Request for obtaining digital certificate for plenipotentiary

1. Order

Choose your security device

SMART CARD

USB KEY

2. Personal data of the plenipotentiary (all data is mandatory)

Name: _____ Surname: _____

Personal tax No.: _____ Date of birth: _____

Place of residence: _____

Personal E-mail: _____ Mobile phone No.: _____

PLEASE PROVIDE US WITH A COPY OF IDENTIFICATION DOCUMENT (ID)

Type of ID: _____ Issuer of ID: _____

ID No.: _____ Validity of ID: _____

In addition to the Halcom CA trust services provider data, the digital certificate shall include data on the request for obtaining digital certificate for a plenipotentiary in accordance with the latest applicable Halcom CA Policy for an advanced qualified digital certificate - on a smart card or USB key or for a standard qualified digital certificate in a cloud (http://www.halcom.com).

The data contained in the qualified digital certificate will be published in the register of issued digital certificates in accordance with the Halcom CA Policy. For data protection purposes, only the register of revoked certificates is publicly available. Access to the directory of issued certificates is only allowed to authorized users who check larger number of issued certificates. Data processing and protection is specifically regulated in the Halcom CA Data Protection Rules and is a subject to the special consent of the future holder. Due to the requirements of applicable regulations, security of legal transactions and technological requirements, it is unfortunately not possible to issue a qualified digital certificate without consent related to data processing and protection.

By signing, I guarantee the authenticity of the provided data. In addition, I agree to immediately notify Halcom CA for any change in the data that could affect the validity of the certificate. I confirm that I have signed the consent for data processing and protection in accordance with the Halcom CA Data Protection Rules and that I acknowledge the content of the Halcom CA Policy and the content of the notice to users of Halcom CA qualified certificates and declare that I will act accordingly.

PIN/PUK code for smart card or USB key will be sent to your personal e-mail address. Please check the correctness of the personal email address entered above. _____

☐ I would like to receive the created smart cards or USB keys to the other address, below:

_____

Place and date	Plenipotentiary signature	Legal representative (IN CAPITALS) signature and stamp of the company

The identification document of legal representative and the data in the request was verified by:

Name and surname (IN CAPITALS)	Phone	Legal entity (unit, stamp)	Signature	Date

Consent for the processing of personal data

I, the undersigned, am acquainted, that Halcom d.d., Dunajska cesta 123, Ljubljana is obliged to process my personal data for the purposes of safety and trust in e-business as qualified trust service provider and data controller in line with the provisions of the applicable regulations, in particular Regulation (EU) No. 910/2014 of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93 / EC (the Regulation eIDAS), General Data Protection Regulation (GDPR) and based on contracts with subscribers of qualified digital certificates or trust services and Data Protection Policy, published on website www.halcom.com. Halcom is a qualified trust service provider and registered in the trust list published by the European Commission.

For the purpose of security of electronic business and in accordance with legislation on trust services Halcom is checking the correctness of personal data against public records, managed by government bodies, or make inquiries with other data controllers to obtain personal data you have not submitted and are necessary to implement your purchase order and issue a qualified certificate or provide other Halcom trust service. When served with a reasonable and lawful demand, Halcom is obliged to provide your personal data to domestic or foreign government bodies, other public authorities, public service providers or alternative dispute resolution bodies. For the purposes of the safe and user-friendly electronic signing in the cloud, Halcom in addition to data on digital certificates and trust services also processes data and documents regarding electronic signatures in the cloud when you use such services.

I give my explicit written consent for the processing of my personal data and allow Halcom d.d., Dunajska cesta 123, Ljubljana, to process, use and store for a definite period my personal data and make data contained in the digital certificate publicly available in Directory of issued digital certificates in accordance with trust services policies. Based on this your explicit consent Halcom provides entities with whom you do business electronically (e.g., banks, insurance companies, major companies, government departments and others) with access to your certificate in the directory and publicly available information contained within and provides information on identification and verification process to the partners providing related services (e.g., electronic identification, electronic signatures, electronic banking, mobile payments) if you agree to this when using their service and insofar as the applicable legislation require mandatory identification.

I am acquainted that I can cancel my consent at any time in writing. However, such cancellation may impact the validity of the qualified certificate or provision of trust services. Likewise, the withdrawal of consent does not affect the storage of information, prescribed as mandatory by applicable legislation.

All other information not contained in the digital certificate is strictly protected and not made public, in accordance with data protection rules and used exclusively for the purposes of secure electronic banking and electronic commerce, and not used for any other purposes.

Personal data concerning digital certificates and trust services are kept in accordance with European (ETSI) standards for 10 years after the expiry of certificates. Other data is stored up to 6 years after the termination of the contractual relationship unless applicable legislation provides otherwise on data retention.

All information on personal data protection is available at www.halcom.com. Any questions and issues related to exercising rights (giving or withdrawal of consent, insight into own personal data, monitoring access to personal data and similar) can be addressed to the Privacy and Regulatory Consistency Commissioner at Halcom CA (Halcom d.d., Halcom CA, Dunajska cesta 123, 1000 Ljubljana, Slovenia. Phone: 01 200 34 86, E-mail: ca@halcom.si).

Place and date

Signature of plenipotentiary person