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**

az **ORGA** Kartensysteme GmbH által előállított és forgalmazott SLE66CX320P mikrochipből és **MICARDO** v2.1 operációs rendszerből álló /hardver verzió SLE66CX320P/m1421b25, szoftver verzió v2.1 64/32 R1.0/ **minősített elektronikus aláírások létrehozására alkalmazható intelligens kártyának** „3-as típusú biztonságos aláírás-létrehozó eszköz”-re vonatkozó, 2003.07.10-én kiállított **HUNG-T-009-2003** számú Tanúsítványát, 2005.07.20-án kiállított **HUNG-FJ-009-2005** számú Felülvizsgálati Jegyzőkönyvét, 2006.07.07-án kiállított **HUNG-FJ2-009-2006** számú Felülvizsgálati Jegyzőkönyvét és a 2009.07.07-án kiállított **HUNG-FJ3-009-2009** számú Felülvizsgálati Jegyzőkönyvét**.**

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

- a korábbi tanúsítás során már DRAFT verzióban megjelent és figyelembe vett SSCD védelmi profilnak való megfelelőségi vizsgálatok;
- az eltelt időszakban nyilvános források között nem jelent meg olyan információ, mely befolyásolná/érvényteleníténé 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**

a 2003.07.10-én kiállított HUNG-T-009/2003 számú Tanúsítvány érvényességét

a) a HUNG-T-009/2003 számú Tanúsítvány 1. számú mellékletében részletezett feltétel-rendszer teljesülése mellett;

b) biztonságos környezetben HUNG-T-009/2003 számú Tanúsítvány 1. számú mellékletében részletezett feltételrendszerből a I.3. és a III.12. érvényességi feltételek teljesítése elhagyható (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-FJ4-009-2009.**

Jegyzőkönyv kelte: 2009. szeptember 30.

A Tanúsítvány kiterjesztett érvényességi ideje évenkénti felülvizsgálati eljárás mellett:

2011. szeptember 24.

PH.

Endrődi Zsolt
Tanúsítási igazgató

dr. Szabó István
Ügyvezető igazgató