

## TANÚSÍTVÁNY (E-MS08T\_TAN-ST-01)

### MELLÉKLETE

<b>Dokumentumazonosító</b>	TAN-ST-01.ME-01	
<b>Projektazonosító</b>	E-MS08T	Microsec Kft. tan. 2008.
<b>MATRIX tanúsítási igazgató</b>	Dr. Szőke Sándor	
<b>MATRIX tanúsító</b>	Hornják Gábor	
<b>Kelt</b>	Budapest, 2008. október 10.	
..... MATRIX tanúsítási igazgató		..... MATRIX tanúsító

## 1 A TANÚSÍTÁS KÖRÜLMÉNYEI

A MATRIX Kft a 9/2005 (VII. 21.) IHM rendeletnek megfelelően az elektronikus aláírási termékek tanúsítására kijelölt független tanúsító szervezet. A MICROSEC Kft. elektronikus aláírási termékek, szolgáltatások fejlesztésével foglalkozó vállalkozás. A MICROSEC és a MATRIX között évek óta rendszeres munkakapcsolat áll fenn, amelynek keretében MATRIX számos MICROSEC által fejlesztett elektronikus aláírási termék tanúsítását végezte el.

2007. elején MICROSEC megkeresésére szakmai egyeztetések kezdődtek a MICROSEC által fejlesztett Microsec MicroCA 1.0 szoftver tanúsítása tárgyában. Az egyeztetések során körvonalazódtak a tanúsítás feltételei. A tanúsítást MICROSEC két egymásra épülő lépésben kívánja elvégeztetni:

- Microsec MicroCA 1.0 Biztonsági Előirányzat tanúsítása (ST)
- Microsec MicroCA 1.0 alkalmazás tanúsítása a Common Criteria követelményrendszere szerint kifejlesztett dokumentáció és a rendszeren végzett független tesztek alapján.

A jelen vizsgálat során azt vizsgáltuk, hogy a fejlesztés során előállított Biztonsági Előirányzat megfelel-e a kötelezően betartandó és a Fejlesztő által önként vállalt normatíváknak.

---

---

## **2 ÉRTÉKELÉSI MÓDSZERTAN**

Az értékelés nyelvezete a Közös Szempontrendszerben meghatározott, melynek címei és azonosítói:

- Az informatikai biztonság értékelésének közös szempontrendszere.  
MSZ ISO/IEC 15408-1 : 1. rész: Bevezetés és általános modell  
MSZ ISO/IEC 15408-2 : 2. rész: A biztonság funkcionális követelményei  
MSZ ISO/IEC 15408-3 : 3. rész: A biztonság garanciális követelményei
- Common Criteria (CC) for Information Technology Security Evaluation, version 2.3, August 2005.  
Part 2: Security functional requirements – CCMB-2205-08-002  
Part 3: Security assurance requirements – CCMB-2205-08-003

Az értékelés módszertanának alapját a Közös Szempontrendszerhez használt módszertani ajánlás képzí. Ennek címe és azonosítója a következő:

- Common Methodology for Information Technology Security Evaluation, Evaluation methodology August 2005 Version 2.3 - CCMB-2005-08-004

## **3 NORMATÍV DOKUMENTUMOKBAN MEGHATÁROZOTT KÖVETELMÉNYEK ÉS MEGÁLLAPÍTÁSOK**

Az értékelés során megvizsgáltuk a kötelező és önként vállalt normatíváknek való megfelelést. Az audit során az alábbi vizsgálatokat elvégeztük el:

- Megfelelés a kötelezően betartandó normatíváknek.
  - 2001. évi XXXV. törvény az elektronikus aláírásról,
  - 3/2005. (III. 18.) IHM rendelet az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről.
- Megfelelés az önként vállalt normatíváknek.
  - Az Európai Parlament és a Tanács 1999/93/EK számú Irányelve az elektronikus aláírással kapcsolatos közösségi keretrendszeréről,
  - Common Criteria (CC) for Information Technology Security Evaluation, version 2.3, August 2005.  
Part 2: Security functional requirements  
Part 3: Security assurance requirements
  - Certificate Issuing and Management Components (CIMC) Protection Profile Version 1.0 (Security Level 2) October 31, 2001,
- Biztonsági körülmények, fejlesztői környezet.

## 4 ÉRTÉKELES TÁRGYA

### 4.1 A Biztonsági Előirányzat azonosítása

<b>ST címe</b>	Microsec MicroCA 1.0 Biztonsági Előirányzat 1.2 – 2008. október 7.
<b>ÉT azonosítása</b>	Microsec MicroCA 1.0
<b>Common Criteria megfelelés</b>	Common Criteria (CC) for Information Technology Security Evaluation, version 2.3, August 2005 Part 2 bővített Common Criteria (CC) for Information Technology Security Evaluation, version 2.3, August 2005 Part 3
<b>Védelmi Profil megfelelés</b>	Certificate Issuing and Management Components (CIMC) Protection Profile Version 1.0 (Security Level 2) CC Part 2 conformant October 31, 2001
<b>Garanciaszint</b>	Evaluation Assurance Level (EAL) 2
<b>Kulcsszavak</b>	Nyilvános kulcsú infrastruktúra, PKI, CIMC, Hitelesítő Központ, CA, MicroCA

### 4.2 A tanúsításhoz a megrendelő által átadott eszközök és dokumentációk

Típus	Tárgy	Verzió	Átadás dátuma	Adat-hordozó
Dokumentáció	Microsec MicroCA 1.0 Biztonsági Előirányzat	1.0	2008. január 24.	elektronikus
Dokumentáció	Microsec MicroCA 1.0 Biztonsági Előirányzat	1.1	2008. szeptember 17.	Elektronikus állomány minősített elektronikus aláírással hitelesítve
Dokumentáció	Microsec MicroCA 1.0 Biztonsági Előirányzat	1.2	2008. október 7.	Elektronikus állomány minősített elektronikus aláírással hitelesítve
Dokumentáció	Fejlesztő nyilatkozata a biztonsági körülményekről		2008. szeptember 17.	Elektronikus állomány minősített elektronikus aláírással hitelesítve
Dokumentáció	Szoftverfejlesztés, szoftver üzemeltetés, szolgáltatások nyújtása. Minőségügyi eljárás	Kiadás 4. 2005. január 1.	2008. szeptember 17.	Elektronikus állomány minősített elektronikus aláírással

---

---

				hitelesítve
Tanúsítvány	ISO 9001:2000 tanúsítvány		2008. szeptember 24.	Elektronikus állomány
Tanúsítvány	ISO 27001:2005 tanúsítvány		2008. szeptember 24.	Elektronikus állomány

### **4.3 Fejlesztő**

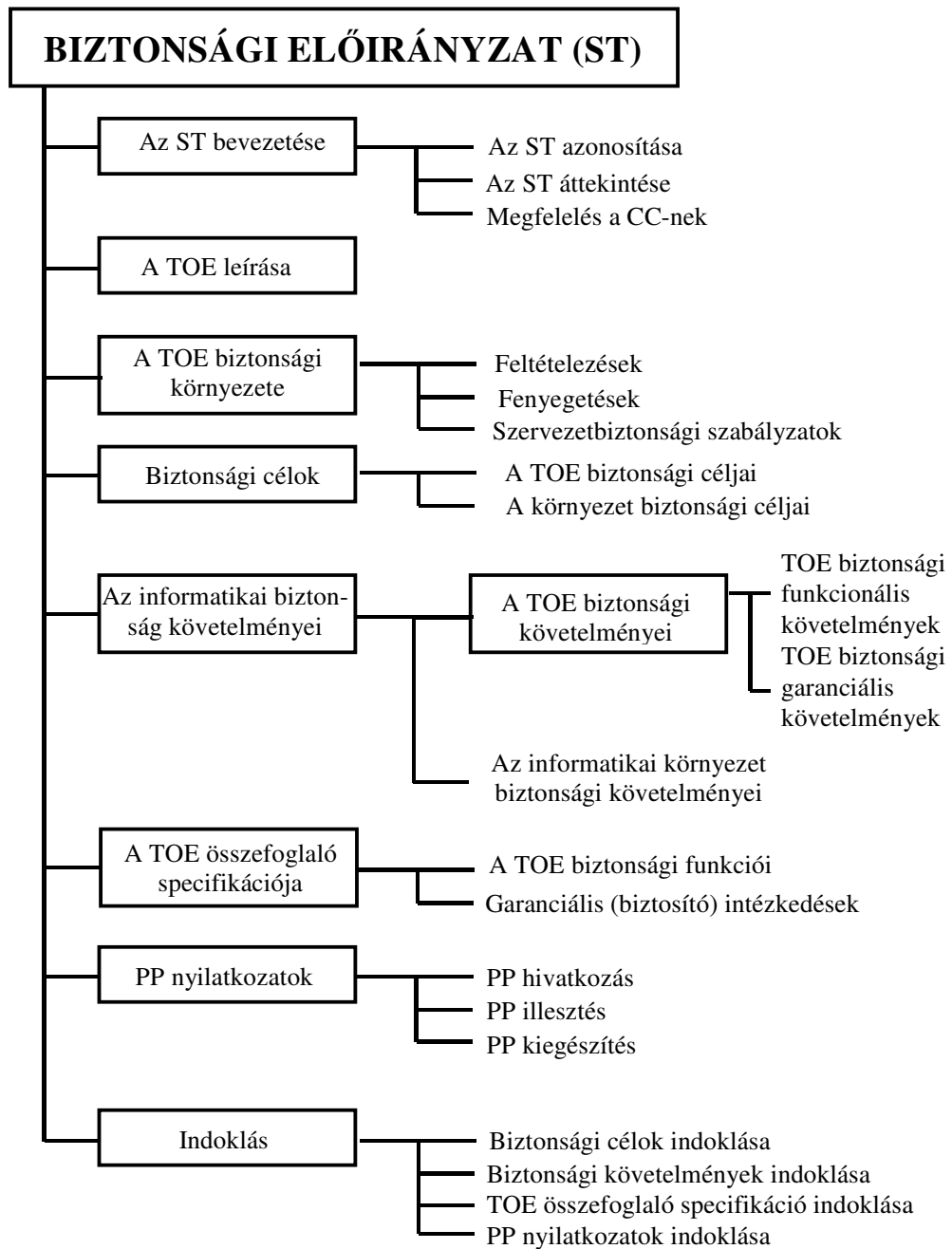
Microsec Számítástechnikai Fejlesztő Kft.  
1022 Budapest, Marczibányi tér 9.

### **4.4 A Biztonsági Előirányzat áttekintése**

A Microsec MicroCA 1.0 olyan alrendszerek összessége, mely tanúsítványok, tanúsítvány visszavonási listák és online tanúsítvány állapot információk kibocsátására, tanúsítványok visszavonására és kezelésére szolgál. A Microsec MicroCA 1.0 Biztonsági Előirányzata azokat a biztonsági követelményeket határozza meg, melyek között az Értékelés Tárgyának működnie kell.

A biztonsági funkcionális és garancia követelmények olyan biztonságos környezetre lettek kialakítva, melyekben megvan a kockázata a kártékony tevékenységnek, de a rendszer jogosult felhasználói nem kártékonyak, valamint az adatkiszivárgás kockázata és hatása a biztonságos környezet miatt elhanyagolható. A Biztonsági Előirányzatban megtalálható a kártékony felhasználók hálózaton keresztüli támadása elleni védelem a kibővített hitelesítési hiba kezelés segítségével. A Biztonsági Előirányzat EAL 2 biztonsági szinttel rendelkezik.

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.

---

---

## **5 MEGFELELŐSÉG A NORMATÍV DOKUMENTUMOK ALAPJÁN**

### **5.1 Megfelelőség**

Az elvégzett részletes vizsgálatok alapján a MATRIX Vizsgáló, Ellenőrző és Tanúsító Kft. megállapítja, hogy a vizsgált területek vonatkozásában a Microsec Kft. által fejlesztett „Microsec MicroCA 1.0 Biztonsági Előirányzat 1.2 – 2008. október 7.” megfelel a kötelező és önként vállalt normatív dokumentumokban foglalt követelményeknek, a megfelelőséget igazoló tanúsítvány kiállítható a kiállítástól számított 3 éves érvényességi idővel.

### **5.2 Biztonsági garanciaszint vállalása**

A megfelelés biztonsági garancia szintje megfelel a Common Criteria EAL 2 szintjének.

## **6 ÉRTÉKELÉSI BIZONYÍTÉKOK**

Az értékeléshez a következő bizonyítékok kerültek felhasználásra:

- Microsec MicroCA 1.0 Biztonsági Előirányzat 1.0 – 2008. január 23.
- Microsec MicroCA 1.0 Biztonsági Előirányzat 1.1 – 2008. szeptember 17.
- Microsec MicroCA 1.0 Biztonsági Előirányzat 1.2 – 2008. október 7.
- A fejlesztő nyilatkozata, hogy a Biztonsági Előirányzat fejlesztésének idejére biztosították a fejlesztéshez szükséges eszközöket, technikát, és biztonságot,
- Szoftverfejlesztés, szoftver üzemeltetés, szolgáltatások nyújtása minőségügyi eljárás,
- ISO 9001:2000 tanúsítvány,
- ISO 27001:2005 tanúsítvány.

## **7 ÉRTÉKELÉSHEZ FELHASZNÁLT AUDIT JELENTÉSEK**

Szakterületi Audit Jelentések:

- Szakterületi Audit Jelentés – 2001. évi XXXV. törvény az elektronikus aláírásról  
(E-MS08T\_SZAJ-ST-01.EAT)
- Szakterületi Audit Jelentés – 3/2005. (III. 18.) IHM rendelet  
(E-MS08T\_SZAJ-ST-02.IHM)

- Szakterületi Audit Jelentés – Az 1999/93 EU irányelvnek való megfelelés vizsgálata  
(E-MS08T\_ SZAJ-ST-03.EUD)
- Szakterületi Audit Jelentés – Közös Szempontrendszer követelményeinek való megfelelés vizsgálata  
(E-MS08T\_ SZAJ-ST-04.CC)
- Szakterületi Audit Jelentés – A fejlesztő által választott Védelmi Profilnak való megfelelés vizsgálata  
(E-MS08T\_ SZAJ-ST-05.PP)
- Szakterületi Audit Jelentés – Biztonsági körülmények, környezet  
(E-MS08T\_ SZAJ-ST-06.KOR)

## 8 RÖVIDÍTÉSEK

Rövidítés	Tartalom
<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>ÉT</b>	Értékelés Tárgya – az a termék, amelynek leírását és rendszertervét a BE (ST) tartalmazza
<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 Tárgya eredeti, angol elnevezése
<b>VP</b>	Védelmi Profil – egy megvalósítandó termék általános, technológia-független leírása, követelményrendszere

**Dokumentum vége**