CERTIFICATE REVIEW RECORD

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) and as a product certification authority accredited by the National Accreditation Body by the document No. NAT-6-0048/2011

on the request of the client

reviewed

the documents HUNG-T-007/2003 Certificate (issued on 16 May 2003), and HUNG-FJ-007/2006 and HUNG-FJ-007/2009 certificate review records

about

the CSA8000 cryptographic adapter

/ERACOM Technologies Group, Eracom Technologies Australia,, Pty.Ltd./
/hardware version: G, Cprov firmware version: 1.10/

that is suitable for the creation of qualified electronic signatures as a „type-3 secure signature creation device"
as a
mutual secure signature creation device for multiple users (signatories) accessing the adapter directly.

The Certification Authority considered the following aspects during the review:
- validity of the FIPS 140-1 Validation Certificate No. 160 /CSA8000 Cryptographic Adapter/ which was the primary document of the former certification;
- examinations as to the conformance to the SSCD Protection Profile issued in draft version and considered during the former certification;
- since the certification new cryptographic parameter recommendations have been published in document ETSI TS 102 176-1 V2.1.1, based on which the NMHH issued decree No. EF/26838-8/2011 for the client regarding the applicable cryptographic algorithms and their parameters;
- in document CWA 14180-1:2004 (Application Interface for smart cards used as Secure Signature Creation Devices – Part1: Basic Requirements) published since the certificate issuance the concept of the secure and non-secure environment have been differentiated, according to which the device can be applied in secure environments.

Based on the aspects above and
taking into consideration of requirements due to legal certainty and the fact that the Hungarian law –primarily the Act XXXV of 2001 on electronic signature and its corresponding regulation– does not mandate contrary and does not require reverse criteria
the Certification Authority extends the validity of the Certificate No. HUNG-T-007/2003 issued on 16 May 2003 for another 3 years

on conditions laid down in Annex 1 of the Certificate HUNG-T-007/2003 and modified according to the following:

1. use of SHA-1 or weaker hash algorithms are not allowed
2. in case of RSA signature algorithm the recommendation for the minimal modulus size (MinModLen): 2048 bits
3. in case of DSA signature algorithm the recommendation for the minimal p prime length (pMinLen): 2048 bits, the minimal q prime length (qMinLen): 224 bits.

Registration number of this Certification Review Record: **HUNG-FJ-007-2012**
Date of the Record: 23 July 2012.
Extended validity period of the certificate under yearly review procedure: 15 May 2015

PH.

Endrődi Zsolt
Certification director

dr. Szabó István
Managing director