ESG de electronische signatuur BV

Certification Practice Statement

Versie 7.8 EN

ESG de electronische signatuur BV

Adres: Horselstraat 1 | 6361 HC Nuth

Tel: +31 (0)495 566 355

info@de-electronische-signatuur.nl
www.de-electronische-signatuur.nl

KvK: 12056805
BTW: NL8220.033.26.B01

Rabobank: 17.69.17.209
Swiftadres: RABONL2U
IBAN: NL96RABO0176917209

Colofon

Versienummer 7.8 EN
Contactpersoon W. Kamminga

Organisatie ESG de Electronische Signatuur B.V.

Index

1. Introduction

1.1 Background

PKI is a method in providing evidence through every form of communication.
For example, proof that the person who is communicating with you on the internet, is indeed the person that he is claiming to be. PKI proof is based on certain numeric pairs that belong together through a mathematic law. Such a numeric pair is called a keypair. The best thing of such a keypair is that you only need one of the keys on each side of the connection to proof that the other side uses the correct key. After all the mathematical law connects the keys in an unbreakable way. Keypairs are managed in a Public Key Infrastructure (PKI). One of the keys is kept secret, Secret key or Private key. De other key will be published publically, Public key.

When the identity data of a person is reliably connected to a public key and the matching privat key is in his exclusive control, that person can be identified based on his public key.

In prooving the identification, all steps of evidence must be checked in context. When the keypair, the sole control en de reliable connection are alle correct, proof has been delivered. The person has been authenticated, Irreversibility established or establishing the trust that confidential data can only be read by the intended person.

ESG de electronische signatuur BV performs as a Trust Service Provider (TSP) under the Trade name 'ESG' the Service that makes a Public Key Infrastructuur usable in practice. ESG generates in a secure environment PKI suitable keypairs. Every secret key is immediately saved on a safe appliance. This applicance, where ESG makes the holder choose his own pin, meets the demands on sole control. In a 'registration procedure', ESG provides the 'Reliable Linking' of a public key to 'Trusted Identifying Data'. These links are verified on the Internet as "electronic certificates", requiring X509. In addition, ESG certifies public keys based on the Certificate Signing Requests (CSR) provided by its subscribers.

1.1.1 Framework of service (PKIoverheid)

The State of the Netherlands has established a Public Key Infrastructure under the name PKIoverheid. PKI government has been implemented in an appointment system that allows generic and large-scale use of 'electronic signature'. In addition, the system facilitates remote identification (authentication) and "confidential communication". The PKI Government Policy Authority (PA) has described the appointment system in its Program of Requirements (PvE) and its associated Certificate Policy (CP). ESG has joined PKI government and conformed to the PvE. ESG also conforms to the current version of the Baseline Requirements for Issuance and Management of Publicly-Trusted Certificates as published at http://www.cabforum.org. Should there be an inconsistency between the PKI Government Program of Requirements part 3b and the relevant Requirements, which does not at least meet the minimum requirements described herein, this is being reviewed by the PA, then the requirements set forth in the Requirements prevail. The services of ESG comply with all requirements laid down by Dutch law and regulations. They provide the basis for the highest available security level of automated services, including electronic communications. They make "reliable authentication possible without

immediate intervention by natural persons" either "that machine verification of identity and authenticity is sufficiently reliable for use in social traffic."

The quality of ESG services is monitored by the PA of PKI government. Every year, the service quality of the ESG services is audited by an independent auditor based on the ETSI EN 319 411-2 and EN 319 411-1 requirements and the additional requirements of the PvE. This audit confirms that ESG's services comply with all the requirements of the relevant standards. This is evidenced by the issuing of a certificate by the independent auditor and the signing of the ESG certificates with the Dutch tribal certificate.

In addition to the fact that ESG's services must meet the requirements of ETSI EN 319 411-2, EN 319411-1 and the PvE, they must also comply with the following laws and regulations:

- Europese Richtlijn elektronische handtekeningen (1999/93/EG)
- Uitvoering EU-verordening elektronische identiteiten en vertrouwensdiensten
- Besluit Vertrouwensdiensten
- Regeling Vertrouwensdiensten
- eIDAS verordening
- Wet elektronisch bestuurlijk verkeer van kracht per 1 juli 2004
- CA/Browser Forum: Network and Certificate System Security Requirements (Netsec).

1.1.2 Creation of the certificate policy

This document is the Certification Practice Statement for ESG and contains the guidelines for using the certificates issued by ESG. The format of this CPS has been applied as much as possible according to the RFC3647 standard.
This CPS is maintained under the responsibility of the management.

1.1.3 Status

Version	established	published	changes
CPS-4.10	04-02-11 ESG management	05-02-11	
CPS-5.3	30-03-12 ESG management	31-03-12	
CPS-5.11	03-07-12 ESG management	03-07-12	
CPS-6.2	21-03-13 ESG management	25-03-13	
CPS-6.3	11-06-13 ESG management	13-06-13	
CPS-6.4	15-07-13 ESG management	15-07-13	
CPS-6.5	10-02-14 ESG management	14-02-14	
CPS-6.6	27-06-2014 ESG management	01-07-14	H5.2.4/ 6.4.1/ 6.5/ 6.9.2/ 8.1/ 9.3/ 9.5
CPS-7.0	05-01-2015 ESG management	5-01-2015	New format of document conform RFC3647
CPS-7.1	21-04-2015 ESG management	21-04-2015	Aanpassing profiel services certificaat.
CPS-7.2	08-04-2016 ESG management	08-04-2016	H3.2, H4.2.1, H6.1.3, H6.2, H6.4.1 use new smartcard, removal QV as supplier.
CPS-7.3	02-08-2016 ESG management	02-08-2016	§ 1.2.4 OID seals, H7 update profiles
CPS-7.4	06-04-2017 ESG management	07-04-2017	Add enddate service KPN in §1.1.4 and §1.2.2
CPS-7.5 EN	29-06-2017 ESG management	30-06-2017	Adjustments due to changes in the scope of the service of ESG per 01-07-2017
CPS-7.6 EN	04-12-2017 ESG management	04-12-2017	Revocation via KPN servicedesk per 4-12-2017 12:00 uur
CPS-7.7 EN	02-04-2019 ESG management	02-04-2019	Yearly check on cps contents
CPS-7.8 EN	09-03-2020 ESG management	09-03-2020	CRL and OCSP publication after ending G2 CA

1.1.4 Stakeholders

The PKI PvE and the CPS of PKI government distinguish the following user community; Subscribers, certificate managers, certificate holders (both natural persons and services) and trusted parties. In addition to the stakeholders mentioned in the CP, this CPS describes; The TSP, the CSO, the LRA and the LRAO. For all these involved, it is important to take note of the PKI Government Requirements Program.

- **CSP (Certification Service Provider)**

ESG is the ultimate TSP. It provides services and certification on the basis of which a certificate holder can reliably identify and authenticate to a trusting party. The management of ESG is responsible for the services described in this document, the implementation of the described directives and the verification of compliance with this. ESG has outsourced a number of activities.

- The 'component services organisation' (CSO),
- The registration procedure.

- **CSO (Component Services Organisation)**

CSO for ESG is 'KPN B.V.'. This organization is responsible for ESG for the certificate generation, the revocation status service and the revocation management service. In addition, it manages the 'High Secure' computing center and the infrastructure for the production of cryptographic elements.

Until 01-07-2017 she will continue to provide these services. After this date, the Certificate Generation Service expires. KPN will continue to provide revocation status service and revocation management service until 23-03-2020.

- **LRA(Local Registration Authority) en LRAO (Local Registration Authority Officer)**

The immediate contact with prospective depositary holders, the registration procedure, has been outsourced to LRAs, or LRAOs. The LRA is the contact point for certificate holders. They are also the party where a certificate holder can get advice and support for purchase, installation and implementation of software. Each LRA has one or more LRA Officers.
Each LRAO is trained by the TSP and represents the TSP in the performance of the verifications and controls provided for the system described here.

- **Subscriber**

The subscriber is one,

- natural person who concludes with ESG to certify public key as certificate holder.
- legal entity that concludes with ESG to certify public keys on behalf of one or more certificate holders.

A subscriber is required to revoke certificates with incorrect content.

- **Certificate holder**

A certificate holder is the subject of a certificate. That is an entity that is marked as the private key holder associated with the public key contained in the certificate. A certificate holder can identify and authenticate, using the ESG certificates, within the limits of applicable regulations. Certificate-based certificates cover the responsibility of the certificate holder by a certificate manager.
A natural person who is a certificate holder is entitled, through the prescribed checks and procedures, to use his certificate together with the key pair in accordance with this CPS.

A service is a 'non natural person' who is the certificate holder. It is a device or system operated by or on behalf of an entity; A person or an organization. To request, or withdraw, a service certificate is intervention by a certificate manager, a natural person who represents the certificate holder.

- **Certificate manager**

A certificate manager is a natural person who is authorized on behalf of the subscriber, that contracting party, to perform all operations with regard to certificate of service. The organizational entity establishes the responsibility adequately and remains responsible.

- **Trusted Party**

A trusting party is any natural or legal person acting in confidence in a received certificate.
A received certificate can and may only be trusted:

- If the certificate's status information has been verified and the Certificate:
- has not been withdrawn;
- not expired;
- the full chain of certificates valid until the certificate of the State of the Netherlands is valid;

- and to the extent that the trust that may be given in the certificate is not restricted by the certificate itself or by this CPS.

1.2 Certificate use

1.2.1 Field of application certificates

The use of service certificates issued under PKI government refers to communication of certificate holders acting on behalf of the subscriber.
The use of personal licenses issued under PKI government refers to communication of personal depository holders.

The TSP is not permitted to limit the use of certificates or the value of the transactions for which certificates may be used within the scope of licenses.

1.2.2 Certificate hierarchy

Certificates are not immediately signed by the Dutch stamp certificate. The Public Key Infrastructure of the Netherlands, has been implemented in a 'three-level certification hierarchy'. At the highest level, the Dutch stamp certificate, 'State of the Netherlands, draws Root CA - G2':

1. in domain 'Overheid en bedrijven' the 'Staat der Nederlanden Organisatie CA - G2'-certificaat. With this (niveau 2) certificate is “ESG CA-certificaat' 2.16.528.1.1003.1.3.5.3.1 (niveau 3) signed.
2. in domain 'Burger' the 'Staat der Nederlanden Burger CA - G2'-certificaat. With this (niveau 2) certificate is 'ESG Burger-CA-certificaat' 2.16.528.1.1003.1.3.3.1.1 (niveau 3) signed.

ESG signs the various end-user certificates with these certificates.

This root will continue to exist until 23-03-2020 and then completely replaced by the G3 root. ESG has produced certificates under the G2 root until 01-07-2017. These certificates have a maximum validity of 2 years. After this date, it will only provide for the revocation of services available for the G2 root.

1.2.3 Certificaat usage

ESG is a Certification Service Provider and, as such, concludes a contract with a subscriber for a certificate holder. In this contract there is an article in accordance with Article 253 of Book 6 of the Dutch Civil Code. This article governs ESG's liability if a trusting party can demonstrate that he has performed all required checks before the certificate has been issued.
Certificates issued under this CPS cannot be used to identify persons in cases where the law requires that the identity of persons be identified only with a document designated in the Identification Act.

1.2.4 Certificate Policies

The PKI Government Certificate Program of the certificates issued by ESG is available at www.logius.nl. ESG indicates the following types of certificate, respectively, for the purpose of the certificate holder in use.

OID	Type
2.16.528.1.1003.1.2.5.1	The personal authentication certificate, containing the public key for identification and authentication of a person
2.16.528.1.1003.1.2.5.2	The personal signature certificate, containing the public key for the qualified electronic signature
2.16.528.1.1003.1.2.5.3	The personal confidentiality certificate, which contains the public key for confidentiality
2.16.528.1.1003.1.2.5.4	The service-bound authentication certificate is used to reliably identify and authenticate a service as belonging to the organizational entity responsible for the service concerned electronically.
2.16.528.1.1003.1.2.5.5	The service confidentiality certificate is used to protect the confidentiality of data exchanged and / or stored in electronic form
2.16.528.1.100.3.1.2.5.7	The service-based irreversibility certificate, is used to verify electronic stamps.
2.16.528.1.1003.1.2.5.6	The server certificate is used to secure a connection between a particular client and a server belonging to the organizational entity mentioned in the relevant certificate
2.16.528.1.1003.1.2.3.1	The personal authentication certificate is used to reliably identify and authenticate persons by electronic means. This concerns both the identification of persons between persons and between persons and computerized means
2.16.528.1.1003.1.2.3.2	The personal signature certificate is used to verify electronic signatures that have "the same legal effects as a handwritten signature" as indicated in Article 15a, paragraphs 1 and 2, in Title 1 of Book 3 of the Civil Code, Section 1A, and are qualified Certificates as referred to in Article 1.1, subsection ss of the Telecom Act
2.16.528.1.1003.1.2.3.3	The personal confidentiality certificate is used to protect the confidentiality of data, which are exchanged and / or stored in electronic form. This concerns both the exchange between individuals and between persons and computerized means

2. Publication and repository responsibilities

2.1 Repositories

The publications maintained by ESG are available 7 days a week and 24 hours a day. Nevertheless, a service may fall due to unforeseen circumstances. In such a case, ESG will ensure that the service is available again within 24 hours.

2.2 Publication of Certification information

ESG publishes on its website www.de-electronische-signatuur.nl:

- The full content of this document
- The terms and conditions
- Information for obtaining a certificate
- Price list / Rates
- Information regarding blocking or withdrawal of:
  - a certificate
  - an encryption key
  - a CA key
- Information regarding change of:
  - an encryption key
  - a CA key
  - (suspicion of) Fraud with
  - an encryption key
  - a CA key
  - Announcements of relevant changes to the Certificate Policy

The website is protected from third party customization and deletion.
Entries in this information are not subject to access control.

3. Identification and Authantication

This section describes how the identification and authentication of license applicants takes place during the initial registration process and what criteria ESG proposes regarding naming.

3.1 Naming

No stipulation.

3.2 Initial identity validation

No stipulation.

3.2.1 Method to prove possession of private key

No stipulation.

3.3 Identification and authentication for re-key requests

The I & A procedure for a routine certificate renewal is the same as that at first registration except that an application for a routine certificate renewal may and may also take place with an available and valid qualified electronic signature.

3.3.1 Identification and authentication for re-key after revocation

ESG does not allow for renewal of certified keys.

3.4 Identification and authentication for revocation requests

The counting password is used to authenticate the retrieval privilege. A certificate manager, holder, may submit a request for revocation of the relevant certificate to ESG by telephone mention of the specified telephone password.
After verification of the specified telecode, ESG will immediately withdraw the certificate. If the certificate manager or holder is not in a position to contact ESG by telephone, the request may also be submitted by a qualified representative of the subscriber identified by ESG.
The reason for withdrawal is always determined by ESG.

4. Certificate life-cycle operational requirements

4.1 Certificate application

No stipulation.

4.2 Certificate application processing

No stipultaion.

4.2.1 Performing identification and authentication functions

No stipulation.

4.2.2 Determining the certificate data

No stipulation.

4.2.3 Determining the organizational data

No stipulation.

4.2.4 Certificate application

No stipulation.

4.3 Certificate issuance

No stipulation.

4.4 Certificate acceptance

No stipulation.

4.4.1 Acceptance personal certificates

No stipulation.

4.4.2 Acceptatance Server certificates

No stipulation.

4.5 Key pair and certificate usage

Normally, certificates are valid for 3 years. If the lifetime of the CA certificate allows, a lifespan of up to 5 years is possible on request. However, this request must be approved by the PA PKI Government. Shorter lifespan can also be produced on request.

The subscriber, certificate holder, or certificate manager, respectively, ensures that the certificate is used exclusively in accordance with the guidelines in this CPS, the Special Terms and Conditions (AVG) for the service of ESG, the electronic signature BV. In addition, he assumes responsibility for soundness and measures to protect the information and communication systems with which he creates electronic messaging.

The subscriber as well as the certificate holder, or the certificate manager, guarantee the completeness and accuracy of the data in his certificates. This includes the obligation to disclose relevant changes through a withdrawal request to the TSP..

The subscriber is responsible for the timely replacement of the certificate in the event of an expiration date of validity and emergency replacement in case of compromise and / or other types of disasters relating to the certificate or of parent certificates. The subscriber is expected to take appropriate measures himself to ensure the continuity of the use of certificates.

4.6 Certificate renewal

ESG does not allow for renewal of PKI Government Certificates.

4.7 Certificate re-key

Keys of Certificate Holders will not be reused after expiry of the validity period or after withdrawal of the corresponding Certificates..

4.8 Certificate modification

ESG does not allow any adjustment of the content of PKI Government Certificates. If the data in the Certificate no longer corresponds to reality, then the Subscriber is required to withdraw the relevant Certificate immediately...

4.9 Certificate revocation and suspension

The validity of a certificate can be blocked. Suspension of a certificate is not allowed. Where a circumstance mentioned in section 4.9.1 occurs, any competent person who is aware of this circumstance is obliged to immediately submit a request for revocation. The reason for withdrawal is recorded, if known.

4.9.1 Circumstances for revocation

The following conditions lead to revocation of a certificate:

- The subscriber indicates that the original request for a certificate was not allowed and the subscriber grants retroactively no consent;
- The TSP has sufficient evidence that the subscriber's private key (which corresponds to the public key in the certificate) is compromised or there is a suspicion of compromise, or there is inherent security weakness, or that the certificate is otherwise Has been abused. A key is considered to be affected in case of unauthorized access or suspected unauthorized access to the private key, lost or presumably lost private key or SSCD, stolen or suspected stolen key or SSCD or destroyed key or SSCD;
- A subscriber does not fulfill his obligations as stated in Logius CP, the corresponding TPS CPS or the agreement that the TSP has concluded with the subscriber;
- The TSP is informed or otherwise aware of a material change in the information contained in the certificate. An example of this is: change of certificate holder name;
- The TSP determines that the certificate has not been issued in accordance with this CP or the corresponding TPS of the TSP or the agreement that the TSP has closed with the subscriber;
- The TSP determines that information in the certificate is incorrect or misleading;
- The TSP ceases its activities and the CRL and OCSP services are not taken over by another TSP.
- The PA of PKI government determines that the technical content of the certificate presents an irresponsible risk to subscribers, trusted parties and third parties (e.g., browser parties).
- Certificates may also be withdrawn as a measure to prevent or combat a calamity. As a matter of urgency, the violation or alleged violation of the TSP private key with which certificates are signed are considered.

Certificates subject to any of the above conditions may not be used and the Subscriber or Certificate Administrator shall submit a withdrawal request to ESG..

4.9.2 Who can request revocation

The revocation of a certificate can be ordered by the:

- subscriber
- Certificate Holder or its legal representatives. (In the domain Burger is the Certificate

holder equal to the subscriber).
- a third party represented by the certificate holder whose representation is stated in the certificate.
- The TSP.

4.9.3 Procedure for revocation request

Cancellation of a certificate must be requested by a qualified person by telephone or email.

Within office hours (Mon till Fri 9:00 – 17:00 hrs):

088–6610621 (email: servicedesk.sbr@kpn.com)

Outside office hours:

088–6610621 (email: esd.24x7@kpn.com)

Report that it is about a revocation of a by ESG issued PKIoverheid certificate, including the Tel Password specified during registration.

Within four (4) hours after an authenticated withdrawal request, ESG will revoke the certificate and issue a new CRL.

4.9.4 Revocation request grace period

A revocation of a certificate is final and can not be reversed.

4.10 Certificate status services

Confidential parties can reasonably trust a certificate if they perform adequate (online) control. The URLs for the services listed below are included in the certificates. The services are basically 7 days a week and 24 hours a day. Nevertheless, a service may fall due to unforeseen circumstances. In such a case, ESG ensures that the service is available again within 4 hours.

4.10.1 CRL (certificate revocation list)

Blocked certificates are included in the block list (CRL). The CRL will be updated daily and within 4 hours after each notification. The block list can be viewed through the LDAP server at any time. Inclusion of a certificate in the CRL is the final confirmation of a block. Certificates are listed on the block list for at least seven years, even after the expiration date.

After the expiry date of the issuing CA the last CRL will be published for at least 1 month.

4.10.2 OCSP (online certificate status protocol)

The validity of a certificate can also be checked via the OCSP according to RFC6960, without precomputed responses.

After the validity date of the issuing CA, the OCSP validation facility will be discontinued.

4.10.3 End of subscription

The duration of an agreement with a subscriber is in principle unlimited. However, ESG renews the agreement with each certificate application that is being placed.

4.11 Key escrow and Recovery

By default, Private Escrow Escrow is not available. ESG does not allow Private Keys to be taken in Escrow.

5. Facility, Management, and Operational Controls

The environment of ESG is certified by ETSI EN 319 411-2 and EN 319 411-1. The quality management system is constantly focused on improving the system through the PDCA cycle. The following chapters describe what operational and physical beveiligingsmaatregelen zijn toegepast op de locatie van haar CSO KPN waar de technische omgeving van ESG is ondergebracht.

5.1 Physical controls

5.1.1 Site location CSO

ESG's CSO is housed at KPN Corporate Market B.V .. This organization distinguishes itself with strictly defined procedures and a high degree of security. KPN B.V. Manages and implements physical and procedural security measures to restrict access to hardware and software used in the CA operations.

5.1.2 KPN B.V

The certification service is managed and delivered from a strictly secure environment within the KPN computing center in Apeldoorn. This environment complies with the laws in force in the government, including, inter alia, the Civil Secrecy Act 1951.
Physical access to the secure environment is achieved through a combination of procedural and (construction) technical measures. Access to the building and the secure environment is monitored by electronic (biometric) and visual means. The access system of the building records the entry and exit of staff and visitors. The building is being monitored by a security company for 7 * 24 hours.

The security systems automatically signal attempts to (on) authorized access. The technical measures are supported by various procedures, including motion sensors that monitor personnel and materials (for cryptographic key management). The technical infrastructure including the security systems is in protected areas with a designated administrator. Access to these rooms is recorded, inter alia, for audit purposes.

Household rules apply for the registration and guidance of third-party visitors and service personnel. Service companies have made arrangements for access to certain rooms. In addition, the building management service checks the incoming and outgoing goods (on the basis of accompanying documents).

The protected environment of KPN offers up to five physical barriers to the production environment. For non-production (offline) storage of, for example, cryptographic hardware and material, six levels apply.

Improper access to the secure environment requires compromising multiple systems. Depending on space, this can be a combination of knowledge, SSCD / SUD, biometric data, access guidance and visual inspection. Additional measures include burglary detection and video recordings. The different access control systems are separated and monitor access to the secure environment. Functional separation in combination with five or six physical barriers ensures that no single individual can access critical equipment from KPN.

KPN has taken numerous measures to prevent and / or reduce emergency situations in the secure environment. Examples of these are:

- Lightning diversion;
- Air-conditioning facilities;
- Backup of electricity using its own electricity supply;
- Construction measures (fire resistance, drainage, etc.);
- Fire prevention by means of automatic and manual fire alarm devices. In combination

with targeted, automated fire extinguishing.

The measures are tested on a regular basis. In case of exceptional situations an escalation plan will enter into force. Police and firefighters are familiar with the specific situation regarding KPN's secure environment.

5.1.3.1 Media storage

Storage media of systems used for PKI Government Certificates are handled safely within the building to protect against unauthorized access, damage and theft. Storage media are carefully removed when they are no longer needed.

5.1.3.2 Waste disposal

KPN has entered into a contract with a professional waste disposal company for the safe disposal of waste, used paper and the like. The staff of KPN is obliged to throw all the waste paper in the enclosed paper containers all over the building.

5.1.3.3 Off-site backup

Media containing data and software is also stored in another KPN building, with a minimum equivalent security level.

5.2 Procedural controls

5.2.1 KPN B.V.

Security tasks and responsibilities, including confidential functions, are documented in job descriptions. These are drawn up on the basis of the separation of tasks and competences and in which the sensitivity of the function has been established. Where applicable, job descriptions distinguish between general functions and specific TSP functions.

For all confidential and administrative tasks that affect the delivery of Certification Services, procedures have been prepared and implemented.

Authorization of TSP staff takes place on the basis of the need-to-know principle.

5.3 Personnel controls

5.3.1 KPN B.V.

5.3.2.1 Trusted roles

KPN has implemented a Trusted Employee Policy. This policy describes among other things which function categories and roles are "trusted". These are mainly related to the management of certificates and key materials, functions involved in system development, management, and maintenance and functions within Security Management, Quality Management and Auditing.

5.3.2.2 Number of persons required per task

For the purpose of performing certain, predefined, key, certificate management, system development, maintenance and management activities, multiple employees are required. The need to enforce a particular activity with several people, including using technical facilities, authorizations in combination with identification / authentication and additional procedures.

5.3.2.3 Division of functions

KPN uses division of functions between executive, decisive and controlling tasks. In addition, there is a separation between system management and operating systems used for PKI Government Certificates, as well as between Security Officer (s), System Auditor (s), System Administrator (s) and Operator (s).

5.3.2.4 Qualifications, experience, and clearance requirements

For the delivery of PKI Government Certificates, KPN puts in staff that possesses sufficient specialist knowledge, experience and qualifications.

KPN has identified from each function what knowledge and experience is required for a proper completion. This is maintained because the developments in the field follow each other quickly. In addition, each employee is registered what knowledge and experience he / she possesses.

5.3.2.5 Trusted Employee Policy

KPN has prepared and implemented a Trusted Employee Policy for its certification services. When drafting and maintaining this policy, the possibilities and impossibilities of generally applicable laws and regulations are carefully considered. This policy has described extensively how to deal with, for example, pre-employment screening, providing a Wji Conduct Statement, and conducting security investigations by services such as General Intelligence and Security Service or the Military Intelligence and Security Service to obtain A statement of no objection. The policy also identifies what capabilities management has if a (future) employee does not want to work or the outcome of the research is not positive.

5.3.2.6 Management and Security

KPN is responsible for procedural security through the application of ITIL management processes. ITIL is a methodology for standardizing IT management processes with the aim of bringing, maintaining and, where possible, improving the quality of these processes.
KPN has separate systems for development, testing, acceptance and production. These systems are managed using previously mentioned ITIL procedures.
Transferring software from one environment to the next takes place in a controlled location, using the Change Management procedure. This procedure includes tracking and capturing versions, making changes and emergency repairs of all operational software.
The integrity of all systems and information used for PKI Government Certificates are protected from viruses, malware and other possible service interruptions through an appropriate combination of physical, logical and organizational measures. These measures are preventive, repressive and corrective in nature. Examples of measures taken are: logging, firewalls, intrusion detection and redundancy of systems.

KPN has provided for timely and coordinated action to respond promptly to incidents and to limit the impact of security breach. All incidents are reported as soon as possible after they have occurred.

If an incident or other event may in any way threaten or affect the reliability of thecertification services and / or the image of the PKI for the government, this will immediately be reported to the PKIO Policy Authority.

5.4 Audit logging procedures

The individual components in the CSO system automatically logs. Manual Protocols are retained both in writing and in protocol files. Logs are regularly investigated for safety-relevant events. All security critical events are reported to the TSP. If necessary via the blocking hotline.

5.4.1 Types of events recorded

ESG handles logging on at least:

- Routers, Firewalls and network system components;
- Database activities and events;
- Transactions;
- Operating systems;
- Access control systems;
- Mail servers;

The following events are logged manually or automatically:

- CA key life cycle management;
- Certificate life cycle management;
- Threats and risks like:
  - Successful and unsuccessful attacks PKI system;
  - Activities of employees on the PKI system;
  - Reading, writing and deleting data;
  - Profile Modifications (Access Management);
  - System out, hardware failure and other abnormalities;
  - Firewall and router activities;
  - Entering and leaving from the space of the CA.

The log files must register at least the following:

- Source addresses (IP addresses if available);
- Target addresses (IP addresses if available);
- Time and date;
- User IDs (if available);
- Event Name;
- Description of the event.

Audit logs are regularly reviewed to see if any significant security or operational events have occurred which may require further action.

5.4.2 Retention period for audit log

The logs will be saved for at least 18 months and then deleted. The consolidated (electronic) audit logs, as well as the manual registrations during the period of validity of the Certificate and, in addition, are kept for a period of at least seven years after the date of validity of the Certificate.

5.5 Records archival

5.5.1 Types of records archived

All paper documents intended for application, control and production of a certificate are stored in KPN's archive and stored for 10 years after archiving. Logs and protocols are secured online for

short term. Only authorized personnel can access these files. Regular backups are made. These backups are archived. These archives will be retained and protected against alteration or destruction for a period of 7 (seven) years and thereafter removed. Only officers of the certification authority, the chief security officer and auditors may review the entire archive. The contents of the archives will not be released in its entirety, except when required by law.

5.5.2 Protection of archive

Certificate holders may review their own registration data. Upon request, KPN will make this information accessible. In addition, KPN may decide to release logs of individual registration transactions when requested by any interested party. A reasonable handling fee will be charged to cover the costs.

5.6 Key changeover

The validity of the CA key is determined by PKI government. Before using the existing CA key, no user certificates with a sufficient amount of time can be issued, a new key will be taken into use. The use of a new CA key does not directly affect certificates previously issued under another CA key. Both the old and new key pairs can be active at the same time. Once all certificates issued under a CA key have expired, the CA key will be rendered unusable.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

ESG is part of the company continuity plan of KPN B.V. The plans include:

- Procedures for controlling incidents and compromising of keys;
- Procedures for withdrawal of certificates;
- Procedures for performance in case of data processing, software, and / or corrupt data issues;
- Procedures for safeguarding business continuity after a disaster.

The plans are brand-related, security-sensitive and confidential. Therefore, they are not widely available.

5.7.2 Dissemination of information

KPN will inform stakeholders as soon as possible. This will be done by sending e-mail and / or public disclosure of the calamity via our website, depending on the extent of the calamity. In addition, KPN will immediately inform the PA (Policy Authority), the NCSC and the auditor and keep in mind any risks, hazards or events that may in any way threaten the reliability of the service and / or image of the PKI for the government Or influence.

5.8 TSP termination

The Certificate Service activities may be terminated by ESG unilaterally, with due observance of the statutory provisions. A proposed termination shall be communicated to both the ACM, Logius, and all subscribers and depositary holders at least 2 months before the termination. Upon termination of the Certificate Service activities, the registry will continue until 6 months after discontinuation of the activities. If these activities are not taken over by another certificate service provider, all issued certificates will be withdrawn.

6. Technical security controls

6.1 Key pair generation

6.1.1 Key pair generation for certifcate holders

No stipulation.

6.1.2 Private key delivery to subscriber

Ni stipulation.

6.1.3 PIN-PUK procedure

No stipulation.

6.1.4 Public key delivery to relying parties

No stipulation.

6.1.5 Key sizes

The key length of a certificate is sha256RSA of at least 2048 bits.

6.1.6 Public key parameters generation and quality checking

The length of cryptographic keys of the certificate holders must meet the requirements set in the lists of cryptographic algorithms and key lengths as defined in ETSI TS 102 176-1.

6.1.7 Key usage purposes

No stipulation.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

The upcoming certificate holder is fully responsible for the security of his own smartcard. The delivered smartcard comes with a defined PIN and PUK. This PIN and PUK are only provided once by ESG. ESG does not use this data storage. Because optimal security requires a card reader with its own PIN path, a numeric PIN is usually used. At no time, a certificate holder may disclose the PIN to another. ESG is not aware of the PIN and therefore accepts no liability for misuse of a PIN.

6.2.1 Cryptographic module standards and controls

All used components have been evaluated and certified according to ETSI. Components, for which the Dutch law requires electronic signature evaluation to ITSEC or Common Criteria, are additionally compliant with those criteria. The hardware security modules comply with FIPS 140-2 Level 3 and / or to EAL 4+. Access to the modules is limited with the use of smart cards.

6.2.2 Timestamping

ESG does not provide time-stamping services.

6.2.3 Private key escrow

ESG does not provide the ability to hold private keys of certificate holders in escrow.

6.2.4 Private key backup

ESG does not allow backing up of private keys by certificate holders.

6.2.5 Private key archiving

Private keys of certificates are not archived.

6.2.6 Private key transfer into or from a cryptographic module

For private keys belonging to ESG CA certificates, which are stored in a cryptographic hardware module, access protection is used that ensures that the keys can not be used outside of the module.

6.2.7 Private key storage on cryptographic module

CA private keys are encrypted stored in hardware cryptographic modules.

6.2.8 Method of activating private key

No stipulation.

6.2.9 Method of deactivating private key

Under specific circumstances, the TSP may determine that the private keys are deactivated, taking into account the applicable safeguards for the sake of care.

If an SSCD is lost by the certificate holder and returned by a vendor to the TSP, this SSCD will be destroyed by her, including the private keys contained therein. The TSP will also check that the corresponding certificates have been withdrawn. If this is not the case, the TSP will immediately withdraw the certificates.

6.2.10 Method for destroying private key

The private keys with which certificates are signed can no longer be used after the end of their life cycle. The TSP ensures adequate destruction, avoiding the ability to redirect the destroyed keys from the residues. If such keys are destroyed, those activities are logged.

6.2.11 Cryptographic Module Rating

The smart card used for storing keys of certificate holders complies with the requirements set in CWA 14169 level EAL4 +.

Instead of using a hardware SUD, the keys of a service certificate may be software-protected if compensatory measures are taken in the vicinity of the system containing the keys. The compensatory measures must be of such quality that it is virtually impossible to steal or copy the keys unnoticed.

The administrator of the service certificates using this software storage facility must at least provide a written declaration at the time of registration that compensatory measures have been taken that meet the aforementioned condition.

The special terms of the TSP state that ESG has the right to carry out a check on the measures taken.

6.3 Other aspects of key pair management

The Root Certificate of PKI Government is verified through the formal publication in the Dutch Official Gazette. In fact, the certificate is included with browsers and other software. The public keys from ESG can be downloaded via the website and PKI government. All issued public keys are kept in administration for 7 years. ESG stores private keys solely on the SSCD / SUD and therefore, after issuing the SSCD, no longer has private keys.

30 days before the validity of a certificate expires, the certificate holder or administrator is notified by email and offered the opportunity to request a new certificate.

6.4 Activation data

6.4.1 Activation data generation and installation

The SSD which is the TSPververt is provided by the TSP with a so-called PIN and PUK. (See 6.1.3). The PIN and PUK are only issued by the TSP to the certificate holder only once. The TSP also has no storage of this PIN and PUK. If the PIN is entered three times incorrectly, the SSCD is blocked, it can only be unblocked by the supplied PUK. If it is entered 5 times incorrectly, the card is blocked and should be replaced.

In the case of a service server certificate in the PKCS # 12 variant, the TSP will generate a one-time PIN. This PIN will be sent separately from the certificate to the certificate manager. Because the TSP did not use the storage of PIN letters, the certificate should be withdrawn at the loss of this PIN..

6.5 Computer security controls

The systems used for issuing or approving certificates are all provided with multifactor authentication. Each TSP operator has a smartcard with a personal certificate and has the smartcard provided with a personal PIN.

These systems are exclusively accessible to the permanent TSP staff.

6.6 Life cycle technical controls

The CSO follows the Certificate Issuing and Management Components (CIMC) Family of Protection Profiles, which defines the requirements for components that extract, retrieve, and manage X.509 (public key) certificates. CIMC is based on the Criteria EAL 4+. The Security Officer periodically verifies the integrity of the components.

6.7 Network security controls

The firewall and computer systems used comply with the state of the art. All systems are minimally configured, only the most necessary software is installed. In addition, these systems are in an independent network. The configuration of the systems and firewall was checked by an independent body.

At least monthly, a security scan is performed on the PKI government infrastructure using an audit tool. The results and measures arising from these scans are documented.
Finally, a Pentecost is conducted on the PKI Internet-facing environment by an independent, experienced, external supplier at least once a year. The findings and measures that come from these Pentecostals are also documented.

7. CRL- en OCSP-profiles

7.1 CRL-profiles

7.1.1 CRL civilian

CRL - Burger				
Base attributes	**OID**	**Critical**	**O/F/R**	**Value**
Version			Fixed	V2 (X.509v3)
SignatureAlgorithm	1.2.840.113549.1.1.11		Fixed	sha256withRSAEncryption
Issuer				
Issuer.countryName	2.5.4.6		Fixed	NL
Issuer.organizationName	2.5.4.10		Fixed	ESG de Electronische Signatuur B.V.
Issuer.commonName	2.5.4.3		Fixed	ESG Burger CA - G2
Update				
ThisUpdate			Required	yymmdd000000Z (date of issuance)
NextUpdate			Required	yymmdd000000Z (ThisUpdate + 24 hours)
revokedCertificates			Required	List of revoked certificates
CRL attributes	**OID**	**Critical**	**O/F/R**	**Value**
AuthorityKey Identifier	2.5.29.35	False		
KeyIdentifier			Fixed	160 bit SHA-1 hash issuerPublicKey
CRLNumber	2.5.29.20	False		
CRLNumber			Required	sequenced number
CRLReason	2.5.29.21	False		
CRLReason			Optional	reason of revocation

7.1.2 CRL Organization

CRL - Organisatie, Beroep, Services, Server				
Base attributes	**OID**	**Critical**	**O/F/R**	**Value**
Version			Fixed	V2 (X.509v3)
SignatureAlgorithm	1.2.840.113549.1.1.11		Fixed	sha256withRSAEncryption
Issuer				
Issuer.countryName	2.5.4.6		Fixed	NL
Issuer.organizationName	2.5.4.10		Fixed	ESG de Electronische Signatuur B.V.
Issuer.commonName	2.5.4.3		Fixed	ESG Organisatie CA - G2
Update				
ThisUpdate			Required	yymmdd000000Z (date of issuance)
NextUpdate			Required	yymmdd000000Z (ThisUpdate + 24 hours)
revokedCertificates			Required	List of revoked certificates
CRL attributes	**OID**	**Critical**	**O/F/R**	**Value**
AuthorityKey Identifier	2.5.29.35	False		
KeyIdentifier			Fixed	160 bit SHA-1 hash issuerPublicKey
CRLNumber	2.5.29.20	False		
CRLNumber			Required	sequenced number
CRLReason	2.5.29.21	False		
CRLReason			Optional	reason of revocation

7.2 OCSP profiles

7.2.1 OCSP civilian

OCSP Responder 1 - Burger				
Base attributes	**OID**	**Critical**	**O/F/R**	**Value**
Version			Fixed	V2 (X.509v3)
SerialNumber			Required	8 bytes Unique identifier
SignatureAlgorithm	1.2.840.113549.1.1.11		Fixed	sha256withRSAEncryption
Issuer				
Issuer.countryName	2.5.4.6		Fixed	NL
Issuer.organizationName	2.5.4.10		Fixed	ESG de Electronische Signatuur B.V.
Issuer.commonName	2.5.4.3		Fixed	ESG Burger CA - G2
Validity				
Validity not before			Required	yymmdd000000Z (date of issuance)
Validity not after			Required	yymmdd000000Z (not before + 3 years)
Subject				
Subject.countryName	2.5.4.6		Required	NL
Subject.commonName	2.5.4.3		Required	ESG Burger CA - G2 OCSP Responder 1
Subject.organizationName	2.5.4.10		Required	ESG de Electronische Signatuur B.V.
subjectPublicKeyInfo	1.2.840.113549.1.1.1		Fixed	RSA (2048 Bits)
Standard Extensions	**OID**	**Critical**	**Optional**	**Value**
AuthorityKey Identifier	2.5.29.35	False		
KeyIdentifier			Required	160 bit SHA-1 hash issuerPublicKey
SubjectKeyIdentifier	2.5.29.14	False		
Key Identifier			Required	160 bit SHA-1 hash subjectPublicKey
KeyUsage	2.5.29.15	True		
KeyUsage			Fixed	digitalSignature
certificatePolicies	2.5.29.32	False		
CertPolicyId			Fixed	2.16.528.1.1003.1.2.5.4
CPS Qualifier	1.3.6.1.5.5.7.2.1		Fixed	http://cps.de-electronische-signatuur.nl
User Notice Qualifier	1.3.6.1.5.5.7.2.2		Fixed	The terms and conditions as mentioned on our website (cps.de-electronische-signatuur.nl), are applicable to all our products and services
BasicConstraints	2.5.29.19	True		
cA			Fixed	False
pathlenConstraints			Fixed	0
CRLDistributionPoints	2.5.29.31	False		
distributionPoint URI			Fixed	http://crl.de-electronische-signatuur.nl/esg/burgercag2.crl
extKeyUsage	2.5.29.37	True		
extKeyUsage			Fixed	id-kp-OCSPSigning (1.3.6.1.5.5.7.3.9)
Private Extensions	**OID**	**Critical**		
ocspNoCheck	1.3.6.1.5.5.7.48.1.5			
ocspNoCheck			Fixed	05 00 (Null)

7.2.2 OCSP Organization

OCSP Responder 1 - Organisatie, Beroep, Services, Server				
Base attributes	**OID**	**Critical**	**O/F/R**	**Value**
Version			Fixed	V2 (X.509v3)
SerialNumber			Required	8 bytes Unique identifier
SignatureAlgorithm	1.2.840.113549.1.1.11		Fixed	sha256withRSAEncryption
Issuer				
Issuer.countryName	2.5.4.6		Fixed	NL
Issuer.organizationName	2.5.4.10		Fixed	ESG de Electronische Signatuur B.V.
Issuer.commonName	2.5.4.3		Fixed	ESG Organisatie CA - G2
Validity				
Validity not before			Required	yymmdd000000Z (date of issuance)
Validity not after			Required	yymmdd000000Z (not before + 3 years)
Subject				
Subject.countryName	2.5.4.6		Required	NL
Subject.commonName	2.5.4.3		Required	ESG Organisatie CA - G2 OCSP Responder 1
Subject.organizationName	2.5.4.10		Required	ESG de Electronische Signatuur B.V.
subjectPublicKeyInfo	1.2.840.113549.1.1.1		Fixed	RSA (2048 Bits)
Standard Extensions	**OID**	**Critical**	**Optional**	**Value**
AuthorityKey Identifier	2.5.29.35	False		
KeyIdentifier			Required	160 bit SHA-1 hash issuerPublicKey
SubjectKeyIdentifier	2.5.29.14	False		
Key Identifier			Required	160 bit SHA-1 hash subjectPublicKey
KeyUsage	2.5.29.15	True		
KeyUsage			Fixed	digitalSignature
certificatePolicies	2.5.29.32	False		
CertPolicyId			Fixed	2.16.528.1.1003.1.2.5.4
CPS Qualifier	1.3.6.1.5.5.7.2.1		Fixed	http://cps.de-electronische-signatuur.nl
User Notice Qualifier	1.3.6.1.5.5.7.2.2		Fixed	The terms and conditions as mentioned on our website (cps.de-electronische-signatuur.nl), are applicable to all our products and services
BasicConstraints	2.5.29.19	True		
cA			Fixed	False
pathlenConstraints			Fixed	0
CRLDistributionPoints	2.5.29.31	False		
distributionPoint URI			Fixed	http://crl.de-electronische-signatuur.nl/esg/organisatiecag2.crl
extKeyUsage	2.5.29.37	True		
extKeyUsage			Fixed	id-kp-OCSPSigning (1.3.6.1.5.5.7.3.9)
Private Extensions	**OID**	**Critical**		
ocspNoCheck	1.3.6.1.5.5.7.48.1.5			
ocspNoCheck			Fixed	05 00 (Null)

8. Compliance audit and other Assessments

8.1 CSO

KPN B.V. Is certified as CSO in accordance with ETSI. This certification ensures that all business processes for the production of certificates and for the online services are precisely described and verified.
The relevant publications of KPN B.V., the audit by BSI's auditor and the KPN B.V. Consulted certificate show this.

8.2 Identity/qualifications of assessor

Certification audits are performed by BSI. BSI is accredited by the Accreditation Board.

9. Other Business and Legal matters

9.1 Fees

No stipulation

9.2 Financial responsibility

The liability of the TSP is settled in accordance with Article 253 BW6.

9.3 Confidentiality of business information

It is forbidden to possess, hold or hold software, documents or correspondence or copies thereof, which he / she has acquired in his / her possession in connection with his / her work with the client. Copy, except as far as and for as long as this is required for the performance of its work for the client.

Employees are prohibited from entering into financial transactions either during or until 2 years after the end of this agreement, either directly or indirectly, involving the client's business, including the purchase or sale of shares in companies belonging to The clientele's clientele when these transactions make use of knowledge acquired by or during the performance of the work, which is not known or should be known to third parties.

If an employee or (legal) person (s) acting on behalf of the employee in a client's business, in what function and capacity, acts in breach of the obligations under the preceding paragraphs, The employee will be entitled to the commissioner without any notice of default, for each violation, forfeit a fine of five thousand Euro per violation and one thousand Euro for each day that the violation continues, without prejudice to the right of the client instead of fine full compensation, With a maximum of fifty thousand euros.

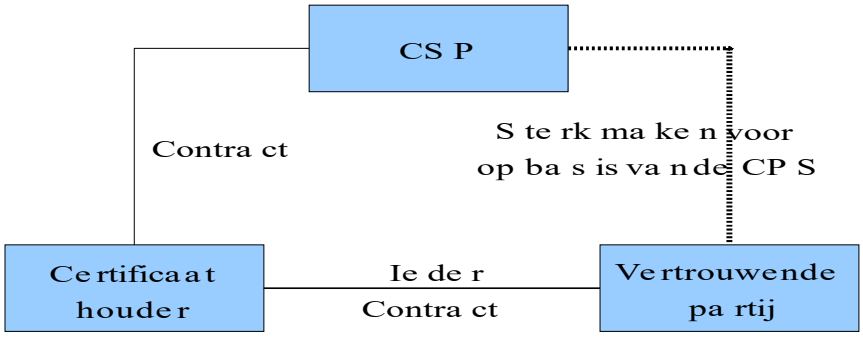
9.4 Privacyof personal information

ESG Electronic Signature BV takes into account the relevant laws and regulations when recording, processing and archiving personal data. The activities and administration of ESG are registered with the registration room under number M1321561.

9.5 Intellectual property rights

The TSP indemnifies the Subscriber for claims by third parties for TSP violations of intellectual property rights. All rights to this CPS are based on the TSP, unchanged copies may be distributed with source information..

9.6 Representations and warranties



9.6.1 Personal certificates

Personal certificates provide a trustworthy party with the natural person with whom they are concerned.

9.6.2 Services certificates

Service certificates provide a trust party with particular assurance of the connection of a service (device or function) with the organizational entity serving the service.

The validity of a certificate should not be confused with the authority of the certificate holder to do a particular transaction on behalf of an organization. PKI government does not control authorization; A trustworthy party must convince himself in another way**.**

9.7 Disclaimers of warranties

The special conditions of the TSP state how the TSP and the parties involved should deal with the restrictions on guarantees.

9.8 Limitations of liability

No stipulation.

9.9 Indemnities

No stipulation.

9.10 Term and termination

The TSP Special Terms and Conditions state how the TSP deals with termination.

9.11 Induvidual notices and communications with participants

Claiming personal notice of adaptation of any publication is explicitly excluded. The exception to this is the reporting obligation that the TSP has to the PA PKI government. The reporting obligation includes incidents as well as providing information about the intention to change the CA structure

9.12 Amendments

In order to respond to changing market conditions, security requirements, changes in legislation, etc., the TSP reserves the right to make changes and adjustments in this documentation. Changes are announced on the internet site www.de-electronic signature and apply from the moment a new CPS becomes effective. If the publication of the CPS has not been established, these two weeks after publication will come into effect. Changes that only concern writing errors or are of editorial nature are provided without prior notice.

The documentation is subject to periodic review, at least once a year, following the annual recertification. Any interested party may report comments on the content to the TSP. The authority to make changes to the documentation remains reserved for the TSP. Each change of the CPS will refresh version number and date.

9.13 Dispute resolution provisions

In cases where disagreement exists regarding the use of the names in a certificate, the TSP shall decide upon the interests in question, insofar as a decision is not required by mandatory Dutch law or other applicable regulations. Complaints and disputes may be submitted to the management board of the TSP. This decides, heard the CSO and, if applicable, the PA. This arrangement shall not affect access to the Dutch court unless the dispute is submitted to the court in charge in the district of Limburg.

9.14 Governing law

All agreements are governed by Dutch law

9.15 Compliance with applicable law

No stipulation.

9.16 Other provisions

If one or more provisions of the CPS in court judgment are invalid or otherwise not applicable, this does not affect the validity and applicability of all other provisions.