FELÜLVIZSGÁLATI JEGYZŐKÖNYV

A **HUNGUARD** Számítástechnikai-, informatikai kutató-fejlesztő és általános szolgáltató Kft. a 9/2005. (VII.21.) IHM rendelet alapján, mint a Magyar Köztársaság Miniszterelnöki Hivatalt Vezető Miniszterének 001/2010 számú Kijelölési okiratával kijelölt tanúsító szervezet és mint a NAT által NAT-6-0048/2011 számon akkreditált terméktanúsító szervezet

az igénylő kérelmére **felülvizsgálta a 2003. május 16-án kiállított**

CSA8000 kriptográfiai adapter

/ERACOM Technologies Group, Eracom Technologies Australia,, Pty.Ltd./

/hardver verzió: G, Cprov förmver verzió: 1.10/

minősített elektronikus aláírások létrehozására alkalmazható

„3-as típusú biztonságos aláírás-létrehozó eszköz"-nek

mint

az adapterhez közvetlenül hozzáférő több felhasználó (aláíró) közös biztonságos aláírás-létrehozó eszközre vonatkozó

HUNG-T-007/2003 számú Tanúsítványát ,a HUNG-FJ-007/2006 és HUNG-FJ-007/2009 Felülvizsgálati Jegyzőkönyveket.

A felülvizsgálat során a Tanúsító szervezet figyelembe vette az alábbi szempontokat:

- a korábbi tanúsítás alapjául szolgáló FIPS 140-1 Validation Certificate No. 160 /CSA8000 Cryptographic Adapter/ tanúsítvány érvényessége;
- a korábbi tanúsítás során már DRAFT verzióban megjelent és figyelembe vett SSCD védelmi profilnak való megfelelőségi vizsgálatok;
- az eltelt időszakban ETSI TS 102 176-1 V2.1.1 dokumentum új kriptográfiai paraméter ajánlásokat tett, ami alapján az NMHH a használható kriptográfiai algoritmusokról és azok paramétereiről az igénylő felé EF/26838-8/2011 számon határozatott hozott.
- a Tanúsítvány kiállítása óta megjelent CWA 14180-1:2004 (Application Interface for smart cards used as Secure Signature Creation Devices – Part1: Basic Requirements: Alkalmazás interfész biztonságos aláírás-létrehozó eszközként használt intelligens kártyákra – Alap követelmények) dokumentumban megkülönböztetésre került a biztonságos és nem biztonságos környezet fogalma, melynek alapján az eszköz biztonságos környezetben alkalmazható.

A fenti szempontok alapján, valamint

tekintetbe véve a jogbiztonságból adódó elvárásokat és azt a körülményt, hogy a magyar jogszabályokban – elsősorban az elektronikus aláírásról szóló 2001. évi XXXV. törvény és a kapcsolódó rendeletek szövegezésében - nem jelent meg ellentétes irányú elvárás- és szempontrendszer,

a Tanúsító szervezet további 3 évre meghosszabbítja a

a 2003. május 16-án kiállított HUNG-T-007/2003 számú Tanúsítvány érvényességét

a HUNG-T-007/2003 számú Tanúsítvány *1. számú mellékletében részletezett –az alábbiak szerint módosított– feltételrendszer teljesülése mellett*.

1. SHA-1 vagy annál gyengébb lenyomatoló algoritmus használata tilos
2. RSA aláírási algoritmus használata esetén a minimális modulus ajánlott mérete (MinModLen) 2048 bit
3. DSA aláírási algoritmus használata esetén az ajánlott minimális p prímhosszúság (pMinLen) 2048 bit, a minimális q prímhosszúság (qMinLen) 224 bit

A Felülvizsgálati Jegyzőkönyv regisztrációs száma: **HUNG-FJ-007-2012**

Jegyzőkönyv kelte: 2012. július 23.

A tanúsítvány kiterjesztett érvényességi ideje évenkénti felülvizsgálati eljárás mellett: 2015. május 15.

PH.

Endrődi Zsolt
Tanúsítási igazgató

dr. Szabó István
Ügyvezető