TANÚSÍTVÁNY

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

tanúsítja,

hogy az **Oberthur Card Systems** által előállított és forgalmazott

IDOneClassIC Card

intelligens kártya termék

tanúsítás tárgyát képező verziója:

ID-One Cosmo 64 RSA v5.4, applet: IDOneClassIC v1.0
platform: P5CT072VOP és
ID-One Cosmo 64 RSA v5.4.1, applet: IDOneCIE v1.01.1
platformok: P5CT072VOP, P5CC072VOP és P5CD072VOP

elektronikus aláírási termék

az 1. számú mellékletben részletezett feltételrendszer teljesülése esetén

megfelel

a 2001. évi XXXV. törvényben szereplő
minősített elektronikus aláírások létrehozására alkalmazható
„3-as típusú biztonságos aláírás-létrehozó eszköz”-nek

Jelen tanúsítvány a HUNG-TJ-049-2010. számú tanúsítási jelentés alapján került kiadásra.
Készült a NetLock Hálózatbiztonsági és Informatikai Szolgáltató Kft. megbízásából.

A tanúsítvány regisztrációs száma: **HUNG-T-049-2010.**
A tanúsítás kelte: 2010. szeptember 30.
A tanúsítvány érvényességi ideje: 2013. szeptember 30.
Melléklet: tulajdonságok, feltételek, követelmények, egyéb jellemzők, összesen 5 oldalon.

PH.

Endrődi Zsolt	dr. Szabó István
Tanúsítási igazgató	Ügyvezető igazgató

1. számú melléklet

A tanúsítvány érvényességi feltételei

Az alábbiakban összefoglaljuk azokat a feltételeket, melyek **együttes** betartása feltétele az IDOneClassIC Card intelligens kártya termék BALE-ként való biztonságos felhasználásának.

Általános érvényességi feltételek

Az alábbi feltételek minden felhasználási mód esetén (tehát a fejlesztő-gyártó cég által igen általánosra tervezett felhasználási kör egészében) szükségesek a megbízható és biztonságos működéshez.

1. Az IDOneClassIC Card intelligens kártya szolgáltatásait igénybe vevő adminisztrátorok és felhasználók (aláírók) jól képzettek és megbízhatóak.
2. Az IDOneClassIC Card intelligens kártya szolgáltatásait igénybe vevő adminisztrátorok és felhasználók betartják a felhasználói dokumentáció által a biztonságos használatra vonatkozó ajánlásokat.

Az CC tanúsítás érvényességi feltételei

3. A CGA minősített tanúsítványokat generál, amelyek tartalmazzák többek között: a) a TOE-t használó aláíró nevét[1], b) az aláíró kizárólagos befolyása alatt álló TOE által tartalmazott SCD-hez tartozó SVD-t, c) a CSP fokozott biztonságú aláírását. (OE.CGA_QCert)
4. A CGA ellenőrzi, hogy az SSCD-e a kapott SVD küldője, valamint ellenőrzi a kapott SVD sértetlenségét. A CGA ellenőrzi az aláíró SSCD-jében lévő SCD és a minősített tanúsítványban szereplő SVD közötti összetartozást. (OE.SVD_Auth_CGA)
5. Ha külső eszköz gondoskodik a humán interfészről a felhasználói hitelesítés során, akkor ennek az eszköznek biztosítania kell a VAD bizalmasságát és sértetlenségét, ahogyan azt az alkalmazott hitelesítési módszer megkívánja. (OE.HI_VAD)
6. Az SCA: a) elkészíti a DTBS-ként bemutatott adat DTBS-reprezentációját, amit az aláíró alá akar írni, a TOE által aláírásra alkalmas formában; b) továbbítja a DTBS-reprezentációt a TOE felé, és lehetővé teszi, hogy a TOE ellenőrizni tudja a DTBS-reprezentáció sértetlenségét; c) hozzácsatolja a TOE által előállított aláírást az adathoz vagy különállóan szolgáltatja azt. (OE.SCA_Data_Intend)
7. A generált SCD/SVD RSA kulcspár ajánlott mérete 2048 bit. Ettől kisebb, de 1020 bitnél nagyobb RSA kulcspár 2011. szeptember 24-ig használható, feltéve, hogy a Hatóság ezt határozatban hamarabb meg nem tiltja.
8. Bármilyen hosszú RSA kulcs generáláshoz legalább 5 bit hosszú nyilvános exponens használata szükséges, azaz értéke>=17.
9. A felhasználó a PIN kód értékét ne válassza hat jegynél rövidebbre.
10. Az aláírási művelet előtt az aláírónak és az SCA-nak azonosítania és hitelesítenie kell magát.

[1] A név lehet álnév is, de ezt a tényt a minősített tanúsítványban jelezni kell.

Az SM (Secure messaging) elhagyásának feltételei

11. Amennyiben az IDOneClassIC Card intelligens kártyát úgy perszonalizálták, hogy az SM (secure messaging) kiépítésre nem képes, akkor a biztonságos környezet kialakításának szükségességéről a végfelhasználót (aláírót) a kártyát kibocsájtó hitelesítés szolgáltatónak egyértelműen tájékoztatni kell.
12. A működtetési környezet biztosítja a TOE által a CGA felé exportált SVD sértetlenségét. A CGA ellenőrzi az összetartozást az aláíró SSCD-jében lévő SCD és a hitelesítés-szolgáltató (CSP) tanúsítvány-generáló funkciója számára adott inputban lévő SVD között. (OE.SVD_Auth)
13. Ha külső eszköz gondoskodik a humán interfészről a felhasználói hitelesítés során, akkor a működtetési környezetnek biztosítania kell a VAD bizalmasságát és sértetlenségét, ahogyan azt az alkalmazott hitelesítési módszer megkívánja. (OE.HI_VAD_NOSM)
14. Az SSCD ellátó szolgáltatás hiteles eszközöket kezel, amelyek a jogosult felhasználó, mint aláíró számára elkészítendő TOE-kat valósítanak meg; perszonalizálja és kibocsátja az SSCD-ként funkcionáló TOE-t az aláírónak. (OE.SSCD_Prov_Service)
15. A működtetési környezet biztosítja, hogy a DTBS/R nem módosítható az SCA és a TOE közötti átvitel során. (OE.DTBS_Protect)
16. Az aláíró meggyőződik arról, hogy az SSCD ellátó szolgáltatástól kapott SSCD-ben tárolt SCD még nem használták. (Ehhez a kibocsájtó megfelelő útmutatót biztosít.) Az aláíró a TOE-t felügyelete alatt tartja és bizalmasan kezeli a VAD-jét. (OE.Signatory)

A biztonságos aláírás-létrehozó eszközként történő használhatóság kiegészítő feltételei

Egy minősített aláírásokat létrehozó aláírónak az IDOneClassIC Card intelligens kártya felhasználása során az alábbi kiegészítő feltételeket is be kell tartania:

17. A BALE-ként használt IDOneClassIC Card intelligens kártyának csak egy felhasználója lehet, az aláíró.
18. Az IDOneClassIC Card intelligens kártyának használatának lezárulását követően a kártyát meg kell semmisíteni, vagy vissza kell juttatni a kibocsátóhoz.
19. A minősített aláírások létrehozására használt magánkulccsal csak minősített aláírást szabad létrehozni. (Így nem szabad fokozott biztonságú aláírás-létrehozására felhasználni.)

2. számú melléklet

Termékmegfelelőségi követelményeket tartalmazó dokumentumok

Az elektronikus aláírásról szóló 2001. évi XXXV. Törvény

CEN/ISSS ESign Workshop – Expert Group F: Protection Profile – Secure Signature-Creation Device Type 3, version: 1.05, EAL4+

3. számú melléklet

A tanúsításhoz figyelembe vett egyéb dokumentumok

Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005

Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 2.3, August 2005

IDOneClassIC CARD Security Target, ref. FQR: 110 3517, edition 4, 16/01/07

IDOne™ ClassIC Card V1.0 Public Security Target (eredeti biztonsági előirányzat kivonat)

Certification Report 2007/02 (IDOneClassIC Card: ID-One Cosmo 64 RSA v5.4 and applet IDOneClassIC v1.0 embedded on P5CT072VOP) (eredeti tanúsítási jelentés)

ANTERAK project: Evaluation Technical Report, ref. ANTERAK_ETR_V1.2, version 1.2, 24/01/07

IDOneClassIC Guidance, ref. FQR : 110 3558, édition: 1 du 20/11/06

Software Requirement Specification, ref. 066771 00 SRS, édition 1-AB du 23/11/06

Rapport de Maintenance ANSSI-CC-2007/02-M02

IDOne Classic Card SSCD Type 3 Proprietary Security Target (új biztonsági előirányzat)

Különbségek az IDOne Classic Card Public Security Target és az IDOne Classic Card SSCD Type 3 Proprietary Security Target között (az eredeti és az új biztonsági előirányzat összehasonlítása)

NETLOCK ID-ONE CLASSIC File Structure and Access Conditions (a Netlock Kft. számára leszállított kártyák megszemélyesítésének részletei)

IDOne Classic Card SSCD Type 3 ÉRTÉKELÉSI JELENTÉS v1.0 Készítette Hunguard Kft.

Kérelem /a tanúsítás elvégzésére/