



CERTIFICATE

HUNGUARD Informatics and IT R&D and General Service Provider Ltd. as a certification authority assigned by the assignment document No. IKF/19519-2/2012-NFM of the Ministry of National Development based on the Ministry of Informatics and Communication Decree 9/2005. (VII.21)

certifies

that the

MobilSign signature creation system R1 version

operated by

Magyar Telekom Nyrt.

*with functionality laid down in Annex 1
and with the secure usage conditions listed in Annex 2*

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-071-2015

Produced on commission of Magyar Telekom Nyrt. (1013 Budapest, Krisztina krt. 55.).

Certificate registration number: HUNG-T-071-2015

Validity start date of the certificate: 24 July, 2015.

Validity end date of the certificate: 24 July, 2018.

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

Budapest 24 July, 2015.

LS

Bálint Szabó
Quality assurance director

Ákos Szűcs
Managing director

Annex 1

Main features of MobilSign system

The target of evaluation (MobilSign) is an information system capable of creating hand-written signature dynamics, linking them with PDF documents, and creating Advanced Electronic Signatures for the resulting documents.

The main goal of MobilSign System, is to provide a way for clients in Magyar Telekom stores to sign contracts using hand-written signatures on tablets. The contract are downloaded from the eStore information system of Magyar Telekom in electronically signed PDF format. The system calculates and stores the dynamics of the hand-writtren signature, creates an evidence record, inserts the hash of the record into the PDF document, finally the PDF document containing the hash of the evidence record and the image of the hand-written signature is signed by an Advanced Electronic Signature.

There is a tool developed for MobilSign that is able to verify the matching of the PDF document and the evidence record in a protected environment and convert the evidence record into a visual representation that can be used by a graphologist to examine the hand-written signature.

The process implemented by the MobilSign system includes the following steps:

- import the contracts that need to be signed by the client from an external information system
- show the contracts that need to be signed to the client
- record the hand-written signature of the client
- encrypt the evidence record created from the hand-written signature
- link the evidence record and the PDF document
- create an Advanced Electronic Signature for the PDF document and acquire a timestamp from a timestamp authority
- initial verification of the signature
- decrypting and presenting the evidence record
- verify the matching of the PDF document and the evidence record

Annex 2

Secure usage terms

- 1 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 certificate validity and to reduce the residual risks:
 - once in a year in the validity period of the certificate (planned system evaluation review),
 - responding to the modifications in the system architecture or functionality (special system evaluation review).
- 2 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 change documentation in details which are commensurate with the former evaluation level.
- 3 In cases when 2 applies, the Certifier evaluates the effects of the modification and decides the necessity of a special system evaluation review in order to maintain the validity of the certificate. When compliance is achieved, the Certifier fills out a Certificate Maintenance Record for the modified system state. The terms of the planned or special system evaluation review must be provided by the Customer.
- 4 The system operators need to ensure that the following security objectives for the operational environment (stated in the System Security Target) are always met.

OE.PM The organization meets the requirements of the following controls of NIST SP 800-53 R4: PM-1, PM-2, PM-5, PM-10.

OE.RA The organization meets the requirements of the following controls of NIST SP 800-53 R4: RA-1, RA-2, RA-3.

OE.PS The organization meets the requirements of the following controls of NIST SP 800-53 R4: PS-4, PS-8

OE.AT The organization meets the requirements of the following controls of NIST SP 800-53 R4: AT-1, AT-2

OE.PE The organization meets the requirements of the following controls of NIST SP 800-53 R4: PE-1, PE-2, PE-3

Annex 3

Product compliance requirements

Requirements

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

Security Requirements for Trustworthy Systems supporting Server Signing; English version CEN/TS 419241:2014

CWA 14170:2004: Security Requirements for Signature Creation System, May 2004

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

Annex 4

Further information on the certification procedure

Developer-independent documents examined during certification

Evaluation report: MobilSign – signature creation system R1 version (by Hunguard Ltd.)

Compliance analysis to the standard requirements:

Compliance of MobilSign R1 to the requirements of CEN/TS 419241
COMPLIANCE EVALUATION REPORT V1.0

Compliance of MobilSign R1 to the requirements of CWA 14170:2004 and
CWA 14171:2004 COMPLIANCE EVALUATION REPORT V1.0

Compliance of MobilSign R1 to the requirements of NIST Special Publication
800-53 Revision 4 defined in the Security Target COMPLIANCE
EVALUATION REPORT V1.0

Method of independent assessment checking compliance to the requirements

The independent evaluation and certification of has been done according to the methodology of KIB recommendation No 28. „Evaluation methodology for systems”.

Evaluation level

MIBÉTS moderate (SAP-F)

Documents about methodology used during evaluation

- MIBÉTS 2009, KIB (Information Technology Committee for Public Services) recommendation No 28. „Evaluation methodology for products”
- MIBÉTS 2009, KIB (Information Technology Committee for Public Services) recommendation No 28. „Guidance to system evaluators”