ESG de electronische signatuur BV

ESG PKI Disclosure Statement

Versie 1.0

Will Kamminga

Inhoudsopgave

Documentbeheer

Datum	Versie	Auteur
24-06-2016	1	Will Kamminga

1 Notice

This PKI Disclosure Statement does not substitute or replace the ESG Certification Practice Statement (PKIoverheid) under which digital certificates are issued by ESG de Electronische Signatuur B.V. (ESG). You must read the ESG CPS published at (https://www.de-electronische-signatuur.nl) before you apply for or rely on a certificate issued by ESG.

The full ESG CPS is defined by two documents:

- This document, the ESG PKI Disclosure Statement (ESG PKI PDS), and
- The ESG CPS.

The purpose of this document is to summarize and present the key points of the ESG CPS in a more readable and understandable format for the benefit of Subscribers and Relying Parties.

ESG is the Certification Authority under the Staat der Nederlanden Root-CA. This is achieved by the Staat der Nederlanden Root-CA (PKIoverheid) issuing a digitally signed CA Certificate that authenticates the Public Key of ESG. ESG is responsible for issuing and managing Digital Certificates to Organization employees, Organizations, non-human subscribers (like Servers and Network Devices).

ESG Policy Authority (ESG PA) is responsible for the governance of the ESG-CA.

ESG is an RA entity which issues, distribute and manages digital certificates, electronic signature tools and methods and any other associated services, which operates with its own physical certification authority (CA).

ESG subject to the approval of PKIoverheid, shall designate specific LRAs perform the Subscriber Identification and Authentication and Certificate request defined in CPS and related documents.

The ESG-CA is hosted in the KPN Trust centers which is responsible for managing ESG-CA operations as per the agreed service levels.

2 Contact Information

Queries regarding this ESG PKI Disclosure Statement shall be directed at:
E-mail: info@de-electronische-signatuur.nl
Tel: +31495566355
Address: Horselstraat 1, NL 6361 HC Nuth

3 Certificate Type, Validation Procedures and Usages

The certificate types supported by ESG are covered under § 1.2.4 in the ESG CPS document.

The ESG-CA signing key is permitted only for signing certificates and CRLs for their defined user communities. For subscribers, key usage depends on type of the certificate.

Certificates issued and distributed from ESG to the Organization employees are normally used by individuals to sign documents, e-mail and encrypt e-mail, data and to authenticate to applications (client authentication).

4 Reliance Limits

ESG does not set reliance limits for Certificates issued under this policy. Reliance limit may be set by other policies, application controls and Dutch applicable law or by Relying Party Agreement. For additional information, refer to "Limited Warranty and Disclaimer/Limitation of Liability" section.

5 Obligations

It is the responsibility of ESG to:

- Ensure that the Hardware Security Modules (HSM's) used for key generation meet the requirements of FIPS 140-2 Level 3 to store the CA keys and take reasonable precautions to prevent any loss, disclosure or unauthorized use of the private key.
- Generate CA private key using multi-person control "m-of-n" split key knowledge scheme.
- Keep confidential, any passwords, PINs or other personal secrets used in obtaining authenticated access to PKI facilities and maintain proper control, procedures for all such personal secrets.

It is the responsibility of the Subscriber to:

- Provide accurate and complete information at all times to ESG, both in the certificate request and verification process defined by the CSP for specific Certificate type to be supplied by ESG;
- Review the issued Certificate to confirm the accuracy of the information contained within it before installation and first use;
- Obtain a certificate; make only true and accurate representation of the required information to ESG;
- Use the Certificate for legal purposes and restrict to those authorized purposes detailed by the ESG CPS;

6 Certificate Status checking Obligations of Relying Parties

If a Relying Party is to reasonably rely upon a Certificate it shall:

- Ensure that reliance on Certificates issued under Certificate Policy is restricted to appropriate uses (see "Certificate Type, Validation Procedures and Usages" which are covered §4.10 in the ESG CPS document).
- Verify the Validity by ensuring that the Certificate has not expired.
- Ensure that the Certificate has not been suspended or revoked by accessing current revocation status information available at the location specified in the Certificate to be relied upon.
- Determine that such Certificate provides adequate assurances for its intended use.

7 Limited Warranty and Disclaimer/ Limitation of Liability

ESG warrants and promises to:

- Provide certification and repository services consistent with the CPS and other
- PKIoverheid Operations Policies and Procedures.
- Use its private signing key only to sign certificates and CRLs and for no other purpose;
- At the time of Certificate issuance; ESG implemented procedure for verifying accuracy of the information contained within it before installation and first use;
- Implement a procedure for reducing the likelihood that the information contained in the Certificate is not misleading;
- Maintain 24 x 7 publicly-accessible repositories with current information and replicates ESG issued certificates and CRLs;
- Perform authentication and identification procedures in accordance with CSP agreement and PKIoverheid Operations Policies and Procedures.
- Provide certificate and key management services including certificate issuance, publication and revocation in accordance with the ESG CP and CPS.
- Subscribers or Relying Parties for making no direct warranties or promises.

ESG does not liable for any loss of the PKI service:

- Due to war, natural disasters, etc.
- Due to unauthorized use of certificates or using it beyond the prescribed use defined by the ESG CPS for the certificates issued by the ESG.

Limitations on Liability:

- ESG will not incur any liability to Subscribers or any person to the extent that such liability results from their negligence, fraud or willful misconduct.
- ESG assumes no liability whatsoever in relation to the use of Certificates or associated Public-Key/Private-Key pairs issued under Certificate Policy for any use other than in accordance with Certificate Policy. Subscribers will immediately indemnify ESG from and against any such liability and costs and claims arising there from.
- ESG will not be liable to any party whosoever for any damages suffered whether directly or indirectly as a result of an uncontrollable disruption of its services.
- End-Users are liable for any form of misrepresentation of information contained in the certificate to relying parties even though the information has been accepted by ESG.

- Subscribers to compensate a Relying Party which incurs a loss as a result of the Subscribers breach of Subscriber's agreement.
- Relying Parties shall bear the consequences of their failure to perform the Relying Party obligations described in the Relying Party agreement.
- Endusers shall bear the consequences of their failure to perform the Registration Authorities obligations described in the CPS.
- ESG denies any financial or any other kind of responsibility for damages or impairments resulting from its CA/RA operation.

8 Applicable Agreements, CPS

Subscriber Agreement is submitted with the Subscriber's Request Form to ESG in order to obtain valid certificate.
ESG-PKI PDS and ESG CPS can be found at (https://www.de-electronische-sigantuur.nl).

9 Privacy Policy

ESG respects need to appropriately control individual's personal information and to know how such information may be used. ESG take reasonable care to ensure that the information submitted during the certificate application, authentication of identity and certification processes will be kept private. ESG will use that information only for the purpose of providing PKI services. The private information will not be sold, rented, leased, or disclosed in any manner to any person or third party without subscriber's prior consent, unless otherwise required by law, or except as may be necessary for the performance of PKI services, for auditing requirements, or as part of the regulatory compliance. For details please see ESG Privacy Policy at (https://www.de-electronische-signatuur.nl).

10 Refund Policy

There is no refund or refund policy.

11 Applicable Law and Dispute Resolution

Applicable laws are the laws and regulations of the Netherlands. PKIoverheid will act in accordance with current legislation in the Netherlands.

Applicable laws and dispute resolution provisions are in accordance with applicable ESG policies and agreements.

12 CA and Repository License, Trust Marks and Audit

ESG shall be subjected to periodic compliance audits, conform ETSI EN 319-411-1 former TS 102 042) and ETSI 319 411-2 which are once a year and after each significant change to the deployed procedures and techniques. ESG shall internally audit each delegated third party's (LRA) compliance against defined requirements on an annual basis.

13 Eligable Subscribers

ESG is responsible for issuing and managing Digital Certificates to Organizations employees, Organizations and non-human subscribers (like Servers and Network Devices) under PKIoverheid Staat der Nederlanden.

14 Certificate Status Information

ESG will publish its CRLs at least once every 24 hours' time, and at the time of any Certificate revocation of its subscribers.

- Notify ESG in the event of any information in the Certificate is, or becomes, incorrect or inaccurate; and
- Notify ESG immediately of a suspected or known key compromise in accordance with the procedures laid down in the ESG Certificate Policy.

For the device or organization certificate the authorized representative represented during the registration process must accept these responsibilities.

WARNING: The CA's private key is the primary means by which its subscribers are certified. This must be protected as its most valuable asset. If this private key is compromised, unauthorized persons could sign fraudulently produced certificates with the key and commit the Issuing Authority to unauthorized obligations and liabilities.