

TANÚSÍTVÁNY (E-MS03T-TAN.PP) MELLÉKLETE

Dokumentumazonosító:	TAN.PP.ME-01	
Projektazonosító:	E-MS03T	MicroSec Kft. 2003
MATRIX tanúsítási igazgató:	Dr. Tuzson Tibor	
MATRIX tanúsító:	Gyányi Sándor	
Kelt:	Budapest, 2003. október 3.	
..... MATRIX tanúsítási igazgató	 MATRIX tanúsító részéről

1. A TANÚSÍTÁS KÖRÜLMÉNYEI

A fejlesztő az MSZ ISO/IEC 15408 Az informatikai biztonság értékelésének közös szempontrendszere (CC) alapján elkészült Biztonsági Specifikáció tanúsítására felkérte a MATRIX Kft. A dokumentum a CC ajánlásnak megfelelően műszaki megvalósítás-független. Az értékelés tárgyának egy kategóriájára, olyan biztonsági követelmény-rendszer amely adott fogyasztói igényeket elégít ki. Ennek megfelelően jelen vizsgálat tárgyát képező PP-t annak érdekében állította elő a fejlesztő, hogy megalapozza az új termék fejlesztésére vonatkozó, CC ajánlásnak való megfelelést, és ezzel összhangban elősegítse a maximális tervezési biztonságra való törekvést, így megalapozva a biztonságra történő tervezést. Ez a módszer az EAT szerinti minősített elektronikus aláírás fejlesztésére irányuló törekvésként értelmezhető.

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

Kötelező érvényű normatívák:

- 2001 évi XXXV. törvény az elektronikus aláírásról
- 16/2001. (IX. 1.) MeHVM rendelet az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről

A fejlesztő önként vállalt normatívái:

- MSZ ISO/IEC 15408:Az informatikai biztonság értékelésének közös szempontrendszere
 - 15408-1: 1. rész: Bevezetés és általános modell
 - 15408-2: 2. rész: A biztonság funkcionális követelményei
 - 15408-2: 3. rész: A biztonság garanciális követelményei

- EU Directive 1999/93/EC of the European Parliament and the council of 13 December 1999 on a Community framework for electronic signatures;
- CWA 14168 - Secure Signature-Creation Devices, version 'EAL 4';
- CWA 14170 – Security Requirements for Signature Creation Applications
- CWA 14171 - Procedures for Electronic Signature Verification
- A Miniszterelnöki Hivatal vezető miniszter 2/2002. (IV. 26.) MeHVM irányelve a minősített elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó biztonsági követelményekről

2. A VIZSGÁLAT TÁRGYA

2.1. A tanúsításhoz a gyártó által átadott eszközök és dokumentációk

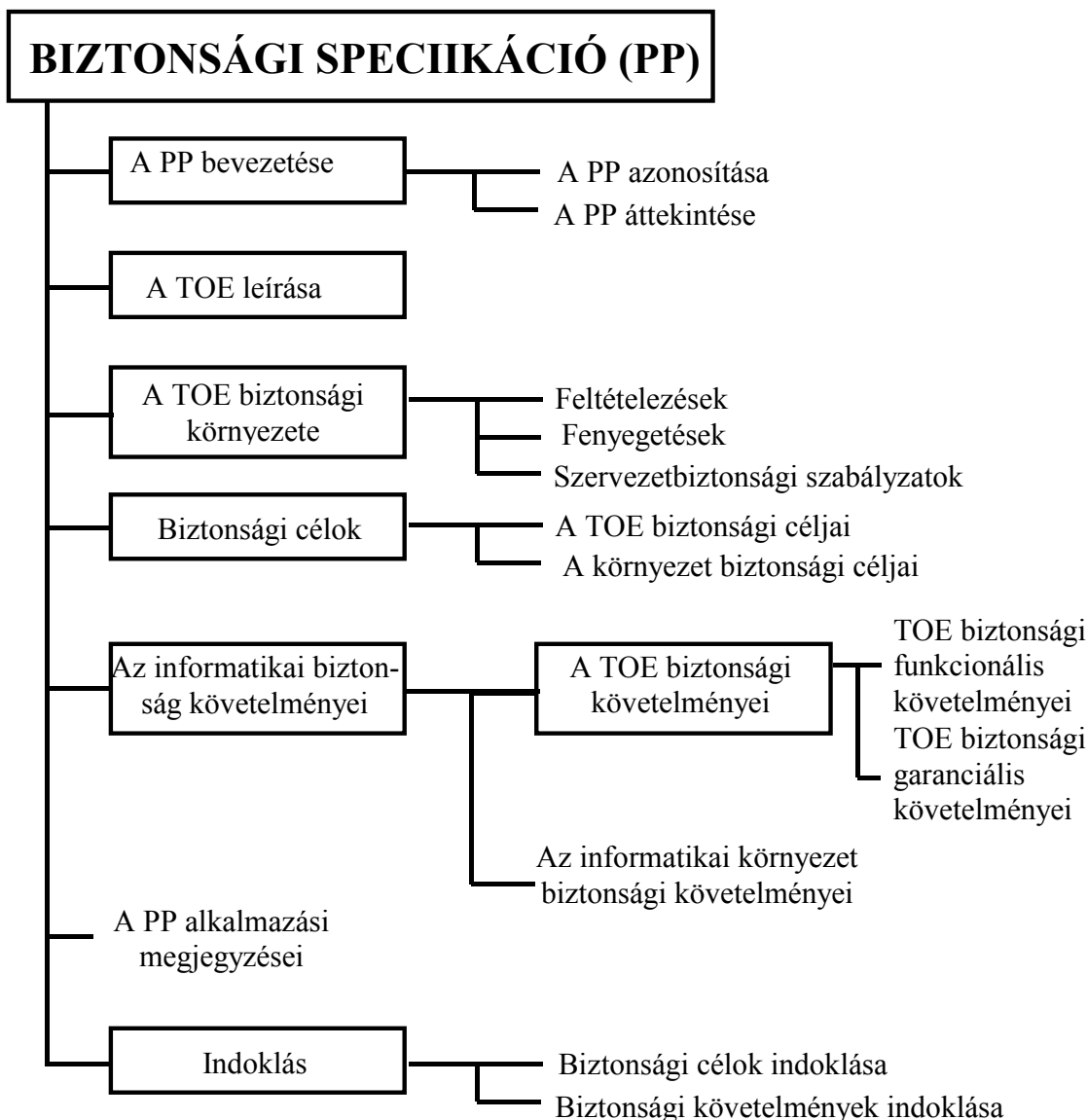
Megnevezés: Biztonsági specifikáció, PP-MS-03/001, Minősített elektronikus aláírás létrehozó és kezelő alkalmazáshoz.

Típus	Tárgy	Verzió	Dátum	Adat-hordozó
Dokumentáció	PP-MS-03/00, Biztonsági specifikáció	2.3	2003. március 26.	elektronikus

3. LEÍRÁS

A fejlesztő által a MATRIX kft. részére átadott PP, az MSZ ISO/IEC 15408 - Az informatikai biztonság értékelésének közös szempontrendszere alapján olyan, vagy a CC-ből származó, vagy explicit módon megadott biztonsági követelményhalmazt tartalmaz, amelynek ajánlatos tartalmaznia egy adott EAL1-EAL7 szintnek megfelelő biztonsági követelményt (esetleg további garancia-összetevőkkel kiegészítve). A PP a TOE-k egy olyan csoportja részére teszi lehetővé a biztonsági követelmények megvalósítás-független kifejezését, amely a biztonsági célok egy adott körével teljes összhangban áll. A PP-t újrafelhasználásra szánták, és olyan TOE követelményeket határoz meg, amelyek hasznosnak és hatásosnak bizonyultak mind a funkcionális, mind a garanciális, azonosított célok kielégítésére. A PP emellett tartalmazza a szóban forgó biztonsági célok és követelmények mögött álló elvek és indokok kifejtését is. A PP eszközt ad a felhasználók számára, hogy hivatkozni tudjanak biztonsági igények valamilyen sajátos, különös körére, és elősegíti a jövőbeli értékelést ezen igények alapján.

A PP szerkezete a CC alapján rendkívül kötött, a következőképpen meghatározott rendszerű:



A PP annak érdekében létrejött dokumentum, hogy egy termék illetve termékcsoport fejlesztésekor előre meghatározott biztonsági követelményrendszert hozzon létre, ezzel elősegítve a termék, és fejlesztésének biztonságát, valamint, hogy ezzel a vásárlói bizalmat is elősegítse a termék iránt.

Mindezeknek megfelelően a vizsgálat tárgyát képező PP-t egy új termék előállítása során lehet felhasználni, illetve a CC megfelelő módszertana alapján, azonosított termék informatikai biztonsági követelményeit és a funkcionális és garanciális biztonsági intézkedéseket tartalmazó ST kidolgozásához vehető igénybe.

4. MEGFELELŐSÉG A NORMATÍV DOKUMENTUMOK ALAPJÁN

4.1. Megfelelőség

A Biztonsági Specifikáció értékelése a CC követelményeknek való megfelelését

vizsgálva a következő minősítést eredményezett:

- **Kiterjeszti (*extended*) a CC 2. részét**

- **Megfelel (*conformant*) a CC 3. részének**

ezzel eleget téve a CC követelményeknek, amely kimondja, hogy az értékelés eredményében a 'megfelelő' minősítésnek olyan nyilatkozatnak kell lennie, amely megadja, hogy milyen mértékben lehet megbízni abban, hogy a PP vagy a TOE teljesíti a követelményeket. Az eredményekben a 2. részből (funkcionális követelmények), a 3. részből (garanciális követelmények), vagy közvetlenül a PP-ről kell kikötéseket tenni.

Jelen kijelentések a következőket takarják:

- A PP kiterjeszti a CC 2. részét, ha a funkcionális követelmények olyan funkcionális összetevőket foglalnak magukban, amelyek nem szerepelnek a 2. részben.
- A PP akkor felel meg a CC 3. részének, ha a garanciális követelmények valamilyen EAL vagy olyan garanciacsomag formájában vannak megfogalmazva, amely csak a 3. részben szereplő garanciaösszetevőkön alapul.

A dokumentum vizsgálata során az is bizonyítást nyert, hogy a dokumentum konzisztens, és műszaki szempontból helyes, és ezért alkalmas arra, hogy a kiértékelendő TOE-hez a követelményekről szóló nyilatkozatként használjuk.

A Biztonsági Specifikáció normatív dokumentumoknak való megfelelését vizsgálva a MATRIX ezirányú módszertan használatával a dokumentumoknak való konformitás megállapítást nyert, kijelenthető tehát, hogy a Biztonsági Specifikáció megfelelő.

Ez a megfelelés jelen körülmények között nem kötelező, de megléte megfelelő alapnak tekinthető a későbbi minősített elektronikus aláírási termék fejlesztéséhez.

4.2. Felhasználási kör

A vizsgálat tárgyának felhasználási körére nézve kikötésként állapítható meg, hogy a dokumentum az elektronikus aláírási témakörbe tartozó elektronikus aláírás létrehozó és kezelő alkalmazás fejlesztéséhez vehető igénybe.

5. RÖVIDÍTÉSEK

CC - MSZ ISO/IEC 15408 Az informatikai biztonság értékelésének közös szempontrendszere

EAT - 2001. évi XXXV. törvény az elektronikus aláírásról

PP – Protection Profile, Biztonsági Specifikáció

ST – Security Target, Biztonsági Előirányzat

TOE – Target Of Evaluation, a Vizsgálat Tárgya

Dokumentum vége