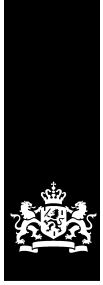


Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Programme of Requirements part 4: Definitions and Abbreviations

Datum 8 July 2013

Publisher's imprint

Version number 3.5
Contact person Policy Authority of PKIoverheid

Organization Logius

Street address
Wilhelmina van Pruisenweg 52

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

T 0900 - 555 4555
servicecentrum@logius.nl

Contents

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

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

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

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

Revision control

Version	**Date**	**Description**
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 June 2013

1 Introduction

1.1 Programme of Requirements

This is part 4 of the Programme of Requirements (PoR) for the PKI for the government. Set out in the PoR are the standards for the PKI for the government. This section concerns the definitions and abbreviations applied within the PKI for the government.

This section explains the terms and abbreviations used in parts 1 to 3 of the PoR. The main purpose of stating these definitions and abbreviations is to provide clarity regarding the terminology used by the PA. This part can also serve as reference document within the Dutch government for PKI-related issues.

1.2 Status

This is version 3.5 of section 4 of the PoR. The current version has been updated up to July 2013 inclusive.

The PA has devoted the utmost attention and care to the data and information incorporated in this part of the PoR. Nevertheless, it is possible that there are inaccuracies and imperfections. The PA accepts no liability for any damage as a consequence of inaccuracies or incompleteness.

1.3 Working method used

The following working method was used in producing this document.

If there is a definition in Dutch law for a certain term, then this definition has been used. If this definition has a general character that is not sufficient for our purposes, an addition is mentioned. The following legislation is used: The Telecommunications Act (Telecomwet) (dossier 25533) and the Electronic Signatures Act (Wet Elektronische Handtekening) (dossier 27743). In this document the legislative document concerned is highlighted by being placed between [ ].
Where this is not in contradiction with Dutch law, terms from the Dutch translation of the Community framework for electronic signatures (directive 1999/93/EG) are used. If a definition is used from this, this is highlighted by being placed in this document between [ ].

Use has also been made of documents from international organizations involved in standardization, particularly in the area of electronic signature. This gives rise to certain complications.

- Not all documents use the same definitions. Where this is the case, we use the publications from official European standardization organizations such as CEN (European Committee for Standardization) and ETSI, and use IETF or NIST, for example, less often.
- There is no official Dutch translation of the documents concerned. Some Dutch organizations have translated these, but these translations sometimes differ strongly from each other. It was decided in this document to translate the original phrasing into Dutch ourselves.
- The majority of available documents only consider rules regarding electronic signatures. In the model of the PKI for the government, also other certificates are considered. This means that some terms from the model of the PKI for the government cannot be adopted directly from the more limited model. Where the difference concerns only a few words, it was decided in this document to apply adjustments immediately as far as possible. If the amendment entails considerably more, the original text will be presented, supplemented with an explanation.
- In professional journals many terms are abbreviated from English. These abbreviations, or even sometimes the English words, are now comprehensively established within professional circles. This practical approach is also followed in this definition list. In cases in which there is a Dutch term for an English term used in the European Directive or the Electronic Signatures Act, the Dutch term is shown between ().
- For spelling, the VanDale dictionary and the "Woordenlijst Nederlandse taal" including the spelling rules have been followed.

1.4 Use

When a definition refers to another definition, the latter should be used. If a shortened form (for example an abbreviation) is placed after the definition, the shortened form is preferable in some cases. The preferred term is underlined for clarification purposes. In this document itself, the abbreviations are only used with their own explanation unless this concerns names of technologies or organizations. An exception is made for CSP, as this abbreviation is already comprehensively established.

Where a literal text is used from the Telecom Act, the Electronic Signatures Act, the Electronic Signatures Decree or the European Directive, this will be stated explicitly. Furthermore, the literal text will be presented in italics and in a smaller font.

2 Definitions

A**pplicant**
A natural person or legal personality who submits an application to a Registration Authority for the issue of a certificate.

Subscriber (E: Subscriber)
A natural person or legal personality who is party to an agreement with a provider of public telecommunications services for the supply of such services. [Telecom Act]

Within the scope of the PKI for the government:
A subscriber enters into an agreement with a CSP on behalf of one or more certificate holders. How the delivery of certificates takes place is organized between the subscriber and the CSP. In the Citizen domain, the subscriber and certificate holder are always the same party.

Accreditation
Procedure whereby the organization that has authority issues formal recognition that an entity is competent to undertake specific tasks.

Advanced electronic signature
See "Advanced electronic signature".

Advanced Encryption Standard – AES
The new standard for encrypting data, determined by NIST and valid for the United States. The AES serves as successor to the much-used DES algorithm and, to a lesser extent, the SHA-1 algorithm. The AES utilises the Rijndael algorithm, developed in Belgium.

Independence and Vulnerability Analysis - I&V analysis
The analysis is implemented with the goal of determining the level of security required to guarantee trusthworthy communication within the infrastructure of the PKI for the government.

A**lgorithm**
A collection of instructions that should be carried out step-by-step in order to carry out a calculation process or resolve a specific type of problem.

Application Programming Interface - API
A formalized collection of invocations and routines that are carried about by an application to utilise supporting services (for example a network). In relation to PKI these are invocations from applications that use cryptographic transactions (encryptions, registrations, etc.).

Asymmetric key pair
A public and private key within public key cryptographics that are connected to each other mathematically so that the public key and the private key are each other's counterpart. If one key is used for encryption, the other has to be used for decryption and vice versa.

Attribute
Information belonging to an object (person or entity) that specifies a characteristic of that entity, such as group membership, a role or other authorization information connected with the holder of an attribute certificate issued for this.

Attribute Certificate (E: Attribute Certificate)
A data structure that contains a collection of attributes plus additional information for an end user, signed with the private key from the AA that issued the certificate.

Attribute Authority – AA (NL: Attribuut Autoriteit)
An authority that awards privileges by signing and issuing attribute certificates. The Attribute Authority is responsible for this during the entire lifecycle of the attribute certificate, not only during registration.

Authentication
1. Verifying someone's identity before information transfer takes place.
2. Verifying the correctness of the sender's message.

In the Electronic Signatures Act, the word "Authentificatie" (authentification) is used. The original English word is "Authentication". In all technical professional journals, however, this is translated as "Authentication". The latter is also applied in this document.

Authenticity certificate
A certificate that, depending on the specific application, is used for authentication or electronic identification.

Authentification
See "Authentication".

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

Authorization
Granting authority to perform actions (such as viewing, modifying or processing) on information or devices.

Policy rule instructing certification organizations' electronic signatures
The policy rule came into force at the same time as the Electronic Signatures Act. The policy rule concerns instructing organizations that assess certification service providers on compliance with the requirements laid down in or in accordance with the Telecommunications Act, pursuant to article 18.16 of the Telecommunications Act.

Profession-related certificate holder
The certificate holder is a practitioner of a recognized profession and in this capacity is a subscriber and therefore a contracting party.
PoR part 3a at 3.2.5-1 states that "Only the following are considered as authentic proof of practising a recognized profession:

a. either a valid proof of registration in a (professional) register recognized by the relevant professional group, to which disciplinary rules stipulated by law apply;
b. or an appointment by a Minister;"

With regard to these two conditions this refers to the following professions (this concerns a restrictive list):

1. Accountants Administration Officer;
2. Lawyer;
3. Patent Agent;
4. Register pilot;
5. Physicians;
   5a. Doctor (for example GPs and medical specialists such as surgeons and psychiatrists);
   5b. Dentist;
   5c. Pharmacist;
   5d. Midwife;
   5e. Physiotherapist;
   5f. Nurse;
   5g. Psychotherapist;
   5h. Healthcare Psychologist;
6. Civil Law Notary;
7. Junior Civil Law Notary;
8. Acting Notary;
9. Court Bailiff;
10. Acting Court Bailiff;
11. Additional Junior Court Bailiff;
12. Patent Agent;
13. Registered Accountant;
14. Veterinary Surgeon
15. Seafarer;
16. (Head) Registrar;
17. Mandated Registrar;
18. Ships Technician;
19. Ship Registration Inspector;
20. Government-appointed Tax Bailiff;
21. Government Bailiff.

Availability
The availability and accessibility of the relevant data. Concerning the infrastructure: the extent to which a system is usable at the moment that it is needed.

Electronic Signature Decree
The electronic signature decree that came into force as General Government Decree at the same time as the Electronic Signatures Act. The decree sets the requirements for granting services for electronic signatures. No. WJZ/03/02264.

Authorized representative

A natural person that is authorized to represent an organization. Authority for representation can flow from the act or from general power of attorney. There can also be more than one natural person, for example, a board of an association, authorized to represent an organization.

The table below describes who is *normally* authorized to represent a certain organization;

Organization	Authorized Representative
Local council	Mayor Council Secretary
Province	Queen's Commissioner
Ministry	Minister Director General Secretary General
School	Director/Head Secretary of the Board
Water Board	Director (Dijkgraaf) Administrator(s)
Care organization	Director Administrator(s)
Association	Administrator(s)
LLV	Administrator(s)
Joint-Stock Company	Administrator(s)
Partnership	All partners or one of the partners as representative of the partnership (i.e. as representative of all partners at the same time) if this is authorized by the other partners.
Sole Trader	Owner
General Partnership	Each partner, who is not excluded is authorized to act 'in the name of the partnership' (i.e. the joint partners)
Limited Partnership	Only active partners: they are authorized to act in the name of the limited partnership and are mainly connected for the obligations contracted in the name of the partnership
Cooperation	Administrator(s)
Profit and Loss Service	Director Administrator(s)
Independent Administrative Body (ZBO)	Director Administrator(s)

Biometrics
A technology for recognising persons or verification on the basis of a unique physical characteristic. For example: iris scan, fingerprint scan, facial recognition.

Blank Cards
Cards (particularly smartcards) that are pre-printed graphically, but not yet provided with key material or personal data.

Bridge Certification Authority – Bridge CA
A Certification Authority serving as pivot in a network of other recognized Certification Authorities that are interoperable. This Certification Authority thus forms thus a bridge between the various Certification Authorities.

CA Certificate
A certificate from a Certification Authority. A special case of this within the PKI for the government is the CA Certificate from the CSP CA, that is issued by the Policy Authority. This certificate is called the CSP certificate. See also the diagram under "Hierarchical model".

CA Signing
The signing of a CA certificate. This can be the case when a CA is produced within the hierarchy. This also takes place for cross-certification. In fact this is mutual CA signing. See also the diagram under "Hierarchical model".

Calamiteit (E: Disaster)
An unplanned situation in which it is expected that the unavailability of one or more services will exceed the agreed threshold values.

CEN Workshop Agreement - CWA
A document from the European Committee for Standardization (CEN) containing advice and proposals for European standardization. In comparison with realising an ETSE standard, the realization of advice from the CWA is much faster. On the other hand an ETSE standard is considered more as an official starting point.

Certificate
An electronic confirmation that connects data for verifying electronic signatures with a certain person and confirms the identity of that person. [Electronic Signatures Act]
Within the scope of the PKI for the government:
The public key of an end user, together with additional information. A certificate is encrypted with the private key of the Certification Authority that issued the public key, which makes the certificate tamper-proof. See also the diagram under "Hierarchical model".

Certificate & Card Management
The procedures concerning maintenance of the certificates and smartcards.

Certificate Identifier - Certificate ID
The unique label of a certificate comprising the name of the Certification Authority and the serial number assigned by the Certification Authority.

Certificaatgeldigheidsduur (E: Certificate validity period)
The time period during which the Certification Authority guarantees the usability of the certificate. The Certification Authority retains validity information concerning the status of a certificate for at least 6 months after the end of the term.

Certificate holder

An entity identified in a certificate as holder of the private key belonging to the public key that is given in the certificate.
In the case of personal certificates the certificate holder will be a natural person, in the case of service certificates the certificate holder will be a function or a machine/server. In the Citizen domain, certificate holder and subscriber are always the same party.

Certificate Profile
A description of the content of a certificate. Each kind of certificate (signature, confidentiality, etc) in each domain has its own content and therefore its own description. This includes, for example agreements regarding naming, etc.

Certificate Generation Service
A service that creates and signs certificates, based on identity and other characteristics verified by the Registration Authority.

Certificate Policy - CP
A written specified collection of instructions that indicate the applicability of a certificate for a certain community and/or application class with common security requirements. Using a CP, end users and relying parties can determine how much trust they can place in the connection between the public key and the identity of the holder of the public key.

Certificate Revocation List – CRL
A publicly accessible and consultable list (database) of revoked certificates, made available, signed and falling under the responsibility of the issuing CSP.

Certificate validity period
See "Certificate validity period".

Certification
A broad (both technical as well as non-technical) evaluation of the security properties of an information system or, as in the framework of the PKI for the government, a management system. Certification is implemented as part of a process that measures the extent to which a management system conforms to an agreed collection of requirements (ETSI TS 101 456). The instruction for certification are recorded in a scheme: Scheme for Certification of Certification Authorities against ETSI TS 101 456.

Certification Services
Issuing, maintaining and revoking certificates by certification service providers as well as other services that are connected with using electronic signatures, identity and confidentiality.

Certification Service Provider
See "Certification Service Provider".

Certification Authority – CA
An organizational network that is a part of a Certification Service Provider or that operates under responsibility of the Certification Service Provider and that is trusted by one or more end users to make (generate) issue and revoke Certificates. A CA can also create keys for end users (optional). See also the diagram under "Hierarchical model".

Certification Practice Statement – CPS
A document that describes the procedures and measures followed by a CSP regarding all aspects of the service. In this, the CPS describes the way in which the CSP satisfies the requirements described in the applicable CP.

Certification Service Provider - CSP (NL: Certificatiedienstverlener)
A natural or legal person that issues certificates or other services provided in connection with electronic signatures. [Electronic Signatures Act]

In the framework of the PKI for the government the CSP can also provide services in connection with identity and confidentiality.
A CSP's function is to issue and manage certificates and key information, including the carriers provided for this (for example smartcards). The CSP also has final responsibility for delivering the certification services. It is not important here if the CSP implements the actual activities itself or contracts this out to others. It is for example not unthinkable that a CSP contracts out the CA function and/or the RA function. See also the diagram under "Hierarchical model".

Certification Service Provider-Certificate Policy – CSP CP
A Certificate Policy concerning the certificate from the CSP.

Client
See "End User".

Client Certificate
See "End User Certificate".

Common Criteria – CC
A collection of internationally accepted semantic aids and constructions to define a customer's security requirements and the safety characteristics of systems and products with IT security functions. Common Criteria form an aid when developing and purchasing such products and systems. Such a product or system is called a TOE during the evaluation on the basis of the Common Criteria.

Common Data Security Architecture - CDSA
This architecture provides an open, platform-independent, interoperable and expandable software framework that comprises APIs that are designed to make computer platforms more secure for applications.
Common Name CN
A name of the certificate holder comprising, in the case of a personal certificate: surname, first name[s] and any initials. The certificate issuer can also be given a CommonName. If so, this will mostly comprise a company name supplemented with the domain applicable to the PKI for the government.

Certificate being compromised
Any infringement of confidentiality in the exclusive use of a component by authorized persons.
In the framework of the PKI for the government, the private key is mostly intended with this component. A key is considered invalidated in the event of:

- unauthorized access or intended unauthorized access;
- lost or possibly lost private key or SSCD;
- stolen or possibly stolen private key or SSCD; or

- destroyed private key or SSCD.

A compromization is a reason for placing a certificate on the Certificate Revocation List.

Cross-certification
An investigation by one or more Certification Authorities implemented according to each other's working method and an assessment of the applicable Certificate Policies and Certification Practice Statements.
The goal of this process is to provide certificates from another PKI with a certain trust level within the "own" PKI, so that it is possible to accept each other's certificates.

Cross-recognition
A situation in which different PKIs recognize each other without signing each other's keys. A consequence of cross-recognition is that end-users of the PKIs can communicate with each other electronically on the same trust level.

Cryptographic Profile
A collection of cryptographic algorithms and other functions relevant for security, such as hash functions, together with the parameter boundaries that are used to make or verify electronic signatures.

Cryptographic Module
The collection of hardware, software and firmware that implements cryptographic processes, or any combination of these, including cryptographic algorithms, and that is contained within the cryptographic boundaries of the module.

CSP certificate
A certificate of a CSP. With the CSP certificate a CSP describes the CAs operating under it. Within the PKI for the government a CSP certificate is issued by the Domain CA under responsibility of the PA (Policy Authority). See also the diagram under "Hierarchical model".

CSP signing
The signing of a CSP certificate. Within the PKI for the government this occurs by using the domain CA's private key under responsibility of the PA (Policy Authority). See also the diagram under "Hierarchical model".

Data Encryption Standard - DES
The standard symmetrical cryptographic method from NIST that uses a 560 bit key. The method uses a 'block cypher' method that splits the text in blocks of 64 bits and then encrypts these according to blocks. DES is a fast algorithm and is generally used. The new Advanced Encryption Standard (AES) is a successor to this.

Data To Be Signed - DTBS
All electronic data that needs to be signed, including the characteristics of the signatory's document and the electronic signature.

Decryption
Rendering the encrypted data legible again using a cryptographic key. In the case of symmetrical encryption, the decryption key is the same as the

encryption key. In the case of asymmetrical encryption the keys are unequal and the keys are then called public key and private key.

Digital Signature
See "Advanced electronic signature".

Digital identity
See "Electronic Identity."

Directory service
A CSP service (or one in cooperation with a CSP) that makes the certificates issued by the Certification Authority accessible on line for the benefit of consulting or relying parties.

Dissemination Service - DS
A service that distributes the certificates among subscribers and, with consent from the subscribers, to relying parties. The service also distributes the Certificate Policies and Certification Practice Statements among the certificate holders, subscribers and relying parties.

Distinguished Name - DN
The unique label of the name of a certificate holder, comprising minimally of: country, name, serial number and (in the case of certificates in the Government/Companies and Organization domain) organization name.

Domain certificate
A certificate issued by the Government CA and Domain CA under responsibility of the Policy Authority (PA).

Domain Certificate Policy – Domain CP
The Certificate Policy relating to a domain certificate.
Domain Certification Authority – Domain CA
The certification authority that produces CSP certificates within a domain.
See also the diagram under "Hierarchical model".

End user (E: End user)
A natural or legal person that has a certificate issued by a CSP, but cannot issue a certificate itself. The term "User" is also sometimes used.

Eindgebruikercertificaat (E: End user certificate)
A certificate issued by a Certification Service Provider to an entity, such as a person, a computer or a piece of information, that cannot issue certificates itself.
Because the end user that receives a certificate from a Certification Service Provider is often referred to as its client, this certificate is also called a client certificate. The term "user certificate" is also sometimes used.

Electronic-signature product (NL: Product voor elektronische handtekeningen)
Software or hardware, or relevant components of this that can be used by certification service providers to provide services in the area of electronic signatures or that can be used for verifying electronic signatures.
[European Directive]

Elektronische handtekening (E: Electronic signature)

A signature that comprises electronic data that are attached to or associated logically with other electronic data and that are used as a means of authentication. [Electronic Signatures Act]

Within the scope of the PKI for the government:
The electronic signature is used to ensure that electronic correspondence and transactions can compete with the time-honoured "signature on paper" on two important points. By placing an electronic signature it is established that someone who says they have signed a document has also actually done this. A person who places an electronic signature, indicates that he/she subscribes to the content of the document. Furthermore, the reader can also check afterwards whether the signature is from the correct person and whether the document has remained unchanged.

Electronic identity
The data in electronic form that is added to or connected in a logical way with other electronic data and functions as unique characteristic of the identity of the owner. Sometimes the term "Digital Identity" is used.

Encryption
A process with which data become encrypted using a mathematical algorithm and a cryptographic key so that these become unreadable for unauthorized persons.
The trustworthiness of the encryption depends on the algorithm, the implementation of this, the length of the cryptographic key and the use discipline.
For symmetric encryption the same secret key is used for encryption and decryption.
For asymmetrical encryption use is made of a key pair. One key, the private key, is only known by the end user of this key and needs to be kept strictly secret. The other, the public key, is distributed among the communication partners. Text encrypted with the private key, can only be decrypted with the accompanying public key and vice versa.

Enhanced Extended Validation Certificates Policy – EVCP+
A Certificate Policy in addition to the NCP+ policy that has to be applied in issuing Extended Validation (EV) SSL certificates on the basis of the EV Guidelines issued by the CAB Forum. This is used in situations in which the use of an SUD is deemed necessary.

Entry
A separate piece of information that is/becomes included in a register, computer etc.

eNIK
The planned electronic Dutch Identity Card that is expected to contain the PKIoverheid Certificates.

Recognized profession
In the framework of the PKI for the government a practitioner of a recognized profession is only considered a natural person who is in possession of:

- either a valid proof of registration in a (professional) register recognized by the relevant professional group, to which disciplinary rules stipulated by law apply;

- or valid proof (e.g. a permit) that the legal requirements in relation to practising a profession, are fulfilled.

European Electronic Signature Standardization Initiative - EESSI
A workshop at European level tasked with making concrete the standardization agreements from the European Directive 1999/93/EC for electronic signatures.

European Telecommunications Standards Institute – ETSI
An organization responsible for determining standards and norms in the area of telecommunications that are valid for the whole of Europe.

European Directive
In the framework of PKI, this alludes to document 1999/93/EC from the European Parliament and Council dated 13 December 1999 concerning a common framework for electronic signatures (Publicatieblad no. L013 of 19/01/2000, p.12-20).

Evaluation Assurance Level - EAL
A package comprising confidentiality components from ISO/EIC 15408 Part 3 that represent a point on the reliability scale as defined in the Common Criteria.

Extended Normalized Certificate Policy – NCP+
A Certificate Policy for non-qualified certificates that gives the same quality level as qualified certificates (in the QCP), but outside the working of the European Directive. This is used in situations in which the use of an SUD is deemed necessary.

Extended Validation SSL certificaten
EV SSL certificates are issued according to the Extended Validation directive in which strict demands are set on verifying the organization that applies for the SSL certificate and the domain for which the certificate is requested. One of the most important properties of an Extended Validation SSL certificate is that this makes the address bar of, for example Internet Explorer (version 7 and further) turn green.

Exclusivity
See "Confidentiality".FINREAD
An open standard for smartcard readers that makes secure authentication possible on the internet. This standard is a result of a European initiative from a number of financial institutions and focuses on being able to implement electronic banking transactions. Within FINREAD (in full: FINancial READer) specifications cryptographic processes are handled by the card reader and not by the smartcard.

Manufacturer
In the framework of the PKI for the government a Manufacturer is an organisation recognised in the Netherlands that conforms demonstrably to the Framework of Standards for producing and distributing a specific type of Autonomous Device in the Netherlands and is then also authorized by the party responsible for establishing the framework.

Federal Information Processing Standard – FIPS
An official standard for the United States and issued by NIST. In the framework of PKI, FIPS 140 ("Security Requirements for Cryptographic

Modules") and FIPS 186-2 ("Digital Signature Standard") are of main importance.

Fully Qualified Domain Name (FQDN)
A Fully-Qualified Domain Name (FQDN) according to the PKloverheid definition, is a full name registered in the Internet Domain Name System (DNS) with which a server on the internet can be identified and addressed uniquely. With this definition a FQDN contains all DNS nodes, up to the name of the Top Level Domain (TLD) concerned, and a FQDN is, in the Internet DNS, registered under a DNS Resource Record (RR) of the type 'IN A" and/or "IN AAAA" and or "IN CNAME".

Examples of FQDNs are
- www.logius.nl
- webmail.logius.nl
- local.logius.nl
- server1.local.logius.nl
- logius.nl (if registered under a DNS RR of the type "IN A" and/or "IN AAAA" and/or "IN CNAME")

Examples of non-FQDNs (and thus not permitted within PKloverheid) are:
- www
- logius.nl (if NOT registered under a DNS RR of the type "IN A" and/or "IN AAAA" and/or "IN CNAME")
- server1.webmail
- server1.local
- server1.

Geavanceerde elektronische handtekening (E: advanced electronic signature)
An electronic signature that fulfils the following requirements:
A. This is linked uniquely to the signatory;
B. This enables the signatory to be identified;
C. This is established using devices that the signatory can keep under its exclusive control;
D. This is linked in such a way to the electronic file to which it relates that every subsequent change of data can be traced;
[European Directive]

In – particularly dated – literature the term "Digital signature" is sometimes used. In comparison to a qualified electronic signature, an advanced electronic signature is not a legally valid signature in all circumstances.

User
See "End User".

User Certificate
See "End User Certificate".

Data for producing electronic signatures
See "Signature creation data".

Data for verifying an electronic signature
See "Signature verification data".

Secret key
A cryptographic key that is used for a symmetrical cryptographic algorithm. In asymmetric cryptography - as used for such things as the PKI for the government - secret keys are not used.

Gekwalificeerd certificaat (E: Qualified certificate)
A certificate that satisfies the requirements set in accordance with article 18.15, second paragraph of the Telecommunications Act, and is issued by a certification provider that satisfies the requirements set in accordance with article 18.15, first paragraph of the Telecommunications Act. [Electronic Signatures Act]

In the framework of the Electronic Signatures Act only the signature certificate is considered. In the framework of the PKI for the government however, two other types of certificates are processed. Only the signature certificate is considered here as a qualified certificate. The confidentiality certificate and the authenticity certificate are not qualified certificates but do have the same trust level within the PKI for the government.

Gekwalificeerde elektronische handtekening (E: Qualified electronic signature)
An electronic signature that fulfils the following requirements:

A. *This is linked uniquely to the signatory;*
B. *This enables the signatory to be identified;*
C. *This is established using devices that the signatory can keep under its exclusive control;*
D. *This is linked in such a way to the electronic file to which it relates that every subsequent change of data can be traced;*
E. *This is based on a qualified certificate as intended in article 1.1, part ss Telecommunications Act; and*
F. *It is generated by a secure tool for producing electronic signatures as intended in article 1.1, part vv Telecommunications Act.*

[Electronic Signatures Act]
Explanation:
The Act intends to make the qualified electronic signature legally valid by making its operation equal to that of the handwritten signature.
It is stated literally in the Act that if an electronic signature satisfies a) to f) the used "method is assumed to be sufficiently trusthworthy." However, no name is given to these types of signatures. In the ETSI standard TS 101 456 the name "Qualified electronic signature" is given to the electronic signature that satisfies that from a) to f). The above-chosen name is thus the most obvious and thus fills the omission in the Act.

Validity data
See "Validity Data".

Glue
Software that forms the bridge between the applicative functions, as run at clients and on servers, and the cryptographic functions, as implemented through smartcards and card readers.

Generic TopLevelDomein (gTLD)
The gTLD is a generic top level domain, a domain name extension that does not belong to a certain country and can be registered in principle by everyone anywhere in the world. Some examples of gTLD's are .com, .edu, .gov, .mil and .org.

Signature certificate
A certificate that is used in placing an electronic signature.

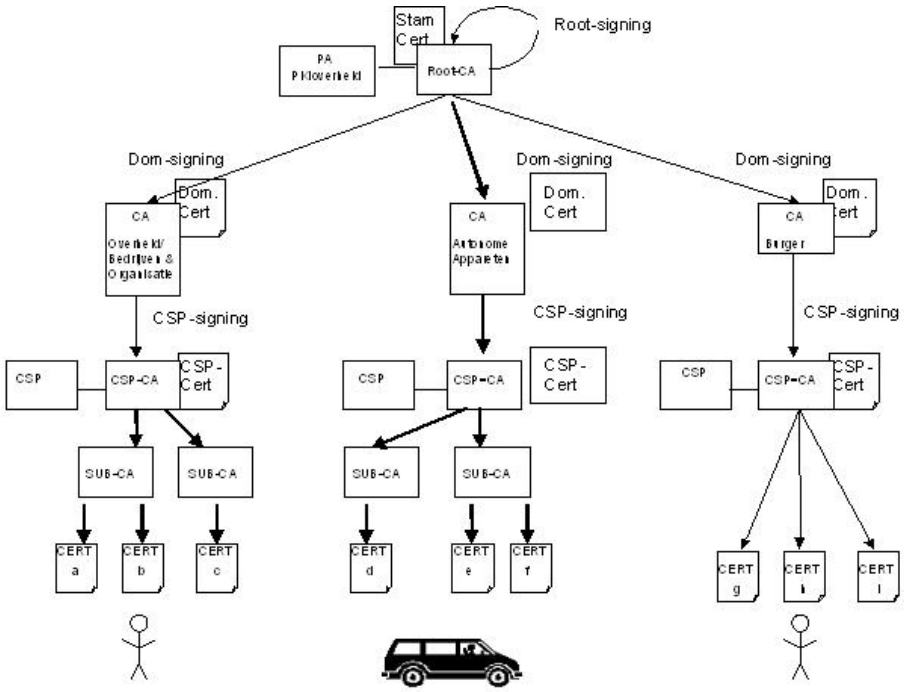
Hardware Security Module - HSM
The peripheral device used on the server side to speed up cryptographic processes. The production of keys should particularly be considered here.

Hash function
A function that transforms a message of random length into a series of fixed length and satisfies the following conditions:

- It is practically unfeasible for a given output to find an input that has this ("one-way") output as a result;
- It is practically unfeasible for a given input to find a second input that has this same ("weak collision-free") output as a result;
- It is practically unfeasible to find two random messages that have the same ("strong collision-free") output as result.

Hash value
The result, (output) of a hash function. The hash value is also called "message digest".

Hierarchical model
The PKI for the government assumes a hierarchical model. This means that trust in a chain is forwarded. An end user can trust all Certification Authorities that fall within the same CA stem.



Identification
Establishing the identity of a person (or business).

Identity and Authentication Certificate
See "Authentication certificate".

Identity Certificate
See "Authenticity certificate".

Incident
An event that does not form part of the standard working of a service and that has caused or can cause an interruption or a reduction in the quality of the service.

Indirect physical manifestation
A concept that is used when a person's identity control is not effected using the personal presence of that person, but is instead effected using tools that give the same certainty as can be obtained by personal presence.

Information Asset
A (stated) part of the information within an organization that is needed for the continuity of work processes (primary and secondary).

Integrity
The security that data are complete and unchanged, irrespective of whether this has occurred intentionally, unintentionally or has occurred in another way.

Internet Engineering Task Force – IETF
An international organization that strives to develop the internet architecture from the technical-scientific viewpoint.

Interoperability
The capacity to realize that different (automated) systems can work together technically.

Party responsible for establishing the framework
In the framework of the PKI for the government a Party responsible for Establishing the Framework is a government agency that:

- for a specific core task has a need for (measurement) data that originates from outside its immediate sphere of influence;
- to safeguard the integrity and authenticity of that (measurement) data, wishes to use specific devices that operate autonomously;
- to safeguard the trustworthiness of specimens of that type of device:
    - draws up a framework of standards for the production, activation, operation, maintenance, collection and use and formulates this in legislation and regulations;
    - based on that framework of standards, authorizes organizations to:
        - produce and distribute devices of a particular type;
        - link certificates to particular devices;
        - replace certificates on particular devices;
        - revoke certificates of particular types of devices.

Key-backup
Making a copy of a private key on issue. It is most often the intention to hand over this copy to an organization that can use this via a key-escrow.

Key-escrow
A storage method for (a copy of) a private key, in which this is lodged with a trusted third party (a so-called "Key Escrow Agency" - KEA). If necessary, authorized involved parties can obtain access to the key.

Key-recovery
The technology with which the key that is needed to decrypt an encrypted message can be converted by a third party.

Country code TopLevelDomein (ccTLD)
The ccTLD (country code Top Level Domain) is the domain name extension for a country or independent territory. A ccTLD is comprised of the 2-letter country code that is determined according to the ISO 3166-1 standard. E.g. .nl, .be and .de.

Suppliers statement
Statement from a supplier in which it asserts under its exclusive responsibility, that a product, process or service complies with a specified standard or other normative document.

Lightweight Certificate Policy – LCP
A Certificate Policy that is used for non-qualified certificates in situations in which a risk-analysis does not justify additional costs associated with the more stringent NCP demands (such as physical appearance during the application process).

Lightweight Directory Access Protocol - LDAP
An open protocol that enables applications to obtain information from directories, such as, for example e-mail addresses and keys.

Local Registration Authority - LRA
The organization entity or function to which the implementation of the task of Registration Authority is assigned, and that physically collects, verifies, registers and forwards the identification data of the applicant in order to issue the certificate.

Message Digest - MD
See "Hash value".

MD5-algorithm
A much used algorithm for creating a cryptographic hash value for a message. The MD5-value of a certificate is unique to that certificate, and is often used to identify a certificate.

Signature creation device
See "Signature creation data".

Signature verification device
See "Signature Verification Device".

Multi-factor authentication
For this form of authentication, a minimum of two authentication techniques are applied simultaneously.

Non-Qualified certificate
A certificate that does not satisfy the requirements stated in accordance with article 18.15, second paragraph of the Telecommunications Act, and/or not is issued by a CSP that satisfies the requirements stated in

accordance with article 18.15 first paragraph of the Telecommunications Act and/or not is applicable to serve for the advanced electronic signature.

Explanation: In the framework of the PKI for the government the Authenticity Certificate and the Confidentiality Certificate are formally non-qualified certificates but, in terms of content, do satisfy the same requirements and therefore have the same security level.

Non-Qualified Certificate – NQC
See "Non-Qualified certificate":

Non-repudiation (NL: Onloochenbaarheid, Onweerlegbaarheid)
The property of a message that demonstrates that certain events or actions have taken place, such as sending and receiving electronic documents.
Within the PKI for the government, non-repudiation (of the content of a message) is proven through means of a signature certificate.

Normalized Certificate Policy – NCP
A Certificate Policy for non-qualified certificates that gives the same quality level as applies to qualified certificates (in the QCP), but is outside the working of the European Directive 1999/93/EC and without a secure user device being required.

Notified body (NL: Aangemelde instantie)
A government body that is nominated by the government of an EU member state and has received notification of this by the EU, to implement tasks regarding conformity test procedures to which is referred in the EU's "New Policy Directives" if a third party is required.
In the framework of electronic signatures such a government body is also referred to as a "designated body" and is as such appointed to determine whether a product satisfies the requirements for SSCDs on the basis of the European Directive 1999/93/EC.

Object Identifier - OID
A row of figures separated by points that designates an object in a unique and permanent way. Within the PKI for the government, OIDs are also awarded to all CPs and to all CAs.

Ondertekenaar (E: Signatory)
(For the application of the Telecommunications Act) The person who uses a signature creation device as intended in article 1.1, part uu Telecommunications Act. [Electronic Signatures Act]
In the framework of the PKI for the government, signatory is understood to be the certificate holder of the signature certificate and the term 'signatory' itself is not used.

Online Certificate Status Protocol - OCSP
A method to monitor the validity of certificates online (and real-time). This method can be used as alternative for consulting the Certificate Revocation List.

Non-repudiation
See "non-repudiation".

Non-repudiation

See "non-repudiation".

Open Card Framework - OCF
By using Java and the Java Virtual Machine (VM) an open architecture will be realized on the basis of which compatible APIs can be delivered. It is therefore desirable that the smartcard reader supports the use of Java and Java VM.

Public Key
See "Public key".

Organization-related certificates
There are two different kinds of organization-related certificates:
1. for persons;
2. for services.

At. 1
For organization-related certificates for persons the certificate holder is part of an organizational entity. The certificate holder has the authority to make a certain transaction on behalf of the organizational entity.

At. 2
For organization-related certificates for services, the certificate holder is:
- a device or a system (a non-natural person), operated by or on behalf of an organizational entity; or
- a function of an organizational entity.

Government
Within the context of PKIoverheid the following are considered to be government and government organizations:
- the whole central government, provinces, local councils, cooperative partnerships on the basis of the Joint Regulations Act and the water boards;
- implementing organizations and services such as inspections, financial services agencies and police services;
- judiciary;
- independent administrative bodies as stated in the ZBO register[1]

Government/Companies and Organization
Within the PKI for the government the Government/Companies and Organization domains comprise all organizations within the government and business world.

Personal Unblocking Key - PUK
The de-blocking code for cryptographic modules.

Personalization
A process in which blank cards are provided with personal data (photo and/or name&address data) and or personal key material.
It is probable that, in the framework of the PKI for the government, the personalization is implemented by two different providers, with one placing the key material in the presence of the end user and the other printing the card with the photo and the relevant personal data.

Personal certificates

1 http://almanak.zboregister.overheid.nl/sites/min_bzk2/index.php

In the case of personal certificates, the certificate holder will be a natural person. The certificate holder is either a part of an organizational entity for which a subscriber is the contracting party (organization-related certificate holder), or the practitioner of a recognized profession and in this capacity is also a subscriber and with this the contracting party (profession-related certificate holder), or a citizen and in this capacity is a subscriber and with this is the contracting party.

PKI for the government
The entire infrastructure that is maintained by the PA PKIoverheid.

PKI-enabled application
An application that is capable of using PKI functions such as placing an electronic signature.

Plug and Play - PnP
A standard for automatic configuration or installation of hardware tools.

Policy Authority – PA
An authority that sets the rules for that part of the hierarchy of a PKI that rests under its authority.

Policy Authority PKIoverheid – PA PKIoverheid
The Policy Authority (PA) for the hierarchy of the PKI for the government. The PA supports the Minister of Ministry of the Interior and Kingdom Relations in maintaining the PKI for the government. The PA's service provision can be divided into the management of the top layer of the infrastructure, admitting CSPs to the infrastructure and supervising the reliability of the PKI for the government. See also the diagram under "Hierarchical model".

Pre-personalization
A process in which white cards are provided with generic material (such as printing or generic keys) but not yet with personal data or personal key material.

Private IP address
An Internet Protocol address (IP address) is an identification number assigned to each device (e.g.. computer, printer) that participates in a computer network that uses the Internet Protocol (TCP/IP) for communication.

Private IP addresses are not routable on the internet and are reserved for private networks. The IP address series that is reserved within IPv4 for private use is (see RFC 1918):
- 10.0.0.0 – 10.255.255.255;
- 172.16.0.0 – 172.31.255.255;
- 192.168.0.0 – 192.168.255.255;

In addition the series from 169.254.0.0 -169.254.255.255 is reserved for Automatic Private IP Addressing (APIPA). These IP addresses may not be used on the Internet.

The IP address series that is reserved within IPv6 for private use is (see RFC 4193):
- fc00::/7

In addition the series from fe80::/10 is reserved for Automatic Private IP Addressing (APIPA). These IP addresses may not be used on the Internet.

Private key
See "Private key".

Private sleutel (E: Private key)
The key of an asymmetrical key pair that should only be known by the holder of this and kept strictly secret.
In the framework of the PKI for the government the private key is used by the user to identify him/herself electronically, place his/her electronic signature or to decrypt an encrypted message.
The term "privé sleutel" (private key) is also often used (including in the European Directive). In the Electronic Signatures Act, the word "private sleutel" is used. Both are intended as translation of the English term "private key".

Private key
See "Private key".

Process owner
A role in process management that defines goal measures, assures the consistent implementation of the process in their area of responsibility, requests resources to work on process improvements and assesses process changes and communicates process changes and improvements to process users.

Product for electronic signatures
See "Electronic-signature product".

Protection Profile – PP
A collection of security requirements, independent of the implementation, for a category of TOEs that needs to satisfy specific customer requirements.

Public key
See "Public key".

Public key cryptography
The system in which a mechanism of public keys and private keys are used. This entails two keys being used. One key is kept secret (the private key) and the other key may be distributed publicly (the public key). Everything that is encrypted with the public key can only be decrypted with the private key and vice versa. It is a form of asymmetric encryption.

Public Key Cryptography Standard - PKCS
A standard in the area of public key cryptography, developed by RSA laboratories. In the framework of the PKI for the government particularly PKCS#7 (Cryptographic Message Syntax Standard), PKCS#10 (Certification Request Syntax Specification), PKCS#11 (Cryptographic Token Interface Standard), PKCS#12 (Personal Information Exchange Syntax Standard) and PKCS#15 (Cryptographic Token Information Format Standard) are of importance.

Public Key Infrastructure - PKI

A compilation of architecture, technology, organization, procedures and rules, based on public key cryptography. The goal is to make reliable electronic communication and reliable electronic services possible.

Publieke sleutel (E: Public key)
The key of an asymmetric Key pair that can be made public.
The public key is used to control the identity of the owner of the asymmetric key pair, to check the electronic signature of the owner of the asymmetric key pair and to verify information for a third party.
The term "openbare sleutel" (public key) is also often used (including in the European Directive). In the Electronic Signatures Act, the word "publieke sleutel" is used. Both are intended as translation of the English term "public key".

Public IP address
Public IP addresses are unique across the world and are routable, visible and accessible from the internet.

Qualified Certificate – QC
See "Qualified certificate":

Qualified Certificate Policy – QCP
A Certificate Policy that contains an implementation of the requirements that are described in article,18.15, first and second paragraph of the Telecommunications Act.

Qualified electronic signature
See "Qualified electronic signature".

Statutory regulation electronic signature
This statutory regulation came into force with the Electronic Signatures Act. The statutory regulation gives further regulations regarding electronic signatures such as technical and organizational elaboration of set requirements. No. WJZ/03/02263.

Register holder
A government body that collects and records data in a register. The register holder is responsible in this for definition and specification of registration and the design of storage and communication facilities to enable reuse. The register holder should satisfy a number of minimum requirements, but also has the freedom to make certain choices in this area. Mostly a register holder also registers other data regarding the objects of which it has established the identity.

Registration Authority – RA
An entity within the responsibility of the CSP. A Registration Authority processes certificate requests and all accompanying tasks in which the verification of the identity of the certificate holder is the most important. The RA has a clear relationship with one or more Certification Authorities: The RA gives - following verification - the assignment to the Certification Authorities for the production of certificates. An RA can, at the same time function for more than one Certification Authority.

Registration service
A service that verifies the identity and, if appropriate, other specific characteristics of a subscriber. The results of this are forwarded to the Certificate Generation Service.

Relying Party - RP
See "Relying Party".

Request for Comments - RFC
A proposal for a standard originating from the IETF. Although an RFC does not have the formal status of a standard, in practice the RFCs as a rule are followed.

Reseller
A person or entity that has been given consent from the CSP to sell PKI certificates to subscribers on behalf of the CSP.

Revocation management service
A service that handles and reports requests that concern the revocation of certificates in order to determine the measures to be taken. The results are distributed via the Revocation Status Service.

Revocation service
A CSP service in which it revokes certificates when: agreements end; errors in the certificate are ascertained; or a private key is compromised that belongs to the public key included in the certificate. The revoked certificates are included in the Certificate Revocation List.

Revocation status information
Information that is needed to demonstrate the validity of a certificate. This information can be made available for example via an Online Certificate Status Protocol or Certification Revocation Lists.

Revocation status service
A service that supplies this certificate information about the revocation status to relying parties. This service can be a real-time service but can also be based on revocation status information that is updated at regular intervals.

Race Integrity Primitives Evaluation Message Digest - RIPEMD
A one-way Hash function. The number of bits of the hash value that flows from this is mostly displayed immediately afterwards. In this way the much used RIPEMD-160 delivers a 160 bit output.

Rivest-Shamir-Adleman algorithm – RSA algorithm
A cryptographic method that uses a double key. The private key is retained by the owner; the public key is published. Data is encrypted with the public key of the recipient and can only be decrypted with the private key of the recipient. The RSA algorithm is calculation intensive which means it is often used to make a digital envelope, that contains an RSA encrypted DES key and with DES encrypted data.

Root (NL: Stam)
The central part of a (PKI) hierarchy to which the entire hierarchy and its security level is attached.

Root certificate
See "Root certificate".

Root Certification Authority – Root-CA (NL: Stam-Certification Authority – Stam-CA)

A Certification Authority that is the centre of the joint trust in a PKI hierarchy. The CA certificate from the Root-CA is self-signed, which means that it is not possible to authenticate the source of the signature on this certificate, only the integrity of the content of the certificate. The Root CA however is trusted because someone else has said so or because people have read the CP and any other documents and found these to be satisfactory.

Root signing
Signing a certificate of the Root CA by the Root CA itself. See also the diagram under "Hierarchical model".

Secure Hash Algorithm - SHA
A certain algorithm that gives a concrete addition to a Hash function. The still much used SHA 1 was developed by the American government and produces a Message Digest of 160 bits. The Advanced Encryption Standard and SHA-2 are successors of this.

Secure Multi-Purpose Internet Mail Extensions – S/MIME
A secure method for sending e-mail. The e-mail clients of both Netscape as well as Microsoft support S/MIME. MIME, as described in RFC 1521, describes how an electronic message needs to be organized. S/MIME describes how encryption information and a certificate can be added as component of the text from the message. S/MIME follows the syntax given in the PKCS#7 document. S/MIME presupposes a PKI for electronic signing of email messages and for the support of encryption of messages and attachments.

Secure Signature Creation Device - SSCD (NL: Veilig middel voor het aanmaken van elektronische handtekeningen)
A tool for producing electronic signatures that satisfies the requirements according to article 18.17, first paragraph of the Telecommunications Act. [Electronic Signatures Act]

The Citizen domains in the PKI for the government has chosen for the smartcard as SSCD. In Government/Companies and Organization domains both smartcards as well as USB tokens can be used, if these meet the requirements.

Secure Sockets Layer - SSL
A protocol created by Netscape to manage the security of message sending in a network and give access to web services. The word sockets refers in this to the method of sending data back and forth between a client and a server programme in a network or between programme layers in the same computer.

Secure User Device – SUD (NL: Veilig gebruikersmiddel)
A tool that contains the user's private key(s), protects the key(s) against compromise and implements electronic signing, authentication or decrypting on behalf of the user.

Security Function - SF
One or more parts of a TOE on which it should be possible to rely on a closely-related partial collection of Certificate Policy regulations regarding enforcing the TOE.

Security policy
The collection of regulations, set down by the security authority, to organize the use and measures regarding security services and facilities.

Self-signed certificate
A certificate for a Certification Authority, signed by that Certification Authority itself. This can only be for a root certificate of a hierarchy.

Services certificate
A certificate with which a function or device, for example a server is linked to a legal person or different organization. In the case of a server, the certificate is used for safeguarding the connection between a certain client and the server that belongs to the organizational entity that is described as subscriber in the certificate concerned. A services certificate is not a qualified certificate.

Session key
A symmetric key that is used once for a message e-messaging or a telephone discussion (a session). After the end of the e-messaging or the telephone conversation, the key is discarded.

Signatory
See "Signatory".

Signature creation data (NL: Gegevens voor het aanmaken van elektronische handtekeningen)
Unique data, such as codes or cryptographic private keys that are used by the signatory to produce an electronic signature. [European Directive]

Signature Creation Device - SCD (NL: Middel voor het aanmaken van elektronische handtekeningen)
C*onfigured software or hardware that is used to implement data for producing electronic signatures.* [Electronic Signatures Act]

Signature verification data (NL: Gegevens voor het verifiëren van een elektronische handtekening)
Data, such as codes or *cryptographic public keys used to verify an electronic signature.* [European Directive]

Signature Verification Device – SVD (NL: Middel voor het verifiëren van een elektronische handtekening)
C*onfigured software or hardware that is used to implement data for verifying electronic signatures.* [European Directive]

Signing key (NL: Tekensleutel)
The private key that is used to place an electronic signature. A distinction can be made between a signing key from a Certification Authority and a signing key from an end user. The end user places his electronic signature with the signing key. The signing key from the Certification Authority is used to sign such things as the certificates issued and to sign the Certificate Revocation List.

Single Sign-On - SSO

A procedure in which only one authentication is needed per session, which means that it is not necessary for end users to authenticate for different applications within one session.

Key monitoring services
The generation, storage, issue or destruction of cryptographic key material that is used to produce or verify electronic signatures. [Statutory regulation electronic signature]
Explanation: Key monitoring services can be implemented by a CSP or (partly) by the certificate holder itself. The concept 'key monitoring service' is not used separately in the context of the PKI for the government.

Key pair
In an asymmetric cryptographic system, this is a private key and is mathematically connected to the public key. This has the property that a public key can be used to verify an electronic signature made with a private key. In the case of encryption, this property means that information that is encrypted with public key can be decrypted with the private key (or vice versa).

Smartcard
A plastic card, the size of a credit card that contains an electronic chip, including a microprocessor, memory space and a feed source. The cards can be used to save information and can be carried easily. In the future, the electronic Dutch Identity Card (eNIK) will be a smartcard.
Stam-Certification Authority – Stam-CA (E: Root Certification Authority - Root-CA)
See "Root Certification Authority".

Stamcertificaat (E: Root certificate)
The certificate of the Root-CA. This is the certificate that belongs to the place from which the trust in all certificates issued by the PKI for the government originate. This certificate is signed by the holder's CA (within the PKI for the government, this is the PA PKIoverheid). All underlying certificates are issued by the holder of the root certificate. See also the diagram under "Hierarchical model".

Strength of Function - SOF
A qualification of a TOE security function that expresses the minimum measures deemed necessary to disconnect the security behaviour of that function through a direct attack on its underlying security mechanisms.

Subject Device Provision Service
A service required if the CSP provides the generation of private and public keys on SSCDs. In that case the Subject Device Provision Service prepares the delivery of SSCDs and implements these and also supplies the private keys to end users in such a way that the confidentiality of this is not compromised and the issue to the intended end users is guaranteed.

Subscriber
See "Subscriber".

Subordinate CA – Sub CA

A Certification Authority that is part of a Certification Service Provider or that operates under the responsibility of the Certification Service Provider. For the PKI for the government the certificate of the Sub CA is signed with the signing key from the CSP Certification Authority. See further "Certification Authority" and also the figure "Hierarchical model".

Target of Evaluation - TOE
A product or system including the corresponding documentation that is subjected to an evaluation.

PKIoverheid Task Force
The project organization realized by the 'PKI for the government'. The PKIoverheid Task Force concluded its activities on 31 December 2002.

Signing Key
See "Signing Key".

Time Stamping Authority – TSA
An entity that provides proof of existence at a specific date at a certain time.

Time Stamping Service – TSS
A CSP service that guarantees that data are produced and sent at a certain date and time.

Time stamping unit
A collection of hardware and software that is maintained as a whole and has one single Time Stamping Signing key active at a random moment.

Toegangscontrolelijst – ACL (E: Access Control List - ACL)
A list that indicates who has rights of access to the various components of a PKI system. The list is a form of authorization.
A TCL is mainly used to control who has access to files and directories on a web server and a directory server.

Token
A secure piece or hardware or software in which the private keys of the end user are stored. A hardware token can also implement cryptographic calculations. Examples of hardware tokens are a smartcard and a USB token.

Trusted Third Party - TTP
See "Certification Service Provider".

Trust List
A list of trusted certificates or trusted Certification Authorities.

USB token
A USB token is a token comparable to a smartcard, but has a different form. It is a medium on which certificates are stored. The difference is that for a USB token, an extra smartcard reader does not need to be installed. Conversely, it is not possible to include end user characteristics on the USB token, such as a photo or personal data.

Validity data
See "Validity Data".

Validity data (NL: Geldigheidsgegevens)
Additional data, collected by the signatory and/or the controlling party invited to check the accuracy and validity of an electronic signature in order to satisfy the requirements of the Certificate Policy.

Secure Signature Creation Device
See "Secure Signature Creation Device".

Verifier
An entity that checks the correctness and validity of an electronic signature. This can be both a relying party as well as a third party that is interested in the validity of an electronic signature.

Confidentiality of Business Information
The guarantee that data actually and finally arrive with the person for whom they are intended, without that someone else can decrypt these. Outside the private sector the term "exclusivity" is also used.

Confidentiality certificate
A certificate in which the public key from the key pair is certificated that is used for confidentiality services.

Vertrouwende partij (E: Relying Party)
A natural person or legal personality who is the recipient of a certificate and operates in trust on the certificate.

Virtual Private Network - VPN
A technology with which a logically-separated network can be built on a generally accessible physical network. The technology is currently used a lot to make possible secure teleworking or flexible working.

Voluntary accreditation
See "Voluntary accreditation".

Vrijwillige accreditatie (E: voluntary accreditation)
A permit in which the rights and obligations concerning the provision of certification services are reported and that, on the request of the involved certification service provider, are issued by the public or private government body taxed with recording and maintaining rights and obligations, when the certification services provider cannot exercise the rights flowing from the permit as long as the decision from the government body has not been received. [European Directive]

Electronic Signatures Act
The Electronic Signatures Act (Wet EH) that was offered in its initial form to the Lower House on 6 May 2003, was ratified by the House of Representatives following a few adaptations. The act has been in force since 21 May 2003. The dossier number is 27 743.

Compulsory Identification Act (WID)
The Compulsory Identification Act (WID: Wet op Identificatieplicht) states which proof of identity can be used to determine the identity of persons.

What Is Presented Is What You See – WIPIWYS
A description of the qualities required from the interface that unambiguously delivers the end user's message consistently with the end user's message.

What You See Is What You Sign - WYSIWYS
A description of the interface's required qualities that unambiguously guarantees what an end user sees on his screen for signing is also that which is provided with his electronic signature.

White card
A card (particularly a smartcard) that is not yet provided with printing or key material.

X.509
An ISO standard that defines a basic electronic format for certificates.

3 Abbreviations

The following abbreviations apply within the document "Programme of Requirements" and the definition list. Where the abbreviated term requires explanation, this explanation is included in the definition list. These terms are indicated in italics.

AA	*Attribute Authority*
ACL	*Access Control List*
AES	*Advanced Encryption Standard*
AID	Application Identifier
API	*Application Programming Interface*
ARL	Authority Revocation List
BM	Biometric Method
BPR	Personal Records and Travel Documents Agency
BSM	Biometric Sensor Unit
CA	*Certification Authority*
CC	*Common Criteria*
CDSA	*Common Data Security Architecture*
CEN	Comité Européen de Normalization
CGA	*Certification Generation Application*
CMS	Cryptographic Message Syntax
CN	*CommonName*
CP	*Certificate Policy*
CPS	*Certification Practice Statement*
CPU	Central Processing Unit
CRA	Card Reader Application
CRL	*Certificate Revocation List*
CSP	*Certification Service Provider*
CWA	*CEN Workshop Agreement*
DES	*Data Encryption Standard*
DN	*Distinguished Name*
DPV	Dedicated Path Validation
DS	*Dissemination Service*
DSA	Digital Signature Algorithm
DTBS	*Data to be signed*
EAL	*Evaluation Assurance Level*
EEMA	European Electronic Messaging Association
EEPROM	Electronically Erasable Programmable Read Only Memory
EESSI	*European Electronic Signature Standardization Initiative*
EFT	Electronic Funds Transfers
EN	Europese Norm (European Standard)
eNIK	*Elelectronic Dutch Identity Card*
ETSI	*European Telecommunications Standards Institute*
EVCP+	*Enhanced Extended Validation Certificates Policy*
FIPS	*Federal Information Processing Standard*
GBA	Municipal Basic Administration
HSM	*Hardware Security Module*
http	HyperText Transfer Protocol
HW	Hardware
ID	Identifier
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IETF	*Internet Engineering Task Force*

IFM	Interface module
I/O	Input/Output
IP	Internet Protocol
ISO	International Organization for Standardization
KEA	Key Escrow Agency
LCP	*Lightweight Certificate Policy*
LDAP	*Lightweight Directory Access Protocol*
LRA	*Local Registration Authority*
MD	*Message Digest*
NAP	National Action Programme Electronic Superhighway
NCP	*Normalized Certificate Policy*
NCP+	*extended Normalized Certificate Policy*
NEN	Dutch Norm
NIST	National Institute of Standards & Technology
NQC	*Non-Qualified Certificate*
OCF	*Open Card Framework*
OCSP	*Online Certificate Status Protocol*
OID	*Object Identifier*
OPTA	Independent Post and Telecommunications Authority
OTAP	Develop, Test, Acceptance and Production Systems
PA	*Policy Authority*
PnP	*Plug and Play*
PDA	Personal Digital Assistant
PDS	PKI Disclosure Statement
PIN	Personal Identification Number
PKCS	*Public Key Cryptography Standard*
PKI	*Public Key Infrastructure*
POP	Proof of Possession
PP	*Protection Profile*
PRNG	Pseudo Random Number Generator / Pseudo Random Noise Generator
PUK	*Personal Unblocking Key*
QC	*Qualified Certificate*
QCP	*Qualified Certificate Policy*
RA	*Registration Authority*
RFC	*Request for Comments*
RIPEMD	*Race Integrity Primitives Evaluation Message Digest*
RND	Random Number
RNG	Random Number Generator
RP	*Relying Party*
RSA	*Rivest-Shamir-Adleman*
S/MIME	*Secure Multi-Purpose Internet Mail Extensions*
SCA	Signature Creation Application
SCD	*Signature Creation Device*
SCE	Signature Creation Environment
SF	*Security Function*
SHA	*Secure Hash Algorithm*
SM	Secure Messaging
SOF	*Strength of Function*
SSCD	*Secure Signature Creation Device*
SSL	*Secure Sockets Layer*
SSM	Secured Signature Module
SSO	*Single Sign-On*
Sub CA	*Subordinate CA*
SUD	*Secure User Device*
SVD	*Signature Verification Device*

TCPA	Trusted Computing Platform Alliance
TOE	*Target of Evaluation*
TTP	*Trusted Third Party*
TSA	Time Stamping Authority
TSP	Time Stamp Protocol
TSS	*Time Stamping Service*
TWS	Trustworthy Systems
USB	Universal Serial Bus
UTC	Coordinated Universal Time
VIR	Regulation Information Security Government Service
VPN	*Virtual Private Network*
WAP	Wireless Application Protocol
WBP	Personal Data Protection Act
WID	Compulsory Identification Act
WIPIWYS	*What Is Presented Is What You See*
WYSIWYS	*What You See Is What You Sign*

4 Revisions

4.1 Amendments from version 3.4 to 3.5

No amendments

4.2 Amendments from version 3.3 to 3.4

4.2.1 New

Not applicable.

4.2.2 Modifications

- Junior Civil-Law Notary included in the list of recognized professions.

4.2.3 Editorial

Not applicable.

4.3 Amendments from version 3.2 to 3.3

4.3.1 New

- Definition of public and private IP address

4.3.2 Modifications

- Definition of Fully-Qualified Domain Name.

4.3.3 Editorial

Not applicable.

4.4 Amendments from version 3.1 to 3.2

4.4.1 New

Not applicable.

4.4.2 Modifications

- Definition of Profession-related Certificate Holder.

4.4.3 Editorial

Not applicable.

4.5 Amendments from version 3.0 to 3.1

4.5.1 New

- Definition of Multi-factor authentication and Reseller.

4.5.2 Modifications

No changes.

4.5.3 Editorial

Not applicable.

4.6 Amendments from versions 2.1 to 3.0

4.6.1 *New*

- Definition of Autonomous Device Certificate, Profession-Related Certificates, Authorized Representative, Enhanced Extended Validation Certificates Policy – EVCP+, Extended Validation SSL Certificates, Generic TopLevelDomein (gTLD), Country code TopLevelDomein (ccTLD), organization-related Certificates, Government, Personal Certificates and Services Certificate

4.6.2 *Modifications*
No changes.

4.6.3 *Editorial*
Not applicable.

4.7 Amendments from version 2.0 to 2.1

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

4.8 Amendments from version 1.2 to 2.0

4.8.1 *New*
Not applicable.

4.8.2 *Modifications*
No changes.

4.8.3 *Editorial*
Not applicable.

4.9 Amendments from version 1.1 to 1.2

4.9.1 *New*
No changes.

4.9.2 *Modifications*
No changes.

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

4.10 Amendments from version 1.0 to 1.1

4.10.1 *New*

- Definition of Fully-Qualified Domain Name (FQDN).

4.10.2 *Modifications*
No changes.

4.10.3 *Editorial*
No changes.

4.11 **Version 1.0**
First version.