TANÚSÍTVÁNY (E-MS06T-TAN-01.ST)
MELLÉKLETE

Dokumentumazonosító:	**TAN-01.ST.ME-01**	
Projektazonosító:	**E-MS06T**	**Microsec Kft. tan. 2006**
MATRIX tanúsítási igazgató:	**Dr. Szőke Sándor**	
Kelt:	Budapest, 2006. október 2.	
	…… MATRIX tanúsítási igazgató	

1. A TANÚSÍTÁS KÖRÜLMÉNYEI

2003-ban a Microsec Kft. az MSZ ISO/IEC 15408 "Az informatikai biztonság értékelésének közös szempontrendszere" (Common Criteria) alapján elkészült Védelmi Profil (PP-MS-03/001 ver.2.3 tanúsítására kérte fel a MATRIX Kft-t, amely tanúsítás során az E-MS03T_TAN.PP jelű Tanúsítvány kiadása megtörtént. 2004-ben a törvényi változások, illetve a fejlesztő módosításai a vizsgált dokumentumon szükségessé tették a tanúsítás felülvizsgálatát. A felülvizsgálat során a MATRIX Kft. a Védelmi Profil (PP-MS-03/001 ver.3.0) új verzióját megfelelőnek találta, amit a T-MS04F1_TANF.PP jelű Felülvizsgálati Jegyzőkönyv kiadásával igazolt.

A Microsec Kft. az elmúlt években a Védelmi Profil alapján több Biztonsági Előirányzatot (BE) és az ezeknek megfelelő alkalmazást is kifejlesztett, amelyek megfelelőségét minden esetben a MATRIX vizsgálta és tanúsította.

2006-ban a Microsec Kft. újabb programverzió fejlesztésébe fogott, amelynek keretében új Biztonsági Előirányzat kifejlesztését határozta el. A BE és az ezen alapuló alkalmazás tanúsítási eljárásának elvégzésére a MATRIX vállalkozott.

A Biztonsági Előirányzat egy azonosított TOE (Target of Evaluation, a Vizsgálat Tárgya) informatikai biztonsági követelményeit taglalja. Előírja azokat a funkcionális és garanciális biztonsági intézkedéseket, amelyeket ez a TOE valósít meg, hogy a felsorolt követelményeket kielégítse. A TOE feladata az EAT szerinti minősített elektronikus aláírás létrehozása és ellenőrzése.

A TOE számára készült ST alkotja a TOE biztonsági sajátosságait és az értékelés hatókörét rögzítő megállapodás alapját. A ST közönsége nem csak a TOE kidolgozásáért és értékeléséért felelős személyekre, de a TOE menedzseléséért, piacra viteléért, beszerzéséért, telepítéséért, elrendezéséért, üzemeltetéséért és használatáért felelős személyekre is kiterjed.

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.

A fejlesztő önként vállalt normatívái:

– **MATRIX által vizsgált normatívák:**

- MSZ ISO/IEC 15408: Az informatikai biztonság értékelésének közös szempontjai
  - o 15408-1:2002 1. rész: Bevezetés és általános modell,
  - o 15408-2:2003 2. rész: A biztonság funkcionális követelményei,
  - o 15408-3:2003 3. rész: A biztonság garanciális követelményei,
- 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,
- CWA 14170:2001 (E) – Security Requirements for Signature Creation Applications,
- CWA 14171:2001 (E) – Procedures for Electronic Signature Verification.
- A Megbízó által készített Védelmi Profil (PP-MS-03/001 ver. 3.0),

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

- MMM 001:2005. Egységes MELASZ formátum elektronikus aláírásokra. Verzió:1.0.
- RFC 3275: XML-Signature Syntax and Processing,
- RFC 3369: Cryptographic Message Syntax (CMS),
- ETSI TS 101 733 V1.6.3.: Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES),
- ETSI TS 101 903 V1.2.2 (2004-04): XML Advanced Electronic Signatures (XAdES),
- ETSI TR 102 038 V1.1.1 (2002-04): TC Security - Electronic Signatures and Infrastructures (ESI); XML format for Signature Policies,

- 20/2004. (IV. 21.) PM rendelet az elektronikus számláról,
- 7/2005. (VII. 18.) IHM rendelet a digitális archiválás szabályairól, valamint az információs társadalommal összefüggő szolgáltatásokkal kapcsolatos elektronikus archiválás szabályairól,
- 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,
- 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, ST-MS-06/002, Minősített elektronikus aláírás létrehozó és kezelő parancssori alkalmazáshoz.

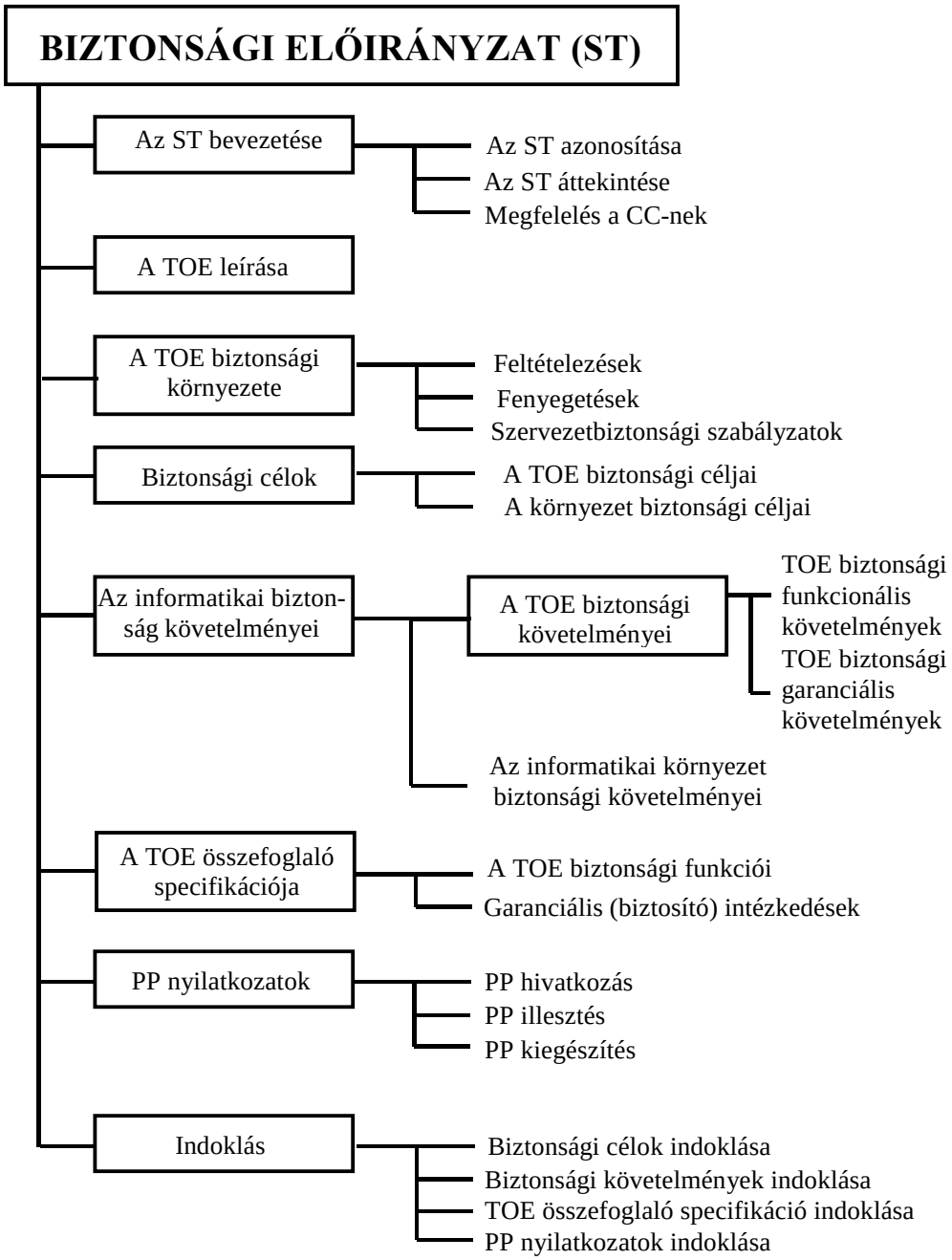
Típus	Tárgy	Verzió	Dátum	Adat-hordozó
Dokumentáció	ST-MS-06/002, Biztonsági előirányzat	1.0	2006. szeptember 2.	elektronikus
Dokumentáció	Fejlesztő nyilatkozata a biztonsági körülményekről		2006. szeptember 2.	papír

3. LEÍRÁS

A fejlesztő által a MATRIX kft. 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 alapján rendkívül kötött, 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 ALC_FLR garanciacsaládnak való megfeleléssel az alábbi kiegészítésekkel:

- A PP-MS-03/001 Védelmi Profil különböző biztonsági szinteket határoz meg egészen EAL 4 szintig. Az EAL 2 szint elemeinek vállalása kötelező érvénnyel előírt, az e feletti szintek vállalása opcionális. A Microsec Kft. az e-Szignó 3.1 minősített elektronikus aláíró parancssori alkalmazás fejlesztéséhez az EAL 3 biztonsági garancia szintet választotta.

- A Microsec Kft. felvállalta – az EAL 3 biztonsági szint követelményei között nem szereplő – ALC_FLR (A termék felfedezett hibáinak javítása) garanciacsaládnak való megfelelést is.

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