TANÚSÍTVÁNY (E-MS09T_TAN-ST) MELLÉKLETE

Dokumentumazonosító	**TAN-ST.ME-01**	
Projektazonosító	**E-MS09T**	**Microsec Kft. ST tanúsítás 2009**
MATRIX tanúsítási igazgató	**Szádeczky Tamás**	
Kelt	**Budapest, 2010. március 31.**	
…….. MATRIX tanúsítási igazgató		

1. A TANÚSÍTÁS KÖRÜLMÉNYEI

A MATRIX Kft. a 9/2005. (VII. 21.) IHM rendeletnek megfelelően a hírközlésért felelős miniszter által az elektronikus aláírási termékek tanúsítására kijelölt független tanúsító szervezet.

A MICROSEC Kft. elektronikus aláírási termékek fejlesztésével és forgalmazásával foglalkozó vállalkozás.

A MICROSEC 2003-ban kifejlesztett egy Védelmi Profilt, majd arra alapozva több Biztonsági Előirányzatot és alkalmazást is. Mivel a Védelmi Profil és az ezen alapuló Biztonsági Előirányzatok érvényessége már lejárt, a folyamatos programfejlesztés és a tanúsíthatóság fenntartása érdekében MICROSEC elhatározta a teljes tanúsítási lánc átdolgozását, frissítését.

A Common Criteria publikációkban elérhető nyilvános információk alapján a MICROSEC úgy döntött, hogy az új tanúsításhoz egy nyilvánosan elérhető és szabadon felhasználható USA kormányzati Védelmi Profilt kíván felhasználni, amelyet más fejlesztők is alapul vesznek termékeik fejlesztése és tanúsítása során.

A ST vizsgálata során tételesen megvizsgáltuk, hogy a ST mennyiben felel meg az előírt és vállalt normatív dokumentumoknak, melyek a következők:

Kötelező érvényű normatívák:

- 2001. évi XXXV. törvény az elektronikus aláírásról,
- 3/2005 (III. 18.) IHM rendelet az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről,
- Nemzeti Hírközlési Hatóság Hivatala Informatikai Szabályozási Igazgatóság HL-21917/2008 határozata a felhasználható biztonságos kriptográfiai algoritmusokról,

valamint a hozzájuk tartozó paraméterekről a mellékletekben foglaltaknak megfelelően.

A fejlesztő önként vállalt normatívái:

- **MATRIX által vizsgált normatívák:**

  - Az Európai Parlament és a Tanács 1999/93/EK számú Irányelve az elektronikus aláírással kapcsolatos közösségi keretrendszerről,

  - A Miniszterelnöki Hivatalt vezető miniszter 2/2002. (IV. 26.) MeHVM irányelve a minősített elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó biztonsági követelményekről,

  - 114/2007. (XII. 29.) GKM rendelet a digitális archiválás szabályairól,

  - US Government Family of Protection Profiles Public Key-Enabled Applications For Basic Robustness Environments (v2.8, May 2007) profil családból származtatott U.S. Government Basic Robustness PKE PP with
    − Certification Path Validation – Basic
    − PKI Signature Generation
    − PKI Signature Verification
    − PKI Encryption using Key Transfer Algorithms
    − PKI Decryption using Key Transfer Algorithms
    − Online Certificate Status Protocol Client
    − Certificate Revocation List (CRL) Validation
    at EAL 3 with augmentation.

- **Fejlesztő, vagy más szervezetek által igazolandó megfelelések:**

  - 46/2007. (XII. 29.) PM rendelet az elektronikus számlával kapcsolatos egyes rendelkezésekről;

  - 12/2005. (X. 27.) IHM rendelet az elektronikus ügyintézési eljárásban alkalmazható dokumentumok részletes technikai szabályairól;

  - 13/2005. (X. 27.) IHM rendelet a papíralapú dokumentumokról elektronikus úton történő másolat készítésének szabályairól;

  - 225/2009. (X. 14.) Korm. rendelet az elektronikus közszolgáltatásról és annak igénybevételéről;

  - 223/2009. (X. 14.) Korm. rendelet az elektronikus közszolgáltatás biztonságáról;

  - 222/2009. (X. 14.) Korm. rendelet az elektronikus közszolgáltatás működtetéséről;

  - Az Informatikai és Hírközlési Minisztérium ajánlása a közigazgatásban alkalmazható időbélyegzés formátum műszaki specifikációjára, 2005. november 1.;

  - Az Informatikai és Hírközlési Minisztérium ajánlása a közigazgatásban alkalmazható végfelhasználói tanúsítványok szerkezetének és adattartalmának műszaki specifikációjára, 2005. november 1.;

- Az Informatikai és Hírközlési Minisztérium ajánlása a közigazgatásban alkalmazható elektronikus aláírás formátumok műszaki specifikációjára, 2005. november 22.;

- Az Informatikai és Hírközlési Minisztérium ajánlása a közigazgatásban alkalmazható elektronikus aláírási szabályzatok készítésére, 2005. november 22.

2. A VIZSGÁLAT TÁRGYA

2.1. A tanúsításhoz a gyártó által átadott eszközök és dokumentációk

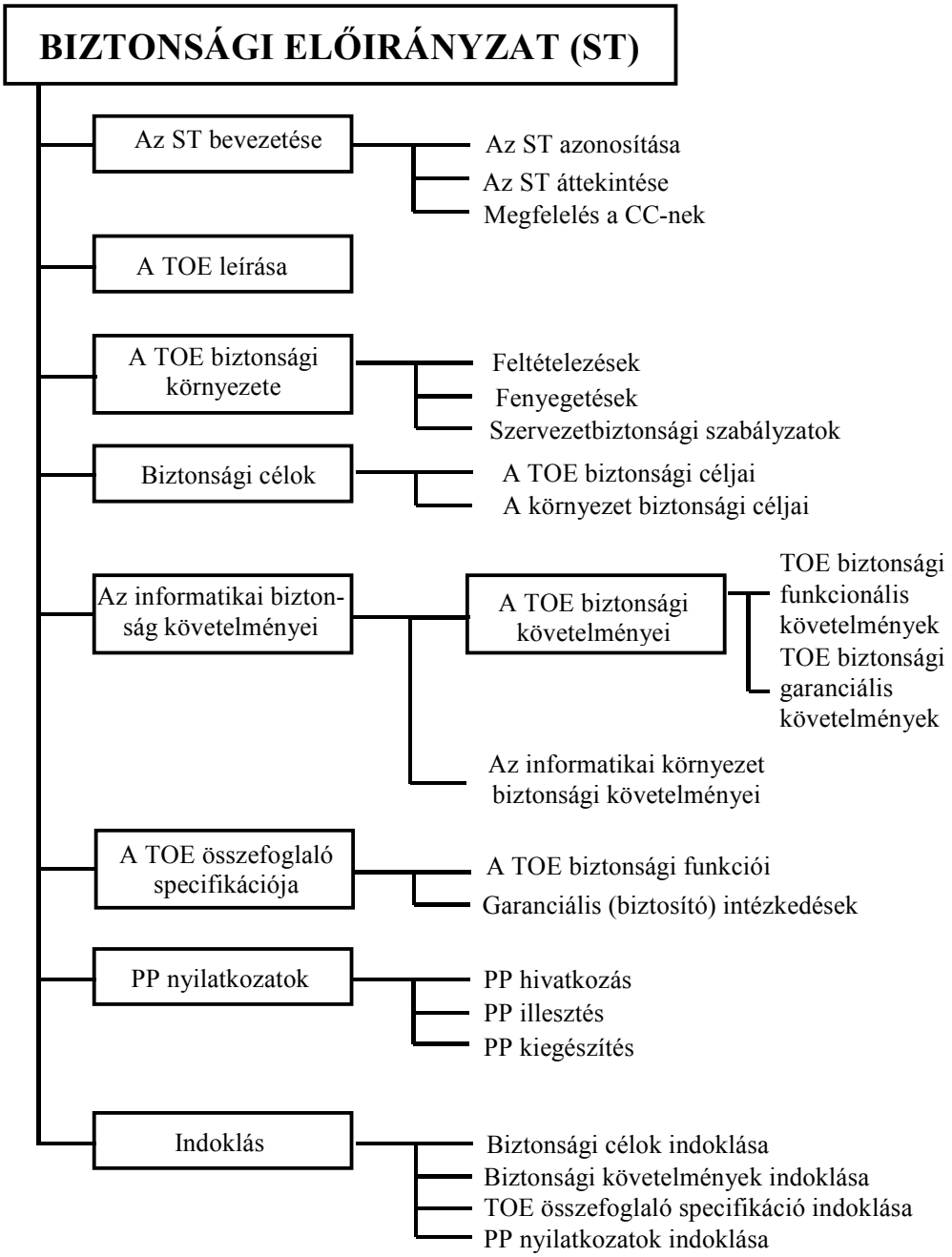
Megnevezés: Biztonsági Előirányzat az e-Szignó minősített aláírás létrehozó és kezelő megbízható modulhoz v1.0.

Típus	Tárgy	Verzió	Dátum	Adat-hordozó
Dokumentáció	BIZTONSÁGI ELŐIRÁNYZAT az e-Szignó minősített aláírás létrehozó és kezelő megbízható modulhoz OID 1.3.6.1.4.1.21528.2.1.3.57	1.0	2010. 02. 15.	elektronikus
Dokumentáció	Fejlesztő nyilatkozata a biztonsági körülményekről		2010. 02. 15.	papír

3. LEÍRÁS

A fejlesztő által a MATRIX részére átadott Biztonsági Előirányzat, az MSZ ISO/IEC 15408 - Az informatikai biztonság értékelésének közös szempontrendszere alapján a biztonsági követelmények olyan halmazát tartalmazza, amelyet vagy a fejlesztő által készített Védelmi Profil, vagy közvetlenül a CC funkcionális és garancia-összetevőire való hivatkozással képeztek, vagy explicit módon adtak meg. A ST adott TOE számára lehetővé teszi a szabványban előírt, és megfelelő biztonsági követelmények megadását. A ST tartalmazza a TOE biztonsági követelményeinek és céljainak összefoglaló előírását, valamint a mögöttes elvek és indokok kifejtését. Az ST az alapja a felek között bármilyen megegyezésnek, amely arról szól, hogy a TOE milyen biztonsági szintet nyújt.

A Biztonsági Előirányzat szerkezete a CC-nek megfelelő, a következőképpen meghatározott rendszerű:



Az ST annak érdekében létrejött dokumentum, hogy egy termék illetve termékcsoport fejlesztésekor előre meghatározott biztonsági követelményrendszer jöjjön létre, ezzel elősegítve a termék és fejlesztésének biztonságát, valamint ezzel a vásárlói bizalmat is elősegítve a termék iránt.

4. MEGFELELŐSÉG A NORMATÍV DOKUMENTUMOK ALAPJÁN

4.1. Megfelelőség

Az elvégzett vizsgálatok alapján megállapítható, hogy a Biztonsági Előirányzat megfelel a MATRIX által normatív dokumentumként kezelt Védelmi Profilnak, illetve a vizsgált kötelező érvényű és a fejlesztő által önként vállalt normatíváknak az 1. pont szerinti

részletezésben. A dokumentum vizsgálata során az is bizonyítást nyert, hogy a dokumentum konzisztens és műszaki szempontból helyes, ezért alkalmas arra, hogy a tervezett elektronikus aláírási termékhez követelményeket rögzítsen.

4.2. Biztonsági garanciaszint vállalása

A megfelelés biztonsági garancia szintje EAL 3+ az alábbiak szerint:

- A Microsec Kft. által készített Biztonsági Előirányzat a Common Criteria szerinti EAL 3 garanciaszintet valósítja meg, kiegészítve az ALC_FLR.2 biztonsági garanciális összetevővel.

4.3. Felhasználási kör

A Vizsgálat Tárgya kizárólag elektronikus aláírás létrehozó és ellenőrző alkalmazás fejlesztéséhez vehető igénybe.

5. RÖVIDÍTÉSEK

Rövidítés	*Tartalom*
BE	Biztonsági Előirányzat - egy megvalósítandó termék biztonsági rendszerterve
CC	Common Criteria - MSZ ISO/IEC 15408. Az informatikai biztonság értékelésének közös szempontrendszere
EAT	2001. évi XXXV. törvény az elektronikus aláírásról
PP	Protection Profile – a Védelmi Profil eredeti, angol elnevezése
ST	Security Target – a Biztonsági Előirányzat eredeti, angol elnevezése
TOE	Target Of Evaluation – a Vizsgálat Tárgya eredeti, angol elnevezése
VP	Védelmi Profil – egy megvalósítandó termék általános, technológia-független leírása, követelményrendszere
VT	Vizsgálat Tárgya – az a termék, amelynek leírását és rendszertervét a BE (ST) tartalmazza

Dokumentum vége