# REQUEST for obtaining digital certificate for plenipotentiary

1. **Choose your security device:**  SMART CARD or  USB KEY

2. **Personal data of the plenipotentiary**

Name: _____ Surname: _____

Personal tax No.: _____ Date of birth: _____

Place of residence: _____

Identification document No.: _____ Issuer of the Identification document: _____

E-mail address: _____ Telephone No.: _____

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 - a smart card or USB key, or for a standard qualified digital certificate in a cloud (http://www.halcom.si).

The data included in the qualified digital certificate will be published in the register of issued digital certificates, in compliance with the Halcom CA Policy. Data processing and protection is specifically regulated by Halcom CA's Privacy Policy, and is subject to the separate consent of future holder of the legal entity. Due to the requirements of the applicable regulations, the security of legal transactions and technological requirements, the issuance of qualified digital certificates is unfortunately not possible without such a consent related to data processing and protection.

I, the undersigned, guarantee the authenticity of the provided data. In addition, I agree to submit without delay any change of data that could affect the validity of the certificate. I confirm that I have signed a consent for the processing and protection of data, in accordance with the Privacy Policy of Halcom CA, and acknowledge the contents of the Halcom CA Policy and the note for the users of qualified certificates of Halcom CA, stating that I will act accordingly.

☐ **Digital certificates on smart cards or USB keys shall be sent to our official address.**

☐ **Digital certificates on smart cards or USB keys shall be sent to address listed 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:** _____ (in capitals) **from** _____ (stamp of the company)

**Signature:** _____

**Stamp and date:** _____

**3. Issued digital certificate data (filled in by Halcom-CA)**

Certificate serial No.: _____

Smart card No.: _____

Certificate issue date: _____

Name and surname of the plenipotentiary: _____

Request received by: _____

Plenipotentiary signature: _____

Addition to form: _____

# CONSENT FOR THE PROCESSING OF PERSONAL DATA

I, the undersigned, give my explicit written consent for the processing of my personal data and allow Halcom d.d. (hereinafter: Halcom CA) to process, use and store for a definite period my personal data as a future, present or past holder of a qualified digital certificate for e-signature, or as a person who represents or is empowered by the legal entity that ordered the qualified certificate for e-signature, e-seal or another trust service. Detailed rules have been defined in Halcom CA's Privacy Policy and the policies of Halcom CA, which are published on the website of Halcom CA.

Halcom CA may verify the accuracy of my data with governmental authorities who administrate public registers, or they may investigate my personal data with the administrators of other databases, with reference to data that was not provided but is needed to satisfy the operational purpose, in accordance with the order for the issue of a qualified certificate or another trust service of Halcom CA.

The data included in the qualified certificate will be published in the register of issued digital certificates, pursuant to the Halcom CA Policy. Any other data that is not included in the digital certificate and has not been published will be strictly protected under the data protection regulations and will not be used for any purposes other than those agreed on. In the case of a justified and legitimate request, personal data can be forwarded to local and foreign national authorities, holders of a public authorisation, public service operators or parties in an out-of-court settlement resolution. I acknowledge that my given consent can be withdrawn at any time in writing, which can affect the validity of the qualified certificate or the performance of trust services.

The processing of personal data shall last from the start of the procedure up to 10 years after the expiry of the issued qualified certificate, or after the end of the procedure if the certificate was not issued, except when the existing legislation requires otherwise.

Halcom CA implements adequate technical and organisational measures to guarantee a high level of personal data security and protection of the rights of persons to whom the data refer, and its IT systems respect the principles of default privacy.

All information on personal data protection is available at http://www.halcom.si. 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, Tržaška cesta 118, 1000 Ljubljana, Slovenia. Phone: 01 200 34 86. Fax: 01 200 33 60. E-mail: ca@halcom.si).

Place and date: _____

Plenipotentiary signature: _____