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

mySigno for PDA and Server v1.0

development kit for advanced electronic signatures

developed by
Argeon Business Services Ltd.

with functionality written down in Annex 1
and with conditions regarding the secure usage 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 of the Republic of Hungary on electronic signature.

This certificate has been issued on the basis of the certification report No. HUNG-TJ-032-2006.
Produced on commission of Argeon Business Services Ltd.

Certificate registration number: **HUNG-T-032-2006.**
Date of certificate: 29. 05. 2006.
Validity period of the certificate: 29. 05. 2009.
Annexes: attributes, conditions, requirements and other features on six pages.

L S.

Endrődi Zsolt
Certification director

dr. Szabó István
Managing director

Annex 1

Overview of the main features of mySigno v1.0

The mySigno v1.0 is a function library capable of creating and verifying advanced electronic signatures designed into a complex system with client and server components.

The mySigno v1.0 is planned to operate in a composite IT system which includes several other functions apart from electronic signature creation and verification (on client side: XML packages compilation, location of handwriting signatures; on server side: archiving of signed packages, storing them in a database etc).

Roles managed by mySigno v1.0:

- **Agent**: Role who provides for the integrity of packages by creating his own digital signature.
- **Verifier:** Automatic verification process on the server side.

Roles that are out of scope of the mySigno v1.0 evaluation but are connected to the secure operation:

- **Server administrator:** Individual who is authorised to do the mySigno server maintenance and settings.
- **PDA administrator:** Individual who is responsible for tasks in connection with PDA module installation and secure settings of parameter files and keys.

The mySigno v1.0 security functions are implemented in application component realised in DLL and are available through development API functions with client functionality of creation of advanced electronic signature and with server functionality of verification of this signature.

The advanced electronic signature uses SHA-1 hash and RSA digital signature algorithm with 1024 key size. In the signature creation environment the private key storage is implemented in PKCS#12 certificate.

The mySigno v1.0 on the client side provides for an interface for the electronic signature creation processes, and on server side for the electronic signature verification processes.

Annex 2

Secure usage terms

Assumptions for the mySigno v1.0 IT environment

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

1. The keys and security functions for the secure operation of mySigno v1.0 are installed securely on the PDA device (A.Init_PDA).
2. The PDA device should be used only with charged battery for creating electronic signature in order to avoid data loss (A.PDA_Physical_Security).
3. It is assumed that the PDA device is under the full control of the agent, and without the permission of the agent the PDA device should not be used by other individuals (A.Signer_Only).
4. The PDA device hosting the mySigno PDA client application is under the control of the signatory and the organisation operating the system (A.Host_PDA_Machine).
5. The mSigno processes are protected from the harmful effects of other processes in the signature creation and verification environment. The mySigno v.0 module should be loaded by only one calling application at a time (A.Separation_and_Exclusion).
6. The PDA user does not modify the content of the library storing the mySigno v1.0 module (A.AccessControl).
7. The mySigno security administrators are trusted, skilled and have the rights and accesses to do their jobs competently (Trusted_Security_Administrator).
8. The security administrator or the calling application has the possibility to check the integrity of the mySigno v1.0 services and parameters (A.Services_Integrity).
9. The signatory agent is present from the time that he has expressed his intent to create the electronic signature to the point of giving his authentication data that is necessary for the private key activation (A.Signatory_Presence).
10. The PDA device contains such external presentation applications which are able to display the document formats that can be put into the package (determined by the signature policy). The signature creation client and the verifier server side recognise and display the same document formats, and these document presentation applications operate with the same settings (A.Packet_Viewers).
11. The server verifying the signatures is physically protected from direct attacks (A.Physical_Security).
12. The host machine running the mySigno v1.0 server module is under the direct control of the verifier (natural or legal person), which assures that the security measures are applied correctly (A.Host_Server_Machine).
13. The mySigno v1.0 server module has access to all of the validation data that are necessary for the signature verification (A.Access_to_Validation_Data).

Further conditions regarding the secure usage

1. The mySigno v1.0 cryptographic module does not support self-issued certificates, nor does support certificate path verification when CRLs are verified with certificate other than the end certificates. The mySigno v1.0 makes binary comparison for the issuer and owner match during building certificate path. Therefore it can be used in such environments where self-issued certificate cannot be found in the certificate path, the CRLs and end certificates are validated with the same CA certificate and in the certificate path the issuer-owner match is a binary match.
2. Technical and procedural measures should be applied in the operational environment of the signature application using mySigno v1.0 development kit 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.
3. Technical and procedural measures should be applied in the operational environment of mySigno v1.0 development library 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.
4. Technical and procedural measures should be applied in the operational environment of mySigno v1.0 development library in order to protect the integrity of functional components of mySigno v1.0 and so to prevent damages done by attackers.
5. Technical and procedural measures should be applied in the operational environment of mySigno v1.0 development library in order to assure that the mySigno v1.0 development library 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 CWA 14170:2004 Working Group Agreement: Security Requirements fro Signature Creation System

CEN CWA 14171:2004 Working Group Agreement: General guidelines for electronic signature verification

CEN CWA 14172-4:2001 Working Group Agreement: Signature-creation application and general gudelines for electronic signature verification

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

ETSI TS 101 862 v1.3.3 Qualified Certificate profile

ETSI SR 002 176-1 v1.2.1 Electronic Signatures and Infrastructures (ESI) Algorithms and Parameters for Secure Electronic Signatures Part 1: Hash functions and asymmetric algorithms

ETSI TS 101 903 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/
RFC3161	Time-Stamp Protocol (TSP)
RFC3275	XML Digital Signatures (XMLDSig)
RFC3280	Certificate and Certificate Revocation List (CRL) Profile
PKCS#1	RSA Cryptographic Standard /RFC2313/
PKCS #11 v2.11:	Cryptographic Token Interface Standard
PKCS #12 v1.0	Personal Information Exchange Information Standard

Annex 4

Further information on the certification procedure

Developers' documents examined during certification

- Request for certification
- Security Target v1.0
- Signature policy v1.0
- Functional specification v1.0
- High level design v1.0
- Compliance analysis v1.0
- Test documentation v1.0
- Test coverage documentation v1.0
- Test depth documentation v1.0
- Administration guide v1.0
- Configuration management v1.0
- Development security v1.0
- Misuse analysis of developers' guide v1.0
- Strength of function analysis v1.0
- Vulnerability analysis v1.0

Developers-independent documents examined during certification

Evaluation report on mySigno for PDA and mySigno Server electronic signature system v1.0 (HunGuard Ltd.)

Method of independent assessment checking the requirement compliance

The evaluation of mySigno v1.0 has been done according to the Hungarian IT Security and Evaluation Scheme (MIBÉTS) methodology. MIBÉTS acknowledges the concepts, principles and criteria of the Common Criteria (MSZ ISO/IEC 15408:2002) for the technological evaluation of information systems and products.

Evaluation level

Moderate (EAL3)

Documents about methodology used during evaluation

- MIBÉTS Publication No 1: General model of National MIBÉTS scheme /v0.95, February 2005/,
- MIBÉTS Publication No 2: Procedures of evaluation and certification /v0.95, February 2005/,
- MIBÉTS Publication No 3: Evaluation methodology 1 – Evaluation methodology of the Security Target /v0.95, February 2005/,
- MIBÉTS Publication No 3: Evaluation methodology 4- Evaluation methodology of the high assurance level /v0.95, February 2005/.