ESG de electronische signatuur BV

ESG PKI Disclosure Statement

Versie 1.1

Will Kamminga

Inhoudsopgave

Documentbeheer

Datum	Versie	Auteur
24-06-2016	1	Will Kamminga
18-10-2016	1.1	Hilde Oomen

1 Notice

This document is the PKI Disclosure Statement herein after referred to as the PDS. This document 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 (cps.de-electronische-signatuur.nl) before you apply for or rely on a certificate issued by ESG.

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

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

ESG shall designate specific LRAs to perform identification of the Subscriber/ Certificate Holder and check the authentication of the Certificate request as defined in the CPS and related documents.

2 Contact Information

Queries regarding this ESG PKI Disclosure Statement shall be directed at:

ESG de electronische signatuur B.V.
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 subjects, key usage depends on the type of certificate.

Certificates issued and distributed from ESG to the Organization employees are used by individuals/ Services to:

- sign documents and e-mails (non-repudiation)
- Encrypt e-mail and data (encryption)
- authentication to applications (authentication).

4 Reliance Limits

Refer to section 9.8 of the CPS (cps.de-electronische-signatuur.nl) for reliance limits. ESG's liability for breach of its obligations pursuant to the ESG CPS shall, in the absence of fraud or wilful misconduct on the part of ESG, be subject to a monetary limit and shall be limited absolutely to the monetary amount set in the CSP.

5 Obligations of ESG

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.

6 Obligations of Subscribers

Digital Certificate Holders are required to act in accordance with the CPS and the relevant Certificate Holder/ Subscriber Agreement. A digital Certificate Holder represents, warrants and covenants with and to ESG, Relying Parties, Application Software Vendors and the Registration Authority processing their application for a Digital Certificate that:

- Both as an applicant for a Digital Certificate and as a Digital Certificate Holder, submit complete and accurate information in connection with an application for a Digital Certificate and will promptly update such information and representations from time to time as necessary to maintain such completeness and accuracy.
- Comply fully with any and all information and procedures required in connection with the Identification and Authentication requirements relevant to the Digital Certificate issued.
- Prompt review, verify and accept or reject the Digital Certificate that is issued and ensure that all the information set out therein is complete and accurate and to notify the Issuing CA, Registration Authority, or ESG immediately in the event that the Digital Certificate contains any inaccuracies.
- Secure the Private Key and take all reasonable and necessary precautions to prevent the theft, unauthorised use of its Private Key (to include password, hardware token or other activation data used to control access to the Participant's Private Key).
- Exercise sole and complete control and use of the Private Key that corresponds to the Certificate Holder's Public Key.
- Immediately notify the Issuing CA, Registration Authority or ESG in the event that their Private Key is compromised, or if they have reason to believe or suspect or ought reasonably to suspect that their Private Key has been lost, damaged, modified or accessed by another person, or compromised in any other way whatsoever.
- Take all reasonable measures to avoid the compromise of the security of integrity of the ESG PKI.
- Forthwith upon termination, revocation or expiry of the Digital Certificate (howsoever caused), cease use of the Digital Certificate absolutely.
- At all times utilise the Digital Certificate in accordance with all applicable laws and regulations.
- Use the signing key pairs for electronic signatures in accordance with the Digital Certificate profile and any other limitations known, or which ought to be known, to the Digital Certificate Holder.
- Discontinue the use of the digital signature key pair in the event that ESG notifies the Digital Certificate Holder that the ESG PKI has been compromised.
- For Qualified Certificates, private keys are generated on a Secure Signature Creation Device (SSCD) in the presence of the Certificate Holder. The individual applying for the Qualified Certificate must undergo a face-to-face identity verification procedure. The Certificate Holder is responsible for directly securing the SSCD with a Personal Identification Number.

6 Certificate Status checking Obligations of Relying Parties

Any party receiving a signed electronic document may rely on that Digital Signature to the extent that they are authorised by contract with the Certificate Holder, or by legislation pursuant to wich that Digital Certificate has been issued, or by commercial law in the jurisdiction in which that Digital Certificate was issued.

In order to be an Authorised Relying Party, a Party seeking to rely on a Digital Certificate issued within the ESG PKI agrees to and accepts the terms and conditions of ESG (cps.de-electronische-signatuur.nl) by querying the existence or validity of; or by seeking to place or by placing reliance upon a Digital Certificate.

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.

The Status of Digital Certificates issued within the ESG PKI is published in a Certificated Revocation List or is made available via Online Certificate Status Protocol checking where available.

7 Limited Warranty and Disclaimer/ Limitation of Liability

ESG warrants and promises to:

- Provide certification and repository services consistent with the CPS
- 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 CPS.

ESG shall not be liable in any event for any loss of profit, loss of sales or turnover, loss or dame to reputation, loss of contracts, loss of customers, loss of the use of any software or data, loss or use of any computer or other equipment, wasted management or other staff time, losses or liabilities under or in relation to any other contracts, indirect loss or damage, consequential loss or damage, special loss or damage. For the purpose of this paragraph, the term “loss” means a partial loss or reduction in value as wels as a complete or total loss.

ESG’s liability to any person for damagers arising under, out of or related in any way to the CPS, the applicable contract or any related agreement, whether in contract, warranty tort or any other legal theory, shall, subject as hereinafter set out, be limited to actual damages suffered by that person, ESG shall not be liable for indirect, consequential, incidental, special, exemplary, or punitive damages with respect to any person, even if ESG has been advised of the possibility of such damages, regardless of how such damages or liability may arise, whether in tort, negligence, equity, contract, statue, common law, or otherwise. As a condition to participation within the ESG PKI (including, without limitation, the use of or reliance upon Digital Certificates), any person that participates within the ESG PKI irrevocably agrees that they shall not apply for or otherwise seek either exemplary, consequential, special, incidental, or punitive damages, and irrevocably confirms to ESG their acceptance of the foregoing and the fact that ESG has relied upon the foregoing as a condition and inducement tot permit that person to participate within the ESG PKI.

Refer to the CPS (cps. de-electronische-signatuur.nl) for further detail as to liability and warranties.

8 Applicable Agreements, CPS

The following documents are available at cps.de-electronische-signatuur.nl:

- Certification Practice Statement
- General terms and conditions ESG
- Special terms and conditions ESG
- ESG PKI disclosure statement

Subscriber Agreement is embedded in the registration forms, produced by ESG's registration portal. (https://bestellen.de-electronische-signatuur.nl).

9 Privacy Policy

ESG respects the need to appropriately control individual's personal information and to know how such information may be used. ESG takes 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.

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. For further details refer to ESG's CPS on cps.de-electronische-signatuur.nl.

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's management system). ESG shall internally audit each delegated third party's (LRA) compliance against defined requirements on an annual basis.