



TANÚSÍTVÁNY

A **HUNGUARD** Számítástechnikai-, informatikai kutató-fejlesztő és általános szolgáltató Kft. a 15/2001. (VIII. 27.) MeHVM rendelet alapján, mint a Magyar Köztársaság Informatikai és Hírközlési Miniszter 002/2004 számú kijelölési okiratával kijelölt tanúsító szervezet

tanúsítja,
hogy a

Pénzügyi Szervezetek Állami Felügyelete
által kifejlesztett

IngridSigno Webservice 2.1.5
aláíró alkalmazás

az 1.számú mellékletben áttekintett funkcionalitással, valamint

a 2. számú melléklet biztonságos felhasználásra vonatkozó feltételek figyelembe vételével

megfelel

**a 2001. évi XXXV törvényben szereplő
fokozott biztonságú elektronikus aláírás**

létrehozásában és ellenőrzésében történő felhasználásra

Jelen tanúsítvány a HUNG-TJ-023-2004. számú tanúsítási jelentés alapján került kiadásra. Készült a Pénzügyi Szervezetek Állami Felügyelete megbízásából.

A tanúsítvány regisztrációs száma: **HUNG-T-023-2004.**

A tanúsítás kelte: 2004. december 14.

A tanúsítvány érvényességi ideje: 2007. december 14.

Melléklet: tulajdonságok, feltételek, követelmények, egyéb jellemzők összesen 5 oldalon.

PH.

Endródi Zsolt
Tanúsítási igazgató

dr. Szabó István
Ügyvezető igazgató



1. számú melléklet

Az IngridSigno Webservice 2.1.5 legfontosabb tulajdonságainak összefoglalása

Az IngridSigno Webservice 2.1.5 aláíró alkalmazás feladata, foglalkoztatók és egyéni vállalkozók magánnyugdíjpénztári tagdíjbevallásának fogadása és azok formai ellenőrzése alapján válasz üzenet generálása és a válasz üzenet fokozott biztonságú elektronikus aláírással történő ellátása.

Az IngridSigno Webservice 2.1.5 az alábbi komponenseket valósította meg:

- Aláírandó adat formattáló
- Adatlenyomat készítő
- Aláírói dokumentum szerkesztő
- Aláírás naplózó
- Hitelesítés szolgáltatóval való kölcsönhatás összetevője

Az alkalmazás Microsoft Windows 98SE/2000/2003/XP operációs rendszeren működik. Az alkalmazás alapja a Kopint-Datorg RT által fejlesztett MultiSigno 2.2.b7 programozói könyvtár. E könyvtárban lévő objektumokon keresztül éri el az operációs rendszer Crypto API-ját, amely a CSP (Crypto Service Provider) segítségével szoftveres úton készíti el magát az aláírást. Az aláírás folyamat során a megfelelő XML struktúrák legenerálódnak az aláírandó adatra az aláírás a CSP-n keresztül készül el.

Az IngridSigno Webservice 2.1.5 jellemző tulajdonságai:

- RFC3275 szabvány szerinti dokumentum formátum
- Szabványos X.509 tanúsítványok kezelése (Windows tanúsítványtárban)
- Tanúsítvány érvényességi állapot teljes körű ellenőrzése.



2. számú melléklet

A biztonságos felhasználás feltételei

Az alábbiakban összefoglaljuk azokat a kötelezően betartandó, a jelen tanúsítvány érvényességére kiható feltételeket, melyek hozzájárulnak az IngridSigno Webservice 2.1.5 aláíró alkalmazás által kezelt aláírások biztonságához.

1. számú feltétel: *Az IngridSigno Webservice 2.1.5 aláíró alkalmazás működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy az aláírási folyamatba ne avatkozhassanak be olyan nem megbízható rendszer és alkalmazási folyamatok, perifériák és kommunikációs csatornák, amelyek nem szükségesek az aláírás-létrehozás alkalmazás működéséhez.*

2. számú feltétel: *Az IngridSigno Webservice 2.1.5 aláíró alkalmazás működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni az alábbiak biztosítására:*

- *vírusok ne ronthassák el az aláíró alkalmazást és az általa meghívott egyéb aláíró összetevőket, valamint*
- *az esetlegesen vírussal fertőzött aláíró összetevőket megfelelően helyre lehessen állítani.*

3. számú feltétel: *Az IngridSigno Webservice 2.1.5 aláíró alkalmazás működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy megvédjék Az IngridSigno Webservice 2.1.5 aláíró alkalmazás funkcionális összetevőinek sértetlenségét, megakadályozva, hogy behatolók elrontsák ezt.*

4. számú feltétel: *Az IngridSigno Webservice 2.1.5 aláíró alkalmazás működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy az IngridSigno Webservice 2.1.5 aláíró alkalmazást, valamint valamennyi az aláírás-létrehozás, aláírás-ellenőrzés folyamatokkal kölcsönhatásba lépő összetevőjét egy biztonságos területen valósítsák meg.*



3. számú melléklet

Termékmegfeleléségi követelmények

Követelményeket és szabványokat tartalmazó dokumentumok

Az elektronikus aláírásról szóló 2001. évi XXXV. törvény

CEN/ISSS/E-Sign; Area G1 14170:2001 munkacsoport egyezmény: Security Requirements fro Signature Creation System

CEN/ISSS/E-Sign; Area G2 14171:2001 munkacsoport egyezmény: Procedures for Electronic Signature Verification

CEN/ISSS/E-Sign; Area V 14172-4:2001 munkacsoport egyezmény: Signature Creation Application and Procedures for Electronic Signature Verification

ETSI TS 101 733 v1.4.0 Electronic Signature Formats

RFC3039 Qualified Certificates Profile

RFC3061 Time-Stamp Protocol (TSP)

RFC3275 XML-Signature Syntax and Processing (XMLDSig)

RFC3280 Certificate and Certificate Revocation List (CRL) Profile

Szabványok

CAPI Microsoft Cryptographic Application Interface

PKCS#1 RSA Cryptographic Standard /RFC2313/

RSA Rivest-Shamir-Adleman (public key cryptosystem) /ANSI X9.31/

SHA-1 Secure Hash Algorithm /FIPS PUB 180-1/



4. számú melléklet

A tanúsítási eljárás egyéb jellemzői

A tanúsításhoz figyelembe vett, fejlesztői dokumentumok

- Kérelem a tanúsítás elvégzéséhez
- IngridSigno Webservice 2.1.5 Telepítési és Üzemeltetési kézikönyv
2004. október 01.
- Követelményspecifikáció PSZÁF elektronikus tagdíjbevallás projekt
2004. augusztus 02.
- Rendszerterv PSZÁF elektronikus tagdíjbevallás projekt 2004. augusztus 12.
- Elektronikus Aláírási Szabályzat OID: 1.3.6.1.4.1.16261.3.2.1.2.3
- Tesztelési terv
2004. szeptember 01.
- Tesztelési tervkiegészítés
2004 szeptember 21.
- Tesztelési jegyzőkönyv
2004. szeptember 28.
- Fejlesztői nyilatkozatok (2004 november 08; 2004 november 30;
2004 december 08)

A tanúsításhoz figyelembe vett, fejlesztőktől független dokumentumok

- Értékelési jelentés a IngridSigno Webservice 2.1 elektronikus aláíró alkalmazásról (készítette: HunGuard Kft)

A követelményeknek való megfelelést ellenőrző vizsgálat garancia szintje

A jelen tanúsítási jelentéshez figyelembe vett a fejlesztőktől független ellenőrző vizsgálat garancia szintje az ISO 15408 /Common Criteria/ **EAL 3**-as szintjéhez hasonló volt. /Az EAL3 a fejlesztőktől független garantált biztonság közepes szintjét biztosítja./

A fejlesztőktől független ellenőrző vizsgálat összefoglalásaként egy értékelési jelentés készült.

Jelen tanúsítási jelentés alapvetően a fejlesztői bizonyítékokra, valamint az értékelési jelentésben megfogalmazott és dokumentált eredményekre épül.

Az értékelés az alábbi garanciaosztályokra terjedt ki:

- kiszállítás és működtetés
- fejlesztés
- útmutató
- tesztek

Az értékelés során, a fentiekén kívül a fejlesztőktől független minta tesztelésre, illetve áthatolás tesztelésre is sor került.