CERTIFICATE

HUNGUARD Informatics and IT R&D and General Service Provider Ltd. as a certification authority assigned by the assignment document No. 113/2007 of the Minister of the Ministry of Economy and Transport of the Republic of Hungary
based on the Ministry of Informatics and Communications Decree 9/2005. (VII.21)

certifies that

IBM 4758 Security Module With CP/Q++

hardware model: 2, Miniboot 0: version A, Miniboot 1 Version A, CP/Q++: 2.41

electronic signature product

manufactured and sold by
IBM Corp.
in the case of the realization of all conditions in Annex 1.

is suitable for

the secure operation of a qualified certification service provider
who provides the following services:

Within the scope of electronic signature certification service:
Generating, storing (qualified) certificate signing keys, signing, saving and recovering (qualified) certificates;
Within the scope of time stamping service:
Generating, storing timestamp signing keys, signing timestamp;
Within the scope of placement of signature creation data in a signature creation device service:
Generating subscriber (signing) key pair;
Within the scope of secure operation of the qualified certification service provider's own information system:
Generating, storing and using infrastructural and reliable management keys.

This certificate has been issued on the basis of the certification report HUNG-TJ-046-2009.
Produced on commission of MÁV INFORMATIKA Inc.

Certificate registration number: **HUNG-T-046/2009.**
Date of the certification: 30.03.2009.
Validity period of this certificate according to IV/15. in Annex 1: 31.12.2009.
Annexes: attributes, conditions, requirements and other features on seven pages.

LS

Endrődi Zsolt
Certification director

dr. Szabó István
Managing director

Annex 1
Validity conditions of the certificate

IBM 4758-002 is a programmable cryptographic card that reacts to interruption and ensures general computer environment and efficient cryptographic support. It supports the realization of wide range of cryptographic functions with the accessibility of specially designed and hardware based algorithms. It is able to accept, run and protect the installed software and its secret data against logical and physical attacks of qualified attackers.

The module consist three main components:

- hardware /inside: random noise generator, SHA-1 computing hardware, interruption sensor and reacting circuits, hardware locks/,
- Miniboot software /two layers (0. and 1.) which forms the basis of IBM 4758-002 and controls the security and configuration of the module/,
- possibility of the development of higher level system software and application layers (2. and 3. layer)

IBM 4758-002 PCI cryptographic coprocessor's hardware, the lower 2 layer (Miniboot Layer 0, 1) of the superposing 4 software and firmware layer and the application layer (Miniboot Layer 2) which consist the CP/Q++ application are satisfy the FIPS 140-1 Level 3 requirements certified by FIPS certification.

If the IBM 4758-002 adapter is used by a qualified certification service provider for its security critical activities (to sign the issued certificates and timestamp responses) it has to comply with further requirements which limit the usability demanding more complementary conditions to be met.

Hereunder we summarize the conditions that collectively form the basis of this certificate's validity.

I. General validity conditions

The following conditions are necessary for every utilization modes (the whole general utilization scope designed by the manufacturer) for reliable and secure operation.

1. During the installation phase of IBM 4758-002 PCI cryptographic coprocessor the rules written in the „IBM 4758 PCI Cryptographic Coprocessor Installation Manual" must be kept.

II. Validity conditions arising from FIPS 140-1 conformity

The following conditions are essential for the IBM 4758-002 adapter to meet FIPS 140-1 Level 3 requirements.

2. Cryptographic functionality in connection with digital signature must be restricted to the following algorithms: **DSA, RSA, SHA-1**.

3. Hardware must be loaded with the following:
   - a FIPS 140 validated Miniboot in segment-1,
   - a FIPS 140 validated CP/Q++ in segment-2. The segment 'owner identifier' must be 2. Do not use identifier 6 in a production system

4. The External User must observe any restrictions documented for FIPS-140 compliant use of the segment-3 application.

III. Complementary conditions for use in qualified certification service

A qualified certification service provider must maintain the following complementary conditions when using the IBM 4758-002 adapter:

5. Minimal p prime length (pMinLen) must be 1024 bit, minimal q prime length must be 160 bit in case of DSA signature algorithm.

6. Only blocks with bit length divisible by 8 can be signed digitally.

7. Those keys which are used to sign qualified certificates are only useable for signing qualified certificates and possibly to sign their certificate revocation lists.

8. The module must take care of key protection when a stored key from a secure cryptographic module is exported. Storing sensitive key data in non-secure mode is prohibited. Storing and saving a qualified certificate signing key is only permitted if other additional security mechanisms are used. This can be done using one of the following:

- "m from n" technique (that is not supported by CSA 8000 but it is later achievable through its standard interface) where m is the quantity of those components from the whole n components which are necessary for the successful initialization of the key. For the recovery from error state the m = 60% * n value is proposed (that is if n=3 then m=2, if n=4 then m=3, if n=5 then m=3, and so on).
- with the following (CSA 8000 supported) methods:
  - saving to a smart card (token),
  - it is encoded by 3DES algorithm,
  - the Key Encryption Key is made from two random components and in compliance with this the simultaneous presence of at least two authorized person is necessary for recovering the private key.

9. Those signing keys that are used for time stamping are only applicable for signing timestamps.

10. In the placement of signature creation data in a signature creation device service if the generation of the subscriber's signing key pair occurs outside the signature creation device (inside the IBM 4758-002 cryptographic module) it must be assured that signing keys for electronic signature are different from other keys, e.g. keys for encryption.

11. In the placement of signature creation data in a signature creation device service if the generation of the subscriber's signing key pair occurs outside the signature creation device (inside the IBM 4758-002 cryptographic module) a secure path between the IBM 4758-002 cryptographic module and the signature creation device must be assured. This path must assure confidentiality, integrity and authenticity by proper cryptographic mechanisms.

12. This certificate is only valid for the current hardware and firmware version /hardware model: 2, Miniboot 0: version A, Miniboot 1: version A, CP/Q++: 2.41/. Upgrade of a new firmware version is only applicable if the following requirements are realized:
    - the new firmware version is authenticated by the developer,
    - the new firmware version was evaluated by an accredited laboratory and a new FIPS certificate was released,
    - usability of the new firmware version in qualified certification service is certified by a designated native organization, and the new version is included in the secure signing products register of the Hungarian National Communications Authority.

IV. Other notes that influence validity

13. Certificates issued by the National Institute of Standards and Technology (NIST) are valid until revocation. So hardware, firmware and software products in the certificates are usable in an unchanged form.

14. Those modules which are certified according to FIPS 140-1 are still secure. FIPS 140-1 certificates should not be issued after 26 May 2002.

15. There are two known attacks against the module. These attacks enable to extract the 3DES key stored in the HSM and extract PIN codes used in banking applications.

    The first attack is the result of bad access control and results the extraction of stored 3DES key. FIPS approved CP/Q++ version 2.41 fixes this error. Physical security safeguards of the qualified CAs also give enough security because physical access to the HSM is necessary to execute an attack.

    Bugtraq 6901 attack appears if the module is used in banking environment. In this case the decryption of PIN codes is possible. This attack doesn't affect the qualified certification service and can be easily avoided with physical security safeguards.

    These two attacks do not affect operation at qualified certification providers. At the same time, the National Communications Authority in its decisions No HL-21917-9,10,11,12,13,14/2008. based on international requirements recommends the SHA-1 hash algorithm for usage in certificate signatures only until the end of 2009. As IBM 4758---002 HSM applies the SHA-1 algorithm according to the documentation, the certification authority limits the validity period of this certificate until this date, 12.31.2009.

V. Conditions regarding the uploaded software to Layer 3 of IBM 4758-002

Underlying examination of FIPS certification was focused to the strength of hardware security which is the most security critical part of the whole module. But Layer 3 would also be uploaded with a software for the correct operation.

Layer 3 software can be considered secure with satisfying the following conditions:

16 Layer 3 of IBM 4758-002 is uploaded with software developed by IBM:

- Layer 3 is a standard PKCS #11 interface developed by IBM

17 Uploaded software is FIPS 140 Level 3 approved /as mentioned in the Security Policy for the Security Module with CP/Q++ part of the IBM 4758 PCI Cryptographic Coprocessor Model 002 page 14, in FIPS 140-1 requirements./ In this case the FIPS requirements must be kept.

Annex 2
PRODUCT SUITABILITY REQUIREMENTS
Requirements documents

Act XXXV of 2001 on electronic signature

Decree 3/2005. (III.18.) IHM on detailed requirements of services in connection with electronic signature and its service providers

Directive 2/2002 (IV.26) MeHVM on security requirements of qualified electronic signature services and its service providers

FIPS 140-1: Security Requirements for Cryptographic Modules

Derived Test Requirements for FIPS 140-1

ETSI TS 101 456 v1.4.3 Policy Requirements for Certification Authorities Issuing Qualified Certificates

ETSI TS 102 176-1 V2.0.0 Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms

CEN 14167-1:2003 Munkacsoport Egyezmény: Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures

NHH decision No HL-21917-9,10,11,12,13,14/2008. on the applicable secure cryptographic algorithms and parameters linked to them

Annex 3
Documents considered in the certification

Request for the certification

Questionnaire for the certification

CEN 14167-2 workgroup agreement: Cryptographic Module for CSP Signing Operation – Protection Profile (CMCSO-PP, HSM-PP)

CEN 14167-3 workgroup agreement: Cryptographic Module for CSP Key Genaration Services – Protection Profile (CMCKG-PP, HSM-PP)

FIPS 140-1 Validation Certificate No. 116 /IBM 4758-002 PCI Cryptographic Coprocessor/ (revoked)

FIPS 140-1 Validation Certificate No. 345 /Security Module with CP/Q++/

IBM 4758 Model 2 Security Policy /June 2000/

Security Policy for the Security Module with CP/Q++ part of the IBM 4758 PCI Cryptographic Coprocessor Models 002 and 023 (PCICC)

IBM PCI Cryptographic Coprocessor General Information Manual /Sixth Edition, May 2002/

IBM 4758 PCI Cryptographic Coprocessor Installation Manual /Second Edition, March, 2000/

Mike Bond, Piotr Zielinski, Decimalisation table attacks for PIN cracking, http://www.cl.cam.ac.uk/TechReports/UCAM-CL-TR-560.pdf

Mike Bond, Richard Clayton, Extracting a 3DES key from an IBM 4758, http://www.cl.cam.ac.uk/~rnc1/descrack/

Frequently Asked Questions for the Cryptographic Module Validation Program