PKI Disclosure Statement

for

eIDAS compliant Qualified Certificates for Electronic Signature

provided by

Trust Service Provider at Ministry of Defence of Slovenia

This PKI Disclosure Statement concerns the qualified certificates issued by Certification Authority at Ministry of Defence of Slovenia (MoD) acting as a Trust Service Provider compliant with Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (eIDAS Regulation). The document contains information and conditions for end-users using services corresponding to Certificate Policy (CP) / Certification Practices Statement (CPS).

1. Trusted service provider contact info

Ministry of Defence of Slovenia
IT and Communication Office
SIMoD-PKI Management Board
Vojkova cesta 55, 1000 Ljubljana, SLOVENIA
Phone: +386 (0)1 230 5314
Fax: +386 (0)1 471 2701
Email: simod-pki@mors.si
WEB: www.simod-pki.mors.si

Revocation requests:
Phone: +386 (0)1 230 5314
Email: simod-pki@mors.si

2. Certificate type, validation procedures and usage

2.1. Certificate type

Certification Authority at MoD with its issuer SIMoD-CA-Restricted issues these types of qualified certificates accordant with ETSI EN 319 411-2:

Certificate Policy Name	Certificate Policy Identifier
QCP-n-qscd	0.4.0.194112.1.2
QCP-n	0.4.0.194112.1.0
QCP-l-qscd	0.4.0.194112.1.3
QCP-l	0.4.0.194112.1.1

Qualified certificates can be issued to:

- natural persons – employees of MoD,
- legal persons - organizational units of MoD and functional or organizational roles established to perform military or other duties in the area of national defence.

2.2. Validation procedures

Qualified certificate is issued to an individual after verification of its identity.

Verification of the individual requesting issuance of a qualified certificate is carried out in person by a registration authority. Registration authority checks data of the individual in the database of employees of MoD then identifies the individual by valid national identity document.

In case of qualified certificates for legal persons the verification of the authorized representative of the organizational unit or individual associated to or acting on behalf of the role is carried out.

At certificate re-key identity can be confirmed by proof of possession of valid certificate and associated private key.

2.3. Usage

SIMoD-CA-Restricted issues qualified certificates with these usage:

CP Name	CP Identifier	Certificate Usage / CP Identifier (2)
QCP-n-qscd	0.4.0.194112.1.2	validation of e-signature 1.3.6.1.4.1.22295.10.1.1.1.1.2
		validation of e-signature, encryption 1.3.6.1.4.1.22295.10.1.1.1.3.2
QCP-n	0.4.0.194112.1.0	validation of e-signature 1.3.6.1.4.1.22295.10.1.1.2.1.2
		validation of e-signature, encryption 1.3.6.1.4.1.22295.10.1.1.2.1.3.2
QCP-l-qscd	0.4.0.194112.1.3	validation of e-seal, encryption 1.3.6.1.4.1.22295.10.1.1.1.3.3.2
QCP-l	0.4.0.194112.1.1	validation of e-seal, encryption 1.3.6.1.4.1.22295.10.1.1.2.3.3.2

The certificates issued by Certification Authority at MoD are for official use only at MoD. Holder of the certificate can use it only to perform duties as an employee of MoD.

3. Reliance limits

Status »qualified« associated to qualified certificates applies on to certificate usage »validation of electronic signature« or »validation of electronic seal«. In no instance can status »qualified« be related to the certificate usage »encryption«.

Certification Authority at MoD keeps data related to its operations including audit logs, versions of CP and CPS seven (7) years after its creation and data related to certificates seven (7) years after the expiration of validity of the certificate, and hence provides supporting evidence.

4. Obligations of subscribers

By applying for the certificate subscriber agrees to conditions stated in CP and CPS. Subscriber is committed to:

- use keys and certificates only for the purposes stated in the CP and CPS,
- check the content of the certificate upon acceptance and immediately inform operational personnel of SIMoD-CA-Restricted about any errors or defects,
- inform operational personnel of SIMoD-CA-Restricted about any changes of data contained in the certificate in eight (8) days after its occurrence,
- not create any electronic signature if the validity period of zhe certificate has expired,
- electronically sign only data with validity shorter than applied certificate or re-apply electronic signature before expiration of current one,
- make his private keys, smart cards or other media containing private keys inaccessible to other persons and take all reasonable measures to prevent loss, disclosure, change and unauthorized use of the private key,
- start a procedure of revocation in the case of security violation or suspicion of security violation to the private key.

5. Certificate status checking obligations of relying parties

A relying party is committed to trust only these qualified certificates:

- that are used in accordance with the declared purpose,
- are appropriate for applicability ranges that were specified in CP and CPS,
- status of the certificate was verified on the basis of the valid Certificate Revocation Lists or OCSP service.

6. Limited warranty & disclaimer/ limitation of liability

6.1. Limited warranty

Certification Authority at MoD limits its liability for the use of single certificate to 5.000,00 EUR.

6.2. Disclaimer/ limitation of liability

Certification Authority at MoD does not take any responsibility for damages, losses, costs and claims as a result of using a certificate and related keys, if:

- the certificate was issued as a result of error, false data in certificate request or other incorrect action of certificate subscriber, certificate user or other physical or legal person beyond control of the Certification Authority at MoD whilst Certification Authority at MoD was acting according to relevant regulations,
- certificate was used after its expiration, revocation and publishing in Certificate Revocation List,
- certificate was modified,
- the private key was compromised or there is a suspicion of its compromise,
- the certificate was used in a contradiction to CP, CPS and other relevant regulation,
- damage is a result of malfunction of hardware or software of the user or third party,
- action in contradiction to CP, CPS and other relevant regulation of any party is a result of forces of nature: fire, flood, gale, other situations such as war, terrorist attack, epidemic, and other natural disasters or disasters caused by people.

7. Applicable agreements, Certification Practices Statement, Certificate Policy

Certification Authority at MoD operates according to national legislation, is compliant with Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (eIDAS Regulation) and its CP and CPS.

Certification Authority at MoD publishes at the repository http://www.simod-pki.mors.si the following documents (in Slovenian language only):

- Certificate Policy,
- Certification Practices Statement.

8. Privacy policy

Subscriber private data is processed in accordance with the applicable Slovenian national legislation for protecting personal data.

Retention period for the registration data is seven (7) years after the validity expiration of the certificate related to registration data.

9. Refund policy

Not applicable. Certification Authority at MoD does not provide certificates for general public.

10. Applicable law, complaints and dispute resolution

Certification Authority at MoD aims for the peaceful and negotiated settlements of the disputes. If not possible the competent dispute resolution body is court of justice of Ljubljana. The disputes shall be resolved applying applicable Slovenian national law.

11. TSP and repository licences, trust marks and audit

Certification Authority at MoD issues qualified certificates as a qualified trust service provider listed on a Slovenian trusted list:

http://www.mju.gov.si/si/delovna_podrocja/informacijska_druzba/elektronske_identitete_in_storitve_zaupanja/zanesljivi_seznam/

Supervision of Certification Authority at MoD as a qualified trust service provider is according to eIDAS Regulation.