



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

Pénztár v4.0.1.12
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
minősített elektronikus aláírás

létrehozásában és ellenőrzésében történő felhasználásra

Jelen tanúsítvány a HUNG-TJ-022-2004. számú tanúsítási jelentés alapján került kiadásra. Készült a Pénzügyi Szervezetek Állami Felügyelete megbízásából.

A tanúsítvány regisztrációs száma: **HUNG-T-022-2004.**

A tanúsítás kelte: 2004. december 14.

A tanúsítvány érvényességi ideje: 2007. december 14.

Melléklet: tulajdonságok, feltételek, követelmények, egyéb jellemzők összesen 7 oldalon.

PH.

Endródi Zsolt
Tanúsítási igazgató

dr. Szabó István
Ügyvezető igazgató



1. számú melléklet

A Pénztár v4.0.1.12 legfontosabb tulajdonságainak összefoglalása

A Pénztár v4.0.1.12 aláíró alkalmazás feladata, foglalkoztatók és egyéni vállalkozók magánnyugdíjpénztári tagdíjbevallásának elkészítésére és azok minősített elektronikus aláírással és időbélyegzővel történő ellátása, a bevallás elküldése a pénztár szerverére és a kapott nyugta üzenet feldolgozása, az azon elhelyezett fokozott biztonságú pénztári aláírás ellenőrzése, a tartalom megjelenítése és a nyugtaüzenet mentése.

Az aláírás a Pénzügyi Szervezetek Állami Felügyelete által készített Elektronikus Aláírási Szabályzat OID: 1.3.6.1.4.1.16261.3.2.1.2.3 alapján valósul meg.

A Pénztár v4.0.1.12 az alábbi komponenseket valósította meg:

- Aláírói dokumentum megjelenítő
- Aláírási tulajdonság megjelenítő
- Aláírandó adat formattáló
- Aláíróval / Ellenőrzővel kölcsönható
- Adatlenyomat készítő
- Aláírói dokumentum szerkesztő
- Aláírás naplózó
- Hitelesítés szolgáltatóval való kölcsönhatás összetevője

Az alábbi komponenseket az operációs rendszer standard hívásain keresztül (Crypto API) a biztonságos aláíró eszköz CSP –je valósítja meg

- Aláíró hitelesítő
- Biztonságos aláíró eszköz és az aláírás eszköz közötti kommunikátor

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 tud kommunikálni a biztonságos aláíró eszközzel. Az aláírás folyamat során a megfelelő XML struktúrák legenerálódnak az aláírandó adatra az aláírás a CSP-n keresztül készül el.

A Pénztár v4.0.1.12 jellemző tulajdonságai:

- XMLDSig szabvány szerinti hiteles dokumentum formátum
- Szabványos X.509 tanúsítványok kezelése (Windows tanúsítványtárban)
- Az RFC 3161 szabvány szerinti időbélyeg szolgáltatás támogatása
- Felhasználó azonosítás támogatása időbélyeg szolgáltatás használatához
- Tanúsítvány érvényességi állapot teljes körű ellenőrzése.
- Aláíró eszköz kezelése (CSP-n keresztül)



2. számú melléklet

A biztonságos felhasználás feltételei

Az alábbiakban összefoglaljuk azokat a kötelezően betartandó, a jelen tanúsítvány érvényességére kiható feltételeket, melyek hozzájárulnak a Pénztár v4.0.1.12 aláíró alkalmazás által kezelt aláírások biztonságához.

- 1. számú feltétel:** A Pénztár v4.0.1.12 aláíró alkalmazáshoz olyan CSP-t kell alkalmazni, amely képes bekérni az aláíró hitelesítő adatot, és azt továbbítani a biztonságos aláíró eszköz számára.
- 2. számú feltétel:** A Pénztár v4.0.1.12 aláíró alkalmazáshoz olyan CSP-t kell alkalmazni, amely aláírás létrehozó rendszer és a BALE közti minden szükséges kommunikációt végrehajt. (CWA14170 14.1 fejezet)
- 3. számú feltétel:** A Pénztár v4.0.1.12 aláíró alkalmazáshoz olyan CSP-t kell alkalmazni, amely képes fizikai interfészen keresztül a BALE-val kommunikálni.
- 4. számú feltétel:** A Pénztár v4.0.1.12 aláíró alkalmazáshoz olyan CSP-t kell alkalmazni, amely képes kiválasztani a BALE-n levő megfelelő alkalmazást.
- 5. számú feltétel:** A Pénztár v4.0.1.12 aláíró alkalmazáshoz használt BALE eszköz kezelő szoftverének biztosítani kell kezelői felületet, amelyen keresztül az aláíró adathoz (privát kulcs) tartozó tanúsítvány a Microsoft tanúsítványtárába telepíthető.
- 6. számú feltétel:** A Pénztár v4.0.1.12 aláíró alkalmazáshoz olyan CSP-t kell alkalmazni, amely képes a Microsoft Tanúsítványtárból kiválasztott tanúsítványhoz tartozó aláírás létrehozó adatot (magánkulcsot) a BALE-n kiválasztani.
- 7. számú feltétel:** A Pénztár v4.0.1.12 aláíró alkalmazáshoz olyan CSP-t kell alkalmazni, amely képes az aláíró hitelesítő adatot és az aláíró hitelesítő összetevőt egy megbízható útvonalon keresztül a BALE-nak átadni.
- 8. számú feltétel:** A Pénztár v4.0.1.12 aláíró alkalmazáshoz olyan CSP-t kell alkalmazni, amely képes az aláírandó adat reprezentánst átadni a BALE-nak, valamint képes visszavenni az elektronikus aláírást.
- 9. számú feltétel:** A Pénztár v4.0.1.12 aláíró alkalmazáshoz olyan CSP-t kell alkalmazni, amely képes megőrizni az aláírandó adat reprezentáns (DTBSR) és valamennyi protokoll adat sértetlenségét.
- 10. számú feltétel:** A Pénztár v4.0.1.12 aláíró alkalmazáshoz olyan CSP-t kell alkalmazni, amely képes megőrizni az aláíró hitelesítő adatok bizalmasságát.

11. számú feltétel: A Pénztár v4.0.1.12 aláíró alkalmazás működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy az aláírási folyamatba ne avatkozassanak be olyan nem megbízható rendszer és alkalmazási folyamatok, perifériák és kommunikációs csatornák, amelyek nem szükségesek az aláírás-létrehozás alkalmazás működéséhez.

12. számú feltétel: A Pénztár v4.0.1.12 aláíró alkalmazáshoz olyan CSP-t kell alkalmazni, amely megőrzi az aláíró hitelesítő adatok bizalmasságát, és biztonságosan törli azokat, amikor már nincs azokra szükség.

13. számú feltétel: A Pénztár v4.0.1.12 aláíró alkalmazáshoz telepíteni kell a BALE eszköz kezelő szoftverét, amely biztosítja a tudáson alapuló hitelesítő adatok lecserélhetőségét.

14. számú feltétel: A Pénztár v4.0.1.12 aláíró alkalmazáshoz olyan CSP-t kell alkalmazni, amely nem jeleníti meg a tudáson alapuló hitelesítő adatot a képernyőn.

15. számú feltétel: A Pénztár v4.0.1.12 aláíró alkalmazáshoz használt BALE eszköz kezelő szoftverének biztosítani kell PIN kód lecserélésénél az új PIN kód kétszeri megadását, a helytelen adatbevitel elkerülése érdekében.

16. számú feltétel: Amennyiben a Pénztár v4.0.1.12 aláíró alkalmazáshoz használt BALE eszköz biometrikus hitelesítő adatokat használ olyan CSP-t kell alkalmazni, amely ezen adatok kriptográfiai védelmét biztosítja.

17. számú feltétel: Amennyiben a Pénztár v4.0.1.12 aláíró alkalmazáshoz használt BALE eszköz vezeték nélküli összeköttetést használ, olyan CSP-t kell alkalmazni, amely a lehallgatás és a zavarás elleni védelmet biztosítja.

18. számú feltétel: A Pénztár v4.0.1.12 aláíró alkalmazás működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy az aláírás-létrehozó eszközzel kommunikáló összetevőt (CSP) ne lehessen jogosulatlanul módosítani.

19. számú feltétel: A Pénztár v4.0.1.12 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.

20. számú feltétel: A Pénztár v4.0.1.12 aláíró alkalmazás működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy megvédjék A Pénztár v4.0.1.12 aláíró alkalmazás funkcionális összetevőinek sértetlenségét, megakadályozva hogy behatolók elrontsák ezt.

21. számú feltétel: A Pénztár v4.0.1.12 aláíró alkalmazás működtetési környezetében technikai és eljárásrendi intézkedéseket kell tenni annak biztosítására, hogy a Pénztár v4.0.1.12 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 for 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
- Pénztár v4.0.1.12 telepítési és üzemeltetési kézikönyv 2004. október 28.
- 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
- Felhasználói kézikönyv (küldő oldal) 2004. november 08.
- 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 Pénztár v4.0.1.12 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.