Author: Luka RIBIČIČ

Document number: 400085-39-10/17

Halcom CA: Certificate Practice Statement (CPS),

Edition: 11

Halcom CA

Certificate Practice Statement (CPS)

English version

Document is valid from: 15.6.2025

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
11	400085-39-10/17	Translation of CPS Izdaja št. 11 (IPS 400085-8-10/17)	L. Ribičič	22.5.2025

Table of Contents

1. INTRODUCTION

(1) This document constitutes the Certificate Practise Statement (hereinafter referred to as the CPS) of a trust service provider (hereinafter referred to as the TSP) in the field of electronic signing, electronic sealing, electronic timestamping, validation and other services.

(2) Halcom CA is the oldest and the largest TSP in Slovenia, which uses the most secure technologies to provide its services in the field of electronic signatures, electronic sealing, electronic time stamping, validation and other services, including the use of QSCD and a secure cloud.

(3) All provisions of the CPS regarding the conduct of Halcom CA are duly transposed and further specified in the provisions of the Internal Rules. These are documents of a confidential nature defining the infrastructure, the provisions concerning the Halcom CA staff (responsibilities, tasks, powers and required conditions to be met by each staff member), physical security (access to premises, handling of hardware and software), software security (server security settings, backups,...) and internal audit (audit of physical access, authorisations,...).

1.1. Overview

(1) The CPS constitutes the general rules of operation of the TSP HALCOM CA for the issuance of certificates, governing the purpose, functioning and methodology of certificates management and security requirements to be met by the TSP HALCOM CA, the subscribers, subjects and third parties relying on these certificates, and the responsibilities of all these parties.

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

- the issuance and the validation of certificates for electronic signatures, certificates for electronic seals, certificates for website authentication or certificates for the provision of other trust services,
- the creation the validation of electronic signatures or electronic seals,
- the preservation of electronic signatures, electronic seals, certificates for electronic signatures or certificates for electronic seals,
- the management of remote electronic signature creation devices or remote electronic seal creation devices,
- the issuance and the validation of electronic attestations of attributes,
- the creation and the validation of electronic timestamps.

(3) The trust service provider Halcom CA operates within Halcom d.d.

(4) Halcom CA issues:

- qualified certificates for electronic signatures
- qualified certificates for electronic stamping,
- qualified certificates for website authentication,
- qualified certificates for attestation of attributes,
- qualified certificates for timestamping.

(5) Halcom CA issues certificates and performs other activities of a TSP in accordance with the applicable legal order of the Republic of Slovenia and the European Union, and in accordance with the eIDAS Regulation, the eIDAS 2.0 Regulation, the ETSI technical requirements, the IETF RFC standards, the 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 and rights and obligations regarding the operation of the Halcom CA Trust Service Provider are described in the following public documents:

- Halcom CA Policy for EU qualified Digital Certificates for legal persons,
- Halcom CA policy for EU qualified digital certificates for natural persons,
- Halcom CA policy for EU qualified time stamping,
- Certificate Practice Statement.

1.1.2 Links between basic documents of TSP Halcom CA

(1) The Policy defines the operational requirements of the TSP and define the operational processes to meet these requirements. The CPS defines the way in which the TSP ensures the technical, organisational and process operational requirements defined in the Halcom CA Policy.

(2) The Policy is a more general document compared to the CPS. The CPS is a more detailed description of the TSP Halcom CA works, the business and operational processes for issuing and managing certificates.

(3) The policy is defined independently of the specific operational unit of the TSP and the CPS is a detailed description of the organisational 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) The internal rules are confidential documents and constitute the business secret of the TSP Halcom CA.

(3) The internal rules contain detailed provisions on:

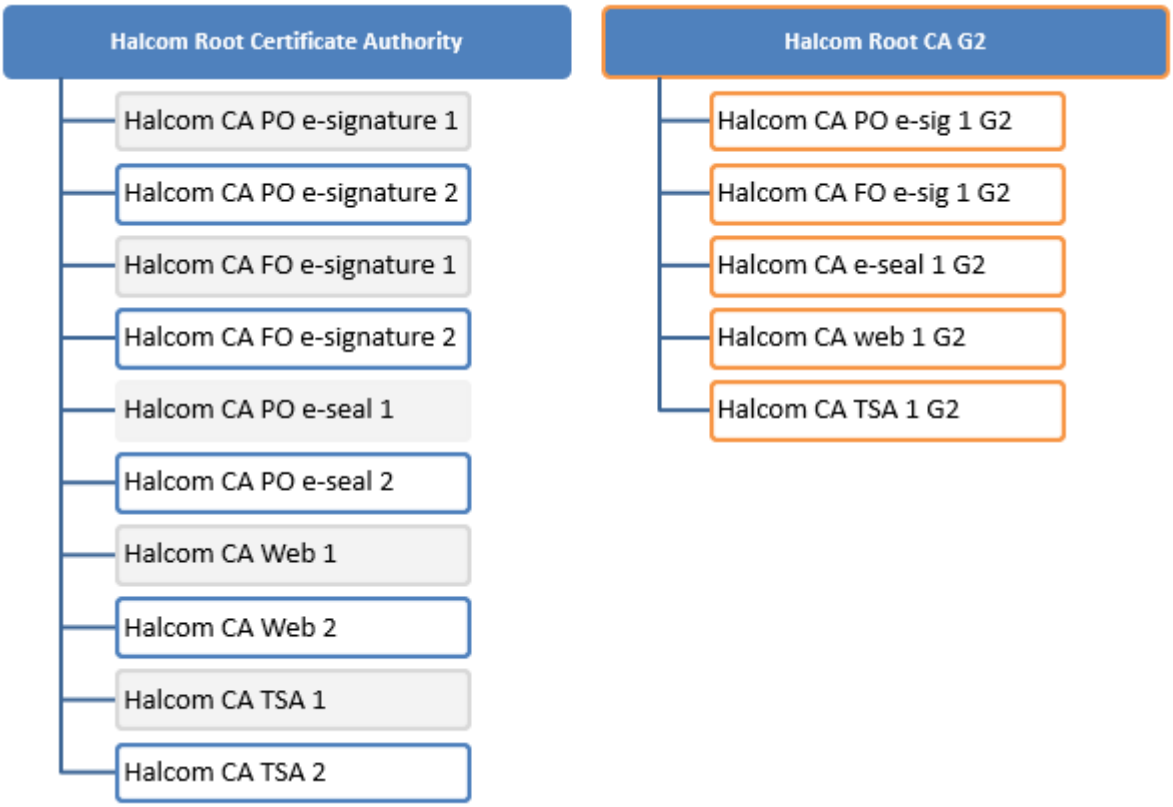
- Halcom CA physical access control system,

- the Halcom CA logical access control system for computer networks,
- Halcom CA system for securing private keys,
- system of distributed responsibility at Halcom CA for private key activation,
- the procedures and personnel involved in the provision of trust services,
- the 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 once a year by an Accredited body.

1.2. Halcom CA Trust Service Provider

(1) Structure of Halcom CA (first and second generation):



(2) Halcom CA is responsible for issuing the following root digital certificates.

Certificate	Purpose of use	Generation
Halcom Root Certificate Authority	Issue of intermediate/subordinate certificates	G1
Halcom Root CA G2	Issue of intermediate/subordinate certificates	G2

(3) Halcom CA is responsible for issuing the following intermediate/subordinate digital certificates.

Certificate	Purpose of use	Generation
Halcom CA FO e-signature 1	Issuing e-signature certificates for natural persons	G1

Halcom CA FO e-signature 2	Issuing e-signature certificates for natural persons	G1
Halcom CA PO e-signature 1	Issuing e-signature certificates for legal persons	G1
Halcom CA PO e-signature 2	Issuing e-signature certificates for legal persons	G1
Halcom CA PO e-seal 1	Issuing e-stamp certificates for legal persons	G1
Halcom CA PO e-seal 2	Issuing e-stamp certificates for legal persons	G1
Halcom CA web 1	Issuing certificates for website authentication	G1
Halcom CA web 2	Issuing certificates for website authentication	G1
Halcom CA TSA 1	Issue of time-stamping certificates	G1
Halcom CA TSA 2	Issue of time-stamping certificates	G1
Halcom CA FO e-sig 1 G2	Issuing e-signature certificates for natural persons	G2
Halcom CA PO e-sig 1 G2	Issuing e-signature certificates for legal persons	G2
Halcom CA PO e-seal 1 G2	Issuing e-stamp certificates for legal persons	G2
Halcom CA web 1 G2	Issuing certificates for website authentication	G2
Halcom CA TSA 2	Issue of time-stamping certificates	G2

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,
- accepting requests for certificates issuance,
- accepting requests for certificates revocation,
- distribution of the necessary documentation to subscribers and certificate subjects,
- transmitting requests and other data 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. Each such organisation shall be contractually bound by the TSP Halcom CA to comply with strict security conditions in accordance with applicable European and Slovenian regulations and international, European and Slovenian standards and recommendations, as well as Halcom CA policies, CPS and internal rules.

(3) The TSP Halcom CA has a geographically dispersed RAs, enabling subscribers' 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 electronic signature	Halcom CA FO e-signature 1	Natural person	Natural person
	Halcom CA FO e-signature 2		
	Halcom CA FO e-sig 1 G2		
	Halcom CA PO e-signature 1	Legal person	Natural person
	Halcom CA PO e-signature 2		
	Halcom CA PO e-sig 1 G2		
Certificates for the electronic seal	Halcom CA PO e-seal 1	Legal person	Device or server
	Halcom CA PO e-seal 2		
	Halcom CA e-seal 1 G2		
Website authentication certificates	Halcom CA web 1	Legal person or exceptionally natural person	Device or server
	Halcom CA web 2		
	Halcom CA web 1 G2		
Electronic time stamp certificates	Halcom CA TSA 1	Trust Service Provider	Device or server
	Halcom CA TSA 2		

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) proving the identity of the subject,
3) signing/sealing electronic documents,
4) encryption and decryption of electronic documents.

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

1) electronic or mobile banking,
2) eGovernment or mGovernment applications,
3) eHealth or mHealth applications,
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 that require the use of a certificate,
7) access control.

(3) Certificates for website authentication are intended for:

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

(4) Secure timestamps are used in a variety of applications and for a variety of purposes that are emerging on the market. Among others, timestamps are used in applications and purposes such as:

1) electronic banking,
2) electronic storage of data, documentary or archival material,
3) eGovernment applications,
4) other applications where it is necessary to ensure that a specific action or fact can be linked to a precise time source .

1.4.2 Prohibited certificate uses

(1) The use of certificates issued in accordance with the policy in contravention of the provisions of the policy or applicable regulations or outside the scope of permitted use set out in the preceding section is prohibited.

(2) Certificates are not 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)
G1 or G2	First and second generation of root and intermediate Halcom CA certificates.
QCert for ESig/ ESeal	Qualified digital certificate issued on a secure medium (QSCD - Qualified signature creation device). Halcom CA can issue the certificate on a smart card, USB smart key or in the cloud (HSM). The certificate is intended for Qualified electronic signing/sealing (QES/Seal).
Cert for Esig/ ESeal	A qualified digital certificate issued in a file for advanced electronic signing/sealing.

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 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 on how to use digital certificates securely,
- 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 under the custody of HALCOM CA. For data protection reasons,

only a register of revoked certificates, which is part of the directory, is publicly available.

(3) The status of revoked certificates shall be published immediately in the register of revoked certificates (see section 4.9.8 for details), other publicly available information or documents shall be published as required.

(4) Access to the directory of issued certificates is only granted to authorised users who are verifying a large 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 five (5) seconds) after their issuance.

(3) The list of revoked certificates shall be refreshed immediately (maximum five (5) seconds) after the revocation 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 (other than those mentioned 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 via the LDAP protocol. Only the register of revoked certificates, which is part of the directory, is publicly accessible.

(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 shall unambiguously and uniquely define the certificate subject, unless otherwise required by either this CPS or by the content of the qualified digital certificate.

3.1.1 Types of names

(1) In accordance with IETF RFC 5280, each certificate shall contain 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 Issuer field. The basic information of the subject contained in the distinguished name of the certificates for natural persons or legal persons are listed in the Subject field 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) Halcom CA may, in accordance with the eIDAS Regulation, eIDAS 2.0, Regulation and ETSI standards for the creation of the distinguished name of foreign natural persons and/or foreign legal person, also use other semantic identifiers of natural persons and legal persons, 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 legal persons "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 supplementing 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) When issuing a qualified digital certificate, the trust service provider Halcom CA may also add an attribute 1.3.6.1.4.1.5939.2.9 in the Subject field, representing the type of certificate (e.g. indicating that it is a qualified digital certificate in the cloud, on a smart card or USB key, etc.).

(7) TSP Halcom CA Certificates:

Type of certificate	Certificate field	Distinguishing name	Generation
Root certificate of the TSP Halcom CA	Issuer and Subject	C= SI O= Halcom d.d. 2.5.4.97 = VATSI-43353126 CN= Halcom Root Certificate Authority	G1
	Issuer and Subject	C= SI O= Halcom d.d. 2.5.4.97 = VATSI-43353126 CN= Halcom Root CA G2	G2
Intermediate/subordinate certificate of TSP Halcom CA	Issuer	C= SI O= Halcom d.d. 2.5.4.97 = VATSI-43353126 CN= Halcom Root Certificate Authority	G1
	Subject	C= SI O= Halcom d.d. 2.5.4.97 = VATSI-43353126 CN= <subordinate certificate name>	
Intermediate/subordinate certificate of TSP Halcom CA	Issuer	C= SI O= Halcom d.d.	G2

		2.5.4.97 = VATSI-43353126 CN= Halcom Root CA G2	
	Subject	C= SI O= Halcom d.d. 2.5.4.97 = VATSI-43353126 CN= <subordinate certificate name>	
End user certificate	Issuer	C= SI O= Halcom d.d. 2.5.4.97= VATSI-43353126 CN= <subordinate certificate name>	G1 and G2
Certificate for electronic signature for legal person	Subject	C= <two-digit ISO country code> O= <organization name> 2.5.4.97= VAT<two-digit ISO country code>-<legal person's tax number> and/or 1.3.6.1.4.1.5939.2.3= <legal person's tax number> CN= <given name and surname> SN= <surname> G= <given name> SERIALNUMBER= TIN<two-digit ISO country code>-subject's TIN> and/or 1.3.6.1.4.1.5939.2.2= <subject's TIN> E= <email>	G1 and G2
Certificate for electronic signature for natural persons	Subject	C= <two-digit ISO country code> CN= <given name and surname> SN= <surname> G= <given name> SERIALNUMBER= TIN<two-digit ISO country code>-<subject's TIN> and/or 1.3.6.1.4.1.5939.2.2= <subject's TIN> E= <email>	G1 and G2
Certificate for electronic stamp	Subject	C= <two-digit ISO country code> O= <organization name> 2.5.4.97= VAT<two-digit ISO country code>-< legal person tax number> and/or 1.3.6.1.4.1.5939.2.3= <legal person's tax number> CN=<name of information system or department> E= <email>	G1 and G2
Website authentication certificate	Subject	C= <two-digit ISO country code> O= <organization name>	G1 and G2

		2.5.4.97= VAT<two-digit ISO country code>-<legal person's tax number> and/or 1.3.6.1.4.1.5939.2.3= <legal person 's tax number> OU= web certificates CN= <website name and domain> SN= <domain> G= <website name> E = <email>	
Time Stamping Certificate	Subject	C= <two-digit ISO country code> O= <organization name> 2.5.4.97= VAT<two-digit ISO country code>-<legal person's tax number> and/or 1.3.6.1.4.1.5939.2.3= <legal person's tax number> CN= <timestamping unit name> E= <email>	G1 and G2

(8) The TSP Halcom CA may use additional fields for the distinguished name of the certificate subjects, if necessary.

3.1.2 Need for names to be meaningful

(1) The name of a natural or legal person that is included in the distinguishing name in accordance with the provisions of section 3.1.1 shall comply with 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 legal person's name or brand if it determines 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 of G1 certificates 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) The TSP shall ensure the use of other unforeseen characters by means of an appropriate combination of letters.

(3) The information of the subject certificate in the distinguished name of G2 certificates shall contain the characters from the UTF-8 code table.

(4) Halcom CA reserves the right to change the format of the distinguished name. The change shall be published on the TSP Halcom CA website at least eight (8) days prior to implementation.

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 authorities, names, designations, trademarks or elements of intellectual property belonging to third parties in violation of 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) Liability in respect of the use of names or trademarks shall be the sole responsibility 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

Proof of possession of the private key corresponding 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 contained in 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 the 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) The TSP Halcom CA shall verify the ownership of the domain indicated by the authorised person of the legal person on the request for a certificate for website authentication with the authorised 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 subjects in accordance with applicable regulations (official document with picture) or shall provide information on subjects from its databases obtained using the procedure by the registration service used for another purpose, which ensures an equivalent level of reliability.

(2) The legal person, as the employer or authorizer of the certificate subject, undertakes to ensure that the certificate subject is familiar and will comply with Halcom CA Policy and applicable regulations.

(3) 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 correctness and functioning 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 specific person who is employed or performs tasks for this legal person.

3.2.6 Criteria for interoperation

(1) The TSP Halcom CA shall not be obliged to contractually cooperate with or guarantee for other providers even if the other service provider has the status of a TSP or TSP issuing qualified digital certificates.

(2) The TSP Halcom CA guarantees to implement mutual recognition only after signing a written contract with other TSP, which must meet a level of security requirements comparable to 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 will 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:

- in person at the RA, where the authorized persons will check the identity of the applicant,
- electronically, but the revocation request must be digitally signed with a qualified certificate to prove the identity of the applicant,
- if subject of the certificate requests the revocation of the certificate by telephone or e-mail, the TSP Halcom CA shall suspend the certificate. Only upon a written request for the certificate revocation, the final revocation of the certificate is carried out.

(2) Detailed procedure for revocation is described in 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 in association with a legal person or legal persons for their devices.

(2) In order to obtain a certificate, the following conditions must be met:

- a 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 subject if the legal person or authorized individual is listed as a person against whom restrictive measures (sanctions) have been imposed by the United Nations, the European Union, the Republic of Slovenia, the United Kingdom, Canada, Australia or the United States of America.

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 the Halcom CA 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 authorises 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 verified.

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.

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

3) 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). The application form shall be submitted by the website owner to the Halcom CA RA and the financial obligations related to the issuance of the certificate shall be settled. Certificate application form can be obtained from Halcom CA RAs 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 timestamping:

1) Timestamping certificates are only intended for TSPs.

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

3) The TSP Halcom CA guarantees that it will only issue a certificate after signing a written contract with another TSP, which must meet a level of security requirements comparable to or higher than that prescribed by the TSP Halcom CA.

4) If an external and independent assessment of the compliance of another TSP is not guaranteed, Halcom CA's authorized persons will review the internal rules of another TSP and his 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 by means of a valid photo ID when visiting the registration service or via the courier service or via the secure electronic portal when delivering the certificate, PIN, password or cloud certificate application form.

(2) TSP Halcom CA's RA may also provide data from its own databases obtained by a procedure used by the RA for other purposes and ensuring an equivalent level of reliability in accordance with the applicable rules.

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

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

4.2.2 Approval or rejection of certificate applications

(1) (1) The authorised persons of the TSP Halcom CA shall approve the application form for obtaining a certificate or reject it in the event of incorrect or incomplete information or non-compliance with the obligations, of which the legal person or the future subject shall be notified in person 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

Halcom CA shall issue a certificate based on the approved purchase order or contract and the financial obligations related to the issuance of the certificate within a maximum of five (5) working 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 associated key pairs consist of clearly separated parts (or functions), with their respective separate subsystems:

  1) pre-personalization of a QSCD (generating keys on the card, setting a password to secure the certificate)
  2) obtaining a certificate application form,
  3) processing of the certificate application form,
  4) preparation of the certificate,
  5) personalization of QSCD (issuing and storing the certificate, printing the subject's data)

6) printing a personal password (PIN code – only if code is sent by registered mail),
7) distributing the certificate and the personal password (PIN code) and the notifications to the subject.

The advance certificate on the QSCD and the associated personal password (PIN) shall be sent to the subject by registered mail, in two separate deliveries, on two separate business days. The personal password (PIN) may also be transmitted to the subject via another secure channel (via a specific website where the subject identifies himself or herself via a specific link received via e-mail and another piece of information known to the subject (e.g. ID number, tax number of the subject, the last four digits or CVV code of a debit or credit card, or similar)). In exceptional cases, the items may also be handed over to the subject in person by authorised persons of the RA.

- Qualified cloud certificates

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

1) processing of the certificate application form,
2) preparation of the certificate and registration and activation code,
3) distributing the registration and activation code and the notification to the subject,
4) generating keys on HSM and issuing a certificate.

The registration and activation code are sent to the subject via two separate channels, the registration code by e-mail and the activation code through another secure channel (secured website/portal where the subject is identified by a special link received via e-mail and another piece of information known to the subject (e.g. ID number, tax number of the subject, the last four digits or CVV code of a debit or credit card, or similar)).In exceptional cases, one of the above codes may be handed over to the subject in person by authorised persons of the RA.

- Standard qualified Digital Certificate

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

1) processing of the certificate application form,
2) preparation of the certificate, reference code and password,
3) distributing the reference code, the password and the notification to the subject,
4) enrolment of the certificate.

The reference code and the password are transmitted to the subject via two separate channels, one by e-mail and the other by another channel (personal delivery by registered mail, by SMS, via a secure web portal where the subject identifies himself with a qualified certificate or a piece of information known only to the subject (e.g. ID number, tax number of the subject, the last four digits or CVV code of a debit or credit card, or similar)). In exceptional cases, the password may be handed over to the subject in person by authorised

persons of the RA.

- Qualified certificates for information systems and website authentication

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

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

- Qualified certificates for timestamps

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

  1) reviewing the security requirements and internal rules of another TSP,
  2) processing and signing the contract for certificate issuance,
  3) obtaining an electronic certificate request,
  4) preparation of a certificate,
  5) personalization and issuance of the certificate,
  6) transmission of the certificate to the TSP.

(2) The subscriber and the subject are not, as a rule, the same person as the TSP Halcom CA or the RA. If the RA orders a certificate for itself or for its authorized employees, such order shall be subject to additional verification by Halcom CA staff.

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

(4) The procedures shall be designed in such a way that they cannot be carried out by a single person.

(5) TSP Halcom CA may, on the basis of a written contract, delegate certain tasks (e.g. printing the subject's data, printing PIN codes, distribution, etc.) to verified external contractors. Halcom CA shall regularly audit such contractors 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 the certificate is stored securely by the TSP Halcom CA on the subject's behalf. Only the access codes for activating the connection to secure cloud are provided to the user, see Sect. 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. Only reference code and the password are transmitted to the subject, see section 4.3.1.

- Certificates for the information systems and website authentication and timestamping

  For website authentication certificates, information systems, and timestamping, the legal person shall initiate key generation locally and set a password to protect them. The TSP Halcom CA generates a certificate on the basis of the received electronic certificate request and sends it back to the legal person, which generates a certificate with the associated key pair using the above-mentioned password.

(2) Upon receipt of the certificate, the certificate subject or legal person shall immediately verify the information contained in the certificate and immediately notify the TSP Halcom CA in the event of any 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:

- get acquainted and act in accordance with the policy before certificate issuing,
- comply with the policy and other applicable regulations,
- after accepting the certificate or activating the certificate, check the data in the certificate and in case of any errors or problems immediately notify Halcom CA or request revocation

of the certificate,

- monitor and comply with all notices of Halcom CA,
- update the necessary hardware and software to work securely with certificates, as notified,
- immediately notify Halcom CA of any changes to the certificate,
- request revocation of the certificate if the private key has been compromised in a way that affects the reliability of use or if there is a risk of misuse,
- request revocation of the certificate in the cloud in case of loss or theft of the mobile device, or if there is a risk of misuse,
- 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 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 guard passwords to protect or access the private key,
- comply with Halcom CA's notices upon expiry or revocation of the certificate.

4.5.2 Relying party public key and certificate usage

(1) The third party relying on the certificate shall:

- 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,
- notify Halcom CA if it becomes aware 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 misuse, or if the information contained 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,
- verify, at the time of use of the certificate, that the certificate is not revoked,
- verify, at the time of use of the certificate, that the digital signature/seal was created during the validity period and for the purpose of the certificate,
- verify the signature of the TSP Halcom CA certificate, which is published in this CPS and also on the Halcom CA website,
- comply with other provisions in the event of concluding an additional agreement on the use of certificates with TSP Halcom CA.

(2) The third party shall use software and hardware to verify the validity of the signature/seal or other cryptographic operation that can credibly verify all of the above requirements for the secure use of certificates.

4.6. Certificate renewal

(1) Only the subject of the certificate can request the certificate renewal. Renewal shall only be possible for standard and advanced qualified digital certificates and qualified cloud certificates.

(2) Upon expiry of the advanced certificate and after one (1) time renewal, the subject shall re-apply for the new certificate.

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

(4) The renewal of certificates for website authentication, information systems, and timestamping shall be done in the same way as the initial order of the certificate (see section 4.1).

4.6.1 Circumstance for certificate renewal

Before the expiry of a digital certificate, subjects of standard, advanced and cloud certificates shall ensure continuity of use of the digital certificate by electronically requesting reissuance. 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 the event of a change in the information affecting the validity of the distinguished name or other information in the certificate, the certificate shall be revoked .

(2) To obtain a new certificate, the procedure for obtaining a new certificate as set out in section 4.1 must be repeated.

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 at any time by the legal person or the subject of the certificate, but it must be required in the case of:

1) Distinguished Name (DN) changes,
2) when the legal person or subject of the certificate changes the significant information related to the certificate (e.g. name or surname, name of legal person, e-mail address, employment, etc.),
3) when it is established or suspected that either signing key has been disclosed or the certificate has been misused,
4) replacing the certificate with another certificate (e.g. when the certificate QSCD or PIN for accessing QSCD is lost).

(2) Halcom CA may also revoke a certificate without the subject's request in the cases referred to in paragraph 1 or at the request of a competent court, criminal or administrative authority.

(3) The certificate may be revoked twenty-four (24) hours a day. Detailed instructions on how to revoke a certificate are published on the Halcom CA website.

(4) Halcom CA will revoke the certificate within a maximum of four (4) hours upon a valid revocation request. In the event of unforeseen circumstances, Halcom CA will exceptionally revoke the certificate within a maximum of eight (8) hours after receipt of a valid revocation request. During this time, the revoked certificate will be marked as revoked and added to the revoked certificate list (CRL). If a certificate subject submits an incorrect revocation request, Halcom CA will inform and provide the subject about with instructions on how 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 certificate subject's private key has been compromised in a way that affects the reliability of use,
- if there is a risk of misuse of the subject's private key or certificate,
- if key information on the certificate has changed or is incorrect.

(2) The TSP Halcom CA shall revoke the certificate, even without a request from the subject, as soon as becomes aware of:

- the information on the certificate is incorrect or the certificate was issued on the basis of incorrect information,

- there was an error in the identity verification at the RA,
- other circumstances affecting the validity of the certificate have changed,
- subject's non-compliance with obligations
- the financial obligations for digital certificates are not settled,
- that the TSP's infrastructure has been compromised in a way that affects the reliability of the certificate,
- the subject's private key has been compromised in a way that affects the reliability of use,
- that Halcom CA will cease issuing certificates or that the TSP has been prohibited from managing certificates and its activities have not been taken over by another TSP,
- that the revocation has been ordered by the competent court, prosecuting authority or administrative body..

(3) The subject of a digital certificate may request, within thirty (30) days of issuance, the re-generation of a personal password (PIN) for advanced certificates or reference code and password for standard certificates or registration and activation codes for cloud certificates in the case of, in case that he/she has forgotten e-access data, and warrants, under civil and criminal liability, that there is no possibility that the private key has been compromised in a way that affects the reliability of use and that there is no risk of misuse of the subject's private key or 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,
- certificate subject,
- the competent court, prosecuting authority 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:

- in person during office hours at the RA,
- electronically twenty-four (24) hours a day, every day of the year, if there is a risk of misuse or unreliability of the certificate, otherwise during the business hours of the public authorities under the applicable law.

(2) If the revocation is requested:

- in person, it is necessary to complete the appropriate revocation request and submit it to the RA;
- electronically, the subject must send an email to Halcom CA requesting cancellation, which must be digitally signed/sealed with a trusted certificate to verify it.
- if the subject requests certificate revocation by telephone or e-mail, the TSP Halcom CA will suspend the certificate. Only upon 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. The TSP shall also provide additional information on the revocation (details of the person requesting the revocation, the reason for the revocation, etc.) upon written request of the legal person or the subject.

(4) Courts, criminal and administrative authorities, which may also request revocation, shall do so in accordance with the laws governing the procedure before them (criminal procedure, litigation, general administrative procedure and others).

(5) The provisions relating to revocation shall apply mutatis mutandis also to the procedures relating to the re-generation of PIN codes for advanced certificates, reference codes and passwords for standard certificates and registration, activation codes for cloud certificates.

4.9.4 Revocation request grace period

The revocation must be requested immediately in the event of possible abuse or unreliability, or similar emergencies. In other cases, the revocation may be requested the first working day during the hours of the registration service (see next section).

4.9.5 Time within which CA must process the revocation request

(1) Upon receipt of a valid revocation request, the TSP Halcom CA shall:

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

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

4.9.6 Revocation checking requirement for relying parties

Before use, third parties relying on the certificate should check the most recently published register of revoked certificates. For reasons of authenticity and integrity, the authenticity of this register, which is digitally signed by Halcom CA, should always be verified.

4.9.7 CRL issuance frequency

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

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

4.9.8 Maximum latency for CRLs

(1) A new register of revoked certificates shall be published:

- in the public directory on the ldap://ldap.halcom.si server immediately (maximum five (5)

seconds),

- on the website http://domina.halcom.si/crls with a maximum delay of 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 eight (8) 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 twenty-fou (24) hours, but before the expiration of the last valid CRL.

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). The OCSP can operate with a maximum delay of one (1) minute from the publication of a new CRL.

4.9.10 On-line revocation checking requirements

Third parties should always check whether the certificate on which they rely has been 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 electronic means, the certificate shall be suspended until the original written request is received.

(2) If the certificate subject, third party or other person, a court, a law enforcement, administrative or related authority, or the TSP itself, expresses suspicion that the certificate is being used in breach of policy or applicable regulations, the certificate shall be suspended pending a 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 available on ldap://ldap.halcom.si/ server via LDAP

protocol and at http://domina.halcom.si/crls via HTTP protocol.

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

(3) Details on publication and access are given in sections 7.2 and 7.3.

4.10.2 Service availability

(1) The validation of the status of certificates shall be available twenty-four (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 publish a register of revoked certificates no later than in eight (8) 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 twenty-fou (24) hours, but before the expiration of the last valid CRL.

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 is not renewed,
- 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 shall design and implement all security measures in accordance with the ISO/IEC 27000 family of standards, FIPS 140-2 Level 3 and/or Common Criteria EAL4+ and ETSI technical requirements .

(2) Halcom CA equipment is located in separate, segregated rooms and is protected by a multi-level

system of physical and technical intrusion protection. The equipment shall be protected against unauthorised access. It is also protected and secured by a fire protection system, an anti-spill system, a ventilation system and a multi-level uninterruptible power supply system.

(3) Halcom CA shall store backup and distribution media in such a way as to prevent, to the greatest extent possible, the loss, intrusion or unauthorised use or alteration of the stored information. For both data recovery and archiving of important information, backup copies are provided and stored in a different location from where the Certificate Management Software is stored to ensure resumption of operations in the event that data at the primary location is destroyed.

(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 system.

(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 system.

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

5.1.2 Physical access

(1) Access to the infrastructure of the trust service provider shall only be granted to authorised persons of the TSP in accordance with their roles , see section 5.2.1.

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

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

5.1.3 Power and air conditioning

(1) The infrastructure of the trust service provider shall be provided with uninterruptible power supply and adequate 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 shall not be exposed to the risk of flooding, except in the event 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 the possibility of fire.

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

5.1.6 Media storage

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

(2) The backup copies of the Halcom CA software and encrypted databases shall be regularly updated and stored in two separate and physically secured rooms at different locations.

5.1.7 Waste disposal

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

(2) Waste disposal shall be carried out by a special committee 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) The operational, organizational and professional correct functioning of the trust service provider Halcom CA shall be supervised by the internal control officer, who shall not perform any tasks related to the certificate management.

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

- employees of Halcom CA and
- RAs.

(3) The employees of the TSP Halcom CA are organised into four organisational groups covering the following subject areas:

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

Organizational group	Role	Basic tasks	Number of persons

Information system management	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	• Managing the TSP certificate process • Assist 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 • Archiving the required system records • Printing PIN codes • Daily system overview	2
	Authorization operator	• Confirmation of certificate issuing and activation of passwords generation	2
	Certification operator	• Pre-personalization of QSCDs • Certificates preparation (processing of signed certificates application forms) • Personalization (creation of certificates on a QSCD, printing 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 to monitor work • Participation and assistance in the annual audit of document inventory of subordinate TSPs	2
	Internal audit officer	• Monitoring safety rules and compliance with them • Monitoring system documentation and control logs for work control	2
Regulatory	Regulatory compliance officer	• Independent and autonomous guidance, privacy and data protection assessments • Ensuring compliance with applicable European and Slovenian regulations, international standards, and recommendations • Providing expert assistance to management and staff in the operational implementation of privacy and regulatory compliance measures	1

5.2.2 Number of persons required per task

(1) Operational roles are designed to prevent, as far as possible, the potential for abuse and are divided among individual, organisational groups:

Organizational group: Information system management

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: Information system management

Role: System administrator

Number of persons: 2

Tasks:

1. Managing the TSP certificate process
2. Assist 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 remote location
2. Administrative functions related to maintaining the TSP
3. Archiving the required system records
4. Printing PIN codes
5. Daily system overview

Organizational group: Certificates management

Role: Authorization operator

Number of persons: 2

Tasks:

1. Confirmation of certificate issuing and activation of passwords generation

Organizational group: Certificates management

Role: Certification operator

Number of persons: 2

Tasks:

1. Pre-personalization of QSCDs
2. Certificates preparation (processing of signed certificates application forms)
3. Personalization (creation of certificates on a QSCD, printing subject's data on a 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 to monitor work
3. Participation and assistance in the annual audit of document inventory of subordinate TSPs

Organizational group: Security and control

Role: Internal audit officer

Number of persons: 2

Tasks:

1. Monitoring safety rules and compliance with them
2. Monitoring system documentation and control logs for work control

Organizational group: Regulatory

Role: Regulatory compliance officer

Number of persons: 1

Tasks:

1. Independent and autonomous guidance, privacy and data protection assessments
2. Ensuring compliance with applicable European and Slovenian regulations, international standards, and recommendations
3. Providing expert assistance to management and staff 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

The authentication and access rights for the performance of individual tasks in accordance with the role of each organisational group, as well as for the performance of the tasks of the RA, are 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

For each role, Halcom CA's internal rules specify with which it may or may not be compatible. Some require the presence of at least two authorised persons. In the event of unforeseen absence of certain employees, their roles will be taken over by other employee, provided that this is not incompatible according to the internal rules.

5.3. Personnel security controls

(1) The operational, organizational and professional functioning of the Halcom CA shall be supervised by an internal audit officer, who shall not perform any tasks related to the certificate management.

(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 no proven criminal record. All personnel receive regular training and additional knowledge in their field of expertise.

5.3.2 Background check procedures

The personnel of TSP shall have appropriate qualifications and experience in accordance with the requirements of applicable regulations and technical standards and recommendations .

5.3.3 Training requirements

All necessary training shall be provided to the personnel carrying out the tasks of the above-mentioned organisational groups and the tasks of the RA .

5.3.4 Retraining frequency and requirements

Personnel shall be 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 unauthorised or negligent performance of tasks shall be applied to the authorised persons of the TSP in accordance with the applicable regulations and internal rules of the TSP Halcom CA

5.3.7 Independent contractor requirements

Any external contractors are subject to the same requirements as authorised persons of the TSP Halcom CA.

5.3.8 Documentation supplied to personnel

The authorized persons of the TSP shall be provided with all necessary documentation in accordance with their respective tasks and responsibilities.

5.4. Audit logging procedures

5.4.1 Types of events recorded

(1) The TSP Halcom CA shall regularly check and record everything that that has a significant impact on:

- infrastructure security,
- operation of all security systems and
- whether there has been any intrusion or attempted intrusion of unauthorised persons into equipment or data.

(2) The details of this shall be set out in the internal rules of the trust service provider Halcom CA in accordance with the Regulation.

5.4.2 Frequency of processing log

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

5.4.3 Retention period for audit log

Logs shall be kept for at least ten (10) years after their creation, unless a longer period is provided for by a specific law.

5.4.4 Protection of audit log

(1) The logs shall be protected in accordance with security mechanisms that ensure the highest level of security.

(2) The details shall be laid down in the internal rules of the trust service provider in accordance with the Regulation.

5.4.5 Audit log backup procedures

(1) Backups of the logs shall be carried out on a daily basis.

(2) The details shall be laid down in the internal rules of the trust service provider 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 shall be laid down in the internal rules of the trust service provider in accordance with the Regulation.

5.4.7 Notification to event-causing subject

The person causing the events does not need to be informed.

5.4.8 Vulnerability assessments

(1) The analysis of logs and the monitoring of the execution of all procedures shall be carried out regularly by authorised persons of the trust service provider or automatically by other security mechanisms on all information and communication devices under the responsibility of the trust service provider.

(2) Vulnerability assessment is based on the analysis of logs, security events and other relevant data.

(3) The details shall be laid down in the internal rules of the trust service provider in accordance with the Regulation.

5.5. Records archival

5.5.1 Types of records archived

The following materials shall be archived by TSP Halcom CA in accordance with the provisions of the applicable regulations:

- logs,
- records,
- any evidence of identity checks carried out on the subject and legal persons,
- all certificate application forms,
- certificates and certificate revocation lists,
- policies,
- CPS,
- publications and notices of the TSP Halcom CA and
- other documents in accordance with the applicable regulations.

5.5.2 Retention period for archive

(1) Long-term data relating to keys and digital certificates shall be kept for at least ten (10) years after the expiry of the certificate to which the data relates, unless a longer period is provided for by a specific law.

(2) Other long-term data shall be kept for at least ten (10) years after their creation, unless a longer period is required by a specific law.

5.5.3 Protection of archive

(1) Long-term stored data shall be stored securely.

(2) The details are laid down in the internal rules of the TSP Halcom CA, in accordance with the applicable regulations, standards and recommendations .

5.5.4 Archive backup procedures

(1) A copy of the long-term archive data shall be stored securely.

(2) The details are laid down in the internal rules of the TSP Halcom CA, in accordance with the applicable regulations, standards and recommendations.

5.5.5 Requirements for timestamping 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) The details are laid down in the internal rules of the TSP Halcom CA, in accordance with the applicable regulations, standards and recommendations.

5.5.7 Procedures to obtain and verify archive information

(1) Access to long-term data shall be restricted to authorized persons.

(2) The details are laid down in the internal rules of the TSP Halcom CA, in accordance with the applicable regulations, standards and recommendations.

5.6. Key changeover of TSP Halcom CA

In the case of a new issued certificate of the TSP Halcom CA, the procedure shall be published on the TSP Halcom CA's website.

5.7. Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

The details are laid down in the internal rules of the TSP Halcom CA, in accordance with the applicable regulations, standards and recommendations.

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

The details are laid down in the internal rules of the TSP Halcom CA, in accordance with the applicable regulations, standards and recommendations.

5.7.3 Entity private key compromise procedures

The details are laid down in the internal rules of the TSP Halcom CA, in accordance with the applicable regulations, standards and recommendations.

5.7.4 Business continuity capabilities after a disaster

The details are laid down in the internal rules of the TSP Halcom CA, in accordance with the applicable regulations, standards and recommendations.

5.8. Halcom CA or RA termination

The details are laid down in the internal rules of the TSP Halcom CA, in accordance with the applicable regulations, standards and recommendations.

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 has been created to the highest security standards in the hardware security module, in the secure environment of the Halcom CA.

(2) Subject keys are generated depending on the type of certificate according to 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

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 timestamping	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	Delivery
Root and intermediate certificates	Private key	no transfer
Advanced certificate	Private keys	delivery of QSCD by registered post
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 timestamping	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 cloud certificates, 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, the keys shall be generated by the subject. The PKCS#10 certificate request is then transferred from the subject's computer to the TSP over a secure network connection.

(4) For standard certificates, the keys shall be generated by the subject. Generation of PKCS#10 certificate request and a certificate issuance is done via Halcom CA software for certificate enrolment.

(5) For timestamping certificates, keys are generated in the hardware security module of the TSP. The PKCS#10 certificate request is transferred to TSP Halcom CA over a secure network connection.

6.1.4 CA public key delivery to relying parties

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

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

6.1.5 Key sizes

Certificate	RSA key length [bit]
Root certificate of TSP Halcom CA	G1 - Minimum 2048 G2 - Minimum 4096
Intermediate/subordinate certificate of TSP Halcom CA	G1 - Minimum 2048 G2 - Minimum 4096
Qualified digital certificate of the user	G1 - Minimum 2048 G2 - Minimum 3072

6.1.6 Public key parameters generation and quality checking

The quality of the TSP Halcom CA key parameters is assured by the software vendor through the use of quality random number generators.

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 private key of the TSP Halcom CA is used for signing certificates and the certificate revocation list, and the public key in the TSP certificate shall be used for signature validation.

(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 shall be 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

The provisions regarding the TSP Halcom CA private key access are set out in the internal rules of the TSP Halcom CA, in accordance with the applicable regulations and the CPS.

6.2.3 Private key escrow

The provisions regarding the TSP Halcom CA private key escrow are set out in the internal rules of the TSP Halcom CA, in accordance with the applicable regulations and the CPS.

6.2.4 Private key backup

The provisions regarding the TSP Halcom CA private key backup are set out in the internal rules of the TSP Halcom CA, in accordance with the applicable regulations and the CPS.

6.2.5 Private key archival

(1) Halcom CA private keys may only be copied and stored by authorised persons of the TSP Halcom CA. Backup copies of keys shall be stored with the same level of protection as keys in use.

(2) Detailed provisions regarding the TSP Halcom CA private key archiving are set out in the internal rules of the TSP Halcom CA, in accordance with the applicable regulations and the CPS.

6.2.6 Private key transfer into or from a cryptographic module

(1) Private keys for advanced certificates shall be created in a QSCD with which they are subsequently transferred to the subject of the certificate.

(2) The private keys for cloud certificates shall be 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 types of certificates shall be created and stored by the subject.

6.2.7 Private key storage on cryptographic module

(1) The private key of the TSP Halcom CA shall be 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,
- timestamping certificates are created and stored in the hardware security module.

6.2.8 Method of activating private key

(1) The procedure for activating the private key of the TSP Halcom CA shall be carried out in a secure manner in accordance with the provisions of the internal rules of the TSP Halcom CA.

(2) Halcom CA recommends that the subjects use a software environment that, upon logout or after a certain elapsed time, disables access to their private key without entering the appropriate password.

(3) The subject of a cloud signing certificate may use a qualified electronic signature service in the cloud. In such a case, the subject, or another sender on his behalf, shall transmit the electronic document to be electronically signed to the TSP Halcom CA by a secure means. The subject shall then authorise the qualified electronic signature in the cloud in a secure manner via a mobile device and using the secure procedure prescribed by the TSP Halcom CA (use of PIN and mobile security procedures). Following the subject's approval, the TSP Halcom CA shall use the subject's private key in the cloud to sign the document electronically and deliver the signed document to the subject or other sender of the document.

(4) In order to protect the confidentiality of the electronic documents, the subject, or another sender on his behalf, may request that the TSP Halcom CA does not require receipt of the entire document as described in previous paragraph, but only the hash value of such a document. In such a case, the subject shall be warned before approving the signature. By approving the signature, the subject accepts that Halcom CA does not provide any verification of the hash value calculation or

other security mechanisms in relation to the electronic document and that the responsibility rests entirely with the subject..

6.2.9 Method of deactivating private key

The procedure for deactivating the private key of the TSP Halcom CA shall be carried out in a secure manner in accordance with the provisions of the internal rules of the TSP Halcom CA.

6.2.10 Method of destroying private key

(1) The procedure for the destruction of the private key of the TSP Halcom CA shall be carried out in a secure manner in accordance with the provisions of the internal rules of the TSP Halcom CA and the instructions of the hardware security module manufacturer. The private key shall be destroyed in such a way that it cannot be restored.

(2) The destruction of private keys of subject's certificates shall be carried out by the subjects. They must use appropriate applications to safely delete certificates.

(3) The private key of a cloud certificate shall be automatically destroyed when the certificate expires. Upon request of the subject, the private key may also be destroyed by TSP Halcom CA before expiry. The private key shall be destroyed in such a way 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 shall archive 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 / public key	20 years
Intermediate (subordinate) certificate	Private / public key	10 years
Advanced certificate	Private / public key	3 years
Standard certificate	Private / public key	3 years
Cloud certificate	Private / public key	1 - 3 years
Certificate for information systems	Private / public key	3 years
Certificate for website authentication	Private / public key	1 - 3 years
Certificate for timestamping	Private / public key	5 years

(2) 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

The personal number (PIN) to use the advanced certificate and the number to unlock the QSCD (PUK) are generated on the Halcom CA site. The personal number must be changed by the subject before the first use of the certificate.

(2) Cloud certificate

The registration and activation codes for the cloud certificates are created on the Halcom CA site. During the activation process, the user sets up his/her personal number (PIN) to access the cloud certificate.

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

Subjects of standard certificates, certificates for information systems and website authentication set their own 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,
- at least 8 characters long,
- the use of words that appear in dictionaries is discouraged .

6.4.2 Activation data protection

(1) Advanced certificate

Personal number for using the advanced certificate (PIN code) and the unlock code (PUK code) to unlock the QSCD are created securely by the TSP Halcom CA. Halcom CA shall distribute both codes to the subject by registered mail, via another secure channel or, exceptionally, in person. Halcom CA recommends that both codes be kept in a secure location to which only the subject has access.

(2) Cloud certificate

The registration and activation code for the cloud certificate is created securely by the TSP Halcom CA TSP. The registration and activation code shall be send to the subject via two separate channels, one by e-mail, and the other by another secure channel. Exceptionally, one of the codes may be handed over to the subject in person by authorised persons of the RA. 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 the password for the enrolment of a standard certificate is created securely by the TSP Halcom CA. During the certificate enrolment, the subject sets his/her own password to protect access to the private keys. Halcom CA recommends that the password is not stored or is stored in a secure location 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 set their own password to protect their 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.

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

6.5.2 Computer security rating

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

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

6.6.3 Life cycle security controls

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

6.7. Network security controls

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

6.8. Timestamping

Not prescribed.

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1. Certificate profile

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

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

(2) All certificates shall include the information specified for qualified certificates in accordance with the eIDAS Regulation and the eIDAS 2.0 Regulation.

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

7.1.1 Version number(s)

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

7.1.2 Certificate extensions

The information in the certificates is listed below.

7.1.2.1 Root certificate profile

Field names	Value or meaning
Basic fields in the certificate	
Version	V3
Serial Number	G1: 0cdf9b
	G2: 6fb450b4a6bbeebb983055e81d53c040
Signature algorithm	G1: Sha256RSA
	G2: RSASSA-PSS
Issuer	G1: C=SI, O=Halcom d.d., 2.5.4.97 = VATSI-43353126 CN=Halcom Root Certificate Authority
	G2: C=SI, O=Halcom d.d., 2.5.4.97 = VATSI-43353126 CN=Halcom Root CA G2
Validity	G1: Valid from: <10.6.2016 07:07:50 GMT > Valid to: <10.6.2036 07:07:50 GMT >
	G2: Valid from: < 19.3. 2025 09:00:00 GMT> Valid to: < 19.3.2045 09:00:00 GMT>
Subject	G1: C=SI, O=Halcom d.d., 2.5.4.97 = VATSI-43353126 CN=Halcom Root Certificate Authority
	G2: C=SI, O=Halcom d.d., 2.5.4.97 = VATSI-43353126 CN=Halcom Root CA G2
Subject Public Key Algorithm	G1: RSA
	G2: RSASSA-PSS
Public Key (... bits)	module, exponent,...
Subject's public key that belongs to the corresponding pair of keys, encrypted with RSA algorithm (RSA Public Key)	G1: at least 2048 bits
	G2: at least 4096 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	G1: 42aea643c79828b0
	G2: 4e14b2790896f4b6
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	SHA1 certificate fingerprint

7.1.2.2 Intermediate certificate profiles for electronic signature

(1) Halcom CA FO e-signature 1

Field names	Value or meaning
Basic fields in the certificate	
Version	V3
Serial Number	0cecac
Signature algorithm	Sha256RSA
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	RSA
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=42aea643c79828b0

Subject Key Identifier, OID 2.5.29.14	48fb3b1399c34ece
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) Halcom CA FO e-signature 2

Field names	Value or meaning
Basic fields in the certificate	
Version	V3
Serial Number	136c17
Signature algorithm	Sha256RSA
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	RSA
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=42aea643c79828b0
Subject Key Identifier, OID 2.5.29.14	48c427a66f6ef02e
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) Halcom CA FO e-sig 1 G2

Field names	Value or meaning
Basic certificate fields	
Version	V3
Serial Number	63fde006151790064fdeecf32742e97c
Signature algorithm	RSASSA-PSS
Issuer	CN = Halcom Root CA G2 2.5.4.97 = VATSI-43353126 O = Halcom d.d. C = SI
Validity	Valid from: <25.03.2025 10:00:00 GMT > Valid to: <25.03.2035 09:00:00 GMT >
Subject	CN = Halcom CA FO e-sig 1 G2 2.5.4.97 = VATSI-43353126 O = Halcom d.d. C = SI
Subject Public Key Algorithm	RSASSA-PSS
Public Key (... bits)	module, eksponent,...
Subject's public key that belongs to the corresponding pair of keys, encrypted with RSA algorithm (RSA Public Key)	key length 4096 bitov
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=4e14b2790896f4b6
Subject Key Identifier, OID 2.5.29.14	47902d7cbd318937
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

(4) Halcom CA PO e-signature 1

Field names	Value or meaning
Basic fields in the certificate	
Version	V3
Serial Number	0cecab
Signature algorithm	Sha256RSA

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	RSA
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=42aea643c79828b0
Subject Key Identifier, OID 2.5.29.14	40f695209b79c209
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

(5) Halcom CA PO e-signature 2

Field names	Value or meaning
Basic fields in the certificate	
Version	V3
Serial Number	136c16
Signature algorithm	Sha256RSA
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	RSA
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=42aea643c79828b0
Subject Key Identifier, OID 2.5.29.14	434d32751603c975
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

(6) Halcom CA PO e-sig 1G2

Field names	Value or meaning
Basic certificate fields	
Version	V3
Serial Number	70cacd5bdedf11534925d1c8c89d22d5
Signature algorithm	RSASSA-PSS
Issuer	CN = Halcom Root CA G2 2.5.4.97 = VATSI-43353126 O = Halcom d.d. C = SI
Validity	Valid from: <25.3.2025 10:00:00 GMT> Valid to: <25.3.2035 09:00:00 GMT>
Subject	CN = Halcom CA PO e-sig 1 G2 2.5.4.97 = VATSI-43353126 O = Halcom d.d. C = SI
Subject Public Key Algorithm	RSASSA-PSS
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 4096 bits
Extensions X.509v3	
CRL Distribution Points, OID 2.5.29.31	URL=ldap://ldap.halcom.si/cn=Halcom%20Root%20CA%20G2,o=Halcom,c=SI?certificaterevocationlist;binary URL=http://domina.halcom.si/crls/halcom_root_ca_g2.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=4e14b2790896f4b6
Subject Key Identifier, OID 2.5.29.14	41753bf986c7cb9c
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

7.1.2.3 Intermediate certificate profiles for electronic seal

(1) Halcom CA PO e-seal 1

Field names	Value or meaning
Basic fields in the certificate	
Version	V3
Serial Number	0e0ed0
Signature algorithm	Sha256RSA
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	RSA
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=42aea643c79828b0
Subject Key Identifier, OID 2.5.29.14	49487650770ab10c
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) Halcom CA PO e-seal 2

Field names	Value or meaning
Basic fields in the certificate	
Version	V3
Serial Number	136c18
Signature algorithm	Sha256RSA
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	RSA
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=42aea643c79828b0
Subject Key Identifier, OID 2.5.29.14	4735c8bc61e25d9e
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) Halcom CA e-seal 1 G2

Field names	Value or meaning
Basic certificate fields	
Version	V3
Serial Number	65a0bbcece218f6ce1136d5d3ad65d43
Signature algorithm	RSASSA-PSS
Issuer	CN = Halcom Root CA G2 2.5.4.97 = VATSI-43353126 O = Halcom d.d. C = SI
Validity	Valid from: <25.03.2025 10:00:00 GMT > Valid to: <25.03.2035 09:00:00 GMT >
Subject	CN = Halcom CA e-seal 1 G2 2.5.4.97 = VATSI-43353126 O = Halcom d.d. C = SI
Subject Public Key Algorithm	RSASSA-PSS
Public Key (... bits)	module, eksponent,...
Subject's public key that belongs to the corresponding pair of keys, encrypted with RSA algorithm (RSA Public Key)	key length 4096 bits
Extensions X.509v3	
CRL Distribution Points, OID 2.5.29.31	URL=ldap://ldap.halcom.si/cn=Halcom%20Root%CA%20G2,o=Halcom,c=SI?certificaterevocationlist;binary URL=http://domina.halcom.si/crls/halcom_root_ca_g2.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=4e14b2790896f4b6
Subject Key Identifier, OID 2.5.29.14	4125fcd8fad6662f
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

7.1.2.4 Intermediate certificate profiles for website authentication

(1) Halcom CA web 1

Field names	Value or meaning
Basic fields in the certificate	
Version	V3
Serial Number	0e0ed2
Signature algorithm	Sha256RSA
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	RSA
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=42aea643c79828b0
Subject Key Identifier, OID 2.5.29.14	48420b17edae9e70
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) Halcom CA web 2

Field name	Value or meaning
Basic certificate fields	
Version	V3
Serial Number	6be5967ab71177ca1478b28751b05cbc

Signature algorithm	Sha256RSA
Issuer	CN = Halcom Root Certificate Authority 2.5.4.97 = VATSI-43353126 O = Halcom d.d. C = SI
Validity	Valid from: <25.03.2025 09:00:00 GMT > Valid to: <25.02.2035 08:00:00 GMT >
Subject	CN = Halcom CA web 2 2.5.4.97 = VATSI-43353126 O = Halcom d.d. C = SI
Subject Public Key Algorithm	RSA
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=42aea643c79828b0
Subject Key Identifier, OID 2.5.29.14	408cacc9cbc74c1f
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) Halcom CA web 1 G2

Field name	Value or meaning
Basic certificate fields	
Version	V3
Serial Number	5b8a526a57748dbaf4198edaa1a80472
Signature algorithm	RSASSA-PSS

Issuer	CN = Halcom Root CA G2 2.5.4.97 = VATSI-43353126 O = Halcom d.d. C = SI
Validity	Valid from: <25.03.2025 10:00:00 GMT > Valid to: <25.03.2035 09:00:00 GMT >
Subject	CN = Halcom CA web 1 G2 2.5.4.97 = VATSI-43353126 O = Halcom d.d. C = SI
Subject Public Key Algorithm	RSASSA-PSS
Public Key (... bits)	module, eksponent,...
Subject's public key that belongs to the corresponding pair of keys, encrypted with RSA algorithm (RSA Public Key)	key lenght 4096 bits
Extensions X.509v3	
CRL Distribution Points, OID 2.5.29.31	URL=ldap://ldap.halcom.si/cn=Halcom%20Root%20CA%20G2,o=Halcom,c=SI?certificaterevocationlist;binary URL=http://domina.halcom.si/crls/halcom_root_ca_g2.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=4e14b2790896f4b6
Subject Key Identifier, OID 2.5.29.14	4e9125213b702aca
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

7.1.2.5 Intermediate certificate profiles for timestamping

(1) Halcom CA TSA 1

Field names	Value or meaning
Basic fields in the certificate	
Version	V3
Serial Number	0e0ed1
Signature algorithm	Sha256RSA
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	RSA
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=42aea643c79828b0
Subject Key Identifier, OID 2.5.29.14	438f8b569f441ed7
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) Halcom CA TSA 2

Field names	Value or meaning
Basic fields in the certificate	
Version	V3
Serial Number	641bf7def92f969c8ca8bb049a033374
Signature algorithm	Sha256RSA
Issuer	CN = Halcom Root Certificate Authority 2.5.4.97 = VATSI-43353126 O = Halcom d.d. C = SI
Validity	Valid from: <25.3.2025 09:00:00 GMT > Valid to: <25.3.2035 08:00:00 GMT >
Subject	CN = Halcom CA TSA 2 2.5.4.97 = VATSI-43353126 O = Halcom d.d. C = SI
Subject Public Key Algorithm	RSA
Public Key (... bits)	module, eksponent,...

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=42aea643c79828b0
Subject Key Identifier, OID 2.5.29.14	4fe0e1a9216e1bbe
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) Halcom CA TSA 1 G2

Field name	Value or meaning
Basic certificate fields	
Version	V3
Serial Number	5e93f17167a040365fb93f24857e768f
Signature algorithm	RSASSA-PSS
Issuer	CN = Halcom Root CA G2 2.5.4.97 = VATSI-43353126 O = Halcom d.d. C = SI
Validity	Valid from: <25.3.2025 10:00:00 GMT > Valid to: <25.3.2035 09:00:00 GMT >
Subject	CN = Halcom CA TSA 1 G2 2.5.4.97 = VATSI-43353126 O = Halcom d.d. C = SI
Subject Public Key Algorithm	RSASSA-PSS
Public Key (... bits)	module, eksponent,...
Subject's public key that belongs to the corresponding pair of keys, encrypted with RSA algorithm (RSA Public Key)	key lenght 4096 bits
Extensions X.509v3	

CRL Distribution Points, OID 2.5.29.31	URL=ldap://ldap.halcom.si/cn=Halcom%20Root%20CA%20G2,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=4e14b2790896f4b6
Subject Key Identifier, OID 2.5.29.14	4e1fe762246a1900
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

7.1.2.6 End-user certificate profiles

Field name	Value or meaning
Basic certificate fields	
Version	V3
Serial Number	unique internal certificate number
Signature algorithm	G1: Sha256RSA
	G2: RSASSA-PSS
Issuer	distinguished name of the issuer (see sections 3.1.1 and 7.1.2.2)
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)
Algoritem za javni ključ, angl. Subject Public Key Algorithm	RSA
Javni ključ, angl. Public Key (... bits)	module, eksponent,...
Subject's public key that belongs to the corresponding pair of keys, encrypted with RSA algorithm (RSA Public Key)	Subject key lenght (see section 6.1.5) G1: at least 2048 bits
	G2: at least 3072 bits
Extensions X.509v3	
CRL Distribution Points, OID 2.5.29.31	Depends on the issuer (see section 7.2.2)
Key Usage, OID 2.5.29.15	Standard, advanced, cloud certificates and certificates for information systems: Digital Signature, Non Repudiation, Key Encipherment Certificates for website authentication: Digital Signature, Key Encipherment Certificates for timestamping: Digital Signature

Authority Key Identifier, OID 2.5.29.35	G1: Halcom CA FO e-signature 1: KeyID=48fb3b1399c34ece Halcom CA FO e-signature 2: KeyID=48c427a66f6ef02e Halcom CA PO e-signature 1: KeyID=40f695209b79c209 Halcom CA PO e-signature 2: KeyID=434d32751603c975 Halcom CA PO e-seal 1: KeyID=49487650770ab10c Halcom CA PO e-seal 2: KeyID=4735c8bc61e25d9e Halcom CA web 1: KeyID=48420b17edae9e70 Halcom CA web 2: KeyID=408cacc9cbc74c1f Halcom CA TSA 1: KeyID= 438f8b569f441ed7 Halcom CA TSA 2: KeyID= 4fe0e1a9216e1bbe
	G2: Halcom CA FO e-sig 1 G2: KeyID=47902d7cbd318937 Halcom CA PO e-sig 1 G2: KeyID=41753bf986c7cb9c Halcom CA e-seal 1 G2: KeyID=4125fcd8fad6662f Halcom CA web 1 G2: KeyID=4e9125213b702aca Halcom CA TSA 1 G2: KeyID= 4e1fe762246a1900
ESEI	Unified number of electronic identification

(4) Key usage field is marked as critical.

(5) The subject of an electronic signature certificate may hold only one valid certificate of the same type, except for the sixty (60) days before the expiry of that certificate, when the subject may renew or obtain a new certificate.

(6) The subject of a certificate for electronic sealing, information systems, website authentication and timestamping may hold more than one valid certificate.

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 subject'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 refuse a request for a certificate if it determines that the email

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 the Halcom CA shall be signed by the trust service provider using the algorithm specified in the signature algorithm value field:

- G1: sha256RSA, identifier: OID 1.2.840.113549.1.1.11 or
- G2: RSASSA-PSS, identifier: OID 1.2.840.113549.1.1.10.

(2) The full set of algorithms, data formats and protocols shall be available from authorised 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 TSP Halcom CA use 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) Halcom CA certificate revocation lists (CRLs) are located under branches:

- G1:
  - CN= Halcom CA FO e-signature 1
    O = Halcom
    C = SI

- CN= Halcom CA FO e-signature 2
  O = Halcom
  C = SI
- CN= Halcom CA PO e-signature 1
  O = Halcom
  C = SI
- CN= Halcom CA PO e-signature 2
  O = Halcom
  C = SI
- CN= Halcom CA PO e-seal 1
  O = Halcom
  C = SI
- CN= Halcom CA PO e-seal 2
  O = Halcom
  C = SI
- CN= Halcom CA web 1
  O = Halcom
  C = SI
- CN= Halcom CA web 2
  O = Halcom
  C = SI
- CN= Halcom CA TSA 1
  O = Halcom
  C = SI
- CN= Halcom CA TSA 2
  O = Halcom
  C = SI

- G2:
  - CN= Halcom CA FO e-sig 1 G2
    O = Halcom
    C = SI
  - CN= Halcom CA PO e-sig 1 G2
    O = Halcom
    C = SI
  - CN= Halcom CA e-seal 1G2
    O = Halcom
    C = SI
  - CN= Halcom CA web 1 G2
    O = Halcom
    C = SI
  - CN= Halcom CA TSA 1 G2
    O = Halcom
    C = SI

(2) The register of revoked intermediate/subordinate certificates shall be updated at least once a year, while the other CRLs shall be refreshed after each revocation of the certificate or at least once a day, if there are no new entries or changes in the CRL (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 shall comply with ITU-T Recommendation for X.509 (2005) and ISO / IEC 9594-8: 2014.

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

- via LDAP protocol and
- via HTTP protocol.

7.2.2 CRL and CRL entry extensions

(1) The CRL shall contain, in addition to other information in accordance with the X.509 Recommendation (the basic fields and extensions are detailed in the table below):

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

7.2.2.1 Root CRL (CRL of intermediate certificates)

Field name	Value or meaning
Basic fields in CRL	
Version	V2
Signature Algorithm	G1: Sha256RSA
	G2: RSASSA-PSS
Signature	podpis Halcom CA
Issuer	G1: CN = Halcom Root Certificate Authority 2.5.4.97 = VATSI-43353126 O = Halcom d.d. C = SI
	G2: CN = Halcom Root CA G2 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)	G1: Halcom Root Certificate Authority: KeyID=42aea643c79828b0
	G2: Halcom Root CA G2: KeyID=4e14b2790896f4b6
issuerAltName (OID 2.5.28.18)	not applicable

deltaCRLindicator (OID 2.5.29.27)	not applicable
issuingDistribuitionPoint (OID 2.5.29.28)	not applicable

7.2.2.2 Intermediate CRLs (CRLs of end-user certificates)

Field name	Value or meaning
Basic fields in CRL	
Version	V2
Signature Algorithm	G1: Sha256RSA
	G2: RSASSA-PSS
Signature	Halcom CA signature
Issuer	Distinguished name of the issuer (see sections 3.1.1 and 7.1.2.2)
Time of issue of CRL (thisUpdate)	Effective date: < time of issue by GMT>
Time of issue of next CRL (nextUpdate)	Effective date: < time of issue by GMT>
Identification of revoked certificates and time of revocation (revokedCertificate)	Next Update: < time of next issue by GMT>
Extensions X.509v2 CRL	
CRL list number	Serial number of CRL list
Authority Key Identifier (OID 2.5.29.35)	G1: Halcom CA FO e-signature 1: KeyID=48fb3b1399c34ece Halcom CA FO e-signature 2: KeyID=48c427a66f6ef02e Halcom CA PO e-signature 1: KeyID=40f695209b79c209 Halcom CA PO e-signature 2: KeyID=434d32751603c975 Halcom CA PO e-seal 1: KeyID=49487650770ab10c Halcom CA PO e-seal 2: KeyID=4735c8bc61e25d9e Halcom CA web 1: KeyID=48420b17edae9e70 Halcom CA web 2: KeyID=408cacc9cbc74c1f Halcom CA TSA 1: KeyID= 438f8b569f441ed7 Halcom CA TSA 2: KeyID= 4fe0e1a9216e1bbe
	G2: Halcom CA PO e-sig 1 G2: KeyID=41753bf986c7cb9c Halcom CA e-seal 1 G2: KeyID=4125fcd8fad6662f Halcom CA web 1 G2: KeyID=4e9125213b702aca Halcom CA FO e-sig 1 G2: KeyID=47902d7cbd318937 Halcom CA TSA 1 G2: KeyID= 4e1fe762246a1900
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

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

7.3. OCSP profile

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

(2) The OCSP (request/response) message profile of the shall be 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 shall have an internal audit officer with appropriate technological and legal skills. Internal audit officer shall not perform tasks related to the management of certificates.

(2) The internal audit officer supervises the work of Halcom CA. In the event of deficiencies being detected, he/she shall order appropriate measures to be taken by Halcom CA to remedy such deficiencies. Halcom CA shall be obliged to carry out the measures under the supervision of internal audit officer.

(3) TSP Halcom CA shall be subject to an external independent audit once a year by an accredited body.

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

8.1. Frequency or circumstances of assessment

(1) The internal audit officer shall carry out an audit at least once a year.

(2) The external auditor for ISO 9001 and ISO 27001 shall carry out an audit once a year.

(3) The external auditor for ETSI standards shall carry out an audit 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 auditor shall have the appropriate technological and legal knowledge.

8.3. Assessor's relationship to assessed entity

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

(2) The external auditor shall 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 being identified, the internal/external officer/auditor shall order appropriate measures to remedy the deficiencies, which Halcom CA shall be obliged to implement, under their supervision. The detailed implementation of the measures shall be set out in the internal rules of the TSP Halcom CA.

8.6. Communication of results

The results of the assessments shall be kept by the TSP Halcom CA.

9. Other Business and Legal Matters

9.1 Fees

Halcom CA shall establish a price list for the use of the certificates, its services, the necessary equipment and infrastructure and publish the price list on its website

9.1.1 Certificate Issuance or Renewal Fees

The prices of certificate issuance and renewal is set out in the current price list.

9.1.2 Certificate Access Fees

Access to the public certificate directory shall be free of charge, unless otherwise agreed by the parties.

9.1.3 Revocation or Status information access fees

The CRL is accessible free of charge to all persons.

9.1.4 Fees for Other Services

The prices for other services, equipment and infrastructure are set in the current price list .

9.1.5 Refund Policy

Not prescribed.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

Halcom CA has adequate liability insurance. More detailed information 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 following information shall be treated confidentially by the TSP Halcom CA :

- all certificate or other application forms,
- any confidential information regarding financial liabilities,
- any confidential information that may be 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) The TSP Halcom CA shall handle all potentially confidential information about subjects and third parties that is necessary for the certificate management services in accordance with the applicable legislation.

9.3.2 Information Not Within the Scope of Confidential Information

The TSP Halcom CA shall make publicly available only business information that is not of a confidential nature under applicable law.

9.3.3 Responsibility to Protect Confidential Information

(1) Halcom CA assumes no responsibility for the content of the data electronically encrypted or signed/sealed by the certificate subject, even if the certificate subject or a third party has complied with all applicable regulations, all provisions of Halcom CA's policies and other rules, or has followed all of Halcom CA's instructions.

(2) Halcom CA accepts no responsibility for any consequences arising from the certificate subject's failure to comply with the security requirements set out in clause 4.5.1 of the CPS.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

Halcom CA carefully protects personal data in accordance with applicable 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 in the relevant registries to prove the identity of the subject or while performing trust services.

(2) The data in certificates and the CRL shall, by the nature of the use of the certificates and the provisions of the applicable regulations and standards, be accessible to third parties relying on the certificates or verifying their validity.

9.4.3 Information Not Deemed Private

There is no other potentially unsecured personal data other than that contained in the certificate and the 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 regulation 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, with specific written consent for the processing of personal data, or subsequently in another written form.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

(1) The TSP Halcom CA shall not disclose any other information about the certificate subjects other than that specified in the certificate, unless the specified information is specifically required for the provision of specific services or applications related to the certificates, and the TSP Halcom CA is authorised to do so (see previous section), or at the request of a competent court, prosecuting, law enforcement, administrative authority or other authorised person. Any such request shall be carefully verified by TSP Halcom CA and the information shall be provided only to the extent necessary and as required by applicable law.

(2) The data shall be provided 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

Provisions on copyright, related and other intellectual property rights :

- all rights related to the private key belong to the subject of the certificate,
- all rights related to the public keys, all certificate data, the directory of certificates, 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 shall:

- comply with its internal rules and other applicable regulations,
- act in line with international recommendations,
- publish all relevant documents that determine its operation (policies, certificate application forms, revocation requests, price lists, instructions for the secure use of qualified digital

certificates, etc.),

- publish on its website all information on those changes to the activities of the trust service provider which affect subjects and third parties in any way,
- ensure that the RA services operate in accordance with the HALCOM CA and other applicable regulations,
- comply with the provisions on the secure handling of personal and confidential information about the TSP, certificate subjects or third parties,
- revoke a certificate and publish it on CRL when it determines that grounds under this Policy or other applicable law exist,
- issue qualified digital certificates in accordance with this CPS and other regulations and recommendations.

(2) The TSP Halcom CA shall also:

- ensure the accuracy of the information on the certificates issued,
- ensure the correct publication of the CRLs,
- ensure the uniqueness of distinguishing names,
- ensure adequate physical security of the premises and access to the premises of the TSP itself,
- professionally ensure the continuous functioning and maximum availability of the services,
- professionally assure the maximum accessibility of services,
- professionally manage the continuous functioning of all other ancillary services,
- with the best effort eliminate any problems encountered in the shortest possible time,
- optimise hardware and software,
- keep users informed on important matters; and
- comply with all other requirements under this CPS.

(3) The TSP Halcom CA shall ensure that its services are available as much as possible, at all times 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 infrastructure as a result of unforeseen breakdowns,
- technical or service interventions due to infrastructure failure outside the remit of The TSP Halcom CA; and
- unavailability as a result of force majeure or an emergency.

(4) TSP Halcom CA shall announce maintenance or upgrading of the infrastructure at least three (3) days before the work is to commence.

(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 obligations or responsibilities of the TSP Halcom CA shall be determined by any mutual agreement with a third party.

9.6.2 RA Representations and Warranties

(1) The RA shall:

- verify the identity of subjects or prospective subjects,
- accept certificate application form for Halcom CA services,
- verify certificate application form,
- issue the necessary documentation to legal persons, subjects or prospective subjects,
- transmit requests and other data in a secure manner to Halcom CA.

(2) The RA is responsible for implementing all provisions of the CPS, policies and other requirements agreed with the TSP Halcom CA.

9.6.3 Subscriber Representations and Warranties

(1) A legal person shall be responsible for:

- the damage caused in the event of misuse of the certificate from the time the revocation is reported until the revocation is made,
- any damage caused, directly or indirectly, by allowing the use or misuse of the certificate subject's certificate by unauthorised persons,
- any other damages arising out of your failure to comply with the provisions of the CPS, Halcom CA's policies and other notices and 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) When using Halcom CA certificates for the first time, the third party relying on the certificate shall carefully read the policy and from then on regularly monitor all Halcom CA notifications.

(2) The third party shall, at all times during the use of the certificate, check carefully that the certificate is not on the CRL.

(3) If the certificate contains information about a third party, the third party shall be obliged to request the revocation of the certificate if it becomes aware that the private key has been compromised in a way that affects the reliability of use, or if there is a risk of misuse, or if the information contained in the certificate has changed.

(4) A third party may rely on such a certificate until it is revoked.

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

9.6.5 Representations and Warranties of Other Participants

Not prescribed.

9.7 Disclaimers of Warranties

TSP Halcom CA shall not be liable for any damages arising from:

- use the certificates for a purpose and in a manner not expressly provided for in this CPS,
- improper or inadequate security of passwords or private keys of subjects, the release of confidential information or keys to third parties and irresponsible behaviour by the subject,
- misuse or hacking of the certificate subject's information system and thus access to certificate data by unauthorised persons,
- malfunctioning of the subject's or third parties' IT infrastructure,
- not validating the data and validity of certificates in CRL,
- not checking the validity period of the certificate,
- conduct of certificate subject or third party in contravention of Halcom CA notices, CPS, policies and other regulations,
- allowing unauthorised persons to use or misuse the subject's certificate,
- a certificate issued with false data and inauthentic data, or other actions by the subject or TSP,
- the use of certificates and the validity of certificates in the event of changes to certificate data, email addresses or changes to the names of subjects,
- infrastructure failure outside the domain of the TSP Halcom CA,
- data encrypted or signed using certificates,
- the subject's conduct in using the certificates, even if the subject or a third party has complied with all the provisions of this CPS, the Halcom CA notices or other applicable regulations,
- the use and reliability of the hardware and software of certificate subjects,
- errors in hash value calculation, hash value verification or other security procedures with respect to the electronic document to be signed, if the subject has requested a cloud signature based solely on the hash value and without submitting the entire electronic document to the TSP.

9.8 Limitations of Liability

Not prescribed.

9.9 Indemnities

The party who caused the damage by failing to comply with the provisions of the CPS and applicable law shall be liable for the damage.

9.10 Term and Termination

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

(2) The CPS shall enter into force on the date of its acceptance by Halcom CA.

9.10.1 Term

The new version or changes to the CPS shall be published eight (8) days in advance on the website of the TSP Halcom CA, indicating the date of entry into force of the CPS.

9.10.2 Termination

(1) Upon publication of the new CPS and the policies, all certificates issued under the policies shall remain subject to those provisions which cannot reasonably be replaced by corresponding provisions under the new policies (e.g. the procedure specifying the method under which the certificate was issued, etc.).

(2) The TSP may issue supplements to individual provisions of the CPS as set out in section 9.12.

9.10.3 Effect of Termination and Survival

(1) The validity of certificates shall be 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 valid until their expiry date and shall, where possible, be treated under the new policy.

9.11 Individual Notices and Communications with Participants

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

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

(3) The contact details of third parties shall be provided in any mutual agreement between the third party and the TSP 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, if there are no significant changes in the operation 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 shall be determined by the TSP Halcom CA.

9.12.2 Notification Mechanism and Period

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

(2) Amendments and supplements 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 from 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 of competent jurisdiction 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) The competent supervisory body and conformity assessment bodies shall supervise the compliance of the TSP Halcom CA with the applicable legislation and regulations.

(2) Halcom CA shall be audited by an accredited conformity assessment body at least every twenty-four (24) months. The purpose of the audit is to confirm whether the TSP and the services it provides comply with the legal requirements.

(3) The internal compliance audit shall be performed by authorised persons within the Halcom CA trust service provider.

9.16 Miscellaneous Provisions

(1) The TSP Halcom CA may conclude mutual agreements with other entities, if this is required by applicable law or other regulations .

(2) If any of the provisions of this CPS is or becomes invalid, the remaining provisions shall not be affected. The invalid provision shall be replaced by a valid one, which shall be as far as possible correspond to the previous one.

9.17 Other Provisions

Not prescribed.

Place and date:
Ljubljana, 26.5.2025

CEO
Gregor Pelhan