HUNGUARD

CERTIFICATE

HUNGUARD Informatics and IT R&D and General Service Provider Ltd. (6 Kékgolyó str. Budapest 1123 Hungary) as a certification authority assigned by the assignment document No. IKF/1262-1/2016-NFM of the Ministry of National Development based on the Ministry of Informatics and Communication Decree 9/2005. (VII.21)

certifies

that the

Kofax Capture Hitelesítő modul (UserSign) v1.0.0

developed by

User Rendszerház Kft.

as an electronic signature product

with the secure usage conditions listed in Annex 1

passes the requirements

for creating and initial verifying advanced electronic signatures

according to the Act XXXV of 2001.
This certificate has been issued based on the certification report
No. **HUNG-TJ-072/a-2016**
Produced on commission of USER Rendszerház Kft.
(*86/b Szépvölgyi str. Budapest 1025*)
Certificate registration number: **HUNG-T-072/a-2016**
Validity start date of the certificate: *04 April 2016*
Validity end date of the certificate: *04 April 2019*
Statements of this certificate must be confirmed in yearly review procedures.
This Certificate has six pages including the Annexes containing validity terms and other attributes.

Budapest, 04 April 2016

LS.

Endrődi Zsolt
Certification director

Szűcs Ákos Balázs
Managing director

Annex 1

Validity terms of the certificate

Security objectives for the environment:

The validity of this certificate depends on the fulfilment of the environmental assumptions listed in the Security Target. The following objectives laid down also in the Security Target apply to the IT environment:

OE.AUDIT_GENERATION The IT Environment will provide the capability to detect and create records of security-relevant events associated with users.

OE.AUDIT_PROTECTION The IT Environment will provide the capability to protect audit information.

OE.AUDIT_REVIEW The IT Environment will provide the capability to selectively view audit information.

OE.Configuration The TOE will be installed and configured properly for starting up the TOE in a secure state.
Note: The installation guide shall be used for the installation and configuration of the TOE.

OE.CORRECT_TSF_OPERATION The IT Environment will provide the capability to test the TSF to ensure the correct operation of the TSF at a customer's site. *Note: The IT Environment is responsible for the verification of the correctness of the executable files of the TOE, configuration files of the TOE and data that can influence the security functions of the TOE.*

OE.CRYPTOGRAPHY_ALT The cryptographic algorithms used by the TOE shall conform the EU policy. The cryptographic algorithms used for electronic signatures are standardized in the EU, information can be obtained from the following specification: ETSI TS 119 312[1]. The specifications are regularly renewed, the user of the TOE has to monitor any changes of the specifications and only use the matching algorithms and parameters with right version of the cryptographic module.

[1] Actual version at certification time is v1.1.1 (2014-11)

OE.DISPLAY_BANNER The IT Environment will display an advisory warning regarding use of the TOE.

OE.MANAGE The IT Environment will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.

OE.MEDIATE The IT Environment will protect user data in accordance with its security policy.

OE.NO_EVIL Sites using the TOE will ensure that administrators are non-hostile, appropriately trained and follow all administrator guidance.

OE.PHYSICAL The non-IT environment will provide an acceptable level of physical security so that the TOE cannot be tampered with or be subject to side channel attacks such as the various forms of power analysis and timing analysis.

OE.RESIDUAL_INFORMATION The IT Environment will ensure that any information contained in a protected resource within its Scope of Control is not released when the resource is reallocated.

OE.SELF_PROTECTION The IT Environment will maintain a domain for its own execution that protects it and its resources from external interference, tampering, or unauthorized disclosure.

OE.TIME_STAMPS; OE.TIME_TOE The IT Environment will provide reliable time stamps, time and the capability for the administrator to set the time used for these time stamps.

OE.TOE_ACCESS The IT Environment will provide mechanisms that control a user's logical access to the TOE.

OE.TOE_PROTECTION The IT Environment will protect the TOE and TOE resources from external interference, tampering, or unauthorized disclosure and modification.

OE.ARCHIVE The IT Environment shall continuously provide the capability to support the verification of the electronic signature.

OE.CERT The signing certificate of the organization shall meet the following requirements:

- for all elements in the certificate chain of the signing certificate the usage of the whitespace characters must be the same for the issuer name and subject name fields
- for all elements in the certificate chain of the signing certificate the usage of the uppercase and lowercase characters must be the same for the issuer name and subject name fields,
- if any element in the certificate chain of the signing certificate has more than one name constraint, than one constraint shall not be met by subject name, while the others are met by subjectAltName.

Condition due to the compliance requirements to CWA 14170 and CWA 14171

UserSignMode parameter in the configuration file of the TOE shall be set to the “live” value.

Annex 2

Documents containing the requirements

CWA 14170 May 2004 Security requirements for signature creation applications

CWA 14171 May 2004 General guidelines for electronic signature verification

Annex 3

Further features of the certification

This certificate has been issued according to the following:

System evaluation report:

- Kofax Capture Hitelesítő modul (UserSign) ÉRTÉKELÉSI JELENTÉS v1.0

Compliance evaluation reports:

- Kofax Capture Hitelesítő modul (UserSign) megfelelése a CWA 14170:2004 és CWA 14171:2004 követelményeinek MEGFELELÉS ÉRTÉKELÉSI JELENTÉS v 1.0

Evaluation level: MIBÉTS moderate (EAL3)

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

Act XXXV of 2001 of the Republic of Hungary on electronic signature

Considered document about methodology

MIBÉTS 2009, KIB (Information Technology Committee for Public Services) recommendation No 28. „Evaluation methodology for products” v4 2008.09.19