Montenegro
Ministry of the Interior

TrustME PKI DISCLOSURE STATEMENT

TSP CONTACT INFO

Certificate Authority: Ministry of the Interior, Montenegro
TrustME PMA: Service for information and communication technologies, information security and technical supervision systems, Ministry of the Interior
Svetog Petra Cetinjskog Boulevard, 22, 81000 Podgorica, Montenegro
E-mail: pma@mup.gov.me

CERTIFICATE TYPE, VALIDATION PROCEDURES AND USAGE

TrustME Trusted Service Provider as part of Ministry of Interrior of Montenegro issues to evry citizen applying for an eID card a pair of digital certificates:

- Qualified certificate for qualified electronic signature;
- Certificate for electronic identification.

These certificates are issued to evry citizen within the scope of local laws in Montenegro and according to TrusteME Certificate Policy and Certificate Practice Statement available at https://ca.elk.gov.me/cpcps. Each citizen undergo proper identification process before eID is isssued.

RELIANCE LIMITS

Advanced qualified digital certificates are issued on QSCD (qualified signature creation device) and are aimed to support qualified electronic signatures and electronic identification such as defined in Regulation (EU) N° 910/2014. All events involved in the certificate life cycle are recorded. Documentation and audit logs are retained as archive records for a period no less than ten (10) years after the end of validity of certificate or event, if applicable.

OBLIGATIONS OF SUBSCRIBERS

Digital Certificate subscribers and subjects are required to act in accordance with the CP/CPS and the relevant Certificate Subject/Subscriber Agreement. In particular:

1. Both as an applicant or subject or subscriber submit complete and accurate information in connection with the certificate and will promptly update such information and representations from time to time as necessary to maintain such completeness and accuracy.
2. Comply fully with any and all information and procedures required in connection with the Identification and Authentication requirements.
3. Promptly review, verify and accept or reject the certificate that is issued and ensure that all the information set out therein is complete and accurate and to notify TrustME CA or Registration Authority immediately in the event of any inaccuracies.
4. Secure the Private Key (with the use of Qualified Signature Creation Device - QSCD) and take all reasonable and necessary precautions to prevent the theft, unauthorized viewing, tampering, compromise, loss, damage, interference, disclosure, modification or unauthorized use of its private Key (e.g. PIN code, smart card/key).
5. Exercise sole and complete control and use of the private Key that corresponds to the subject's public key.
6. Immediately notify TrustME CA or Registration Authority 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.
7. Take at all times all reasonable measures to avoid the compromise of the security or integrity of the TrustME trust services and PKI and use certificate, key pair and all services accordance with all applicable laws and regulations.

8. Forthwith upon termination, revocation or expiry of the certificate, cease use of the certificate.

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:

1. authorized in the jurisdiction in which that certificate was issued or used;
2. the appropriateness of the use of the certificate for any given purpose is allowed by the CP/CPS;
3. by querying the existence or validity of the certificate;
4. by assessing that the certificate is being used in accordance with its Key-Usage field extensions;
5. by assessing that the certificate is valid at the time of reliance by reference to Online Certificate Status Protocol or Certificate Revocation List Checks.

The status of certificates issued by TrustME is published in a Certificate Revocation List and is made available via Online Certificate Status Protocol checking. Please see CPS for locations where this information is made available (https://ca.elk.gov.me/cpcps).

LIMITED WARRANTY AND DISCLAIMER/LIMITATION OF LIABILITY

TrustME shall not in any event be liable for any loss of profits, loss of sales or turnover, loss or damage 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 (save as may arise directly from breach of the CP/CPS), 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, and for the purpose of this paragraph, the term "loss" means a partial loss or reduction in value as well as a complete or total loss. Refer to the CP/CPS for further detail as to liability and warranties.

APPLICABLE AGREEMENTS, CPS, CP

The following documents are available online https://ca.elk.gov.me:

1. Certificate Policy
2. Certification Practice Statement
3. Certificate Subject Agreement
4. Certificate Subscriber Agreement
5. Request for revocation

REFUND POLICY

Not applicable.

APPLICABLE LAW, COMPLAINTS AND DISPUTE RESOLUTION

Law of Montenegro and dispute resolution by courts of Montenegro.

TSP AND REPOSITORY LICENSES, TRUST MARKS, AND AUDIT

In the provision of trust services TrustME is accredited by Accreditation Body appointed by Ministry of Public Administration, Digital Society and Media of Montenegro at least on two year basis.