Author: Luka RIBIČIČ

Document number: 400085-39-9/17

Halcom CA: Certificate Practice Statement (CPS),

Edition: 10

Halcom CA

Certificate Practice Statement (CPS)

English version

Document is valid from: 15.6.2024

Edition	Number of document and attachments	Change description	Author	Date of change
1	400085-38-0/17	Translation of CPS Izdaja št. 2 (IPS 400085-8-2/17)	L. Ribičič	27.2.2018
2	400085-39-1/17	Translation of CPS Izdaja št. 3 (IPS 400085-8-3/17)	L. Ribičič	1.6.2018
3	400085-39-2/17	Translation of CPS Izdaja št. 4 (IPS 400085-8-4/17)	L. Ribičič	24.5.2019
4	400085-39-3/17	Translation of CPS Izdaja št. 5 (IPS 400085-8-5/17)	S. Lazić	29.4.2020
5	400085-39-4/17	Translation of CPS Izdaja št. 6 (IPS 400085-8-6/17)	S. Lazić	3.2.2021
6	400085-39-5/17	Translation of CPS Izdaja št. 7 (IPS 400085-8-7/17)	S. Lazić	21.5.2021
7	400085-39-6/17	Translation of CPS Izdaja št. 8 (IPS 400085-8-8/17)	S. Lazić	13.4.2022
8	400085-39-6/17	Version unification (editorial correction)	L. Ribičič	24.6.2022
9	400085-39-8/17	Translation of CPS Izdaja št. 9 (IPS 400085-8-8/17)	S. Lazić	23.5.2023
10	400085-39-9/17	Translation of CPS Izdaja št. 10 (IPS 400085-8-10/17)	L. Ribičič	22.5.2024

Table of Contents

1. INTRODUCTION

(1) This document represents Certificate Practice Statement (hereinafter referred to as CPS) of the trust service provider in the field of electronic signatures, electronic stamps, electronic time-stamps, validation and other services.

(2) Halcom CA is the oldest and the biggest trust service provider (hereinafter referred to as TSP) in Slovenia, which for the executing of its services in the field of electronic signatures, electronic stamps, electronic time-stamps, validation and other services uses the safest technologies, including the usage of QSCD and secure cloud.

(3) All provisions in CPS regarding the operation of HALCOM CA are duly transferred and further specified in the provisions of the internal policy which represents a confidential part of the internal rules and is composed of confidential documents which define the infrastructure, provisions as regards the employees of HALCOM CA (competences, tasks, authorizations and requisite conditions of individual staff members), physical protection (access to premises, handling of hardware and software), software protection (server security settings, security copies...) and internal audit (audit over physical access, authorizations...).

1.1. Overview

(1) CPS represents general regulations of TSP HALCOM CA for issuing certificates, regulates the purpose, functioning and methodology of certificates management and security requirements to be met by TSP HALCOM CA, the subscribers, subjects and third parties referring to these certificates, and the responsibility of all the persons mentioned.

(2) Halcom CA is a provider of the following services:

- Qualified certificates for electronic signatures,
- Qualified service of validation of validity of electronic signatures,
- Qualified service of electronic signatures storage,
- Qualified certificates for electronic seals,
- Qualified service of validation of validity of electronic seals,
- Qualified service of electronic seals storage,
- Qualified electronic time-stamp,
- Qualified certificates for website authentication.

(3) TSP Halcom CA operates within Halcom d.d.

(4) Halcom CA issues:

- Qualified digital certificates for electronic signing,
- Qualified digital certificates for electronic sealing,

- Qualified digital certificates for website authentication and
- Qualified digital certificates for time-stamping.

(5) Halcom CA issues certificates and performs other activities of a TSP in accordance with valid regulations of the legal order of Republic of Slovenia and European Union, and in accordance with eIDAS regulation, technical requirements by the ETSI, IETF RFC standards, ISO/IEC family of standards and other related standards.

(6) Halcom CA publishes the list of registration authorities, that enable certificates acquisition, on its web pages.

1.1.1 Basic documents of the TSP Halcom CA

More detailed rules, conditions, rights and obligations regarding the operation of the TSP Halcom CA are described in the following public documents:

- Halcom CA Policy for qualified digital certificates for legal persons,
- Halcom CA Policy for qualified digital certificates for natural persons,
- Halcom CA Policy for qualified digital certificates for website authentication,
- Halcom CA Policy for qualified time-stamping,
- Certificate Practice Statement.

1.1.2 Links between basic documents of TSP Halcom CA

(1) The policy defines the requirements of the TSP, and the CPS provides operational processes to meet these requirements. Certificate practice statement (CPS) defines how the trust provider provides technical, organizational and process requirements for business, which are defined in Halcom CA policy.

(2) The policy is a more general document than the CPS. The CPS provides a more detailed description of how TSP Halcom CA works, and business and operational processes of certificates issuing and management.

(3) The policy is defined independently of the specific operating unit of the TSP, and the CPS is a detailed description of the organizational structure and operational processes of the TSP Halcom CA.

1.1.3 Standards

Halcom CA issues certificates and performs other activities of the TSP in accordance with the applicable law of the Republic of Slovenia and the European Union, and in accordance with the technical requirements of ETSI, the IETF RFC standard and the ISO / IEC family of standards and other related standards.

1.1.4 Halcom CA Internal Rules

(1) A detailed description of the HALCOM CA infrastructure, operations, infrastructure management procedures and oversight of the security policy of its operation is determined by its internal rules.

(2) Internal rules are confidential documents and constitute the business secret of the TSP Halcom CA.

(3) The internal rules contain detailed provisions on:

- System of physical control of entry into the premises of Halcom CA,
- System of logical control of approaches to computer networks Halcom CA,
- Halcom CA system for securing private keys,
- System of distributed responsibility at Halcom CA for private key activation,
- Procedures and personnel involved in the provision of trust services,
- Procedures in unpredictable circumstances (fire, flood, earthquake, breach of premises or information system of a TSP).

(4) Halcom CA is subject to an external independent audit carried out annually by an Accredited body.

1.2. Halcom CA Trust Service Provider

(1) Halcom CA is responsible for issuing the following qualified digital certificates:

- Halcom Root Certificate Authority (root certificate)
- Halcom CA PO e-signature 1 (intermediate/subordinate certificate for qualified digital certificates for legal persons),
- Halcom CA PO e-signature 2 (intermediate/subordinate certificate for qualified digital certificates for legal persons),
- Halcom CA FO e-signature 1 (intermediate/subordinate certificate for qualified digital certificates for natural persons),
- Halcom CA FO e-signature 2 (intermediate/subordinate certificate for qualified digital certificates for natural persons),
- Halcom CA PO e-seal 1 (intermediate/subordinate certificate for qualified digital certificates for electronic seals)
- Halcom CA PO e-seal 2 (intermediate/subordinate certificate for qualified digital certificates for electronic seals)
- Halcom CA web 1 (intermediate/subordinate certificate for qualified digital certificates for website authentication)
- Halcom CA TSA 1 (intermediate/subordinate certificate for qualified time-stamps)

- User certificates:

  1. Natural persons:

     - Certificates for electronic signing,
     - Website authentication certificates.

  2. Legal persons:

     - Certificates for electronic signing (natural persons representing legal persons),
     - Website authentication certificates,
     - Certificates for electronic sealing,

1.3. PKI participants

1.3.1 Halcom CA Trust Service Provider

Halcom CA is a TSP that issues and manages certificates for electronic signing, electronic sealing, electronic time-stamping, validation and other services. The TSP Halcom operates within Halcom d.d.

1.3.2 Halcom CA Registration Authority

(1) Registration authority (hereinafter referred to as RA) performs the following tasks for the TSP:

- verification of the identity of a natural persons, legal persons, natural persons identified in association with a legal person, legal representatives of a legal person and other relevant data for managing certificates,
- receiving certificate application forms,
- receiving requests for revoking certificates,
- issue the necessary documentation to the subject or future subjects,
- transmitting application forms, requests and other information in a secure manner to the TSP Halcom CA.

(2) The TSP Halcom CA may authorize other organizations in the business and public sectors, in addition to their RA, to perform the tasks of the RA or other tasks authorized by TSP Halcom CA. Halcom CA will oblige each such organization with a contract to fulfil the strict security conditions in accordance with the applicable European and Slovenian regulations and international, European and Slovenian standards and recommendations and policies, CPS and internal rules of Halcom CA.

(3) The TSP Halcom CA has a geographically dispersed RAs, enabling future subjects easy registration in their hometown or a town nearby. Information about the locations of the RAs is available on the TSP Halcom CA website.

1.3.3 Certificate Subscribers and Subjects

(1) The subscriber/subject of the certificate may be a natural person or a legal person (depending on the type of certificate)

Service	Issuer	Subscriber	Subject
Certificates for legal persons (e-signature)	Halcom CA PO e-signature 1	Legal person	Natural person
Certificates for legal persons (e-signature)	Halcom CA PO e-signature 2	Legal person	Natural person
Certificates for electronic seals	Halcom CA PO e-seal 1	Legal person	Device / server
Certificates for electronic seals	Halcom CA PO e-seal 2	Legal person	Device / server
Certificates for website authentication	Halcom CA web 1	Legal person / natural person	Server
Certificates for natural persons	Halcom CA FO e-signature 1	Natural person	Natural person
Certificates for natural persons	Halcom CA FO e-signature 2	Natural person	Natural person
Certificates for electronic time-stamps	Halcom CA TSA 1	TSP	Device / server

1.3.4 Relying parties

(1) Third parties are persons who rely on issued certificates and other services of TSP Halcom CA and may be natural or legal persons.

(2) Third parties must follow the instructions of the TSP Halcom CA and must always check the validity of the certificate (revocation), the purpose of the use of the certificate, the validity period of the certificate (expiration), etc. More detailed obligations and responsibilities of third parties are given in sections 4.5.2. and 9.6.4.

(3) Third parties are not necessarily subjects of TSP Halcom CA certificates or digital certificates from other providers of trust services.

1.4. Certificate usage

Halcom CA manages (issues and checks, revokes, renews, stores, publishes) qualified certificates for electronic signing, electronic sealing, website authentication, and time-stamping. Certificates are intended for natural persons and legal persons.

1.4.1 Appropriate certificate uses

(1) Electronic signature/seal certificates are intended for signing/sealing unilateral or mutual communications between subjects of certificates and for use in different applications and for various purposes that occur on the market. Among other things, certificates can be used for purposes such as:

1) identification of the subject,
2) the disclosure of the identity of the subject,
3) signing/sealing documents in electronic form,
4) encrypting and decrypting documents in electronic form.

(2) The electronic signature/seal can be used in applications such as

1) electronic or mobile banking,
2) applications of eGovernment or mGovernment,
3) applications eHealth or mHealth,
4) signing/sealing electronic or mobile forms,
5) secure connections with public sector bodies and organizations and with other legal or natural persons,
6) other applications or services in which certificate is required,
7) access control.

(3) Website authentication certificates are intended for:

1) identification of the website,
2) the disclosure of the identity of the website,
3) access control,
4) establishing secure connections.

(3) Secure time-stamps are used in various applications and for various purposes that appear on the market. Among other things, time-stamps are used in applications such as:

1) electronic banking,
2) electronic storage of data, documentary or archival material,
3) applications of eGovernment,
4) other applications where the proof of a particular action or fact must be guaranteed with the exact time source.

1.4.2 Prohibited certificate uses

(1) The use of certificates issued in accordance with policies is prohibited contrary to the provisions of the policies or regulations in force or outside the scope of the permitted use specified in the previous section.

(2) Certificates are not intended for resale.

1.5. Policy administration

1.5.1 Organization administering the document

(1) The CPS and policies are managed by the TSP Halcom CA, which operates within the Halcom d.d.

(2) Manager address:

Halcom d.d.
Dunajska cesta 123
1000 LJUBLJANA
Slovenia

1.5.2 Contact person

(1) For questions relating to CPS and policies, you can contact TSP authorized persons who can be reached at the address and the telephone numbers listed below.

(2) Halcom CA address:

Halcom CA
Dunajska cesta 123
1000 LJUBLJANA
Slovenia
Tel.: (+386) 01 200 34 86
E-mail: ca@halcom.com
E-mail for revocation: ca_preklici@halcom.com

1.5.3 Person determining CPS suitability for the policy

In accordance with their responsibilities, authorized personal of the TSP Halcom CA is responsible for Halcom CA compliance with CPS and policies.

1.5.4 CPS approval procedures

(1) With the aim of ensuring legality, safety, and quality, any proposal for a new CPS is subject to both technological and legal review prior to the approval of the Chief Executive Officer of Halcom d.d.

(2) The TSP may issue updates as specified in section 9.12 for individual provisions.

1.6. Definitions and acronyms

1.6.1 Definitions

CA	Trust service provider that issues certificates (Certificate authority or Certificate agency).
CPName	The name of the Certification policy that is uniquely linked to the international certification policy object identifier (CPOID).
CP	Certificate Policy. The policy governs the purpose, operation, and methodology of managing the service, and the responsibilities and safety requirements to be met by the TSP, certificate subscriber or subject and third parties who rely on these certificates/services.
CPS	The certificate practice statement represents the general rules of the TSP.
CPOID	An international number that identifies the certificate policy object identifier.
CRL	Certificate revocation list
DN	Unique distinguished name
LDAP	Lightweight directory access protocol is a protocol that provides access to the directory and is specified by the IETF (Internet engineering task force) recommendation of the IETF RFC 3494.
S/MIME	Secure multipurpose internet mail extensions
SSL	Secure sockets layer
TLS	Transport layer security
PKI	Public key infrastructure
QSCD	Qualified signature creation device (secure carrier for private keys)
EŠEI	Unified number of electronic identification (sln. Enotna številka elektronske identifikacije)

1.6.2 Acronyms

Trust service provider (TSP)	A natural or legal person who issues certificates or performs other trust services.

Certificate repository (central directory)	Certificate repository in compliance with X.500 guidelines, where certificates are stored as recommended by guidelines X.509 ver. 3, which can be accessed via the LDAP protocol.
Identification	Identification means the procedure for the use of personally identifiable information in a physical or electronic form that uniformly represents either a natural or legal person or a natural person representing a legal person.
Registration Authority (RA)	The service or person accepting certificate applications forms, revocation requests, identifying and verification of the identity of future subscribers and subjects on behalf of the TSP.
Distinguished Name	Unique name in the certificate (DN), which unambiguously and uniquely defines the user in the directory structure.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1. Repositories

(1) The TSP Halcom CA shall make publicly available on Halcom CA website at http://www.halcom.com/ everything in connection with its operation, notices to the subject and third parties and other relevant documents.

(2) Documents that are publicly accessible are:

- price list,
- the certificate policies (CPs),
- certificate practice statement of the TSP (CPS)
- certificate application forms, revocation requests and other service contracts of a TSP,
- instructions for the safe use of digital certificates,
- information on the applicable regulations and standards relating to the operation of the TSP, and
- other information relating to the operation of Halcom CA.

(3) The documents which constitute a confidential part of the internal rules of the TSP Halcom CA are not publicly available.

2.2. Publication of certification information

(1) The CPS and new policies are published according to the indication in section 9.10.

(2) All TSP certificates are based on X.509 standard and are published in the central directory on the server ldap.halcom.si, which is in the custody of HALCOM CA. For the protection of data, only a

register of revoked certificates, included in the directory, is publicly available.

(3) The status of revoked certificates shall be published immediately in the register of revoked certificates (detailed in section 4.9.8.), other publicly available information or documents are published as needed.

(4) Access to the directory of issued certificates is only allowed to authorized users who validate the larger number of issued certificates.

2.3. Time or frequency of publication

(1) The CPS or the new policy shall be published no later than the next working day after its acceptance.

(2) Halcom CA ensures that the certificates are published in the central directory immediately (maximum 5 seconds) after their release.

(3) The list of revoked certificates shall be refreshed immediately (maximum 5 seconds) after the revoking of the certificate in Halcom CA's public register of revoked certificates. With a few minutes delay, the list of revoked certificates is also published to websites.

(4) Publicly available information or documents (except for the above) are published as needed.

2.4. Access controls on repositories

(1) The central directory is accessible on the server ldap.halcom.si, TCP port 389 by the LDAP protocol. Only the register of revoked certificates, which is part of the directory, is publicly available.

(2) With appropriate technical information security measures, Halcom CA provides controls that prevent unauthorized adding, changing or deleting data in the public directory of certificates.

3. IDENTIFICATION AND AUTHENTICATION

3.1. Naming

Distinguished names, contained in the certificate, unambiguously and uniquely identify the certificate subject unless otherwise required by either this CPS or with the content of the qualified digital certificate.

3.1.1 Types of names

(1) In accordance with IETF RFC 5280, each certificate contains information about the subject and the TSP in the form of a distinguished name. The distinguished name is designed in accordance with IETF RFC 5280 and X.501 standard.

(2) TSP is listed in the issued certificate in the field Issuer. The basic information of the subject contained in the distinguished name of the certificates for natural persons or legal persons are listed in the field Subject of the issued certificate.

(3) The serial number, which is also included in the distinguished name, is determined by the TSP Halcom CA (more in section 3.1.5).

(4) Under the eIDAS Regulation and ETSI standards, Halcom CA may, in the formation of the distinctive name of foreign natural persons and/or foreign business entities, also use other semantic identifiers of natural persons and business entities, such as "PNO", "IDC" or "PAS" and ISO 3161-1 country code for identification based on national identification number or passport or identity card number for natural persons and business entities "NTR" and ISO 3161-1 country code for identification based on identifier from the national trade register or local identifier (two characters according to the local definition within the specified country and name registration authority, identifying a national scheme that is considered appropriate for national and European level).

(5) For qualified certificates used to identify payment service providers, under Article 34 (1) of Commission Delegated Regulation (EU) 2018/389 amending Directive (EU) 2015/2366 as regards regulatory technical standards for strong customer authentication and common and secure open communication standards (RTS SCA), the following shall be used: semantic identifier "PSD" with ISO 3161-1 country code, the role of the payment service provider, the name of the competent authority (NCA) where the payment service provider is registered and the registration number of the payment service provider indicated in the official records of that authority.

(6) Trust service provider Halcom CA may add to the field Subject an attribute 1.3.6.1.4.1.5939.2.9 which indicates type of certificate (e.g. indicates what type of certificate was issued : cloud qualified digital certificate or qualified digital certificate issued on smart car/USB token).

- TSP Halcom CA Certificates:

Certificate type	Field name	Distinguished name
Root Certificate	Issuer and Subject	C= SI O= Halcom d.d. 2.5.4.97 = VATSI-43353126 CN= Halcom Root Certificate Authority
Intermediate/ subordinate certificate for legal persons	Issuer	C= SI O= Halcom d.d. 2.5.4.97 = VATSI-43353126 CN= Halcom Root Certificate Authority
	Subject	C= SI O= Halcom d.d. 2.5.4.97= VATSI-43353126 CN= Halcom CA PO e-signature 1 or CN= Halcom CA PO e-signature 2

Intermediate/ subordinate certificate for natural persons	Issuer	C= SI O= Halcom d.d. 2.5.4.97 = VATSI-43353126 CN= Halcom Root Certificate Authority
	Subject	C= SI O= Halcom d.d. 2.5.4.97= VATSI-43353126 CN= Halcom CA FO e-signature 1 or CN= Halcom CA FO e-signature 2
Intermediate/ subordinate certificate for electronic seals	Issuer	C= SI O= Halcom d.d. 2.5.4.97 = VATSI-43353126 CN= Halcom Root Certificate Authority
	Subject	C= SI O= Halcom d.d. 2.5.4.97= VATSI-43353126 CN= Halcom CA PO e-seal 1 or CN= Halcom CA PO e-seal 2
Intermediate/ subordinate certificate for website authentication	Issuer	C= SI O= Halcom d.d. 2.5.4.97 = VATSI-43353126 CN= Halcom Root Certificate Authority
	Subject	C= SI O= Halcom d.d. 2.5.4.97= VATSI-43353126 CN= Halcom CA web 1
Intermediate/ subordinate	Issuer	C= SI O= Halcom d.d. 2.5.4.97 = VATSI-43353126

certificate for time-stamping		CN= Halcom Root Certificate Authority
	Subject	C= SI O= Halcom d.d. 2.5.4.97= VATSI-43353126 CN= Halcom CA TSA 1

- End User Certificates

Certificate type	Field name	Distinguished name
Certificate for legal persons (e-signature)	Issuer	C= SI O= Halcom d.d. 2.5.4.97= VATSI-43353126 CN= Halcom CA PO e-signature 1 or CN= Halcom CA PO e-signature 2
	Subject	C= SI O= <name of legal person> 2.5.4.97=<VAT+2 character ISO country code-identifier> and/or 1.3.6.1.4.1.5939.2.3=<VAT number of legal person> CN=<name and surname> SN= <surname> G= <name> SERIALNUMBER=<TIN+2 character ISO country code-identifier> and/or 1.3.6.1.4.1.5939.2.2= <TIN number of natural person> E= <e-mail>
Certificate for natural persons (e-signature)	Issuer	C= SI O= Halcom d.d. 2.5.4.97= VATSI-43353126

		CN= Halcom CA FO e-signature 1 or CN= Halcom CA FO e-signature 2
	Subject	C= SI CN=<name and surname> SN= <surname> G= <name> SERIALNUMBER=<TIN+2 character ISO country code-identifier> and/or 1.3.6.1.4.1.5939.2.2=<TIN number of natural person> E= <email>
Certificate for electronic seals	Issuer	C= SI O= Halcom d.d. 2.5.4.97= VATSI-43353126 CN= Halcom CA PO e-seal 1 or CN= Halcom CA PO e-seal 2
	Subject	C= SI O= <name of legal person> 2.5.4.97=<VAT+2 character ISO country code-identifier> and/or 1.3.6.1.4.1.5939.2.3= <VAT number of legal person> CN=<name of the information system or department> E= <email>
Certificate for website authentication	Issuer	C= SI O= Halcom d.d. 2.5.4.97= VATSI-43353126 CN= Halcom CA web 1

	Subject	C= SI O= <name of legal person> 2.5.4.97=<VAT+2 character ISO country code-identifier> and/or 1.3.6.1.4.1.5939.2.3= <VAT number of legal person> OU= server or web certificates CN=<website name and domain> SN= <domain> G= <website name> E = <e-mail>
Certificate for time-stamping	Issuer	C= SI O= Halcom d.d. 2.5.4.97= VATSI-43353126 CN= Halcom CA TSA 1
	Subject	C= SI O= <name of legal person or trust service provider> 2.5.4.97=<VAT+2 character ISO country code-identifier> and/or 1.3.6.1.4.1.5939.2.3= <VAT number of legal person> CN=<name of the certificate or time-stamping service> E= <e-mail>

3.1.2 Need for names to be meaningful

(1) The designation of a natural or legal person that is included in the distinguishing name in accordance with the provisions of section 3.1.1 must meet the following requirements:

- it must be uniquely registered in a business or other official registry,
- it must be meaningfully connected with the natural or legal person,

- the maximum length can be forty-two (42) characters.

(2) In the case of certificate for website authentication, the website name must be a fully qualified domain name.

(3) Halcom CA reserves the right to reject the firm, name or brand of a legal person if it finds:

- that it is inappropriate or offensive,
- it is misleading to third parties or already belongs to another legal or natural person,
- that it is contrary to the applicable regulations.

3.1.3 Anonymity or pseudonymity of subscribers

The use of anonymous names or pseudonyms is not allowed.

3.1.4 Rules for interpreting various name forms

(1) The information of the subject certificate in the distinguished name shall contain the letters of the English alphabet and the remaining characters shall be converted as follows:

Character	Conversion
Č	C
Ć	C
Đ	DJ
Š	S
Ž	Z
Ü	UE
Ö	OE
Ø	OE
ß	SS
Ñ	N
Ŕ	RZ

(2) With the appropriate combination of letters, the TSP shall ensure the use of other unforeseen characters.

3.1.5 Uniqueness of names

Distinguished names are unique for each issued certificate and unambiguously and uniquely identify the subject in the directory structure.

3.1.6 Recognition, authentication, and role of trademarks

(1) Legal or natural persons may not claim the names of state bodies or local community bodies, names, designations, trademarks or other intellectual property elements that would belong to third parties and thereby infringe intellectual property rights or other rights of third parties or the provisions of applicable regulations.

(2) Possible disputes shall be solved exclusively by the affected party and the subject of the certificate.

(3) Responsibility concerning the use of names or of protected trademarks is exclusively on the side of the legal person. TSP Halcom CA is not obliged to check and/or warn the subject or the legal person.

3.2. Initial identity validation

The identity of future subject at the time of the first issue of the certificate is checked at the TSP's RA or directly at the TSP Halcom CA. Halcom CA checks the data of the future subject and legal person in the relevant registers prior to the issue of the certificate.

3.2.1 Method to prove possession of private key

Demonstration of having a private key belonging to the public key in the certificate is ensured by secure procedures before and at certificate acceptance and by the PKCS#10 standard.

3.2.2 Authentication of organization identity

(1) Information on a legal person is given by the distinguished name, see section 3.1.1 and 3.1.2.

2) The legal representative of a legal person with his signature guarantees for the accuracy of the data on documentation for obtaining a certificate.

(3) The TSP Halcom CA shall verify the correctness of the data of the legal person and the identity of the responsible person with the relevant services, official records or through official documentation.

(4) Halcom CA shall on the basis of request for a certificate for website authentication verify the ownership of the domain (indicated on the request) at the authorized domain registrar.

3.2.3 Authentication of individual identity

(1) Trust service provider Halcom CA's registration authority shall indisputably establish the identity of certificate holders in accordance with applicable regulations (official document with picture) or provide data on holders from its databases obtained using the procedure by the registration service used for another purpose, which provides for an equivalent assurance.

(2) The TSP Halcom CA shall verify the subject's personal information in the relevant registers unless otherwise specified by the applicable regulations.

3.2.4 Non-verified subscriber information

Halcom CA does not verify the accuracy and operation of subject's e-mail address.

3.2.5 Validation of authority

The legal representative of a legal person, by signing certificate application form, guarantees that he wishes to obtain a certificate for a legal person and/or a certain natural person who is employed or performs tasks for this legal person.

3.2.6 Criteria for interoperation

(1) The TSP Halcom CA is not obliged to contract or to guarantee for other trust service providers even if the other TSP has the status of a qualified TSP or a TSP of qualified digital certificates.

(2) The TSP Halcom CA ensures that mutual recognition is permitted only after signing a written contract with other TSPs, but only if they meet the level of security requirements that are comparable or higher than that prescribed by the TSP Halcom CA.

(3) If an external and independent assessment of the compliance of another TSP is not guaranteed, Halcom CA's authorized persons review the internal rules of another TSP and his compliance with security requirements.

(4) The cost of the necessary infrastructure required by TSP Halcom CA for mutual recognition is borne by another TSP.

3.3. Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

The identity of the subjects in the reissuing of the certificate shall be checked:

- at the RA of TSP Halcom CA
- based on the already issued valid digital certificate issued by the TSP, where the TSP Halcom CA checks the data of the legal person and/or natural person in the relevant registers.

3.3.2 Identification and authentication for re-key after revocation

Verification of subjects is in accordance with the provisions of section 3.2.3.

3.4. Identification and authentication for revocation request

(1) A request for certificate revocation shall be submitted by the legal person or by the subject:

- personally to the RA, where the authorized persons verify the identity of the applicant,
- electronically, but the revocation request must be digitally signed with a qualified certificate, thereby showing the identity of the applicant,
- if subject of the certificate requests submits the revocation of the certificate by telephone or e-mail, the TSP Halcom CA determines the suspension of the certificate. The actual revocation of the certificate is carried out on the basis of a written request for the certificate revocation.

(2) Detailed procedure for revocation: section 4.9.3.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1. Certificate Application

4.1.1 Who can submit a certificate application

(1) Future subject of certificates are natural persons, natural persons identified in association with a legal person or legal persons for their devices.

(2) To obtain a certificate, the following conditions must be met:

- completed and by the physical presence submitted certificate application form or contract at the RA,
- identification obligations,
- financial obligations.

(3) No certificate shall be issued to the prospective holder if the business entity or authorized individual is listed as a person against whom restrictive measures (sanctions) of the United Nations, the European Union, the Republic of Slovenia, the United Kingdom, Canada, Australia or the United States of America are applied.

4.1.2 Enrollment process and responsibilities

(1) Qualified certificates for natural persons in association with legal person:

1) The certificate shall be issued on the basis of a duly completed and signed certificate application form by the legal representative of the legal person and the future subject of the certificate. The legal representative submits the certificate application form to Halcom CA's RA and settles financial obligations related to the issue of the certificate. Certificate application forms can be obtained from Halcom CA RAs and from Halcom CA website. The service price list is publicly available on Halcom CA website.

2) By signing the certificate application form, the legal representative also authorizes the natural person in association with legal person (subject of a digital certificate) to validly sign, on behalf and for account of a legal person, an electronic certificate application form for renewal of existing digital certificate or issuing a new one with the same data in accordance with at the moment applicable policy and the price list of the TSP Halcom CA, but only on condition that a secure electronic signature can be validated.

3) The legal representative of the legal person shall submit the certificate application form in writing.

4) Before issuing the certificate application form, Halcom CA informs the legal person and the future subject with the policy and CPS of the TSP Halcom CA.

5) Before issuing the certificate application form, Halcom CA informs the future subject with the policy, the CPS and operation of the TSP Halcom CA.

(2) Qualified certificates for natural persons:

1) The certificate shall be issued on the basis of a duly completed and signed certificate application form by the future subject of the certificate (natural person). Natural person submits the certificate application form to the Halcom CA RA and settles the financial obligations related to the issue of the certificate. Certificate application forms can be obtained from Halcom CA RA and from Halcom CA website. The service price list is publicly available on Halcom CA website.

2) The future subject of the certificate shall submit the certificate application form in writing.

3) Before issuing a certificate application form, Halcom CA informs the future subject with the policy, CPS and the operation of the TSP Halcom CA.

(3) Qualified certificates for electronic seals:

1) The certificate is issued on the basis of a duly completed and signed certificate application form by the legal representative of the legal person. The legal representative submits the certificate application form to Halcom CA's RA and settles financial obligations related to the issue of the certificate. Certificate application forms can be obtained from Halcom CA RAs and from Halcom CA website. The service price list is publicly available on Halcom CA website.

2) By signing the certificate application form, the legal representative allows the electronic renewal of existing digital certificate or the issuance of a new one with the same data in accordance with at the moment applicable policy and price list of the TSP Halcom CA, but only on condition that the qualified electronic seal can be validated.

3) The legal representative of the legal person shall submit the certificate application form in writing.

4) Before issuing the certificate application form, Halcom CA informs the future subject with the CPS, the policy and the operation of the TSP Halcom CA.

(4) Qualified certificates for website authentication:

1) A certificate is issued on the basis of a duly completed and signed certificate application form by the website owner (natural person or legal representative of a legal person). Website owner submits the certificate application form to the Halcom CA RA and settles the financial obligations related to the issue of the certificate. Certificate application form can be obtained from Halcom CA RA and from Halcom CA website. The service price list is publicly available on Halcom CA website.

2) The website owner shall submit the certificate application form in writing.

3) Before issuing the certificate application form, Halcom CA informs the future subject with the policy, CPS and the operation of the TSP Halcom CA.

(5) Qualified certificates for time-stamping:

1) Certificates for time-stamping are intended only for TSPs.

2) The TSP Halcom CA is not obliged to contract with other TSP even if another TSP has the status of a qualified TSP.

3) The TSP Halcom CA ensures that the certificate will be issued exclusively after signing a written contract with another TSP, which must meet the level of security requirements that are comparable or higher than that prescribed by TSP Halcom CA.

4) If an external and independent assessment of the compliance of another TSP is not guaranteed, the authorized persons of Halcom CA shall review the internal rules of another TSP and its compliance with security requirements.

5) Before issuing the certificate application form, Halcom CA informs the future subject with the policy, CPS and the operation of the TSP Halcom CA.

(6) Halcom CA reserves the right to reject the certificate application form without a specific written explanation due to inadequate data, documentation or excessive security or legality.

4.2. Certificate application processing

4.2.1 Performing identification and authentication functions

(1) The authorized person of the RA shall verify the identity of the legal representative and/or the subject with a valid identity document with a picture when visiting the RA or through the courier service upon the delivery of the certificate.

(2) Trust service provider Halcom CA's registration authority may provide data on holders also from its databases obtained using the procedure by the registration authority used for another purpose, which provides for an equivalent assurance.

(3) The authorized persons are obliged to verify the identity of the legal person and/or the future subject or all the data that are listed in the certificate application form and are available in official records or other official valid documents.

(4) The RA shall check the completed certificate application forms and accept the original documentation and communicate them in a secure manner to Halcom CA.

4.2.2 Approval or rejection of certificate applications

(1) Authorized persons of the TSP Halcom CA approve the certificate application form or in case of incorrect or inaccurate data or failure to fulfil obligations refuse it, about what the legal person or the future subject is immediately informed personally or by e-mail.

(2) In the case of approval, Halcom CA shall notify the future subject, prior to the issue of the certificate, in accordance with the applicable regulations.

4.2.3 Time to process certificate applications

Based on previously approved certificate application form and settled financial obligations related to the issue of the certificate, Halcom CA shall issue the certificate no later than in five working (5) days from the receipt of payment.

4.3. Certificate issuance

4.3.1 TSP Halcom CA actions during certificate issuance

(1) The production process for the issue of a certificate depends on the type of certificate:

- Advanced Qualified Certificates

  The production process for certificates and for two key pairs consists of clearly separated parts (or functions), with their respective separate subsystems:

  1) pre-representation of a QSCD (generating keys on the card, setting a password to secure the certificate)
  2) obtaining a certificate application form,
  3) examination of the certificate application form,
  4) preparation of the certificate,
  5) creating a QSCD (issuing and storing a certificate, printing the subject's data)
  6) printing a personal password (PIN code – only if code is sent by registered mail),
  7) distribution of certificate and personal password (PIN code) and notifications to the subject.

  The advanced certificate on the QSCD and the associated personal password (PIN code) is sent to the subject by registered mail, in two separate deliveries, on two separate business days. Personal password (PIN code) can also be sent through another secure channel (through a secured website where the holder is identified via a special link received via e-mail and another known information to the holder (e.g. ID number, personal tax number, last four digits of CVV code of payment or credit card or similar). Exceptionally, the delivery may also be handed over to the subject by the authorized person of the Halcom CA RA in person.

- Qualified cloud certificates

  The production process for certificates and for one key pair consists of clearly separated parts (or functions), with their respective separate subsystems:

  1) examination of the certificate application form,
  2) preparation of the certificate and registration and activation code,
  3) the transmission of the registration and activation code and the notification to the subject,

4) generating keys on a secure cloud storage and issuing a certificate.

The registration and activation code are sent to the holder via two separate channels, registration code by e-mail, activation code through another secure channel (secured webside/portal where the holder is identified via a special link received by e-mail and another piece of known information to the holder (e.g. ID number, personal tax number, last four digits of CVV code of payment or credit card or similar).. In exceptional circumstances, one of the above codes may be handed over to the holder in person by an authorized person of the Halcom CA's registration authority.

- Standard Qualified Digital Certificate

  The production process for certificates and for one key pair consists of clearly separated parts (or functions), with their respective separate subsystems:

  1) examination of the certificate application form,
  2) preparation of the certificate and reference number and authorization code,
  3) the transmission of the reference and authorization code and the notification to the subject,
  4) enrolment of the certificate.

  The reference code is transmitted to the subject by e-mail, and the authorization code is distributed by registered mail. Exceptionally, the authorization code may be handed over to the subject by the authorized person of the Halcom CA RA in person.

- Qualified certificates for website authentication and information systems

  The production process for certificates and one key pair consists of clearly separated parts (or functions), with their respective separate subsystems:

  1) examination of the certificate application form,
  2) obtaining an electronic certificate request,
  3) personalization and issue of a certificate,
  4) transmission of the certificate to the subject.

- Qualified certificates for time-stamps

  The production process for certificates and one key pair consists of clearly separated parts (or functions), with their respective separate subsystems:

  1) an overview of the security requirements and internal rules of another TSP,
  2) examination and signing of the contract for the issue of a certificate,
  3) obtaining an electronic certificate request,

4) preparation of a certificate,

5) personalization of a certificate,

6) transmission of the certificate to TSP.

(2) The subscriber and the subject are not, as a rule, the same person as the Halcom CA or the Halcom CA RA. If the Halcom CA RA orders a certificate for itself or for its authorized employees, such certificate application form is additionally carefully checked by Halcom CA staff.

(3) If Halcom CA orders a certificate for itself or for its authorized persons, the issue of all such certificates is additionally carefully checked by the internal audit officer and the regulatory compliance officer.

(4) Procedures are designed in such a way that they cannot be performed by a single person by themselves.

(5) Trust service provider Halcom CA may based on a written contract authorize verified external contractors for certain tasks (e.g. printing the subject's data, printing PIN codes, distribution, etc.). Halcom CA shall regularly audit these subcontractors and guarantee for any tasks performed by them as performed by Halcom itself.

4.3.2 Notification to subscriber by the CA of issuance of certificate

See the previous section.

4.4. Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

(1) The procedure of certificate acceptance depends on the type of certificate:

- Advanced certificates

  In the case of advanced certificates, the acceptance of the certificate is not applicable, since the future subject receives the certificate on the QSCD and the associated personal password (PIN code) by registered post or through another secure channel It can exceptionally be handed over by an authorized Halcom CA in person, see section 4.3.1.

- Cloud certificates

  In the case of cloud-based certificates, a certificate is not required to be accepted, as it is safely stored by the Halcom CA trustee under the authorization of the subject. Only the codes for accessing a secure cloud certificate are transmitted to the subject, see section 4.3.1.

- Standard certificates

  In the case of standard certificates, the future subject, in accordance with instructions, enrols the certificate with the help of Halcom CA software for the certificate enrolment. Authorization code is distributed by registered mail to the future subject, see section 4.3.1.

- Certificates for the website authentication, information systems, and time-stamp

  For website authentication certificates, information systems, and time-stamp, the legal person locally triggers the generation of keys and sets the password to protect them. The TSP Halcom CA creates a certificate on the basis of the received certificate request and sends it to a legal person that creates a certificate with the associated key pair using the above-mentioned password.

(2) The subject of the certificate or the legal person must upon acceptance of the certificate immediately verify the information in the certificate and immediately notify the Halcom CA in case of possible errors or problems.

4.4.2 Publication of the certificate by the CA

The procedure is described in section 2.

4.4.3 Notification of certificate issuance by the CA to other entities

The TSP Halcom CA does not inform third parties of the issuance of an individual certificates. The RA may obtain information of issued certificates for which it has accepted the certificate application forms.

4.5. Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

(1) The subject or the future subject of the certificate shall be obliged:

- get acquainted and act in accordance with the policy before certificate issuing,
- to comply with the policy and other applicable regulations,
- after receiving the certificate or activating the certificate, verify the information in the certificate and in case of possible errors or problems immediately inform Halcom CA or request certificate revocation,
- monitor and comply with all notices of Halcom CA,
- according to the notices, update the necessary hardware and software for safe work with certificates,
- immediately notify Halcom CA of any changes that relate to the certificate,
- request revocation of the certificate if the private key has been compromised in a manner that affects the reliability of use or if there is a risk of abuse,
- request revocation of the certificate in the cloud at the loss or theft of the mobile device, or if there is a risk of abuse of it,
- use the certificate for the purpose specified in the certificate (see section 7.1.), and in the manner specified by Halcom CA policy.

(2) The subject or the future subject of the certificate shall also be obliged, as regards the protection of the private key, to:

- carefully protect the data for enrolment or activation of the certificate from unauthorized persons,
- keep a private key and certificate in the manner and on the devices for securely storing private keys in accordance with the notices and recommendations of Halcom CA,
- protect the private key and any other confidential information with an appropriate password in accordance with the recommendations of Halcom CA or protect it so that only the subject has access to them,
- carefully protect passwords for protection or access to a private key,
- operate in accordance with Halcom CA notices after expiration or revocation of the certificate.

4.5.2 Relying party public key and certificate usage

(1) A third party who relies on a certificate must:

- handle and use certificates in accordance with the policy and other applicable regulations,
- carefully examine all the risks and responsibilities involved in the use of certificates and determine the policy for how to use it,
- inform Halcom CA if it finds that the private keys of the subject of the certificate are compromised in a manner that affects the reliability of use or if there is a risk of abuse, or if the data specified in the certificate has changed,
- rely on the certificate only for the purpose specified in the certificate (see section 6.1.1) and in the manner specified by the policy,
- at the time of use of the certificate, check if the certificate is not in the register of revoked certificates,
- at the time of use of the certificate, validate that the digital signature/seal was created during the validity period and with the appropriate purpose of the certificate,
- at the time of use of the certificate, validate the signature of the TSP Halcom CA, which is published in this CPS and also on the Halcom CA website,
- comply with other provisions in case of additional agreement on the use of certificates with the Halcom TSP CA is concluded.

(2) To validate the validity of the signature/seal or other cryptographic operations third party must use software and hardware, which can credibly validate all of the above requirements for the safe use of certificates.

4.6. Certificate renewal

(1) Only the subject of the certificate can request the certificate renewal.

(2) After expiration of an advanced certificate, the subject shall, after a single (1x) renewal, re-apply for the new certificate.

(3) Prior to the expiration of the certificate, the certificate subject may apply electronically for the issue of a new digital certificate, which he electronically signs with a valid certificate.

(4) The process for renewal of time-stamping and websites authentication certificates is the same as the first acquisition of the certificate (see section 4.1).

4.6.1 Circumstance for certificate renewal

Prior to the expiration of the validity of the digital certificate, certificate subject shall ensure the continuity of the use of digital certificate by submitting an electronic renewal application form. However, the certificate application form for new certificate can also be submitted after the validity of the digital certificate expires.

4.6.2 Who may request renewal

Only the subject of the certificate can request the certificate renewal.

4.6.3 Processing certificate renewal requests

The procedure ensures that the legal person and/or the natural person applying for the renewal of the certificate is in fact the subject of the certificate and that the public key has not changed.

4.6.4 Notification of new certificate issuance to subscriber

See section 4.3.2.

4.6.5 Conduct constituting acceptance of a renewal certificate

See section 4.4.1.

4.6.6 Publication of the renewal certificate by the CA

The procedure is described in section 2.

4.6.7 Notification of certificate issuance by the CA to other

Halcom CA does not inform legal persons and other organizations about the issue of an individual certificates.

4.7. Certificate re-key

4.7.1 Circumstance for certificate re-key

Not supported.

4.7.2 Who may request certification of a new public key

Not supported.

4.7.3 Processing certificate re-keying requests

Not supported.

4.7.4 Notification of new certificate issuance to subscriber

Not supported.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

Not supported.

4.7.6 Publication of the re-keyed certificate by the CA

Not supported.

4.7.7 Notification of certificate issuance by the CA to other entities

Not supported.

4.8. Certificate modification

(1) In case information in the certificate or distinctive name has changed, the certificate must be revoked.

(2) In order to obtain a new certificate, it is necessary to repeat the procedure for obtaining a new certificate, as indicated in Section 4.1.

4.8.1 Circumstance for certificate modification

Not supported.

4.8.2 Who may request certificate modification

Not supported.

4.8.3 Processing certificate modification requests

Not supported.

4.8.4 Notification of new certificate issuance to subscriber

Not supported.

4.8.5 Conduct constituting acceptance of modified certificate

Not supported.

4.8.6 Publication of the modified certificate by the CA

Not supported.

4.8.7 Notification of certificate issuance by the CA to other entities

Not supported.

4.9. Certificate revocation and suspension

(1) The revocation of the certificate may be requested by the legal person or the subject of the certificate at any time but must be required in the case of:

1) changes in the distinguished name (DN),

2) when the legal person or subject of the certificate replaces the key information related to the certificate (name or surname, name of legal person, e-mail address, employment, etc.)

3) when it is established or suspected that either the disclosure of the key for signing or the misuse of the certificate occurred,

4) replacement of the certificate with another certificate (eg. when the certificate, QSCD or PIN for accessing QSCD is lost).

(2) Halcom CA may revoke the certificate even without the subject's request in the cases referred to in the first paragraph or on the request of the competent court, misdemeanour bodies or administrative units.

(3) The revocation of the certificate is possible 24 hours a day, every day of the year. Detailed instructions for revoking the certificate are published on the Halcom CA website.

(4) On the basis of the correct request for revocation, Halcom CA will revoke the certificate within four (4) hours at the latest. In case of occurrence of unforeseen circumstances, Halcom CA will exceptionally revoke the certificate no later than eight (8) hours after receipt of the correct request for revocation of the certificate. During this time, the revoked certificate will be marked as revoked and added to the registry of revoked certificates (CRL). If the subject of the certificate has submitted an incorrect request to revoke the certificate, Halcom CA will inform the subject about the incorrect request and instruct him/her to submit a correct revocation request.

4.9.1 Circumstances for revocation

(1) The revocation of the certificate must be requested by the legal person or the subject in the case of:

- if the private key of the certificate subject was compromised in a manner that affects the reliability of use,
- if there is a risk of abuse of the private key or the subject's certificate,
- if information in the certificate have changed or are incorrect.

(2) The TSP Halcom CA revokes the certificate even without the subject's request as soon as it becomes known:

- that the information in the certificate is incorrect or that the certificate was issued on the basis of incorrect information,
- that there was an error in verifying the identity of the data at the RA,

- that other circumstances affecting the validity of the certificate have changed,
- failure of the subject to comply with the obligations,
- that the financial obligations for digital certificates are not settled,
- that the infrastructure of a TSP has been compromised in a manner that affects the reliability of the certificate,
- the private key of the certificate subject has been compromised in a manner that affects the reliability of use,
- that Halcom CA will cease issuing certificates or that the TSP has been prohibited to manage certificates and its activities have not been taken over by another TSP,
- that the revocation has been ordered by the competent court, misdemeanour or administrative body.

(3) The subject of a digital certificate may require re-generating a personal password (PIN code) for advanced certificates thirty (30) days after issuing or reference number and authorization codes for standard certificates or registration and activation codes for the cloud certificate in case that he has forgotten e-access data and guarantees under civil and criminal responsibility there is a no possibility that the private key is/will be compromised in a manner that affects the reliability of use and that there is no risk of abuse of the private key or the subject's certificate.

4.9.2 Who can request revocation

Revocation of the certificate may be requested by:

- an authorized person of TSP Halcom CA,
- the legal representative of a legal person,
- subject,
- the competent court, misdemeanour or administrative body.

4.9.3 Procedure for revocation request

(1) Revocation may be requested by the legal representative of the legal person or the subject:

- personally during office hours at the RA,
- electronically twenty-four (24) hours per day, all days of the year, in the case of the possibility of misuse or unreliability of the certificate, otherwise at the official business time of the state authorities.

(2) If the revocation is requested:

- in person, it is necessary to complete the appropriate request for revocation of the certificate and submit it to the RA;
- electronically, the subject must send an electronic message to Halcom CA with a revocation

request, which must be digitally signed/sealed with a trusted certificate for its validation.

- if the subject requested certificate revocation through a telephone or e-mail, TSP Halcom CA will suspend the certificate. On the basis of a written request for the revocation of the certificate, actual revocation of certificate will be carried out.

(3) The legal person or the subject must always be informed of the date, time and the reasons of the revocation.

(4) Courts, misdemeanours and administrative bodies, who may also request revocation, do so in accordance with the laws and official proceedings (criminal proceedings, civil proceedings, general administrative procedure and others).

(5) The provisions relating to the revocation shall reasonably apply to procedures relating to the re-generating PIN codes for advanced certificates or reference number and authorization codes for standard certificates and registration and activation codes for certificates in the cloud.

4.9.4 Revocation request grace period

The revocation must be requested immediately if there is a possibility of abuse, unreliability or in similar urgent cases. In other cases, the revocation may be requested on the first working day within official office hours of the RA.

4.9.5 Time within which CA must process the revocation request

(1) The TSP Halcom CA upon acceptance of a valid revocation request:

- at the latest within four (4) hours, revokes the certificate if a revocation is submitted due to the risk of abuse or unreliability etc.,
- otherwise, the first working day after acceptance of the request for revocation.

(2) Upon revocation, such a certificate is immediately (maximum 5 seconds) added to the register of revoked certificates.

4.9.6 Revocation checking requirement for relying parties

Prior to use, third parties who rely on the certificate must check the latest published register of revoked certificates. For the sake of credibility and integrity, it is always necessary to check the credibility of this register, which is digitally signed by Halcom CA.

4.9.7 CRL issuance frequency

The register of revoked certificates is refreshed (for access to the registry, see section 7.2.3):

- after each certificate revocation,
- at least once a day, if there are no new records or changes in the register of revoked certificates, about twenty-four (24) hours after the last refresh.

4.9.8 Maximum latency for CRLs

(1) The publication of a new register of revoked certificates shall be performed:

- in the public directory on server ldap://ldap.halcom.si immediately (maximum 5 seconds),
- on the website http://domina.halcom.si/crls with a delay of no more than ten (10) minutes.

(2) The TSP Halcom CA ensures the maximum availability of its services, all days of the year, without taking into account unforeseen circumstances. In the event of unforeseen failures and unplanned technical or service interventions on the infrastructure, Halcom CA will publish a register of revoked certificates no later than in 8 (eight) hours. In the event of unforeseen circumstances arising as a result of force majeure or extraordinary events, Halcom CA will exceptionally publish a register of revoked certificates within 24 hours, but before the expiration of the last valid register of revoked certificates.

4.9.9 On-line revocation/status checking availability

On-line certificate status protocol (OCSP) is supported in accordance with European and international standards and recommendations (see section 7.3). On-line certificate status protocol (OCSP) may work with a delay of up to one (1) minute from the publication of the new registry.

4.9.10 On-line revocation checking requirements

Third parties must always check whether the certificate they rely on is revoked.

4.9.11 Other forms of revocation advertisements available

Not supported.

4.9.12 Special requirements re-key compromise

Not specified.

4.9.13 Circumstances for suspension

(1) If the certificate subject requests revocation by telephone or electronically, the certificate shall be temporarily suspended pending the receipt of the original written request.

(2) If the subject of the certificate, third party or other person, court, misdemeanour, administrative body, related authorities or the TSP himself, expresses the suspicion that the certificate is in contravention of the policy or the applicable regulations, the certificate shall be temporarily suspended until the final decision.

4.9.14 Who can requests suspension

See section 4.9.13.

4.9.15 Procedure for suspension request

See section 4.9.13.

4.9.16 Limits on suspension period

See section 4.9.13.

4.10. Certificate status services

4.10.1 Operational characteristics

(1) The register of revoked certificates is publicly posted on ldap://ldap.halcom.si/ server under the LDAP protocol and at http://domina.halcom.si/crls under the HTTP protocol.

(2) On-line certificate status protocol is available at http://ocsp.halcom.si.

(3) Details of issuing and access are in sections 7.2 in 7.3.

4.10.2 Service availability

(1) The validation of the status of certificates is constantly available 24 hours a day, every day of the year.

(2) The TSP Halcom CA ensures the maximum availability of its services, all days of the year, without taking into account unforeseen circumstances. In the event of unforeseen failures and unplanned technical or service interventions on the infrastructure, Halcom CA will re-enable validation of the certificate status no later than 8 (eight) hours. In case of occurrence of unforeseeable circumstances as a result of force majeure or extraordinary events, Halcom CA will exceptionally enable the validation of the status of certificates within 24 hours, but before the expiration of the last valid register of revoked certificates.

4.10.3 Optional features

Not prescribed.

4.11. End of subscription

Relationship between the subject or legal person and TSP shall be terminated if:

- the subject's certificate expires and he does not renew it,
- the certificate is revoked and the subject does not apply for a new one.

4.12. Key escrow and recovery

4.12.1 Key escrow and recovery policy and practices

Not supported.

4.12.2 Session key encapsulation and recovery policy and practices

Not supported.

4.12.3 Procedure for requesting a revealing of the copy of the decryption keys

Not supported.

5. MANAGEMENT, OPERATIONAL, AND PHYSICAL CONTROLS

(1) Halcom CA designs and implements all security measures in accordance with the family of

ISO/IEC 27000 standards and with FIPS 140-2 Level 3 and the ETSI technical requirements.

(2) Halcom CA equipment is installed in separate rooms and is protected by a multi-level system of physical and burglary technical protection. The equipment is protected against unauthorized access. It is also protected by a fire protection system, with the anti-spillage system, ventilation system, and multi-stage uninterruptible power supply.

(3) Halcom CA stores backup and distribution media in such a way that the loss, intrusion or unauthorized use or alteration of stored information is prevented to the greatest extent possible. Both for data recovery and for archiving important information, backups are provided and stored also in a different location than primary certificate management software, to ensure re-operation in cases of data loss on the primary location.

(4) A detailed description of the Halcom CA infrastructure, operations, infrastructure management procedures and the control of the security policy of its operation is determined by its internal rules.

5.1. Physical security controls

(1) The equipment of a TSP is protected by a multi-level system of physical and electronic security.

(2) The protection of the TSP's infrastructure shall be carried out in accordance with the recommendations of the highest level of protection.

(3) The complete description of TSP infrastructure, its management procedures and the protection is determined by the internal rules of the TSP.

5.1.1 Site location and construction

(1) The equipment of the TSP Halcom CA is located in special, secured, separate rooms.

(2) It is secured with a multi-level system of physical and electronic security.

(3) The detailed provisions are contained in the internal rules of the TSP Halcom CA.

5.1.2 Physical access

(1) Access to the TSP's infrastructure is only available to authorized persons of the TSP in accordance with their tasks and authorizations, see section 5.2.1.

(2) All accesses are protected in accordance with legislation and recommendations.

(3) The detailed provisions are contained in the internal rules of the TSP Halcom CA.

5.1.3 Power and air conditioning

(1) The infrastructure of a TSP shall have an uninterrupted power supply and appropriate air conditioning systems.

(2) The details are specified in the internal rules of the TSP Halcom CA.

5.1.4 Water exposures

(1) The infrastructure of a TSP is not exposed to the risk of flooding, except in case of force majeure.

(2) The details are specified in the internal rules of the TSP Halcom CA.

5.1.5 Fire prevention and protection

(1) The premises of the trust service provider shall be protected against any possible outbreak of a fire.

(2) The details are specified in the internal rules of TSP Halcom CA.

5.1.6 Media storage

(1) Data carriers, whether in paper or electronic form, shall be stored safely in protected installations.

(2) The backup copies of the Halcom CA software and encrypted databases are regularly updated and stored in two separate and physically protected areas at different locations.

5.1.7 Waste disposal

(1) Halcom CA ensures the safe disposal and destruction of documents in physical and electronic form.

(2) The disposal of waste shall be carried out by a special commission in accordance with the internal rules of the TSP Halcom CA.

(3) The details of this are specified in the internal rules of the trust provider of Halcom CA.

5.1.8 Off-site backup

See section 5.1.6.

5.2. Procedural controls

5.2.1 Trusted roles

(1) Operational, organizational and professional functioning of TSP Halcom CA is managed by an internal audit officer responsible for managing certificates.

(2) The authorized persons of TSP Halcom CA include:

- employees of Halcom CA and
- RAs.

(3) Employees of TSP Halcom CA are allocated to four organizational groups covering the following substantive areas:

- information system management,
- certificates management,
- security and control,
- regulatory.

Organizational group	Role	Basic tasks	Number of persons
Management of the information system	Head system administrator	• Preparing the initial system configuration • Initial setting of parameters for new subordinate TSPs • Set up of the initial network configuration • Preparation of data carriers for emergency restart of the system in case of catastrophic loss of the system • Secure storage and distribution of copies and upgrades to a separate location	2
	System administrator	• Procedures for issuing certificates management • Assistance to subordinate TSPs • Authorizing subordinate TSPs • Access the certificate signing protocol • Secure storage and distribution of copies and upgrades to a separate location	2
Certificates management	System operator 1	• Preparation of system copies, upgrading and restoring software, securely storing and distributing copies and upgrades remote location • Administrative functions related to maintaining the TSP database and help to research	2

		deviations from the rules • Changes to the name of the server and/or network address • Performing archiving of required system records • Printing PIN codes • Daily system overview	
	Authorization operator	• Confirmation of certificates and activation of passwords generation	2
	Certification operator	• Pre-personalization of QSCDs • Preparation of certificates (processing of signed certificates application forms) • Personalization (creation of certificates on a QSCD, subject's data on a QSCD) • Distribution of certificates	2
	Code operator	• Distribution of PIN codes	2
	Registration officer	• Identification of certificate subscribers/subjects	2
	Revocation officer	• Preparation of revocation requests • Revocation of certificates	2
Security and control	Security administrator	• Determining safety rules and monitoring their compliance • Reviewing system documentation and control logs for monitoring the work • Personal cooperation and assistance in the annual inventory of subordinate TSPs	2
	Internal audit officer	• Control of safety rules and	2

		their compliance • Monitoring system documentation and control logs for work control	
Regulatory	Regulatory compliance officer	• Independent directing, privacy protection and personal data protection • Ensuring compliance with applicable European and Slovenian regulations, international standards, and recommendations • Expert assistance to management and employees in the operational implementation of privacy and regulatory compliance measures	1

5.2.2 Number of persons required per task

(1) Operational work roles are designed to prevent the possibility of abuse as far as possible and are divided among individual, organizational groups:

Organizational group: Management of the information system

Role: head system administrator

Number of persons: 2

Tasks:

1. Preparing the initial system configuration
2. Initial setting of parameters for new subordinate TSPs
3. Set up of the initial network configuration
4. Preparation of data carriers for emergency restart of the system in case of catastrophic loss of the system
5. Secure storage and distribution of copies and upgrades to a separate location

Organizational group: Management of the information system

Role: system administrator

Number of persons: 2

Tasks:

1. Procedures for issuing certificates management
2. Assistance to subordinate TSPs
3. Authorizing subordinate TSPs
4. Access the certificate signing protocol
5. Secure storage and distribution of copies and upgrades to a separate location

Organizational group: Certificates management

Role: System operator 1

Number of persons: 2

Tasks:

1. Preparation of system copies, upgrading and restoring software, securely storing and distributing copies and upgrades to a remote location
2. Administrative functions related to maintaining the TSP database and help to research deviations from the rules
3. Changes to the name of the server and/or network address
4. Performing archiving of required system records
5. Printing PIN codes
6. Daily system overview

Organizational group: Certificates management

Role: Authorization operator

Number of persons: 2

Tasks:

1. Confirmation of certificates and activation of passwords

Organizational group: Certificates management

Role: Certification operator

Number of persons: 2

Tasks:

1. Pre-personalization of QSCDs
2. Preparation of certificates (processing of signed certificate application forms)
3. Personalization (creation of certificates on QSCD, printing subject's data on QSCD)
4. Distribution of certificates

Organizational group: Certificates management

Role: Code operator

Number of persons: 2

Tasks:

1. Distribution of PIN codes

Organizational group: Certificates management

Role: Registration officer

Number of persons: 2

Tasks:

1. Identification of certificate subscribers/subjects

Organizational group: Certificates management

Role: Revocation officer

Number of persons: 2

Tasks:

1. Preparation of revocation requests
2. Revocation of certificates

Organizational group: Security and control

Role: Security administrator

Number of persons: 2

Tasks:

1. Determining safety rules and monitoring their compliance
2. Reviewing system documentation and control logs for monitoring the work
3. Personal cooperation and assistance in the annual inventory of subordinate TSPs

Organizational group: Security and control

Role: Internal audit officer

Number of persons: 2

Tasks:

1. Control of safety rules and their compliance
2. Monitoring system documentation and control logs for work control

Organizational group: Regulatory

Role: Regulatory compliance officer

Number of persons: 1

Tasks:

1. Independent directing, privacy protection and personal data protection
2. Ensuring compliance with applicable European and Slovenian regulations, international standards, and recommendations
3. Expert assistance to management and employees in the operational implementation of privacy and regulatory compliance measures

(2) The minimum number of employees for each role is specified.

5.2.3 Identification and authentication for each role

Identification of the identity and access rights for the performance of individual tasks in accordance with the role of each organizational group as well as for the performance of the tasks of the RA is ensured by security mechanisms and control procedures in accordance with the internal rules of the TSP Halcom CA.

5.2.4 Roles requiring separation of duties

The internal rules of Halcom CA precisely specify which role may be/not be compatible with another. For some tasks, the presence of at least two authorized persons is required. In the event of an unforeseen absence of certain employees, their role is assumed by another employee, if this is not incompatible with the internal rules.

5.3. Personnel security controls

(1) The operational, organizational and professional functioning of the Halcom CA is led by an internal audit officer who does not perform tasks related to the management of certificates.

(2) The internal audit officer shall oversee the work of Halcom CA. In the event of detected deficiencies, the internal audit officer shall take appropriate measures to remedy these deficiencies. Halcom CA is obliged to implement the specified measures under supervision of internal audit officer.

5.3.1 Qualifications, experience, and clearance requirements

Halcom CA employs reliable and professionally qualified personnel who have not been prosecuted for any criminal offense. All staff is regularly trained and gain additional knowledge from their field of expertise.

5.3.2 Background check procedures

The staff of the trust services provider shall comply with the requirements of the applicable regulations and technical standards and recommendations of the appropriate qualifications and experience.

5.3.3 Training requirements

Persons who perform the tasks of the above organizational groups and the tasks of the RA are provided with all necessary training.

5.3.4 Retraining frequency and requirements

Staff is trained according to needs and/or updates regarding the operation of the TSP Halcom CA's infrastructure.

5.3.5 Job rotation frequency and sequence

Not prescribed.

5.3.6 Sanctions for unauthorized actions

Sanctions in case of unauthorized or negligent performance of tasks are performed for authorized persons by the TSP in accordance with the applicable rules and internal rules of the TSP Halcom CA.

5.3.7 Independent contractor requirements

Any potential independent contractors are subject to the same requirements as authorized persons of the TSP Halcom CA.

5.3.8 Documentation supplied to personnel

The authorized persons of the TSP are provided with all necessary documentation in accordance with their duties and tasks.

5.4. Audit logging procedures

5.4.1 Types of events recorded

(1) The TSP Halcom CA regularly checks and records everything that significantly affects:

- security of infrastructure,
- operation of all security systems and
- whether an intrusion or attempted of intrusion of unauthorized persons against equipment or data has occurred.

(2) Detailed information on this is determined in accordance with the Regulation and internal rules of the TSP Halcom CA.

5.4.2 Frequency of processing log

The TSP Halcom CA daily performs security checks of its infrastructure or logs.

5.4.3 Retention period for audit log

The audit logs are kept for at least ten (10) years after their occurrence unless a special law provides for a longer period.

5.4.4 Protection of audit log

(1) Audit logs are protected in accordance with security mechanisms that guarantee the highest level of security.

(2) The details are determined in the internal rules of the TSP in accordance with the Regulation.

5.4.5 Audit log backup procedures

(1) The backup copies of the audit logs are performed daily.

(2) The details are determined in the internal rules of the TSP in accordance with the Regulation.

5.4.6 Audit collection system

(1) Data are collected either automatically or manually, depending on the type of data.

(2) The details are determined in the internal rules of the TSP in accordance with the Regulation.

5.4.7 Notification to event-causing subject

It is not necessary to inform the event-causing subject.

5.4.8 Vulnerability assessments

(1) Log analysis and supervision of the execution of all procedures shall be carried out regularly by authorized persons of the TSP or automatically with other security mechanisms on all information and communication devices within the control of the TSP.

(2) The vulnerability assessment is conducted on the basis of log analysis, security events, and other relevant data.

(3) The details are determined in the internal rules of the TSP in accordance with the Regulation.

5.5. Records archival

5.5.1 Types of records archived

Halcom CA archives the following materials in accordance with the provisions of the applicable regulations:

- logs,
- records,
- all evidence of the completed identification of the subject and legal persons,
- all certificate application forms,
- certificates and certificate revocation list,
- policies,
- CPS,
- announcements and notifications from the TSP Halcom CA and
- other documents in accordance with the applicable regulations.

5.5.2 Retention period for archive

(1) Long-term stored data relating to keys and digital certificates shall be kept for at least ten (10) years after the expiration of the certificate to which the information relates if a special law does not provide for a longer period.

(2) Other long-term stored data shall be kept for at least ten (10) years after their occurrence, if a special law does not demand a longer period.

5.5.3 Protection of archive

(1) Long-term stored data is safely stored.

(2) Detailed arrangements are in accordance with the applicable regulations, standards and recommendations set out in the internal rules of TSP Halcom CA.

5.5.4 Archive backup procedures

(1) A copy of the long-term archive data is safely stored.

(2) Detailed arrangements are in accordance with the applicable regulations, standards and recommendations set out in the internal rules of TSP Halcom CA.

5.5.5 Requirements for time-stamping of records

Not prescribed.

5.5.6 Archive collection system

(1) Data shall be collected in a manner consistent with the type of document.

(2) Detailed arrangements are in accordance with the applicable regulations, standards and recommendations set out in the internal rules of TSP Halcom CA.

5.5.7 Procedures to obtain and verify archive information

(1) Access to long-term data is only available to authorized persons.

(2) Detailed arrangements are in accordance with the applicable regulations, standards and recommendations set out in the internal rules of TSP Halcom CA.

5.6. Key changeover of TSP Halcom CA

In the case of issued new certificate of the TSP Halcom CA, the process will be published on the TSP Halcom CA website.

5.7. Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

Detailed arrangements are in accordance with the applicable regulations, standards and recommendations set out in the internal rules of TSP Halcom CA.

5.7.2 Computing resources, software, and/or data are corrupted

Detailed arrangements are in accordance with the applicable regulations, standards and recommendations set out in the internal rules of TSP Halcom CA.

5.7.3 Entity private key compromise procedures

Detailed arrangements are in accordance with the applicable regulations, standards and recommendations set out in the internal rules of TSP Halcom CA.

5.7.4 Business continuity capabilities after a disaster

Detailed arrangements are in accordance with the applicable regulations, standards and recommendations set out in the internal rules of TSP Halcom CA.

5.8. Halcom CA or RA termination

Detailed arrangements are in accordance with the applicable regulations, standards and recommendations set out in the internal rules of TSP Halcom CA.

6. TECHNICAL SECURITY CONTROLS

6.1. Key pair generation and installation

6.1.1 Key pair generation

(1) TSP Halcom CA key pair for signing and validating signatures was created to the highest security standards in the safe environment of the TSP Halcom CA.

(2) The keys of the subjects shall be generated depending on the type of certificate in accordance with the table below.

Type of certificate	Key	Key generation
Root and intermediate certificates Halcom CA	Key pair	in the hardware security module of the TSP
Advanced certificate	Two key pairs	on a QSCD in the safe environment the TSP Halcom CA
Standard certificate	Key pair	on the subject's computer
Cloud certificate	Key pair	in the hardware security module of the TSP
Certificate for information systems	Key pair	in the safe environment of the certificate subject
Certificate for website authentication	Key pair	in the safe environment of the certificate subject
Certificate for the time-stamp	Key pair	in the hardware security module of the TSP

6.1.2 Private key delivery to subscriber

The private key delivery method is described in the table below.

Type of certificate	Key	Key generation

Root and intermediate certificates Halcom CA	Private key	no transfer
Advanced certificate	Private keys	delivery of QSCD with the registered mail
Standard certificate	Private key	no transfer
Cloud certificate	Private key	no transfer
Certificate for information systems	Private key	no transfer
Certificate for website authentication	Private key	no transfer
Certificate for the time-stamp	Private key	no transfer

6.1.3 Public key delivery to certificate issuer

(1) For Advanced Certificates, keys are generated on a QSCD in the secure environment of the TSP Halcom CA.

(2) For certificates in the cloud, the keys are generated in the hardware security module in the secure environment of the TSP Halcom CA.

(3) For certificates for information systems and website authentication, keys are generated by the subject. The PKCS#10 certificate request is then transferred from the subject's computer to the TSP via a secure network connection.

(4) For standard certificates, the keys are generated by the subject. PKCS#10 certificate request and a certificate is issued through the Halcom CA software for the acquisition of a digital certificate.

(5) For time-stamp certificates, keys are generated in the hardware security module by the TSP. The PKCS#10 certificate request is transferred to TSP via a secure network connection.

6.1.4 CA public key delivery to relying parties

The TSP Halcom CA public key certificate is delivered to the subject or accessible to relying parties:

- in the public directory ldap://ldap.halcom.si under the LDAP protocol (see section 2.3),
- in the PEM form at http://domina.halcom.si/crls, whereby the credibility of the certificate must be further validated.

6.1.5 Key sizes

Certificate	Key length according to RSA [bit]
Root certificate Halcom CA	At least 2048
Intermediate certificate Halcom CA	At least 2048

User certificates	At least 2048

6.1.6 Public key parameters generation and quality checking

The quality of TSP Halcom CA key parameters is provided by the software manufacturer, using quality random number generator.

6.1.7 Key usage purposes (as per X.509 v3 key usage field)

(1) The key usage purpose of certificates is in accordance with X.509 v.3 and specified in the certificate fields *keyUsage* and *extended keyUsage*.

(2) The TSP Halcom CA private key is intended for signing certificates and CRLs, and the public key in the certificate of the TSP is used to validate the validity of the signature.

(3) The certification profile is described in section 7.1.

6.2. Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

The private key of the TSP Halcom CA is protected in a hardware security module that is certified according to FIPS 140-2 level 3 and/or Common Criteria EAL4 +.

6.2.2 Private key (n out of m) multi-person control

In accordance with the applicable regulations and the CPS, the access to TSP Halcom CA's private key is specified in the internal rules of the TSP Halcom CA.

6.2.3 Private key escrow

In accordance with the applicable regulations and the CPS, the TSP Halcom CA's private key escrow is specified in the internal rules of the TSP Halcom CA.

6.2.4 Private key backup

In accordance with the applicable regulations and the CPS, the TSP Halcom CA's private key backup is specified in the internal rules of the TSP Halcom CA.

6.2.5 Private key archival

(1) Halcom CA private keys can be copied and stored only by authorized persons of the TSP Halcom CA. Backup keys are stored with the same level of protection as the keys in use.

(2) In accordance with the applicable regulations and the CPS, the TSP Halcom CA' s private key archival is specified in the internal rules of the TSP Halcom CA.

6.2.6 Private key transfer into or from a cryptographic module

(1) Private keys for advanced certificates shall be generated in a QSCD which is subsequently transferred to the subject of the certificate.

(2) The private keys for cloud certificates are generated and stored in a hardware security module that is certified according to FIPS 140-2 level 3 and/or Common Criteria EAL4 +

(3) Private keys of other certificates are created and stored by the subject.

6.2.7 Private key storage on cryptographic module

(1) The private key of the Halcom CA TSP is stored in a hardware security module that is certified according to FIPS 140-2 Level 3 and/or Common Criteria EAL4 +.

(2) Subject's private keys of:

- advanced certificates are created and stored on a QSCD,
- cloud certificates are created and stored in a hardware security module,
- standard certificates are created and stored by the subject,
- certificates for information systems are created and stored by the subject,
- certificates for website authentication are created and stored by the subject,
- time-stamp certificates are created and stored in the TSP' s hardware security module.

6.2.8 Method of activating private key

(1) Halcom CA's private key activation procedure is performed in a safe manner in accordance with the internal rules of the Halcom CA TSP.

(2) Halcom CA recommends to the subjects to use environment which, when logged out or after some time period, disables access to their private key without entering the appropriate password.

(3) The subject of a cloud certificate may use the qualified signature service in the cloud. In such a case, the subject or, on his behalf, other sender shall, in a secure manner, provide to the TSP Halcom CA the electronic document, which shall be by electronically signed. The subject of the certificate, then securely and in accordance with TSP's procedures (using PIN and mobile security procedures) approves a qualified electronic signature in the cloud. Based on the approval of the subject, TSP Halcom CA uses the subject's private key and electronically signs the document and delivers it to the subject or to another sender of the document.

(4) In order to protect the confidentiality of the electronic documents, the subject may explicitly request in writing that the TSP Halcom CA does not need an entire electronic document, as described in previous paragraph, but only the hash value of such a document. In such a case, Halcom CA delivers only electronic signature to the subject or other sender. TSP Halcom CA does not provide the verification of the calculated hash value or other security mechanisms for electronic document, therefore all responsibility is entirely on the subject's part.

6.2.9 Method of deactivating private key

The Halcom CA TSP private key deactivation process is performed in a safe manner in accordance with the internal rules of the Halcom CA TSP.

6.2.10 Method of destroying private key

(1) The procedure for destruction of the private key of Halcom CA TSP takes place in a safe manner in accordance with the internal rules of the Halcom CA TSP and the instructions of the manufacturer of the hardware security module. Private key is destroyed in a way that it cannot be restored.

(2) The destruction of private keys on the part of subjects is within the competence of the subjects. They must use appropriate applications to safely delete certificates.

(3) The private key of cloud certificate is automatically destroyed after the expiration of the certificate. Based on subject's written request a cloud certificate private key may be destroyed before the expiration date by authorized person of the Halcom CA. Private key is destroyed so that it cannot be restored.

6.2.11 Cryptographic Module Rating

The hardware security modules are in accordance with standards given in section 6.2.1.

6.3. Other aspects of key pair management

6.3.1 Public key archival

The Halcom CA TSP archives its public key and public keys of subjects, as specified in section 5.5.

6.3.2 Certificate operational periods and key pair usage periods

(1) Validity depends on the type of certificate.

Type of certificate	Key	Validity
Root certificate	Private key	20 years
	Public key	20 years
Intermediate (subordinate) certificate	Private key	10 years
	Public key	10 years
Advanced certificate	Private key	3 years
	Public key	3 years
Standard certificate	Private key	3 years
	Public key	3 years
Cloud certificate	Private key	1-3 years
	Public key	1-3 years
Certificate for information systems	Private key	3 years
	Public key	3 years
Certificate for website authentication	Private key	1-3 years

	Public key	1-3 years
Certificate for time-stamp	Private key	5 years
	Public key	5 years

(3) In specific cases, Halcom CA may also determine a different validity period for each certificate.

6.4. Activation data

6.4.1 Activation data generation and installation

(1) Advanced certificate

A personal identification number (PIN code) for using the advanced certificates and the PIN unlock key (PUK code) are generated in the secure environment of the TSP Halcom CA. PIN code must be changed by the subject before the first use of the certificate.

(2) Cloud certificate

The registration and activation code for the Cloud certificates are generated in the secure environment of the TSP Halcom CA. In the activation process, the subject sets his personal code (PIN code) to access the certificate in the cloud.

(3) Standard certificate, certificate for information systems and website authentication

Owners of standard certificates, information system certificates and website authentication themselves determine a password to protect access to their private keys. Halcom CA recommends the use of secure passwords:

- mixed use of upper and lower case letters, numbers and special characters,
- lengths of at least 8 characters,
- it is not recommended to use words that are written in dictionaries.

6.4.2 Activation data protection

(1) Advanced certificate

Personal password for using the advanced certificate (PIN code) and the unlock key (PUK code) to unlock a QSCD are created securely by the Halcom CA TSP. Halcom CA distributes both passwords to the certificate subject by post, through another secure channel or exceptionally hands it over in person. Halcom CA recommends that both passwords are kept in a safe place to which only the subject has access.

(2) Cloud certificate

The registration and activation code for the cloud certificate is created securely by the Halcom CA TSP. The registration and activation code is transmitted to the subject via two separate channels, one by e-mail, and the other by another secure channel (secure web portal accessible

with a qualified certificate, by registered mail or other similar secure channel). Exceptionally, one of the above codes may be handed over to the subject by the authorized person of the Halcom CA RA in person. Codes are intended only for activating access to a cloud certificate, during which the subject sets his personal code (PIN code).

(3) Standard certificate

The reference number and authorization code for the enrolment of a standard certificate is created securely by the Halcom CA TSP. In the process of receiving the certificate, the subject himself sets a password to protect access to his private keys. Halcom CA recommends that the password is not stored or it is stored in such way that only the subject has access to it.

(4) Certificate for information systems and website authentication

Subjects of certificates for information systems and website authentication themselves set a password to protect their private keys. Halcom CA recommends that the password for access to the private key is not stored or it is stored in such way that only the subject has access to it.

6.4.3 Other aspects of activation data

Not prescribed.

6.5. Computer security controls

6.5.1 Specific computer security technical requirements

Detailed arrangements are in accordance with the applicable regulations, standards and recommendations set out in the CPS and internal rules of Halcom CA TSP.

6.5.2 Computer security rating

Detailed arrangements are in accordance with the applicable regulations, standards and recommendations set out in the CPS and internal rules of Halcom CA TSP.

6.6. Life cycle technical controls

6.6.1 System development controls

Halcom CA uses software and hardware that is certified according to FIPS 140-2 Level 3 and/or Common Criteria EAL4 +.

6.6.2 Security management controls

Detailed arrangements are in accordance with the applicable regulations, standards and recommendations set out in the CPS and internal rules of Halcom CA TSP.

6.6.3 Life cycle security controls

The detailed technical requirements are specified in the internal rules of the Halcom CA TSP.

6.7. Network security controls

Detailed arrangements are in accordance with the applicable regulations, standards and recommendations set out in the CPS and internal rules of Halcom CA TSP.

6.8. Time-stamping

Not prescribed.

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1. Certificate profile

(1) In accordance with CPS and policies, Halcom CA issues:

- advanced certificates,
- cloud certificates,
- standard certificates,
- certificates for information systems,
- certificates for website authentication and
- time-stamp certificates.

(2) All certificates include information in accordance with the eIDAS Regulation for qualified certificates.

(3) The Halcom CA TSP's certificates follow the X.509 standard.

7.1.1 Version number(s)

All Halcom CA TSP's certificates follow the X.509 standard v. 3.

7.1.2 Certificate extensions

The data in the certificates are listed below.

(1) Root certificate profile - Halcom Root Certificate Authority

Field names	Value or meaning
Basic fields in the certificate	
Version	V3
Serial number	unique internal certificate number
Signature algorithm	Sha256RSA (OID 1.2.840.113549.1.1.11)

Issuer	CN = Halcom Root Certificate Authority 2.5.4.97 = VATSI-43353126 O = Halcom d.d. C = SI
Validity	Valid from: <10.6.2016 07:07:50 GMT > Valid to: <10.6.2036 07:07:50 GMT >
Subject	CN = Halcom Root Certificate Authority 2.5.4.97 = VATSI-43353126 O = Halcom d.d. C = SI
Subject Public Key Algorithm	rsaEncryption (OID 1.2.840.113549.1.1.1)
Public Key (... bits)	module, exponent, ...
Subject's public key that belongs to the corresponding pair of keys, encrypted with RSA algorithm (RSA Public Key)	key length 2048 bits
Extensions X.509v3	
Key Usage, OID 2.5.29.15	Certificate Signing, Off-line CRL Signing, CRL Signing
Subject Key Identifier, OID 2.5.29.14	42 ae a6 43 c7 98 28 b0
Basic Constraints, OID 2.5.29.19	Subject Type=CA Path Length Constraint=None
Additional identification (not part of the digital certificate)	
Certificate Fingerprint – SHA1	Certificate Fingerprint by SHA1

(2) Profile of intermediate certificates

- Halcom CA PO e-signature 1

Field names	Value or meaning
Basic fields in the certificate	
Version	V3

Serial Number	unique internal certificate number
Signature algorithm	Sha256RSA (1.2.840.113549.1.1.11)
Issuer	CN = Halcom Root Certificate Authority 2.5.4.97 = VATSI-43353126 O = Halcom d.d. C = SI
Validity	Valid from: <15.6.2016 10:34:13 GMT > Valid to: <15.6.2026 10:34:13 GMT >
Subject	CN = Halcom CA PO e-signature 1 2.5.4.97 = VATSI-43353126 O = Halcom d.d. C = SI
Subject Public Key Algorithm	rsaEncryption (OID 1.2.840.113549.1.1.1)
Public Key (... bits)	module, exponent, ...
Subject's public key that belongs to the corresponding pair of keys, encrypted with RSA algorithm (RSA Public Key)	key length 2048 bits
Extensions X.509v3	
CRL Distribution Points, OID 2.5.29.31	URL=ldap://ldap.halcom.si/cn=Halcom%20Root%20Certificate%20Authority,o=Halcom,c=SI?certificaterevocationlist;binary URL=http://domina.halcom.si/crls/halcom_root_certificate_authority.crl
Key Usage, OID 2.5.29.15	Certificate Signing, Off-line CRL Signing, CRL Signing
Authority Key Identifier, OID 2.5.29.35	KeyID=42 ae a6 43 c7 98 28 b0
Subject Key Identifier, OID 2.5.29.14	40 f6 95 20 9b 79 c2 09
Basic Constraints, OID 2.5.29.19	Subject Type=CA Path Length Constraint=None
Additional identification (not part of the digital certificate)	

Certificate Fingerprint – SHA1	Certificate Fingerprint by SHA1

- Halcom CA PO e-signature 2

Field names	Value or meaning
Basic fields in the certificate	
Version	V3
Serial Number	unique internal certificate number
Signature algorithm	Sha256RSA (1.2.840.113549.1.1.11)
Issuer	CN = Halcom Root Certificate Authority 2.5.4.97 = VATSI-43353126 O = Halcom d.d. C = SI
Validity	Valid from: <03.04.2023 07:00:00 GMT > Valid to: <03.04.2033 07:00:00 GMT >
Subject	CN = Halcom CA PO e-signature 2 2.5.4.97 = VATSI-43353126 O = Halcom d.d. C = SI
Subject Public Key Algorithm	rsaEncryption (OID 1.2.840.113549.1.1.1)
Public Key (... bits)	module, exponent, ...
Subject's public key that belongs to the corresponding pair of keys, encrypted with RSA algorithm (RSA Public Key)	key length 3072 bits
Extensions X.509v3	
CRL Distribution Points, OID 2.5.29.31	URL=ldap://ldap.halcom.si/cn=Halcom%20Root%20Certificate%20Authority,o=Halcom,c=SI?certificaterevocationlist;binary URL=http://domina.halcom.si/crls/halcom_root_certificate_authority.crl

Key Usage, OID 2.5.29.15	Certificate Signing, Off-line CRL Signing, CRL Signing
Authority Key Identifier, OID 2.5.29.35	KeyID=42 ae a6 43 c7 98 28 b0
Subject Key Identifier, OID 2.5.29.14	43 4d 32 75 16 03 c9 75
Basic Constraints, OID 2.5.29.19	Subject Type=CA Path Length Constraint=None
Additional identification (not part of the digital certificate)	
Certificate Fingerprint – SHA1	Certificate Fingerprint by SHA1

- Halcom CA FO e-signature 1

Field names	Value or meaning
Basic fields in the certificate	
Version	V3
Serial Number	unique internal certificate number
Signature algorithm	Sha256RSA (1.2.840.113549.1.1.11)
Issuer	CN = Halcom Root Certificate Authority 2.5.4.97 = VATSI-43353126 O = Halcom d.d. C = SI
Validity	Valid from: <15.6.2016 10:34:15 GMT > Valid to: <15.6.2026 10:34:15 GMT >
Subject	CN = Halcom CA FO e-signature 1 2.5.4.97 = VATSI-43353126 O = Halcom d.d. C = SI
Subject Public Key Algorithm	rsaEncryption (OID 1.2.840.113549.1.1.1)
Public Key (... bits)	module, exponent,...

Subject's public key that belongs to the corresponding pair of keys, encrypted with RSA algorithm (RSA Public Key)	key length 2048 bits
Extensions X.509v3	
CRL Distribution Points, OID 2.5.29.31	URI:ldap://ldap.halcom.si/cn=Halcom%20Root%20Certificate%20Authority,o=Halcom,c=SI?certificaterevocationlist;binary URL=http://domina.halcom.si/crls/halcom_root_certificate_authority.crl
Key Usage, OID 2.5.29.15	Certificate Signing, Off-line CRL Signing, CRL Signing
Authority Key Identifier, OID 2.5.29.35	KeyID=42 ae a6 43 c7 98 28 b0
Subject Key Identifier, OID 2.5.29.14	48 fb 3b 13 99 c3 4e ce
Basic Constraints, OID 2.5.29.19	Subject Type=CA Path Length Constraint=None
Additional identification (not part of the digital certificate)	
Certificate Fingerprint – SHA1	Certificate Fingerprint by SHA1

- Halcom CA FO e-signature 2

Field names	Value or meaning
Basic fields in the certificate	
Version	V3
Serial Number	unique internal certificate number
Signature algorithm	Sha256RSA (1.2.840.113549.1.1.11)
Issuer	CN = Halcom Root Certificate Authority 2.5.4.97 = VATSI-43353126 O = Halcom d.d. C = SI
Validity	Valid from: <03.04.2023 07:00:00 GMT > Valid to: <03.04.2033 07:00:00 GMT >

Subject	CN = Halcom CA FO e-signature 2 2.5.4.97 = VATSI-43353126 O = Halcom d.d. C = SI
Subject Public Key Algorithm	rsaEncryption (OID 1.2.840.113549.1.1.1)
Public Key (... bits)	module, exponent,...
Subject's public key that belongs to the corresponding pair of keys, encrypted with RSA algorithm (RSA Public Key)	key length 3072 bits
Extensions X.509v3	
CRL Distribution Points, OID 2.5.29.31	URI:ldap://ldap.halcom.si/cn=Halcom%20Root%20Certificate%20Authority,o=Halcom,c=SI?certificaterevocationlist;binary URL=http://domina.halcom.si/crls/halcom_root_certificate_authority.crl
Key Usage, OID 2.5.29.15	Certificate Signing, Off-line CRL Signing, CRL Signing
Authority Key Identifier, OID 2.5.29.35	KeyID=42 ae a6 43 c7 98 28 b0
Subject Key Identifier, OID 2.5.29.14	48 c4 27 a6 6f 6e f0 2e
Basic Constraints, OID 2.5.29.19	Subject Type=CA Path Length Constraint=None
Additional identification (not part of the digital certificate)	
Certificate Fingerprint – SHA1	Certificate Fingerprint by SHA1

- Halcom CA PO e-seal 1

Field names	Value or meaning
Basic fields in the certificate	
Version	V3
Serial Number	unique internal certificate number
Signature algorithm	Sha256RSA (1.2.840.113549.1.1.11)

Issuer	CN = Halcom Root Certificate Authority 2.5.4.97 = VATSI-43353126 O = Halcom d.d. C = SI
Validity	Valid from: <22.4.2017 08:00:00 GMT > Valid to: <22.4.2027 08:00:00 GMT >
Subject	CN = Halcom CA PO e-seal 1 2.5.4.97 = VATSI-43353126 O = Halcom d.d. C = SI
Subject Public Key Algorithm	rsaEncryption (OID 1.2.840.113549.1.1.1)
Public Key (... bits)	module, exponent,...
Subject's public key that belongs to the corresponding pair of keys, encrypted with RSA algorithm (RSA Public Key)	key length 2048 bits
Extensions X.509v3	
CRL Distribution Points, OID 2.5.29.31	URL=ldap://ldap.halcom.si/cn=Halcom%20Root%20Certificate%20Authority,o=Halcom,c=SI?certificaterevocationlist;binary URL=http://domina.halcom.si/crls/halcom_root_certificate_authority.crl
Key Usage, OID 2.5.29.15	Certificate Signing, Off-line CRL Signing, CRL Signing
Authority Key Identifier, OID 2.5.29.35	KeyID=42 ae a6 43 c7 98 28 b0
Subject Key Identifier, OID 2.5.29.14	49 48 76 50 77 0a b1 0c
Basic Constraints, OID 2.5.29.19	Subject Type=CA Path Length Constraint=None
Additional identification (not part of the digital certificate)	
Certificate Fingerprint – SHA1	Certificate Fingerprint by SHA1

- Halcom CA PO e-seal 2

Field names	Value or meaning
Basic fields in the certificate	
Version	V3
Serial Number	unique internal certificate number
Signature algorithm	Sha256RSA (1.2.840.113549.1.1.11)
Issuer	CN = Halcom Root Certificate Authority 2.5.4.97 = VATSI-43353126 O = Halcom d.d. C = SI
Validity	Valid from: <03.04.2023 07:00:00 GMT > Valid to: <03.04.2033 07:00:00 GMT >
Subject	CN = Halcom CA PO e-seal 2 2.5.4.97 = VATSI-43353126 O = Halcom d.d. C = SI
Subject Public Key Algorithm	rsaEncryption (OID 1.2.840.113549.1.1.1)
Public Key (... bits)	module, exponent,...
Subject's public key that belongs to the corresponding pair of keys, encrypted with RSA algorithm (RSA Public Key)	key length 3072 bits
Extensions X.509v3	
CRL Distribution Points, OID 2.5.29.31	URL=ldap://ldap.halcom.si/cn=Halcom%20Root%20Certificate%20Authority,o=Halcom,c=SI?certificaterevocationlist;binary URL=http://domina.halcom.si/crls/halcom_root_certificate_authority.crl
Key Usage, OID 2.5.29.15	Certificate Signing, Off-line CRL Signing, CRL Signing
Authority Key Identifier, OID 2.5.29.35	KeyID=42 ae a6 43 c7 98 28 b0
Subject Key Identifier, OID 2.5.29.14	47 35 c8 bc 61 e2 5d 9e

Basic Constraints, OID 2.5.29.19	Subject Type=CA Path Length Constraint=None
Additional identification (not part of the digital certificate)	
Certificate Fingerprint – SHA1	Certificate Fingerprint by SHA1

- Halcom CA web 1

Field names	Value or meaning
Basic fields in the certificate	
Version	V3
Serial Number	unique internal certificate number
Signature algorithm	Sha256RSA (1.2.840.113549.1.1.11)
Issuer	CN = Halcom Root Certificate Authority 2.5.4.97 = VATSI-43353126 O = Halcom d.d. C = SI
Validity	Valid from: <22.4.2017 08:00:00 GMT > Valid to: <22.4.2027 08:00:00 GMT >
Subject	CN = Halcom CA web 1 2.5.4.97 = VATSI-43353126 O = Halcom d.d. C = SI
Subject Public Key Algorithm	rsaEncryption (OID 1.2.840.113549.1.1.1)
Public Key (... bits)	module, exponent,...
Subject's public key that belongs to the corresponding pair of keys, encrypted with RSA algorithm (RSA Public Key)	key length 2048 bits
Extensions X.509v3	
CRL Distribution Points, OID 2.5.29.31	URL=ldap://ldap.halcom.si/cn=Halcom%20Root%20Certificate%20Authority,o=Halcom,c=SI?certificaterevocationlist;binary URL=http://domina.halcom.si/crls/halcom_root_certificate_authority.crl

Key Usage, OID 2.5.29.15	Certificate Signing, Off-line CRL Signing, CRL Signing
Authority Key Identifier, OID 2.5.29.35	KeyID= 42 ae a6 43 c7 98 28 b0
Subject Key Identifier, OID 2.5.29.14	48 42 0b 17 ed ae 9e 70
Basic Constraints, OID 2.5.29.19	Subject Type=CA Path Length Constraint=None
Additional identification (not part of the digital certificate)	
Certificate Fingerprint – SHA1	Certificate Fingerprint by SHA1

- Halcom CA TSA 1

Field names	Value or meaning
Basic fields in the certificate	
Version	V3
Serial Number	unique internal certificate number
Signature algorithm	Sha256RSA (1.2.840.113549.1.1.11)
Issuer	CN = Halcom Root Certificate Authority 2.5.4.97 = VATSI-43353126 O = Halcom d.d. C = SI
Validity	Valid from: <22.4.2017 08:00:00 GMT > Valid to: <22.4.2027 08:00:00 GMT >
Subject	CN = Halcom CA TSA 1 2.5.4.97 = VATSI-43353126 O = Halcom d.d. C = SI
Subject Public Key Algorithm	rsaEncryption (OID 1.2.840.113549.1.1.1)
Public Key (... bits)	module, exponent,...

Subject's public key that belongs to the corresponding pair of keys, encrypted with RSA algorithm (RSA Public Key)	key length 2048 bits
Extensions X.509v3	
CRL Distribution Points, OID 2.5.29.31	URL=ldap://ldap.halcom.si/cn=Halcom%20Root%20Certificate%20Authority,o=Halcom,c=SI?certificaterevocationlist;binary URL=http://domina.halcom.si/crls/halcom_root_certificate_authority.crl
Key Usage, OID 2.5.29.15	Certificate Signing, Off-line CRL Signing, CRL Signing
Authority Key Identifier, OID 2.5.29.35	KeyID=42 ae a6 43 c7 98 28 b0
Subject Key Identifier, OID 2.5.29.14	43 8f 8b 56 9f 44 1e d7
Basic Constraints, OID 2.5.29.19	Subject Type=CA Path Length Constraint=None
Additional identification (not part of the digital certificate)	
Certificate Fingerprint – SHA1	Certificate Fingerprint by SHA1

(3) End user certificate profile

- Halcom CA PO e-signature 1 and Halcom CA PO e-signature 2

Field names	Value or meaning
Basic fields in the certificate	
Version	V3
Serial Number	unique internal certificate number
Signature algorithm	Sha256RSA (OID 1.2.840.113549.1.1.11)
Issuer	CN = Halcom CA PO e-signature 1 or CN = Halcom CA PO e-signature 2 2.5.4.97 = VATSI-43353126 O = Halcom d.d. C = SI

Validity	Valid from: <start of validity by GMT> Valid to: <end of validity by GMT>
Subject	distinguished name of the subject, see section 3.1.1.
Subject Public Key Algorithm	rsaEncryption (OID 1.2.840.113549.1.1.1)
Public Key (... bits)	module, exponent,...
Subject's public key that belongs to the corresponding pair of keys, encrypted with RSA algorithm (RSA Public Key)	key length is min. 2048 bits, see section 6.1.5.
Extensions X.509v3	
CRL Distribution Points, OID 2.5.29.31	URI:ldap://ldap.halcom.si/cn=Halcom%20CA%20PO%20e-signature%201,o=Halcom,c=SI?certificaterevocationlist;binary URL=http://domina.halcom.si/crls/halcom_ca_po_ e-signature_1.crl Or URI:ldap://ldap.halcom.si/cn=Halcom%20CA%20PO%20e-signature%202,o=Halcom,c=SI?certificaterevocationlist;binary URL=http://domina.halcom.si/crls/halcom_ca_po_ e-signature_2.crl
Key Usage , OID 2.5.29.15,	Advanced certificates: Digital Signature, Non Repudiation, Key Encipherment Cloud certificates: Digital Signature, Non Repudiation
Authority Key Identifier, OID 2.5.29.35	KeyID=40 f6 95 20 9b 79 c2 09 or KeyID= 43 4d 32 75 16 03 c9 75
UNEI	Unified number of electronic identification (see section 7.1.2.1)

- Halcom CA FO e-signature 1 and Halcom CA FO e-signature 2

Field names	Value or meaning

Basic fields in the certificate	
Version	V3
Serial Number	unique internal certificate number
Signature algorithm	Sha256RSA (OID 1.2.840.113549.1.1.11)
Issuer	CN = Halcom CA FO e-signature 1 or CN = Halcom CA FO e-signature 2 2.5.4.97 = VATSI-43353126 O = Halcom d.d. C = SI
Validity	Valid from: <start of validity by GMT> Valid to: <end of validity by GMT>
Subject	distinguished name of the subject, see section 3.1.1.
Subject Public Key Algorithm	rsaEncryption (OID 1.2.840.113549.1.1.1)
Public Key (... bits)	module, exponent,...
Subject's public key that belongs to the corresponding pair of keys, encrypted with RSA algorithm (RSA Public Key)	key length is min. 2048 bits, see section 6.1.5.
Extensions X.509v3	
CRL Distribution Points, OID 2.5.29.31	URI:ldap://ldap.halcom.si/cn=Halcom%20CA%20FO%20e-signature%201,o=Halcom,c=SI?certificaterevocationlist;binary URL=http://domina.halcom.si/crls/halcom_ca_fo_e-signature_1.crl or URI:ldap://ldap.halcom.si/cn=Halcom%20CA%20FO%20e-signature%202,o=Halcom,c=SI?certificaterevocationlist;binary URL=http://domina.halcom.si/crls/halcom_ca_fo_e-signature_2.crl

Key Usage, OID 2.5.29.15	Advanced certificates: Digital Signature, Non Repudiation, Key Encipherment Standard certificates: Digital Signature, Non Repudiation, Key Encipherment Cloud certificates: Digital Signature, Non Repudiation
Authority Key Identifier, OID 2.5.29.35	KeyID=48 fb 3b 13 99 c3 4e ce Or KeyID= 48 c4 27 a6 6f 6e f0 2e
UNEI	Unified number of electronic identification (see section 7.1.2.1)

- Halcom CA PO e-seal 1 and Halcom CA PO e-seal 2

Field names	Value or meaning
Basic fields in the certificate	
Version	V3
Serial Number	unique internal certificate number
Signature algorithm	Sha256RSA (OID 1.2.840.113549.1.1.11)
Issuer	CN = Halcom CA PO e-seal 1 or CN = Halcom CA PO e-seal 2 2.5.4.97 = VATSI-43353126 O = Halcom d.d. C = SI
Validity	Valid from: <start of validity by GMT> Valid to: <end of validity by GMT>
Subject	distinguished name of the subject, see section 3.1.1.
Subject Public Key Algorithm	rsaEncryption (OID 1.2.840.113549.1.1.1)
Public Key (... bits)	module, exponent,...
Subject's public key that belongs to the corresponding pair of keys, encrypted with RSA algorithm (RSA Public Key)	key length is min. 2048 bits, see section. 6.1.5.

Extensions X.509v3	
CRL Distribution Points, OID 2.5.29.31	URI:ldap://ldap.halcom.si/cn=Halcom%20CA%20PO%20e-seal%201,o=Halcom,c=SI?certificaterevocationlist;binary URL=http://domina.halcom.si/crls/halcom_ca_po_ e-seal_1.crl Or URI:ldap://ldap.halcom.si/cn=Halcom%20CA%20PO%20e-seal%202,o=Halcom,c=SI?certificaterevocationlist;binary URL=http://domina.halcom.si/crls/halcom_ca_po_ e-seal_2.crl
Key Usage, OID 2.5.29.15	Digital Signature, Non Repudiation, Key Encipherment
Authority Key Identifier, OID 2.5.29.35	KeyID= 49 48 76 50 77 0a b1 0c Or KeyID= 47 35 c8 bc 61 e2 5d 9e
UNEI	Unified number of electronic identification (see section 7.1.2.1)

- Halcom CA web 1

Field names	Value or meaning
Basic fields in the certificate	
Version	V3
Serial Number	unique internal certificate number
Signature algorithm	Sha256RSA (OID 1.2.840.113549.1.1.11)
Issuer	CN = Halcom CA web 1 2.5.4.97 = VATSI-43353126 O = Halcom d.d. C = SI

Validity	Valid from: <start of validity by GMT> Valid to: <end of validity by GMT>
Subject	distinguished name of the subject, see section 3.1.1.
Subject Public Key Algorithm	rsaEncryption (OID 1.2.840.113549.1.1.1)
Public Key (... bits)	module, exponent,...
Subject's public key that belongs to the corresponding pair of keys, encrypted with RSA algorithm (RSA Public Key)	key length is min. 2048 bits, see section 6.1.5.
Extensions X.509v3	
CRL Distribution Points, OID 2.5.29.31	URI:ldap://ldap.halcom.si/cn=Halcom%20CA%20web%201,o=Halcom,c=SI?certificaterevocationlist;binary URL=http://domina.halcom.si/crls/halcom_ca_web_1.crl
Key Usage, OID 2.5.29.15	Digital Signature, Key Encipherment
Authority Key Identifier, OID 2.5.29.35	KeyID= 48 42 0b 17 ed ae 9e 70
UNEI	Unified number of electronic identification (see section 7.1.2.1)

- Halcom CA TSA 1

Field names	Value or meaning
Basic fields in the certificate	
Version	V3
Serial Number	unique internal certificate number
Signature algorithm	Sha256RSA (OID 1.2.840.113549.1.1.11)
Issuer	CN = Halcom CA TSA 1 2.5.4.97 = VATSI-43353126 O = Halcom d.d. C = SI

Validity	Valid from: <start of validity by GMT> Valid to: <end of validity by GMT>
Subject	distinguished name of the subject, see section 3.1.1.
Subject Public Key Algorithm	rsaEncryption (OID 1.2.840.113549.1.1.1)
Public Key (... bits)	module, exponent,...
Subject's public key that belongs to the corresponding pair of keys, encrypted with RSA algorithm (RSA Public Key)	key length is min. 2048 bits, see section 6.1.5.
Extensions X.509v3	
CRL Distribution Points, OID 2.5.29.31	URI:ldap://ldap.halcom.si/cn=Halcom%20CA%20TSA%201,o=Halcom,c=SI?certificaterevocationlist;binary URL=http://domina.halcom.si/crls/halcom_ca_tsa_1.crl
Key Usage, OID 2.5.29.15	Digital Signature, Key Encipherment
Authority Key Identifier, OID 2.5.29.35	KeyID=43 8f 8b 56 9f 44 1e d7

(4) Key usage field is marked as critical.

(5) The subject of a certificate for electronic signing may have one valid certificate of the same type, except for sixty (60) days prior to the expiration of this certificate, when the subject can obtain a new certificate.

(6) The subject of a certificate for electronic sealing, information systems, website authentication and a time-stamp may have several valid certificates.

7.1.2.1 Unified number of electronic identification

In accordance with Article 24 of Electronic Identification and Trust Services Act (ZEISZ), Article 52 of the Decree on the determination of means of electronic identification and the use of a central service for online registration and electronic signature, the holder's Unified Number of Electronic Identification (EŠEI) is written into a qualified certificate for electronic signature, electronic seal or website authentication as a private extension of the qualified certificate. For this, an independent extension field written as ASN.1 notation is used:

SEQUENCE:
OBJECT_IDENTIFIER : '1.3.6.1.4.1.58536.1.1.1.1.1' <OID extension for EŠEI value of natural person>
OCTET_STRING :
IA5String : 'xxxxxxxxxxxx' <value>

SEQUENCE:
OBJECT_IDENTIFIER : '1.3.6.1.4.1.58536.1.1.1.1.2' <OID extension for EŠEI value of legal person>
OCTET_STRING :
IA5String : 'xxxxxxxxxxxx' <value>

7.1.2.2 Requirements for e-mail address

(1) Halcom CA reserves the right to reject a request for a certificate if it finds that the e-mail address is:

- inappropriate or offensive,
- it is misleading for relying parties,
- contrary to the applicable regulations and standards.

(2) No other restrictions on the electronic address are prescribed.

7.1.3 Algorithm object identifiers

(1) Certificates issued by Halcom CA are signed by the TSP using the algorithm specified in the signature algorithm field: the value "sha256RSA, identification code: OID 1.2.840.113549.1.1.11.

(2) A complete set of algorithms, data formats and protocols is available from authorized persons of the TSP Halcom CA.

7.1.4 Name forms

See section 3.1.1.

7.1.5 Name constraints

Name constraints are not prescribed.

7.1.6 Certificate policy object identifier

See section 7.1.2.

7.1.7 Usage of Policy Constraints extension

Usage of policy constraints extension is not prescribed.

7.1.8 Policy qualifiers syntax and semantics

Certificates issued by the Halcom CA TSP use the specific policyQualifiers information that is in accordance with the IETF RFC and ETSI standards.

7.1.9 Processing semantics for the critical Certificate Policies extension

Not supported.

7.2. CRL profile

(1) Registers of revoked Halcom CA certificates (CRL) are located in branches:

- CRL for intermediate/subordinate certificates:

  CN= Halcom Root Certificate Authority

  O = Halcom

  C = SI
- CRL for e-signature certificates for legal persons:

  CN= Halcom CA PO e-signature 1 or CN= Halcom CA PO e-signature 2

  O = Halcom

  C = SI
- CRL for e-signature certificates for natural persons:

  CN= Halcom CA FO e-signature 1 or CN= Halcom CA FO e-signature 2

  O = Halcom

  C = SI
- CRL for e-seal certificates for legal persons:

  CN= Halcom CA PO e-seal 1 or CN= Halcom CA PO e-seal 2

  O = Halcom

  C = SI
- CRL for website authentication certificates:

  CN= Halcom CA web 1

  O = Halcom

  C = SI
- CRL for time-stamping certificates:

  CN= Halcom CA TSA 1

  O = Halcom

  C = SI

(2) The register of revoked intermediate/subordinate certificates shall be updated at least once a year, while other CRLs shall be updated after each revocation of the certificate or at least once a day, in the absence of new records or changes in CRLs (24 hours after the last refresh).

(3) The CRLs shall contain the unique serial number of the revoked certificate and the time and date of the revocation.

7.2.1 Version number(s)

(1) The CRLs corresponds to the ITU-T Recommendation for X.509 (2005) and ISO / IEC 9594-8: 2014.

(2) CRLs are permanently accessible in the public directory of certificates (see Section 2.3):

- by LDAP protocol and

- by HTTP protocol.

7.2.2 CRL and CRL entry extensions

(1) The CRL, in addition to other data in accordance with recommendation X.509, contains (the basic fields and extensions are detailed in the table below):

- serial numbers of revoked certificates and
- time and date of revocation.

(2) Root CRL (CRL of intermediate certificates)

Field name	Value or meaning
Basic fields in CRL	
Version	V2
Signature Algorithm	Sha256RSA
Signature	Halcom CA signature
Distinguished name of the TSP (Issuer)	CN = Halcom Root Certificate Authority 2.5.4.97 = VATSI-43353126 O = Halcom d.d. C = SI
Time of issue of CRL (thisUpdate)	Effective date: <time of issue by GMT>
Time of issue of next CRL (nextUpdate)	Next Update: < time of next issue by GMT>
Identification of revoked certificates and time of revocation (revokedCertificate)	Serial Number: <identification number of revoked digital certificate > Revocation Date: <time of revocation by GMT>
Extensions X.509v2 CRL	
CRL list number	Serial number of CRL list
Authority Key Identifier (OID 2.5.29.35)	KeyID=42 ae a6 43 c7 98 28 b0
issuerAltName (OID 2.5.28.18)	not applicable
deltaCRLindicator (OID 2.5.29.27)	not applicable
issuingDistribuitionPoint (OID 2.5.29.28)	not applicable

(3) Intermediate CRLs

- Halcom CA PO e-signature 1 or Halcom CA PO e-signature 2

Field name	Value or meaning
Basic fields in CRL	
Version	V2
Signature Algorithm	Sha256RSA
Signature	Halcom CA signature
Distinguished name of the TSP (Issuer)	CN = Halcom CA PO e-signature 1 or CN = Halcom CA PO e-signature 2 2.5.4.97 = VATSI-43353126 O = Halcom d.d. C = SI
Time of issue of CRL (thisUpdate)	Effective date: < time of issue by GMT>
Time of issue of next CRL (nextUpdate)	Next Update: < time of next issue by GMT>
Identification of revoked certificates and time of revocation (revokedCertificate)	Serial Number: <identification number of revoked digital certificate> Revocation Date: <time of revocation by GMT>
Extensions X.509v2 CRL	
CRL list number	Serial number of CRL list
Authority Key Identifier (OID 2.5.29.35)	KeyID= 40 f6 95 20 9b 79 c2 09 or KeyID= 43 4d 32 75 16 03 c9 75
issuerAltName (OID 2.5.28.18)	not applicable
deltaCRLindicator (OID 2.5.29.27)	not applicable
issuingDistribuitionPoint (OID 2.5.29.28)	not applicable

- Halcom CA FO e-signature 1 or Halcom CA FO e-signature 2

Field name	Value or meaning

Basic fields in CRL	
Version	V2
Signature Algorithm	Sha256RSA
Signature	Halcom CA signature
Distinguished name of the TSP (Issuer)	CN = Halcom CA FO e-signature 1 or CN = Halcom CA FO e-signature 2 2.5.4.97 = VATSI-43353126 O = Halcom d.d. C = SI
Time of issue of CRL (thisUpdate)	Effective date: < time of issue by GMT>
Time of issue of next CRL (nextUpdate)	Next Update: < time of next issue by GMT>
Identification of revoked certificates and time of revocation (revokedCertificate)	Serial Number: <identification number of revoked digital certificate> Revocation Date: <time of revocation by GMT>
Extensions X.509v2 CRL	
CRL list number	Serial number of CRL list
Authority Key Identifier (OID 2.5.29.35)	KeyID= 48 fb 3b 13 99 c3 4e ce Or KeyID= 48 c4 27 a6 6f 6e f0 2e
issuerAltName (OID 2.5.28.18)	not applicable
deltaCRLindicator (OID 2.5.29.27)	not applicable
issuingDistribuitionPoint (OID 2.5.29.28)	not applicable

- Halcom CA PO e-seal 1 or Halcom CA PO e-seal 2

Field name	Value or meaning
Basic fields in CRL	
Version	V2
Signature Algorithm	Sha256RSA

Signature	Halcom CA signature
Distinguished name of the TSP (Issuer)	CN = Halcom CA PO e-seal 1 or CN = Halcom CA PO e-seal 2 2.5.4.97 = VATSI-43353126 O = Halcom d.d. C = SI
Time of issue of CRL (thisUpdate)	Effective date: < time of issue by GMT>
Time of issue of next CRL (nextUpdate)	Next Update: < time of next issue by GMT>
Identification of revoked certificates and time of revocation (revokedCertificate)	Serial Number: <identification number of revoked digital certificate> Revocation Date: <time of revocation by GMT>
Extensions X.509v2 CRL	
CRL list number	Serial number of CRL list
Authority Key Identifier (OID 2.5.29.35)	KeyID=49 48 76 50 77 0a b1 0c Or KeyID= 47 35 c8 bc 61 e2 5d 9e
issuerAltName (OID 2.5.28.18)	not applicable
deltaCRLindicator (OID 2.5.29.27)	not applicable
issuingDistribuitionPoint (OID 2.5.29.28)	not applicable

- Halcom CA web 1

Field name	Value or meaning
Basic fields in CRL	
Version	V2
Signature Algorithm	Sha256RSA
Signature	Halcom CA signature

Distinguished name of the TSP (Issuer)	CN = Halcom CA web 1 2.5.4.97 = VATSI-43353126 O = Halcom d.d. C = SI
Time of issue of CRL (thisUpdate)	Effective date: < time of issue by GMT>
Time of issue of next CRL (nextUpdate)	Next Update: < time of next issue by GMT>
Identification of revoked certificates and time of revocation (revokedCertificate)	Serial Number: <identification number of revoked digital certificate> Revocation Date: <time of revocation by GMT>
Extensions X.509v2 CRL	
CRL list number	Serial number of CRL list
Authority Key Identifier (OID 2.5.29.35)	KeyID=48 42 0b 17 ed ae 9e 70
issuerAltName (OID 2.5.28.18)	not applicable
deltaCRLindicator (OID 2.5.29.27)	not applicable
issuingDistribuitionPoint (OID 2.5.29.28)	not applicable

- Halcom CA TSA 1

Field name	Value or meaning
Basic fields in CRL	
Version	V2
Signature Algorithm	Sha256RSA
Signature	Halcom CA signature
Distinguished name of the TSP (Issuer)	CN = Halcom CA TSA 1 2.5.4.97 = VATSI-43353126 O = Halcom d.d. C = SI
Time of issue of CRL (thisUpdate)	Effective date: < time of issue by GMT>

Time of issue of next CRL (nextUpdate)	Next Update: < time of next issue by GMT>
Identification of revoked certificates and time of revocation (revokedCertificate)	Serial Number: <identification number of revoked digital certificate> Revocation Date: <time of revocation by GMT>
Extensions X.509v2 CRL	
CRL list number	Serial number of CRL list
Authority Key Identifier (OID 2.5.29.35)	KeyID= 43 8f 8b 56 9f 44 1e d7
issuerAltName (OID 2.5.28.18)	not applicable
deltaCRLindicator (OID 2.5.29.27)	not applicable
issuingDistribuitionPoint (OID 2.5.29.28)	not applicable

7.2.3 Publication of the CRL

Halcom CA publishes CRLs in the public directory on the ldap://ldap.halcom.si server under LDAP protocol and http://domina.halcom.si/crls under HTTP protocol.

7.3. OCSP profile

(1) On-line certificate status protocol is available at http://ocsp.halcom.si.

(2) The OCSP message profile (request/response) is in accordance with the IETF RFC recommendation.

7.3.1 Version number(s)

The TSP Halcom CA uses OCSP version 1 messages in accordance with the IETF RFC recommendation.

7.3.2 OCSP extensions

OCSP (request/answer) service messages support the Nonce extension, which is not marked as critical.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

(1) Halcom employs internal audit officer with appropriate technological and legal knowledge. Internal audit officer does not perform tasks related to the management of certificates.

(2) The internal audit officer shall oversee the work of Halcom CA. In the event of detected deficiencies shall take appropriate measures to remedy these deficiencies. Halcom CA is obliged to implement specified appropriate measures under internal audit officer supervision.

(3) Halcom CA is annually subject to an external independent audit carried out by an accredited body.

(4) All relevant ETSI standards are available on HALCOM CA web page.

8.1. Frequency or circumstances of assessment

(1) The internal audit officer shall perform an assessment at least once a year.

(2) The external audit officer for ISO 9001 and ISO 27001 shall perform an assessment at least once a year.

(3) The external audit officer for ETSI Standards shall perform an assessment at least once a year.

8.2. Identity/qualifications of assessor

(1) The internal audit officer shall have the appropriate technological and legal knowledge.

(2) The external audit auditor shall have the appropriate technological and legal knowledge.

8.3. Assessor's relationship to assessed entity

(1) The internal audit officer does not perform tasks related to the management of certificates.

(2) The external audit auditor does not perform tasks related to the management of certificates.

8.4. Topics covered by assessment

Areas of assessment are defined in the internal rules of the TSP Halcom CA.

8.5. Actions taken as a result of deficiency

In the event of deficiencies or errors identified, the internal/external control officer/auditor shall take appropriate measures to remedy the deficiencies, which Halcom CA is obligated to implement under their supervision. The implementation of the measures is detailed in the internal rules of the TSP Halcom CA.

8.6. Communication of results

The results of the assessments are archived by the TSP Halcom CA.

9. Other Business and Legal Matters

9.1 Fees

Halcom CA determines the price list for certificates, services, necessary equipment and infrastructure and publishes such price list on its website.

9.1.1 Certificate Issuance or Renewal Fees

The prices of certificate issuance and renewal are determined by the valid price list.

9.1.2 Certificate Access Fees

Access to the public directory of certificates is free unless the contracting parties agree otherwise.

9.1.3 Revocation or Status

The CRL is available to all persons free of charge.

9.1.4 Fees for Other Services

The prices of other services, equipment and infrastructure are determined by a valid price list.

9.1.5 Refund Policy

Not prescribed.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

Halcom CA has adequately insured responsibility. Detailed information on insurance is available on the website.

9.2.2 Other Assets

Not prescribed.

9.2.3 Insurance or Warranty Coverage for End-Entities

Not prescribed.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

(1) The TSP Halcom CA protects the confidentiality of the following data:

- all certificate or other application forms,
- any confidential information regarding financial liabilities,
- any confidential information that is the subject to mutual agreements with third parties, and
- all other matters covered in the internal rules of the TSP Halcom CA in accordance with the Regulation.

(2) Trust service provider Halcom CA shall handle all possible confidential information about subjects and third parties that are strictly necessary for certificate management services in accordance with applicable law.

9.3.2 Information Not Within the Scope of Confidential Information

The TSP Halcom CA publicly publishes only such business information that is not confidential in accordance with applicable law.

9.3.3 Responsibility to Protect Confidential Information

(1) Halcom CA assumes no responsibility for the contents of the data encrypted or signed/sealed by the subject of the certificate, even if the certificate subject or a third party has complied with all applicable regulations, all policy provisions, and other Halcom CA rules, or has taken into account all its instructions.

(2) Halcom CA assumes no responsibility for the consequences arising because the certificate subject has failed to comply with the security requirements stated in section 4.5.1 of this CPS.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

Halcom CA carefully protects personal data in accordance with European and Slovenian regulations, international standards and recommendations, performs regular risk assessments and provides privacy by design and by default. Halcom' s regulatory compliance officer acts as an official data protection officer.

9.4.2 Information Treated as Private

(1) Protected data is all personal data that TSP Halcom CA obtains from certificate application forms for its services or in appropriate registries to prove the identity of the subject or during the performance of the trust services.

(2) Due to the nature of the use of the certificates and the provisions of the applicable regulations and standards, the information in the certificates and the CRL is accessible to third parties who rely on certificates or validate their validity.

9.4.3 Information Not Deemed Private

There is not unprotected data other than those indicated in the certificate and CRL.

9.4.4 Responsibility to Protect Private Information

The trust service provider Halcom CA is responsible for data protection in accordance with the applicable data protection rules and the provisions of the internal data protection policy.

9.4.5 Notice and Consent to Use Private Information

The subject shall authorize the TSP Halcom CA to process personal data stated in the certificate application form, by special written consent for the processing of personal data, or for other cases later in another statement in written form.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

(1) The TSP Halcom CA shall not provide other data related to subjects of certificates other than those specified in the certificate, unless certain data is specifically required for the provision of specific services or application associated with certificates, and the individual has provided consent to TSP Halcom CA (see in the previous section), or at the request of the competent court, law enforcement body, administrative unit or other authorized person. Any such request shall be carefully reviewed by Halcom CA and data transferred only to the extent necessary by the

applicable regulations.

(2) The data shall be transmitted without written consent only in cases where so stipulated by the applicable European or Slovene legislation.

9.4.7 Other Information Disclosure Circumstances

Not prescribed.

9.5 Intellectual Property

Copyright and related or other intellectual property rights:

- all rights related to the public key belong to the subject of the certificate,
- all rights related to the public keys, all certificate data, the directory of certificates and the CRL data, data from CPs and CPS belong to Halcom CA.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

(1) The TSP Halcom CA is obliged to:

- act in accordance with its internal rules and other applicable regulations,
- act in accordance with international recommendations,
- publish all relevant documents that determine its operation (policies, certificate application forms, revocation requests, price lists, instructions for safe use of qualified digital certificates, etc.),
- publish on its website all information about changes in the activity of TSP, which in any way affect the certificate subjects and third parties,
- ensure the operation of the notification services in accordance with the provisions of HALCOM CA and other applicable regulations,
- comply with the provisions regarding the secure processing of personal and confidential information about TSP, certificate subjects or third parties,
- revoke the certificate and publish it on CRL upon discovery of reasons under this CPS or other applicable regulations,
- issue qualified digital certificates in accordance with this CPS and other regulations and recommendations.

(2) The TSP Halcom CA shall be obliged to:

- ensure the correctness of the data of the issued certificates,
- ensure the correct publication of the CRL,

- ensure the uniqueness of distinctive names,
- ensure the proper physical security of the premises and access to the premises of the TSP,
- professionally ensure the continuous functioning and maximum availability of the service,
- professionally assure the maximum accessibility of services,
- professionally manage the continuous functioning of all other accompanying services,
- with the best effort eliminate any problems encountered in the shortest possible time,
- manage the optimization of hardware and software used,
- inform users about important issues and
- meet all other requirements in accordance with this policy.

(3) The TSP Halcom CA ensures the maximum availability of its services, all days of the year, except in the following cases:

- planned and pre-announced technical or service interventions on the infrastructure,
- unplanned technical or service interventions on the infrastructure as a result of unforeseen failures,
- technical or service interventions due to infrastructure failure outside the competence of Halcom CA and
- inaccessibility as a result of force majeure or extraordinary events.

(4) TSP Halcom CA shall announce maintenance or upgrading of the infrastructure at least three (3) days prior to the commencement of activities.

(5) TSP Halcom CA is solely responsible for all the information in this document and for the implementation of all the provisions in this CPS.

(6) Other liabilities or obligations of TSP Halcom CA may be determined by a possible mutual agreement with a third party.

9.6.2 RA Representations and Warranties

(1) The RA shall be obliged to:

- check the identity of the subjects or future subjects,
- receive certificate application form for Halcom CA services,
- check certificate application form,
- issue the necessary documentation to legal persons, subjects or future subjects,
- submit order forms and other information in a secure way to Halcom CA.

(2) The RA shall be responsible for the implementation of all the CPS provisions, policies and other requirements agreed upon with the TSP Halcom CA.

9.6.3 Subscriber Representations and Warranties

(1) A legal person is responsible for:

- damages incurred in the event of misuse of the certificate from the revocation submission to the revocation,
- any damage that is either directly or indirectly caused by the use or abuse of the subject's certificate by unauthorized persons,
- any other damage resulting from failure to comply with the CPS, policies, and other notices of Halcom CA and the applicable regulations.

(2) The obligations of the subjects regarding the use of certificates are set out in Section 4.5.1.

9.6.4 Relying Party Representations and Warranties

(1) Upon the first use of Halcom CA certificates, the third party relying on the certificate shall carefully read the policy and from then onwards regularly monitor all the notices of Halcom CA.

(2) Always, at the time of use of the certificate, a third party shall validate thoroughly if the certificate is not listed in the CRL.

(3) If the certificate contains information about a third party, such party shall request the revocation of the certificate if it finds that the private key has been compromised in a manner that affects the reliability of the use or if there is a risk of abuse, or if data indicated in the certificate has changed.

(4) A third party may rely on such a certificate until the revocation of the certificate.

(5) A third party may at any time request any information regarding the validity of any issued certificate, policy provisions, and Halcom CA notices.

9.6.5 Representations and Warranties of Other Participants

Not prescribed.

9.7 Disclaimers of Warranties

TSP Halcom CA is not liable for any damage resulting from:

- the use of certificates for any purpose or in a manner not explicitly provided for in this CPS,
- incorrect or inadequate protection of the passwords or private keys of the subjects, the disclosure of confidential data or keys to third parties and the irresponsible conduct of the subject,
- abuse or intrusion into the information system of the certificate subject and, hence, information on certificates by unauthorized persons,
- inaction or malfunction of the information infrastructure of the certificate subject or third

parties,

- not validating the data and validity of certificates in the CRL,
- not checking the validity period of the certificate,
- conduct by the subject of a certificate or a third party contrary to Halcom CA notices, policy and other regulations,
- enabling usage or abuse of the subject's certificate to unauthorized persons,
- the issued certificate with false information or unreliable data or other such acts of the subject or TSP,
- the use of certificates and the validity of certificates after changes in the certificate data, e-mail addresses or changes in the names of the subject,
- infrastructure failure outside the domain of the TSP Halcom CA,
- data encrypted or signed using certificates,
- conduct of subjects in the use of certificates, even if the subject or a third party has complied with all the provisions of this CPS, notices of Halcom CA or other applicable regulations,
- the use and reliability of hardware and software operation of the certificate subjects
- errors calculating hash value, verification of hash value or other security procedures regarding the electronic document to be signed if the subject has requested electronic signature in the cloud solely on the basis of a hash value and without sending the entire electronic document to TSP Halcom CA.

9.8 Limitations of Liability

Not prescribed.

9.9 Indemnities

The party that failed to comply with the policy provisions and applicable legislation is liable for damages caused by such failure.

9.10 Term and Termination

(1) Halcom CA reserves the right to change CPS and upgrade its infrastructure without prior notification to subjects of certificates.

(2) The CPS shall enter into force on the day it is adopted by Halcom CA.

9.10.1 Term

New version changes to the CPS shall be made public on the website of the TSP Halcom CA eight (8) days prior to its validity and with the date of entry into force clearly marked.

9.10.2 Termination

(1) After publishing the new CPS and policies, for all the certificates issued on the basis of policies those (old) provisions remain in force that can not reasonably be replaced by the relevant provisions under the new policies (for example, the procedure determining the manner under which a certificate was issued, etc.).

(2) The TSP may issue amendments to the CPS provisions as set out in Section 9.12.

9.10.3 Effect of Termination and Survival

(1) The validity of certificates is governed by policies.

(2) The new CPS, and thus the new policy, does not affect the validity of certificates issued under previous policies. Such certificates shall remain in force until the expiry date, where possible, they shall be dealt with in accordance with the new policy.

9.11 Individual Notices and Communications with Participants

(1) Contact details of the TSP are published on the website and are given in section 1.3.1.

(2) The contact details of the subjects are given in the certificate application forms.

(3) Contact details of third parties shall be provided in a mutual agreement between the third party and the trusted service provider Halcom CA.

9.12 Amendments

9.12.1 Procedure for Amendment

(1) Changes or amendments to the CPS may be published by the TSP in the form of amendments and supplements to the CPS where there are no significant changes in the performance of the TSP.

(2) The amendments shall be adopted in accordance with the same procedure as the CPS.

(3) The method for marking amendments and additions is determined by the TSP Halcom CA.

9.12.2 Notification Mechanism and Period

(1) The TSP Halcom CA shall determine the beginning and the end of validity of amendments and supplements.

(2) Changes and amendments shall be published on the Halcom CA website eight (8) days prior to their entry into force.

9.13 Dispute Resolution Provisions

(1) All complaints by subjects of certificates shall be solved by the regulatory compliance officer.

(2) Any dispute between the subject of a certificate or a third party and Halcom CA shall be resolved by the competent court in Ljubljana, Slovenia.

9.14 Governing Law

The law of the European Union and the Republic of Slovenia shall govern all issues.

9.15 Compliance with Applicable Law

(1) Supervision of the compliance of the TSP Halcom CA with the applicable legislation and regulations is carried out by the competent inspectorate and accredited conformity assessment bodies.

(2) TSP Halcom CA shall be reviewed by the accredited conformity assessment body at least every 24 months. The purpose of the audit is to verify that the TSP and the qualified trust services it provides meet legal requirements.

(3) Internal compliance verification shall be performed by authorized persons within the TSP Halcom CA.

9.16 Miscellaneous Provisions

(1) TSP Halcom CA may enter into mutual agreements with other TSPs if so provided by the applicable law or other regulations.

(2) If any of the provisions of this policy is or becomes invalid, this shall not affect other provisions. An invalid provision is replaced by a valid one, which must be as close as possible to the purpose which the invalid provision sought to achieve.

9.17 Other Provisions

Not prescribed.

Place and date:
Ljubljana, 22.5.2024

CEO
Tomi Šefman