CERTIFICATE

HUNGUARD Informatics and IT R&D and General Service Provider Ltd. as a certification authority assigned by the assignment document No. 001/2010 of the Minister of the Prime Minister's Office of the Republic of Hungary based on the Ministry of Informatics and Communication Decree 9/2005. (VII.21)

certifies that the

IDOneClassIC Card

manufactured and sold by
Oberthur Card Systems

electronic signature smartcard product

with the following certified components and versions:

ID-One Cosmo 64 RSA v5.4, applet: IDOneClassIC v1.0
platform: P5CT072VOP and
ID-One Cosmo 64 RSA v5.4.1, applet: IDOneCIE v1.01.1
platforms: P5CT072VOP, P5CC072VOP és P5CD072VOP

is suitable for

the application of creating qualified electronic signatures according to the Act XXXV of 2001 as a Type-3 secure signature creation device

This certificate has been issued on the basis of the evaluation report HUNG-TJ-049-2010.
Produced on commission of NetLock Informatics and Network Privacy Services Ltd.
Registration number: **HUNG-T-49-2010.**
Date of the certification: September 30, 2010
Validity of this certificate in case of yearly revision: September 30, 2013
Annexes: conditions, requirements, documents in five pages.

LS

Endrődi Zsolt
Certification director

dr. Szabó István
Managing director

Annex 1

Validity conditions of the certificate

The following sections summarise those conditions which **jointly** must be maintained so that users securely use the IDOneClassIC Card smart card as SSCD.

I. General validity conditions

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

1. Administrators and users (signers) using IDOneClassIC Card smartcard product's services are well-trained and reliable.
2. Administrators and users using the services of IDOneClassIC Card smartcard observe the secure usage recommendations found in User and Administrator Guidance.

II. Validity conditions due to CC certification

3. The CGA generates qualified certificates which include inter alia: (a) the name[1] of the signatory controlling the TOE, (b) the SVD matching the SCD implemented in the TOE under sole control of the signatory, (c) the advanced signature of the CSP. (OE.CGA_QCert)
4. The CGA verifies that the SSCD is the sender of the received SVD and the integrity of the received SVD. The CGA verifies the correspondence between the SCD in the SSCD of the signatory and the SVD in the qualified certificate. (OE.SVD_Auth_CGA)
5. If an external device provides the human interface for user authentication, this device will ensure confidentiality and integrity of the VAD as needed by the authentication method employed. (OE.HI_VAD)
6. The SCA: (a) generates the DTBS-representation of the data that has been presented as DTBS and which the signatory intends to sign in a form which is appropriate for signing by the TOE, (b) sends the DTBS-representation to the TOE and enables verification of the integrity of the DTBS-representation by the TOE (c) attaches the signature produced by the TOE to the data or provides it separately. (OE.SCA_Data_Intend)
7. Recommended size of the generated SCD/SVD RSA key-pair is 2048 bits. RSA key-pair with less than 2048 but more than 1020 bits may be used until 24.09.2011 if the responsible Authority does not prohibit it earlier.
8. For the generation of RSA keys of whatever length it is recommended to use a public exponent with length at least 5 bits i.e. with value >= 17.
9. The user should not select a PIN code with less than 6 characters long.

[1] The name can be an alias, but this fact should be indicated in the qualified certificate.

10. Before a signature operation is processed the Signatory and the SCA must be identified and authenticated in advance.

III. Conditions for usage without SM (Secure messaging)

11. In case the IDOneClassicIC Card smart card has been personalized such that it is not able to establish secure messaging (SM), then the necessity of maintaining a trustworthy environment must be communicated to the end user (signatory) by the card issuer certification service provider.
12. The operational environment ensures the integrity of the SVD exported by the TOE to the CGA. The CGA verifies the corresponence between the SCD in the signatory's SSCD and the SVD in the input given to the certificate generation function of the CSP. (OE.SVD_Auth)
13. When an outer device provides the human interface during the user authentication process, then the operational environment must ensure the integrity and confidentiality of the VAD as it is required by the applied authentication method. (OE.HI_VAD_NOSM)
14. The SSCD Provisioning Service handles authentic devices that implement the TOE to be prepared for the legitimate user as signatory personalises and delivers the TOE as SSCD to the signatory. (OE.SSCD_Prov_Service)
15. The operational environment ensures that the DTBS/R cannot be altered in transit between the SCA and the TOE. (OE.DTBS_Protect)
16. The signatory makes sure of the fact that the SCD stored in the SSCD given from the SSCD Provisioning Service has not been used before. (In order to do this the issuer provides a proper guidance.) The signatory keeps the TOE under his/her sole control and maintains the confidentiality of the VAD. (OE.Signatory)

III. Supplementary conditions for qualified certification service provision

During the usage of IDOneClassIC Card a signatory creating qualified electronic signatures must keep the following supplementary rules:

17. IDOneClassIC Card used as an SSCD has a sole user, the signatory.
18. After the end of usage of IDOneClassIC Card smart card the card must be disposed or must be returned o the issuer.
19. Private key used for creating qualified signatures must be used only for creating qualified signatures (therefore it should not be used for advanced electronic signatures).

Annex 2
PRODUCT CONFORMANCE REQUIREMENTS
Requirements document

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

CEN/ISSS ESign Workshop – Expert Group F: Protection Profile – Secure Signature-Creation Device Type 3, version: 1.05, EAL4+

Annex 3

Further documents considered during certification

Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005

Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 2.3, August 2005

IDOneClassIC CARD Security Target, ref. FQR: 110 3517, edition 4, 16/01/07

IDOne™ ClassIC Card V1.0 Public Security Target (Original Security Target Lite)

Certification Report 2007/02 (IDOneClassIC Card: ID-One Cosmo 64 RSA v5.4 and applet IDOneClassIC v1.0 embedded on P5CT072VOP) (Original Certification Report)

ANTERAK project: Evaluation Technical Report, ref. ANTERAK_ETR_V1.2, version 1.2, 24/01/07

IDOneClassIC Guidance, ref. FQR : 110 3558, édition: 1 du 20/11/06

Software Requirement Specification, ref. 066771 00 SRS, édition 1-AB du 23/11/06

Rapport de Maintenance ANSSI-CC-2007/02-M02

IDOne Classic Card SSCD Type 3 Proprietary Security Target (New Security Target)

Differences between IDOne Classic Card Public Security Target and IDOne Classic Card SSCD Type 3 Proprietary Security Target (Comparison of the original and the new Security Targets)

NETLOCK ID-ONE CLASSIC File Structure and Access Conditions (Details on personalization of cards delivered to Netlock Ltd.)

IDOne Classic Card SSCD Type 3 EVALUATION REPORT v1.0 produced by Hunguard Ltd.

Request for certification