HUNGUARD

CERTIFICATE

HUNGUARD Informatics and IT R&D and General Service Provider Ltd. (6 Kékgolyó str. Budapest 1123 Hungary) as a certification authority

certifies, that

CECE Software System v1.1.0

developed by

Certus Software Zrt.

as software product providing IT security functions

complies

with the Security Target specified in Annex 3 at the EAL3 assurance level according to MSZ EN ISO/IEC 15408-3:2020

This certificate has been issued on the basis of the Certification report
HUNG-TJ-15408-001-2022

Produced on commission for
Certus Software Zrt. (13 Csillaghegyi road Budapest 1037 Hungary).

Certificate registration number: **HUNG-T-15408-001-2022**
Validity start date of the certificate: 14 January, 2022
Validity end date of the certificate: 14 January, 2025

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

Budapest, 14 January, 2022

Digitálisan aláírta: Endrődi Zsolt Attila	PH.	*Digitálisan aláírta:* Szűcs Ákos Balázs
Endrődi Zsolt Attila Certification director		Szűcs Ákos Balázs Managing director

Annex 1

Validity terms of the certificate

Security objectives for the IT environment:

The conclusions of the evaluation relies on the environmental assumptions listed in the Security Target.

The following objectives are not handled by CECE Software System v1.1.0 but are expected from the IT environment:

OE.COMPETENT_USERS: The users (persons using TOE) should be well-intended and follow the guidance document available online (CECE Web Manager).

OE.FIRMWARE_NOT_PREVENTING: The target computer’s firmware (BIOS) settings that can interfere with the erasing process should be properly configured, hence not preventing the erasure process performed by CECE Drive Eraser. The Android OS or iOS settings that can interfere with the erasing process should be properly configured, hence not preventing the erasure process performed by CECE Android Eraser or CECE iOS Eraser respectively.

OE.FUNCTIONAL_STORAGE: The target storage drives that are going to be erased by CECE Drive Eraser should behave as expected and expose the full storage capability to the operating system. Moreover, the controllers of the target devices should correctly transmit the commands related to erasure and retrieval of erasure verification data. The target Android and iOS devices should expose the full storage area where the user data is stored to the CECE Android Eraser and CECE iOS Eraser respectively.

OE.ACCURATE_SYSTEM_TIME: The operational environment should provide correct system time.

OE.TRUSTED_NETWORK: The operational environment should provide TOE with a network with a trusted network where there are no malicious attacks against the TOE components coming from the interfaces connected to the network.

OE.PROPER_INTEGRITY_TRACEBILITY: The CECE Web Manager should decrypt, sign and time-stamp erasure reports in order to prove the data erasure process applied to each device.

Annex 2

Document containing the requirements

MSZ EN ISO/IEC 15408-1:2020 Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model

MSZ EN ISO/IEC 15408-2:2020 Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components

MSZ EN ISO/IEC 15408-3:2020 Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components

Annex 3

Further features of the certification

This certificate has been issued according to the following:

- System evaluation report: CECE Software System v1.1.0 v1.0, száma: CA081-01/P/E/ETR

The assessment covered the conformanve claims declared in Chapter 2 of the following security target:

- Security Target for CECE Software System v0.9 /16 December 2021/

Evaluation level: EAL3

Considered document about methodology

MSZ EN ISO/IEC 18045:2020 Information technology — Security techniques — Methodology for IT security evaluation