Document number: 800404-9-0/26
Ljubljana, October 2026

Hal E-Bank Security Statement

for End Users

1. Purpose of This Statement

This public statement is intended for companies and individuals that use the Hal E-Bank family of products and need general information about the security of the solution, including for internal risk management, audits or regulatory obligations such as NIS2 or DORA.

This public statement provides a high-level overview for Hal E-Bank users and explains where more detailed questions should be directed.

Hal E-Bank services are provided to banks under contractual agreements. Your contractual relationship for the e-banking service is with your bank (or with each bank whose accounts you manage in Hal E-Bank) not with Halcom. Each bank holds your accounts, executes your payments and remains responsible for the service it provides to you. Therefore, questions about accounts, transactions, personal data, service availability and incidents affecting your account should be directed to your bank.

Halcom provides the Hal E-Bank application and acts as an ICT service provider to these banks. Detailed technical and operational security information is confidential and is shared with banks under those agreements.

2. Roles and Responsibilities

Your bank – provides the e-banking service to you, is responsible for your accounts and payments, and is the controller of the personal data processed in e-banking. If you use Hal E-Bank for accounts at several banks, each bank is responsible for its own accounts and services.

Halcom – develops the Hal E-Bank software which you use, and, where agreed with a bank, jointly operates that bank's e-banking infrastructure. As a qualified trust service provider (Halcom CA), Halcom also issues the qualified digital certificates used to log in and sign payment orders. Questions about installing and using the Hal E-Bank client software and about Halcom digital certificates can be directed to Halcom.

You (client) – are responsible for protecting your credentials and the environment in which the solution is installed (e.g. devices and workstations), as described in section 5.

3. How Hal E-Bank Protects Your Data and Payments

Hal E-Bank family of products are designed to ensure the integrity, authenticity, confidentiality and non-repudiation of e-banking data. The key security measures are:

Strong customer authentication – access to accounts and authorization of payments require strong customer authentication in line with PSD2. Hal E-Bank uses a qualified digital certificate stored on a smart card or USB key together with the corresponding PIN.

Protected private keys – the private key on a smart card or USB key cannot be extracted from the device and is protected by a PIN; the device locks after repeated incorrect PIN entries.

Digital signatures and dynamic linking – payment orders are digitally signed, and each authorization is linked to the amount and payee of the payment, so orders cannot be altered without detection.

Encryption – data exchanged between you, Halcom and your bank is encrypted in transit at every stage using modern cryptographic algorithms; web access uses TLS 1.2 or higher.

Restricted access – access to client data is restricted to persons authorized by the bank and to authorized Halcom personnel where access is required for approved technical interventions. Halcom personnel use strong authentication, and system access is logged and subject to review.

Secure operations – systems operated by Halcom are hosted in physically secured facilities that meet internationally recognised standards, including 24-hour monitoring, redundant power and communication links, and a geographically separate disaster recovery site.

Privacy by design – processing of personal data is logged, and data minimisation, pseudonymisation and encryption are applied to operational logs, in line with the GDPR.

Incident management and continuity – Halcom monitors its systems for security events and handles incidents under a defined incident management process. Incidents affecting the service are reported to the affected banks, which inform their clients where required. Business continuity and disaster recovery arrangements are tested regularly.

Secure development – Hal E-Bank is developed under a secure software development process that includes security testing before release. Installation packages and updates are digitally signed by Halcom so that their origin and integrity can be verified.

4. Certifications and Regulatory Framework

ISO/IEC 27001:2022 – Halcom's information security management system has been certified against ISO/IEC 27001 since 2010, is currently certified to ISO/IEC 27001:2022 and is audited every year by independent and certified auditor.

ISO 9001:2015 – Halcom's quality management system is certified to ISO 9001:2015.

eIDAS – Halcom CA is a qualified trust service provider under Regulation (EU) No 910/2014 (eIDAS).

PSD2 – Hal E-Bank supports strong customer authentication and dynamic linking as required by the PSD2 Regulatory Technical Standards. Compliance with PSD2 RTS is audited on an annual basis by accredited auditors.

GDPR – Hal E-Bank supports banks, as data controllers, in meeting their obligations under Regulation (EU) 2016/679, including logging of personal data processing.

DORA – as an ICT third-party service provider to financial entities, Halcom supports banks in meeting applicable contractual, monitoring and testing requirements under Regulation (EU) 2022/2554 (DORA).

Copies of current certificates are available from Halcom web site.

5. Your Security Responsibilities

E-banking security is shared between the bank, Halcom and you. To keep your e-banking secure:

- Keep your PIN and other credentials secret. Never store them with your smart card or USB key, and do not share your card, key or credentials with anyone.
- Remove the smart card or USB key from the device when you are not using e-banking.
- Use an operating system supported by both its vendor and the applicable Hal E-Bank version, and install current security updates and anti-malware protection.
- Install updates to Hal E-Bank and the certificate security software promptly, and download software only from official Halcom or bank sources.
- Check payment details carefully before signing, and never sign orders you did not prepare or do not recognise.
- Be alert to requests to reveal confidential information. Neither Halcom nor your bank will ask you to disclose your PIN or password by e-mail, text message or phone. Do not approve login or payment requests that you did not initiate without verifying where the request came from.
- For companies: use multi-user authorization for payments, grant access rights on a least-privilege basis and remove the rights of users who leave or no longer need access.
- If your smart card or USB key is lost or stolen, or you suspect misuse, revoke the certificate at Halcom CA immediately and notify your bank.
- Do not turn off or disable security mechanisms in the application or on your device.
- Include the workstation on which Hal E-Bank is installed in your own backup.
- Access-control arrangements. **Be extremely careful about whom you allow to access your workstation physical or remotely.**

6. Software Updates and Vulnerability Management

Halcom continuously maintains Hal E-Bank family of products through security testing, monitoring and remediation of identified vulnerabilities. Security updates are delivered through the application update mechanism or through your bank. Applications and the supporting infrastructure undergo regular penetration testing and security reviews, including those conducted by independent experts.

Suspected security vulnerabilities should be reported to vulnerabilities@halcom.com. Reports are handled confidentially and, where necessary, in coordination with the affected banks.

Please find more details on how to report a vulnerability in our Responsible Disclosure Policy.

7. Supplier and Security Questionnaires

Because the e-banking service is provided under your agreement with your bank, and the EULA covers only your use of the Hal E-Bank software, Halcom cannot complete individual security questionnaires or disclose confidential details of its infrastructure, controls or audit results to end users.

We recommend that you:

- use this statement and Halcom's certificates as evidence for Halcom as part of your supply chain assessment evidence;
- record each bank as the supplier of its e-banking service, and Halcom as the provider of the Hal E-Bank application and an ICT service provider to those banks (a fourth party from your perspective for the e-banking service);

- direct further questions about the e-banking service to your bank, which assesses and oversees Halcom as its ICT service provider;
- contact Halcom directly only for questions about the Hal E-Bank client software licence and Halcom digital certificates, where you have a direct relationship with Halcom.

8. Contact

Halcom Helpdesk
Slovenia: +386 1 200 33 69, helpdesk@halcom.si, (workdays 8:00–16:30)
Serbia: + 381 11 303 24 32, helpdesk@halcom.rs, (workday 08:00 – 17:00)
Bosnia and Herzegovina: + 387 33 263 064, helpdesk@halcom.ba, (workdays 8:00–16:00)
Albania: contact your bank

Halcom second level support: for customer speciality agreed in agreement support@halcom.si

Contact for reporting security vulnerabilities: vulnerabilities@halcom.com

Halcom Headquarters
Halcom d.d., Dunajska cesta 123, 1000 Ljubljana, Slovenia

CEO

Gregor Pelhan