

## TANÚSÍTVÁNY (E-MS13T\_TAN-ST) MELLÉKLETE

Dokumentumazonosító	TAN-ST.ME-01	
Projektazonosító	E-MS13T	Microsec Zrt. ST tanúsítás 2013
MATRIX tanúsítási igazgató	Hodován Attila	
Kelt	Budaörs, 2013. augusztus 8.	
 ..... MATRIX tanúsítási igazgató		

### 1. A TANÚSÍTÁS KÖRÜLMÉNYEI

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

A MICROSEC Zrt. 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.

2010-ben a tanúsíthatóság fenntartása érdekében MICROSEC elhatározta a teljes tanúsítási lánc átdolgozását, frissítését, amelynek során a tanúsításhoz egy nyilvánosan elérhető és szabadon felhasználható USA kormányzati Védelmi Profilt (Public Key-Enabled Application Family of Protection Profiles) használt, amelyet más fejlesztők is alapul vesznek termékeik fejlesztése és tanúsítása során.

2011 augusztusában a fenti Védelmi Profil tanúsítványát nem újította meg az USA kormányzata, azonban a Védelmi Profil mind a mai napig megfelelő minőségben tartalmazza az elektronikus aláírási termékek védelmével kapcsolatos követelményeket, így a MICROSEC Zrt. a továbbiakban is erre alapozza Biztonsági Előirányzatát.

Az ST vizsgálata során tételesen megvizsgáltuk, hogy az 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 Média- és Hírközlési Hatóság E-szolgáltatás-felügyeleti Osztály EF-26838-10/2011 számú határozata a felhasználható biztonságos kriptográfiai algoritmusokról, valamint a hozzájuk tartozó paramétereikről 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 keretrendszerrel,
- 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;
- 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*

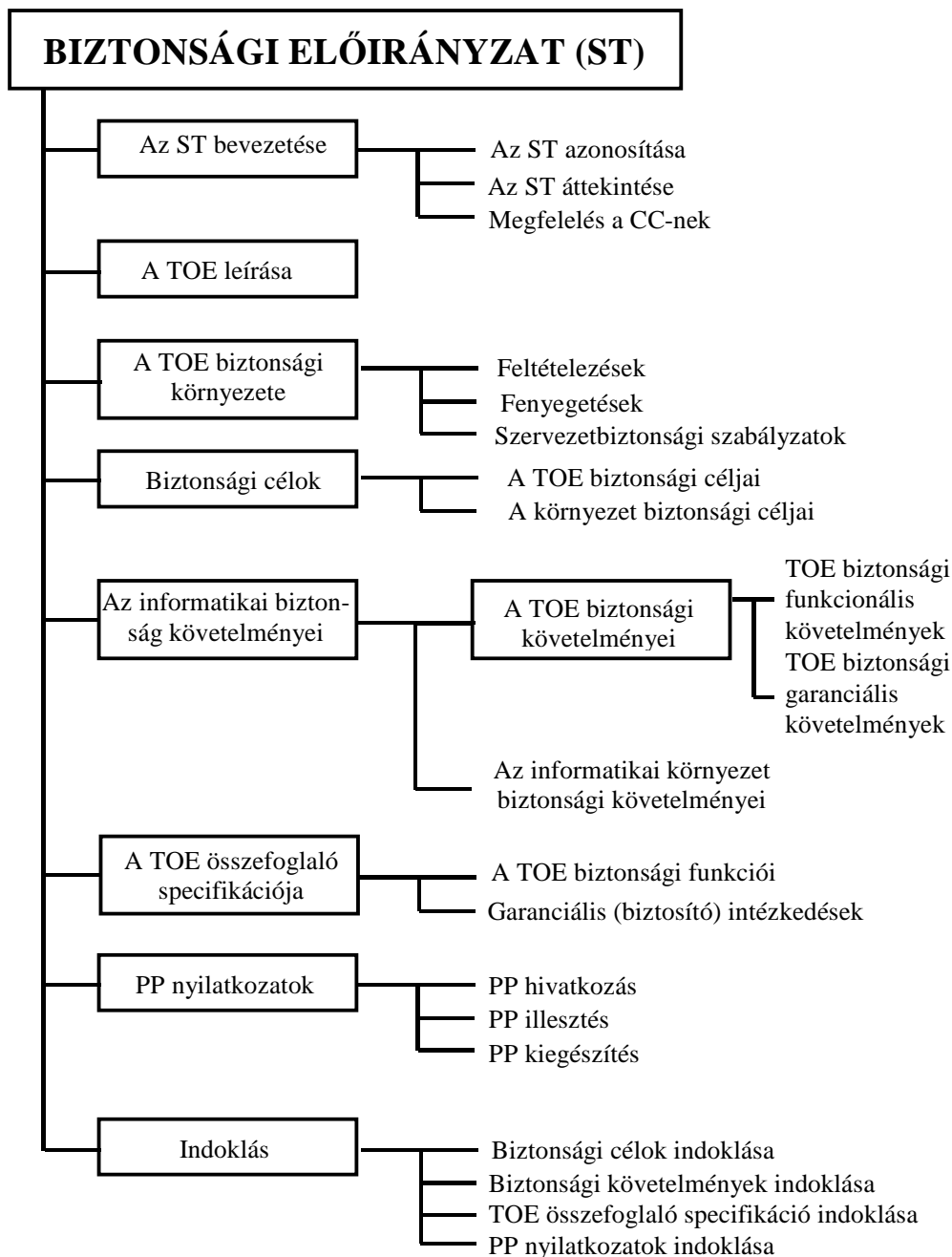
Megnevezés: Biztonsági Előirányzat az e-Szignó minősített aláírás létrehozó és kezelő megbízható modulhoz v1.1.

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	1.1	2013. 05. 15.	elektronikus

## 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. Az ST adott TOE számára lehetővé teszi a szabványban előírt, és megfelelő biztonsági követelmények megadását. Az 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 Zrt. 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 Tárnya kizárólag elektronikus aláírás létrehozó és ellenőrző alkalmazás fejlesztéséhez vehető igénybe.

### 5. RÖVIDÍTÉSEK

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

Dokumentum vége