CERTIFICATE

HUNGUARD Informatics and IT R&D and General Service Provider Ltd. as a certification authority assigned by the assignment document No. 002/2006 of the Minister of the Ministry of Informatics and Communication (MIC) of the Republic of Hungary based on the MIC Decree 9/2005. (VII.21)

certifies

that the

XadesMagic
electronic signature application development kit
for advanced electronic signatures
V1.0

developed by

SDA Stúdió Kft.

with functionality laid down in Annex 1

and with the secure usage conditions listed in Annex 2

passes the requirements

for the development of secure applications meeting the applicable standards for creating and verifying advanced electronic signatures according to the Act XXXV of 2001.

This certificate has been issued on the basis of the certification report
No. HUNG-TJ-034-2006.
Produced on commission of SDA Stúdió Kft.

Certificate registration number: **HUNG-T-034-2006.**
Date of certificate: 20.11.2006.
Validity period of the certificate: 20.11.2009.
Annexes: attributes, conditions, requirements and other features on six pages.

LS

Endrődi Zsolt Certification director	dr. Szabó István Managing director

Annex 1

Main features of XadesMagic v1.0

XadesMagic v1.0 is a development kit for implementing standard-compliant (based on X.509 standard) public key-enabled applications. Public key services supported by the development kit are:

- Generating advanced electronic signature with algorithm parameters supported by the Crypto API, using private key stored in Windows certificate-repository or cryptographic hardware device.
- Verifying electronic signatures together with services for certification path building and validation.
- Producing hash value for the signature creation with SHA-1, SHA-256, SHA-384, SHA-512 or Ripemd-160 algorithms.
- Request and verification of time stamps.
- Request and verification of revocation information (CRL, OCSP).

Based on this such applications can be developed with XadesMagic v1.0 that are capable of providing for confidentiality, integrity, authentication and non-repudiation services on the grounds of PKI technology.

XadesMagic v1.0 development library has the following public key services:

- It securely manages keys, trust points and certificates;
- It accepts and processes X.509 v3 public key certificates;
- It is capable of obtaining the necessary certificates and revocation data (from the location specified in the CPD extension of the certificate);
- It verifies the validity of every certificate based on procedures specified in the X.509 standard [ISO 9594-8] including revocation checks;
- It accesses accurate and trusted time-source for the purpose of the verification of date and time information of certificates, revocation data and application data;
- It collects, stores (embedding into the signature structure) data necessary for the verification of the signatures in the future;
- It supports HAES-Ready XAdES electronic signature format.

Annex 2

Secure usage terms

Assumptions for the XadesMagic v1.0 IT environment

The following assumptions (also specified in the Security Target) are made for the environment:

1. Authorised users are trusted to properly perform their assigned functions (AE.Authorized_Users).
2. XadesMagic v1.0 development kit is properly installed and configured (AE.Configuration).
3. The IT environment of XadesMagic v1.0 contains a trusted cryptographic module (CryptoAPI), which performs cryptographic operations (AE.Crypto_Module).
4. The XadesMagic v1.0 environment protects XadesMagic v1.0 from unauthorised physical access (AE.Physical_Protection).
5. The certificate and certificate revocation information are available to XadesMagic v1.0 (AE.PKI_Info).
6. XadesMagic v1.0 environment provides accurate system time with required precision in GMT format (AE.Time).
7. XadesMagic v1.0 environment provides access to the time-stamping provider (AE.TimeStamp).

Further secure usage conditions

1. Signature applications developed by XadesMagic v1.0 should operate only under a signature policy that uses at most the following X509v3 certificate extensions:
   - ExtendedKeyUsage
   - KeyUsage
   - BasicConstraints
   - CRLDistributionPoints
   - SubjectAlternativeName
   - IssuerAlternativeName
2. For signature applications developed by XadesMagic v1.0 such CSP driver should be used that is capable to keep the integrity of Data To Be Signed Representation (DTBSR) and all protocol data.
3. For signature applications developed by XadesMagic v1.0 such CSP driver should be used that is capable to keep the confidentiality of signatory’s authentication data, or the signature application should be used in a protected environment where management, operational and technological measures guarantee the confidentiality of signatory’s authentication data.
4. Management, operational and technological measures should be applied in the operational environment of signature application using XadesMagic v1.0 in order to assure that non-trusted system and application processes, peripheral devices and communication channels not necessary for signature creation applications should not be able to interfere with the signature process.

5. For signature application using XadesMagic v1.0 development kit
    a. a CSP driver should be used that is capable of setting a time limit for the period that can elapse from entering signatory's authentication data until the starting the signature generation;
    b. or the application should fulfil the requirement by requesting the authentication data after starting the signature generation.
6. For signature application using XadesMagic v1.0 development kit
    a. a CSP driver should be used that is capable of terminating the signature process after a timeout, restarting the process by requiring the re-entering of signatory's authentication data, and informing the signatory about the necessity of this restart;
    b. or the application should fulfil for the requirement by requesting the authentication data after starting the signature generation.
7. Management, operational and technological measures should be applied in the operational environment of XadesMagic v1.0 in order to provide for the following:
    a. viruses will not damage the signature application and other signature components used by it, and
    b. signature components accidentally infected by viruses will be recovered correctly.
8. Management, operational and technological measures should be applied in the operational environment of XadesMagic v1.0 in order to protect the integrity of functional components of XadesMagic v1.0 and so to prevent damages done by attackers.
9. Management, operational and technological measures should be applied in the operational environment of XadesMagic v1.0 in order to assure that the XadesMagic v1.0 itself and all of its components interacting with signature creation, signature verification processes are implemented in a secure area.

Annex 3

Product compliance requirements

Documents containing requirements and standards

Requirements

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

CEN/ISSS/E-Sign 4170:2004 Working Group Agreement: Security Requirements for Signature Creation System

CEN/ISSS/E-Sign 14171:2004 Working Group Agreement: Procedures for Electronic Signature Verification

CEN/ISSS/E-Sign 14172-4:2001 Working Group Agreement: Signature Creation Application and Procedures for Electronic Signature Verification

ETSI SR 102 176-1 v1.2.1 Electronic Signatures and Infrastructures (ESI) Algorithms and Parameters for Secure Electronic Signatures Part 1: Hash functions and asymmetric algorithms

ETSI TS 101 733 v1.6.3 CMS Advanced Electronic Signatures (CAdES)

ETSI TS 101 903 v1.2.2 XML Advanced Electronic Signatures (XAdES)

Standards

RSA	Rivest-Shamir-Adleman (public key cryptosystem) /ANSI X9.31/
SHA-1	Secure Hash Algorithm /FIPS PUB 180-1/
RFC 2560:	PKIX - Online Certificate Status Protocol – OCSP
RFC3161	Time-Stamp Protocol (TSP)
RFC3275	XML Digital Signatures (XMLDSig)
RFC3280	Certificate and Certificate Revocation List (CRL) Profile
PKCS#1	RSA Cryptographic Standard /RFC2313/

Annex 4

Further information on the certification procedure

Developers' documents examined during certification

- Security Target v1.0
- Functional specification v1.0
- High level design v1.0
- Compliance analysis v1.0
- Administrator's guide v1.0
- Test documentation 2006.09.26.
- Test coverage documentation v1.0
- Test depth documentation v1.0
- Configuration management documentation v1.0
- Development security documentation v1.0
- Developers' vulnerability assessment v1.0
- Target of evaluation ready for testing (development kit ready for testing with SDA-Magic program)

Developers-independent documents examined during certification

Evaluation report on XadesMagic v1.0 electronic signature development library for advanced electronic signatures v1.0 (by HunGuard Ltd.)

Method of independent assessment checking the requirement compliance

The independent evaluation and certification of XadesMagic v1.0 has been done according to the methodology of CEM (Common Evaluation Methodology) v2.3.

Evaluation level

EAL3

Documents about methodology used during evaluation

- MSZ/ISO/IEC 15408:2003 Information technology – Security technology – Common Criteria of Information Security Evaluation
- Common Criteria for Information Technology Security Evaluation (CC) Part 1: Introduction and general model - Version 2.3, August 2005
- Common Criteria for Information Technology Security Evaluation (CC) Part 2: Security functional requirements - Version 2.3, August 2005
- Common Criteria for Information Technology Security Evaluation (CC) Part 3: Security assurance requirements - Version 2.3, August 2005
- Common Methodology for Information Security Evaluation (CEM), Version 2.3, August 2005