PKI DISCLOSURE STATEMENT

CPName: Halcom CA PO e-seal 1

TSP CONTACT INFO

Halcom CA
Tržaška 118, 1000 Ljubljana, Slovenia
Tel.: (+386) 01 200 34 86
Fax: (+386) 01 200 33 60
E-mail: ca@halcom.si

The above contact info can also be used for all certificate related information revocation requests. These may also be directed to any registration authority of Halcom CA (see list on www.halcom.com).

CERTIFICATE TYPE, VALIDATION PROCEDURES AND USAGE

Qualified Certificate for authorized business entity issued within the scope of eIDAS Regulation, for which the individual applying for the Qualified Personal Digital Certificate must undergo a face-to-face identity verification procedure.

Applicable policy is for certificates issued to the public and issued under the following data:

OID CPOID:1.3.6.1.4.1.5939.5.3.2 (advanced qualified digital certificate and cloud certificate)

OID CPOID:1.3.6.1.4.1.5939.5.4.2 (standard qualified digital certificate)

Original title in Slovenian: "Politika za EU Kvalificirana digitalna potrdila za elektronske žige".

RELIANCE LIMITS

Advanced qualified digital certificates are issued on QSCD (qualified signature creation device) and are aimed to support qualified electronic seals such as defined in Regulation (EU) N° 910/2014.

Standard qualified digital certificates are aimed to support the advanced electronic seals based on a qualified certificate 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 Halcom CA or Registration Authority immediately in the event of any inaccuracies.
4. Secure the Private Key (with the use of Secure Signature Creation Device - SSCD) 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 Halcom 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 Halcom CA 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 Halcom CA is published in a Certificate Revocation List (http://domina.halcom.si/crls/ to HTTP protocol and ldap://ldap.halcom.si according to LDAP protocol) and is made available via Online Certificate Status Protocol checking (http://ocsp.halcom.si).

LIMITED WARRANTY AND DISCLAIMER/LIMITATION OF LIABILITY

Halcom CA 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 at www.halcom.com:

1. Certificate Policy
2. Certification Practice Statement
3. Privacy Policy
4. Certificate Subject Agreement
5. Personal Data Consent
6. Request for revocation

PRIVACY POLICY

Data contained within a certificate is considered public information. Personal data obtained during the registration process is protected to the full extent of EU legislation on personal data protection (General Data Protection Regulation and others) and will not be released without prior consent of the relevant certificate holder, unless required otherwise by law or to fulfil the requirements of the CP/CPS.

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.

Refer to the Halcom CA Privacy Policy at https://pomoc.halcom.com/wp-content/uploads/2018/07/Pravila-varstva-podatkov-V1.pdf .

REFUND POLICY

Not applicable.

APPLICABLE LAW, COMPLAINTS AND DISPUTE RESOLUTION

Law of Republic of Slovenia (European union member state) and dispute resolution by courts of Republic of Slovenia.

TSP AND REPOSITORY LICENSES, TRUST MARKS, AND AUDIT

In the provision of trust services, Halcom CA maintains several certifications. These include:

1. Qualified Trust Service Provider under eIDAS Regulation and standard EN 319 401, EN 319 411-1, EN 319 411-2, EN 319 412-1, EN 319 412-3, EN 319 412-5 (Slovenia, European union; supervised by Ministry of Public Administration of Republic of Slovenia and audited by Bureau Veritas on an annual basis);
2. ISO/IEC 9001 Certificate (issued by Bureau Veritas based on audit on an annual basis);
3. ISO /IEC 27001 Certificate (issued Bureau Veritas based on audit on an annual basis).