguards the trustworthiness of the root certificates and the domain certificates and the Intermediary certificate by applying adequate security measures. These security measures, as well as the way in which the PA supervises the CSPs, are described in the CPS of the PA. By assessing the CPS of the PA, the relying party can establish whether they trust a certificate that is issued within the State of the Netherlands CA structure or the State of the Netherlands EV Root CA structure. The hierarchical structure enables a relying party avoiding having to assess in detail every CPS of the CSPs within the PKI for the government. Finally, the trustworthy functioning of the PA has to be established frequently by having an audit performed by external auditors.

4 Summary of the Programme of Requirements

The diagram below shows the structure of the PoR, followed by a short explanation of each part.

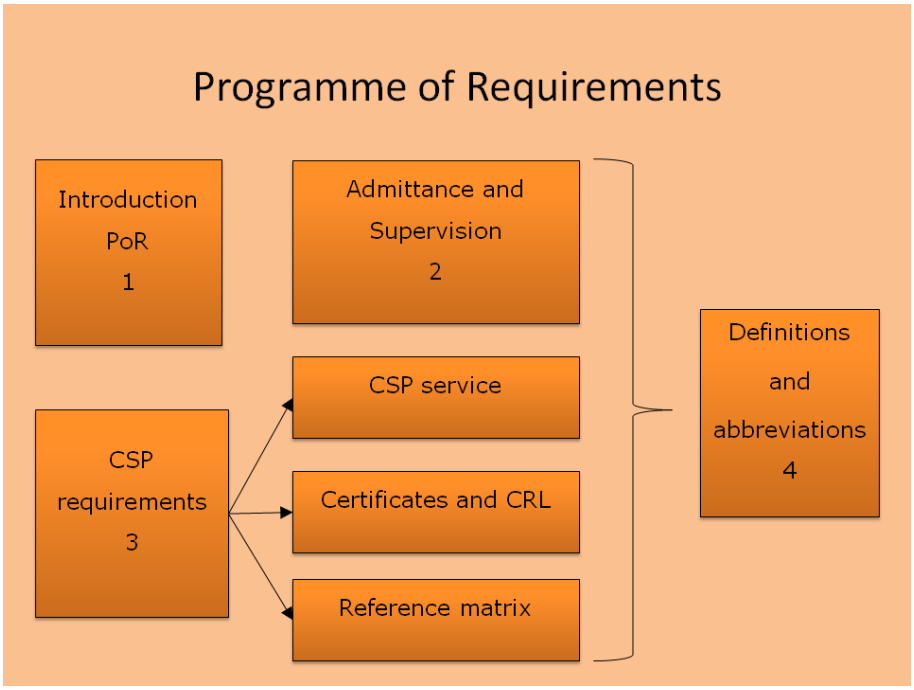

Figure 4: Structure of the Programme of Requirements

Part 1: Introduction to the Programme of Requirements
Part 1 provides an introduction to the PoR and the PKI for the government in general. It also outlines how the applicable requirements are set out within the PKI for the government. Mainly aimed at relying parties, certificate holders and process owners, this part provides important information to gain an understanding of the PKI for the government and corresponding standards system, without a profound knowledge of PKI being required.

Part 2: Admittance to and regulation within the PKI for the government.
The PoR lays down requirements which CSPs have to fulfil. Part 2 describes how a CSP can join the PKI for the government, can demonstrate compliance with the requirements and which formalities have to be met. It also describes how the PA supervises the CSPs that have joined.

Part 3: Certificate Policies
The so-called Certificate Policies (CPs) are incorporated in part 3. The CPs for personal certificates for the Government/Companies domains, Organization domain and Citizen domain are included in part 3a and 3c respectively. Three types of certificates can be issued within each domain. The requirements for these three types of certificates are specified in three CPs. As the requirements within these three CPs are largely the same, it has been decided to incorporate the three CPs for these three types of certificates in one document. There are, in fact, three logical CPs incorporated in one document.

The CPs for services certificates that can be issued in the Government/Companies domains and Organization domain are included in part 3b. Also included in part 3b are the logical CPs for the various types of services certificates incorporated in one document.

The CPs for autonomous device certificates that can be issued in the Autonomous Devices domain are incorporated in part 3d. Also included in part 3d are the logical CPs for the various types of services certificates incorporated in one document.

The CP for PKIoverheid EV SSL certificates is incorporated in part 3e. In part 3e there is only one CP as there is only one type of EV SSL certificate.

In each CP, there is a reference matrix in which a reference is included to the applicable requirements within the PKI for the government. Here a distinction is made between Dutch legislation, ETSI EN 319 411-2 in case of personal certificates, ETSI TS 102 042 in the case of non-personal certificates and the PKIo requirements. The applicable Dutch legislation and ETSI standards are comprehensively covered in www.logius.nl/pkioverheid. The detailed PKIo requirements are, of course, included in the CP itself.

Part 4: Definitions and abbreviations
The definitions and abbreviations used in the PoR are explained in part 4.

5 Revisions

5.1 Amendments between version 3.5 and 3.6

5.1.1 Amendments

Amendments have been made concerning the introduction of G3 root certificate and the certification against ETSI EN 319 411-2 within the PKI for the government.

5.2 Amendments between version 3.4 and 3.5

No changes.

5.3 Amendments between version 3.3 and 3.4

No changes.

5.4 Amendments between version 3.2 and 3.3

No changes.

5.5 Amendments between version 3.1 and 3.2

No changes.

5.6 Amendments between version 3.0 and 3.1

No changes.

5.7 Amendments between version 2.1 and 3.0

5.7.1 New

The following paragraphs are new in connection with the introduction of Extended Validation within the PKI for the government:

- Paragraph 2.3.3;
- Paragraph 2.4.3;
- Paragraph 2.4.4.

5.7.2 Amendments

The following paragraphs have been modified in connection with the introduction of Extended Validation within the PKI for the government:

- Paragraph 1.5;
- Paragraph 2.3;
- Paragraphs 2.4, 2.4.1 and 2.4.2;
- Paragraph 3.1.1;
- Paragraph 3.2.2;
- Chapter 4.

5.7.3 Editorial

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

5.8 Amendments between version 2.0 and 2.1

5.8.1 Editorial

Only a few editorial changes have been made but these do not affect the content of the information.

5.9 Amendments between version 1.2 and 2.0

5.9.1 New

The following paragraphs are new in connection with the introduction of the Autonomous Devices Domain within the government's PKI:

- Paragraph 2.3.3.

5.9.2 Amendments

The following paragraphs have been modified in connection with the introduction of the Autonomous Devices Domain within the government's PKI:

- Paragraph 2.3;
- Paragraph 2.5.1;
- Chapter 3.

5.9.3 Editorial

Only a few editorial changes have been made but these do not affect the content of the information.

5.10 Amendments between version 1.1 and 1.2

5.10.1 New

The following paragraphs are new in connection with the creation of the State of the Netherlands Root CA - G2 within the government's PKI:

- Paragraph 2.4.

5.10.2 Amendments

- Paragraph 2.2;
- Paragraph 2.4.2;
- Chapter 4.

5.10.3 Editorial

Only a few editorial changes have been made but these do not affect the content of the information.

5.11 Amendments between version 1.0 and 1.1

No changes.

5.12 Version 1.0

First version.