



FELÜLVIZSGÁLATI JEGYZŐKÖNYV

A HUNGUARD Számítástechnikai-, informatikai kutató-fejlesztő és általános szolgáltató Kft. a 9/2005.(VII. 21.) IHM rendelet alapján, mint a Magyar Köztársaság Gazdasági és Közlekedési Miniszterének 113/2007 számú kijelölési okiratával kijelölt terméktanúsító szervezet évenkénti felülvizsgálati eljárása során **felülvizsgálta a 2003. május 16-án kiállított**

CSA8000 kriptográfiai adapter

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

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

minősített elektronikus aláírások létrehozására alkalmazható

„3-astípusú 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 és HUNG-FJ-007/2006 Felülvizsgálati Jegyzőkönyvét.

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 megfelelési vizsgálatok;
- az eltelt időszakban nyilvános források között nem jelent meg olyan információ, mely befolyásolná/érvénytelenítené a modul biztonságos működését;
- 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 feltételrendszer teljesülése mellett.

Figyelembe véve azonban, hogy mind az ETSI TS 102 176-1 V2.0.0 és az azon alapuló HL-21917-9,10,11,12,13,14/2008 NHH határozatok a BALE által használt RSA 1024 illetve SHA-1 algoritmusokat 2009-től nem ajánlják elektronikus aláírás felhasználására, amennyiben a Hatóság megtiltja ezen adott paraméterű algoritmusok használatát, vagy a szakirodalomban megjelennek ezek gyengeségére vonatkozó konkrét adatok, akkor jelen tanúsítvány érvényességét a tanúsító szervezet visszavonja.

A Felülvizsgálati Jegyzőkönyv regisztrációs száma: **HUNG-FJ-007-2009**

Jegyzőkönyv kelte: 2009. május 15.

A tanúsítvány kiterjesztett érvényességi ideje évenkénti felülvizsgálati eljárás mellett: 2012. május 15.

PH.

Endrődi Zsolt
Tanúsítási igazgató

dr. Szabó István
Ügyvezető