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 006/2002 számú kijelölési okiratával kijelölt terméktanúsító szervezet

tanúsítja,

hogy a
Utimaco Safeware AG
által kifejlesztett és forgalmazott

SafeGuard Sign&Crypt Software Development Kit aláíró alkalmazás fejlesztő készlet

2.0-ás verzió

elektronikus aláírási termék

a 2. számú melléklet biztonságos felhasználásra vonatkozó feltételeinek figyelembe vételével

megfelel

a 2001. évi XXXV. törvényben szereplő

fokozott biztonságú elektronikus aláírás

létrehozása és ellenőrzése céljából történő szabványos és biztonságos alkalmazások fejlesztéséhez, az 1. számú mellékletben áttekintett funkcionalitásra.

Jelen tanúsítvány a HUNG-TJ-012-2003. számú tanúsítási jelentés alapján került kiadásra. Készült a Noreg Információvédelmi Kft. megbízásából.

A tanúsítvány regisztrációs száma: **HUNG-T-012/2003.**
A tanúsítás kelte: 2003. szeptember 23.
A tanúsítvány érvényességi ideje: 2006. szeptember 23.
Mellékletek: tulajdonságok, feltételek, követelmények, egyéb jellemzők, összesen: oldalon.

PH.

Tanúsítási igazgató: Ügyvezető igazgató

1. számú melléklet

A SafeGuard Sign&Crypt SDK v 2.0 legfontosabb tulajdonságainak összefoglalása

Áttekintés

A SafeGuard Sign&Crypt SDK (a továbbiakban SDK) egy fejlesztő készlet, melynek segítségével különböző felhasználói igényeket kielégítő alkalmazói programok (aláírás alkalmazás összetevők) fejleszthetők, s építhetők be egy elektronikus üzenetkezelő rendszerbe. A segítségével fejleszthető alkalmazói programok digitális aláírások kezelésére, aszimmetrikus kulcsok felhasználására, illetve üzenetek titkosítására és dekódolására is használhatók.

Az SDK a SafeGuard Sign&Crypt alaptermék funkcionalitására épül, mely digitális aláírásra és üzenet titkosításra szolgáló rendszer (s egy párhuzamos ITSEC értékelés és tanúsítás tárgya volt). Az SDK segítségével egy fejlesztő az SDK részét képező CryptWare Client Server API által biztosított funkcionalitásokat saját rendszerébe integrálhatja.

Az SDK segítségével elérhető funkciók segítségével egy feladótól a fogadóhoz továbbított adatokra egyaránt biztosítható az adatok hitelessége, sértetlensége, letagadhatatlansága és bizalmassága.

A SafeGuard Sign&Crypt SDK egy kliens-szerver rendszernek tekinthető, melyben a CryptWare Client Server API és a mögötte álló SafeGuard Sign&Crypt kernel működik szerverként, a CryptWare Client Server API funkciókat meghívó alkalmazás pedig kliensként.

A SafeGuard Sign&Crypt SDK a következő feladatokhoz biztosít funkciókat:

- a kliens alkalmazás és a SafeGuard Sign&Crypt CryptWare Client Server API közötti kommunikáció elindítása és leállítása,
- intelligens kártyáról vagy titkosított lokális fájlból származó magánkulcsok használata,
- a dokumentum fogadói számára biztosított adatbázisokban tárolt nyilvános kulcsok használata,
- digitális aláírás létrehozása, speciális protokolloknak megfelelő formattálás és a fájl tartalom titkosítása,
- a fájl tartalom dekódolása és a digitális aláírás ellenőrzése.

Digitális aláírás létrehozására és ellenőrzésére egy aszimmetrikus kulcsrendszert (aszimmetrikus titkosító algoritmust) használ az SDK.

Titkosításra és dekódolásra egy szimmetrikus titkosító algoritmust használ az SDK.

Biztonsági funkciók

Az SDK az alábbi biztonsági funkciókat valósítja meg:

Digitális aláírás létrehozás (SF1)
A digitális aláírás a fájl bináris tartalmára készül.
Az aláírások az adatokra számolt lenyomat (hash) értékre vonatkoznak, s maga az aláírás az aláíró (intelligens kártyán vagy helyi adatbázisban tárolt) magánkulcsával történő aszimmetrikus titkosítás.
A dokumentum aláírásán kívül még a hitelesítés-szolgáltató által kibocsátott tanúsítványt is a dokumentumhoz csatolódik, mely bizonyítja az aláíró azonosságát. Ez a tanúsítvány tartalmazza az aláíró nyilvános kulcsát is. Az aláíró hitelessége azzal bizonyított, hogy jogosult felhasználója az intelligens kártyának vagy ismeri az adatbázisban tárolt magánkulcshoz való hozzáférés jelszavát.
A felhasználó tájékoztatást kap az adatok helyes aláírásáról, s ezt az információt meg is kell erősítenie.

/A digitális aláírásra az SHA-1, MD-5 és RIPEMD-160 lenyomatoló (hash) függvények, valamint az RSA aszimmetrikus titkosító algoritmus (legalább 768 bites kulcsméret mellett) használhatók./

Digitális aláírás ellenőrzés (SF2)
Az SF1 által létrehozott aláírást is tartalmazó dokumentum ellenőrzése egyrészt a lenyomat érték dekódolását jelenti a fogadott aláírásból, a küldő nyilvános kulcsának felhasználásával, másrészt a fogadott dokumentumra új lenyomat érték számítását. A két összetartozó lenyomat érték összehasonlítása dönti el, hogy a dokumentum valóban hiteles és változatlan-e (a két érték azonos-e).
A felhasználó tájékoztatást kap a fogadott dokumentum helyes ellenőrzéséről, s ezt az információt meg is kell erősítenie.
Egy dokumentum aláírójának azonosítója és nyilvános kulcsa a dokumentumhoz csatolt tanúsítványból nyerhető ki, mely a hitelesítés-szolgáltató (intelligens kártyán vagy helyi adatbázisban tárolt) nyilvános kulcsával ellenőrizhető.

Szimmetrikus adat titkosítás/dekódolás (SF3)
Az aláírás után a dokumentum adatai és az aláírás titkosításra kerül egy szimmetrikus titkosító algoritmussal.
Az adat dekódolására még a fogadó általi aláírás ellenőrzés előtt kerül sor.
A titkosításra felhasznált kulcs véletlenekből előállított munkaszakasz kulcs, melyet a dokumentum részeként a fogadóhoz továbbítanak, a fogadó nyilvános kulcsával titkosítva. Egyedül a fogadó képes dekódolni ezt a munkaszakasz kulcsot saját magánkulcsával, majd ennek segítségével a dokumentumot és annak aláírását. Több fogadó (címzett) is lehetséges, ilyenkor több titkosított nyilvános kulcs mezőt (benne a munkaszakasz kulcs különböző titkosított képével) kell a dokumentumhoz csatolni.

/Adat titkosításra a DES, Triple-DES és IDEA szimmetrikus titkosító algoritmusok választhatók./

2. számú melléklet

A biztonságos felhasználás feltételei

Az alábbi feltételek betartása hozzájárul a SafeGuard Sign&Crypt SDK v 2.0 segítségével fejlesztett aláíró alkalmazások fokozott biztonságához.
A feltételek között vannak kötelezően betartandó, a tanúsítvány érvényességére kiható feltételek, és vannak olyan feltételek, amelyek az aláírások biztonságára jelentős befolyással bírnak, ezért fokozott (nem minősített) aláíráshoz, ahol a lehetőség adott, ezen feltételek betartása erősen ajánlott.

a) Kötelezően betartandó feltételek:

1. Az elvárt hardver környezet biztosítása

Amennyiben a SafeGuard Sign&Crypt SDK-hoz (és a segítségével fejlesztett alkalmazói programokhoz) intelligens kártyát használnak, akkor:
az alábbi típusú kártyaolvasót kell alkalmazni:

- CardMan vagy
- CardMan Compact, illetve

az alábbi típusú intelligens kártyákat kell alkalmazni:

- SLE CR80S (T-COS operációs rendszerrel, a kártyán 768 bites RSA műveletekkel),
- SLE 44CR80S (CardOS operációs rendszerrel, a kártyán 1024 bites RSA műveletekkel).

2. Az elvárt szoftver környezet biztosítása

A SafeGuard Sign&Crypt SDK a következő operációs rendszereken használható:

- Windows 95,
- Windows NT 4.0 munkaállomás és szerver.

3. Biztonságos konfigurálás

Biztonságos alkalmazások fejlesztése érdekében az API függvényeit a „SafeGuard Sign&Crypt SDK programozói útmutató biztonságos alkalmazásokhoz” dokumentum alábbi utasításainak megfelelően kell használni:

- Valamennyi SDK függvény hívás esetén (a CCSClose kivételével) a visszatérési kódot ellenőrizni kell,
- Abban az esetben, ha egy SDK függvény visszatérési kódja problémát jelez, a felhasználót tájékoztatni kell a problémáról, az alkalmazás kapcsolatát a SafeGuard Sign&Crypt Kernel felé le kell zárni, s egy üresjárat állapotba kell visszatérni.
- Egy fájl kezelő biztonsági függvénynek paraméterként átadandó magánkulcsot (pontosabban az ezt meghatározó adatokat) az SDK-tól közvetlenül a meghívás előtt kell lekérni, s érvényességét ellenőrizni kell. Érvénytelenség esetén a függvényt nem szabad meghívni.
- Egy fájl kezelő biztonsági függvénynek paraméterként átadandó nyilvános kulcsot (pontosabban az ezt meghatározó adatokat) az SDK-tól közvetlenül a meghívás előtt kell lekérni, s érvényességét ellenőrizni kell. Érvénytelenség esetén a függvényt nem szabad meghívni.

- Különösen a digitális aláírás létrehozás / ellenőrzés függvények üzemmód paraméterét kell helyesen beállítani ahhoz, hogy a dokumentumokra biztonságos digitális aláírás létrehozás és ellenőrzés valósuljon meg. (A paraméternek tartalmaznia kell az „S”, illetve „E” karaktereket, a dokumentum digitális aláírása, illetve titkosítása érdekében.)

4 Az ITSEC által értékelt algoritmusok használata

Csak az alábbi, az ITSEC értékelés során megvizsgált kriptográfiai algoritmusokat hívják meg:

- lenyomatoló (hash) függvény
  - SHA-1,
  - MD-5,
  - RIPEMD-160,
- aszimmetrikus titkosító algoritmus
  - RSA (legalább 768 bites kulcsméret mellett)
- szimmetrikus titkosító algoritmus
  - DES (CBC, 56 bites kulcsméret),
  - Triple-DES (CBC, 112 bites kulcsméret),
  - IDEA (CBC, 128 bites kulcsméret),

b) Ajánlások a fokozott biztonságú aláírás-alkalmazásokhoz:

5 Eljárásrendi/szervezeti védelmi intézkedések

Eljárásrendi/szervezeti védelmi intézkedésekkel kell támogatni az aláíró alkalmazások fejlesztését megvalósító számítógép(ek)re irányuló olyan támadások kivédését, melyek manuális hozzáférésen, illetve adathordozóról történő adatbevitelen alapulnak. Garantálni kell, hogy a fejlesztés technikai környezete, valamint a fejlesztett programok és az ehhez felhasznált fejlesztő készlet funkcióit ne lehessen manipulálni, melyet különösen vírus és Trójai faló bejuttatása okozhat. Minden újonnan telepített szoftvernek manipulációtól mentesnek kell lennie.

6. konfigurációmenedzselési eljárások

Az aláíró alkalmazásokat fejlesztő környezetben konfigurációmenedzselési eljárások kidolgozásával és betartásával kell garantálni a fejlesztett termékek sértetlenségét azzal, hogy fegyelmet és ellenőrzést követelnek meg a fejlesztendő termék és más ezzel összefüggő információ pontosításában és módosításában.

A védett működtetési környezetben történő felhasználás járulékos feltétele:

7. Mester példányok alkalmazása

Amennyiben a fejlesztő környezetnek hálózati kapcsolatai is vannak a 6. feltételben elvárt konfigurációmenedzselési eljárásokon kívül rendszeres időnként ellenőrizni kell a fejlesztő készlet és a fejlesztett aláíró alkalmazás verziók sértetlenségét, az elkülönítetten is letárolt mester példányok időszakos összehasonlításával.

3. számú melléklet

TERMÉKMEGFELELŐSÉGI KÖVETELMÉNYEK

Követelményeket és szabványokat tartalmazó dokumentumok

Követelmények

Az elektronikus aláírásról szóló 2001. évi XXXV. törvény

CEN/ISSS/E-Sign; Area G1, 14170 munkacsoport egyezmény: Security Requirements for Signature Creation Systems

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

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

4. számú melléklet

A tanúsítási eljárás egyéb jellemzői

A tanúsításhoz figyelembe vett egyéb fejlesztői dokumentumok

Kérelem a tanúsítás elvégzésére

Kérdőív a tanúsítás kérelmezéséhez

A tanúsításhoz figyelembe vett, fejlesztőktől független dokumentumok

Certification Report /SafeGuard Sign&Crypt Software Development Kit version 2.0, Utimaco Safeware AG/ debisZERT-DSZ-ITSEC-04008-1999

Certification Report /SafeGuard Sign&Crypt version 2.2, Utimaco Safeware AG/ debisZERT-DSZ-ITSEC-04007-1999

A követelményeknek való megfelelést ellenőrző független vizsgálat garancia szintje

ITSEC E2

A SafeGuard Sign&Crypt SDK v 2.0 biztonsági funkciók értékelt erőssége

közepes szintű