HUNGUARD

CERTIFICATE

HUNGUARD Informatics and IT R&D and General Service Provider Ltd. (6 Kékgolyó str. Budapest 1123 Hungary) as a certification authority accredited by the accreditation document No. NAH-6-0048/2023 of National Accreditation Authority by applying the certification system HUNG_TMK-2-eIDAS_20230710 **certifies,** that

the qualified certificate issuing trust service system

provided by FaceKom Services Zrt.

as an electronic information system applied for trust services according to 910/2014/EU regulation in relation to electronic signatures and infrastructures

complies

with the ETSI EN 319 411-2 V2.4.1 (2021-11) Policy and security requirements for Trust Service Providers issuing certificates;
Part 2: Requirements for trust service providers issuing EU qualified certificates European Standard.
This certificate has been issued on the basis of the Certification report
HUNG-TJ-ESIGN-R-024-2023

Produced on commission for FaceKom Services Zrt.
(*3 Deák Ferenc Square, Budapest, 1052 Hungary*)

Certificate registration number: **HUNG-T-ESIGN-R-024-2023**
Validity start date of the certificate: 28 December, 2023
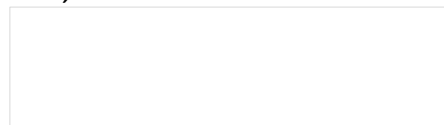Validity end date of the certificate: 28 December, 2025

This Certificate has six pages including the Annexes containing validity terms and other attributes.

Budapest, 28 December, 2023

PH.

Endrődi Zsolt Attila
Certification director

Szűcs Ákos Balázs
Managing director

HUNGUARD

Annex 1

Validity terms of the certificate

1 The trust service where the certified electronic information system applied in based on:

Category of Service [1]:	Qualified certificate issuing trust service http://uri.etsi.org/TrstSvc/Svctype/CA/QC Certificate validity status information service issuing Online Certificate Status Protocol (OCSP) http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP/QC Certificate validity status information services issuing and signing Certificate Revocation Lists (CRLs) http://uri.etsi.org/TrstSvc/Svctype/Certstatus/CRL/QC
Name of Service:	Qualified certificate issuing trust service for electronic signature
Identifiers of Trusted Service Policy:	OID: 1.3.6.1.4.1.59035.1.1.4.20231215
Type of certificate policies:[2]	QCP-n-qscd, NCP+
Identifier of Practice Statement of Trusted Service:	OID: 1.3.6.1.4.1.59035.1.1.6.20231215

Root certification unit: FaceKom Root CA 2023	Subject: C=HU, O= FaceKom Services Zrt., CN= **FaceKom Root CA 2023**
	
	Issuer C=HU, O= FaceKom Services Zrt., CN= **FaceKom Root CA 2023**
	
	SHA-256 lenyomatok:
	
	`17CE6B842E343C172116DD58AC348B60`
	`DA52BA7158BA071D62E172620413552B`

Productive certification unit:	Subject: C=HU, O= FaceKom Services Zrt., CN= **FaceKom QTSP CA 2023** Issuer: C=HU, O= FaceKom Services Zrt., CN= FaceKom Root CA 2023

---

1 Based on ETSI TS 119 612 V2.2.1 (2016-04) 5.5.1.1 chapter

2 Based on ETSI EN 319 411-2 V2.4.1 (2021-11) 5.3 chapter

2 Review of the system evaluation must be enforced in the following cases in order to confirm the results of the initial system evaluation certified in this document, to maintain the validity of certificate:

- once a year in the validity period of the Certificate (planned system evaluation review),
- responding to the main modifications in the system architecture or functionality (special).

3 Significant changes in the architecture or functionality of the system under operation must be reported by the Customer to the Certifier within 30 days after the modification went into operation. Furthermore, the Customer must send the documentation of the change in detail, which are commensurate with the former evaluation level. The Certifier evaluates the effects of the modification and decides on the necessity of a special system evaluation review in order to maintain the certificate validity.

4 When compliance is achieved, the Certifier fills out a Certificate Maintenance Record for the actual system state. The Customer must provide the terms of the planned or special system evaluation review.

Annex 2

Document containing the requirements

ETSI EN 319 411-2 V2.4.1 (2021-11) Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates

ETSI EN 319 411-1 V1.3.1 (2021-05) Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements

ETSI EN 319 401 V2.3.1 (2021-05) Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers

Annex 3

Further features of the certification

This certificate based on contract signed on 09 June 2022 and the assessment started on 04 September 2023. This certificate has been issued according to the following:

- Evaluation report for Facekom Sevices Zrt as a qualified trusted service provider based on ETSI EN 319 401 V2.3.1 (2021-05) standard CA089-01_P-2023-ÉJ1

- Evaluation report for Facekom Sevices Zrt as a qualified trusted service provider qualified certificate issuance service based on ETSI EN 319 411-2 V2.4.1 (2021-11) standard CA089-01_P-2023-ÉJ2

Locations of assessment:

Central Site with offices, location of RA activities	1052 Budapest, Deák Ferenc tér 3.
Rackforest serverroom	1132 Budapest, Budapest, Victor Hugo u. 11-5. emelet, 1132 2,5 km away from central site
Rackforest (Dataplex) serverroom	1087 Budapest, Asztalos Sándor út 13. 5 km away from central site

Considered laws

REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

2015 CCXXII. law the general rules of electronic administration and trust services

24/2016. (VI. 30.) BM Decree on detailed requirements of trust services and trust service providers

541/2020 (XII. 2.) Government Decree on other identification methods recognised at national level that provide equivalent assurance to personal presence in the case of trust services

Considered document about methodology

ETSI TS 119 461 V1.1.1 (2021-07) Policy and security requirements for trust service components providing identity proofing of trust service subjects

ETSI TS 119 431-1 V1.2.1 (2021-05) Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev

MSZ EN 419 241-1:2018 Trustworthy Systems Supporting Server Signing – Part 1 General System Security Requirements

ISO/IEC 27002:2022 Information security cybersecurity and privacy protection - Information security controls

NIST Special Publication 800-53 Revision 4 Security and Privacy Controls for Federal Information Systems and Organizations

NIST Special Publication 800-53A Revision 4 Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans (December 2014)

Contact:

HUNGUARD Kft., 6 Kékgolyó street, 1123 Budapest, Hungary
Tel: +36 1 792 0880; Fax: +36 1 445 0414
e-mail: iroda@hunguard.hu