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 felülvizsgálati eljárása során **felülvizsgálta**

a **Giesecke & Devrient** GmbH, Germany által előállított és forgalmazott P8WE5032v0G mikrochip-ből, STARCOS SPK 2.3 v 7.0 operációs rendszerből és StarCert v 2.2 digitális aláírás alkalmazásból álló

minősített elektronikus aláírások létrehozására alkalmazható intelligens kártyának

„3-as típusú biztonságos aláírás-létrehozó eszköz”-re vonatkozó, 2003.09.24-én kiállított **HUNG-T-011/2003** számú Tanúsítványát, a 2005.09.24-án kiállított **HUNG-FJ-011/2005** számú Felülvizsgálati Jegyzőkönyvét és a 2006.09.24.-én kiállított **HUNG-FJ2-011/2006** számú Felülvizsgálati Jegyzőkönyvét.

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

- a HUNG-T-011/2003 tanúsítás során már DRAFT verzióban megjelent és figyelembe vett SSCD védelmi profilnak való megfelelőségi vizsgálatok;
- egyes algoritmusokat /ld. alább/ leszámítva, az eltelt időszakban nyilvános források között nem jelent meg olyan információ, mely befolyásolná/érvénytelenítené a kártya biztonságos működését;
- a Tanúsítvány kiállítása óta megjelent CWA 14890-1:2004 (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, mely 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 az RSA 1024-es, valamint az SHA-1 algoritmusok használhatóságának időpontjáig / c) pont/**, de legfeljebb további 2 évre meghosszabbítja**

a 2003.09.24-én kiállított HUNG-T-011/2003 számú Tanúsítvány érvényességét

a) a HUNG-T-011/2003 számú Tanúsítvány 1. számú mellékletében részletezett feltétel-rendszer teljesülése mellett;

b) biztonságos környezetben a HUNG-T-011/2003 számú Tanúsítvány 1. számú mellékletében részletezett feltételrendszer teljesülése mellett a III.5 érvényességi feltétel teljesítése nélkül is (mely feltételt helyettesítheti a biztonságos aláírói környezet garantálása).

c) 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-FJ3-011-2009.**

Jegyzőkönyv kelte: 2009. szeptember 18.

A Tanúsítvány kiterjesztett érvényességi ideje évenkénti felülvizsgálati eljárás mellett:

2011. szeptember 24.

PH.

Endrődi Zsolt
Tanúsítási igazgató

dr. Szabó István
Ügyvezető igazgató