Margaréta
Kártya Menedzsment Rendszer
v2.0

Biztonsági előirányzat

Verzió:	2.0
Dátum:	2010.09.30
Megrendelő:	Noreg Kft.
Fájl:	Margareta_biztonsagi_eloiranyzat_v2.0.doc
Minősítés:	Nyilvános
Oldalak:	62

Tartalomjegyzék

Változás kezelés

Verzió	Dátum	Leírás	Készítette
0.1	2010.07.10.	Szerkezeti vázlat	Makádi Zsolt
0.2	2010.09.01.	Első változat (1,2, 6. 7. fejezetek)	Makádi Zsolt
0.3	2010.09.12.	Pontosított változat	Makádi Zsolt
0.4	2010.09.24.	Kiegészített változat (3.-5. fejezetek)	Makádi Zsolt
0.5	2010.09.27.	Pontosított változat	Makádi Zsolt
2.0	2010.09.30.	Véglegesített változat: Margaréta 2.0	Makádi Zsolt

1. Bevezetés

Ez a fejezet dokumentum-kezelő és áttekintő információkat tartalmaz.

Az "ST hivatkozás" alfejezet egyértelműen azonosítja a biztonsági előirányzatot.

A "TOE hivatkozás" alfejezet egyértelműen azonosítja az értékelés tárgyát.

A „TOE áttekintés” alfejezet összefoglalja a TOE használatát és fő biztonsági tulajdonságait, valamint azonosítja a TOE típusát és a TOE által megkövetelt valamennyi nem TOE hardvert/szoftvert/förmvert.

„TOE leírás” alfejezet leírja a TOE fizikai és logikai hatókörét.

1.1. ST hivatkozás

Cím:	Margaréta Kártya Menedzsment Rendszer v2.0 - Biztonsági előirányzat
Verzió szám:	2.0
Dátum:	2010.09. 30
Szerző:	Kovács Tamás, Makádi Zsolt

1.2 TOE hivatkozás

Az értékelés tárgya:	Margaréta Kártya Menedzsment Rendszer
Az értékelés tárgya rövid neve:	Margaréta rendszer
Verzió szám:	v2.0
Dátum:	2010. 09. 30.
Szponzor szervezet:	Noreg Kft.

1.3. TOE áttekintés

A Margaréta Kártya Menedzsment Rendszer intelligens kártyák és USB tokenek (a továbbiakban kártyák) kezelését valósítja meg, a kártyák teljes életciklusában.

Legfontosabb funkciói az alábbiak:

- regisztrációs feladatok ellátása,
- kártyák kezelése (kibocsátás, nyilvántartás, állapot kezelés, kártya műveletek végrehajtása),
- kártyákon tárolt tanúsítványok kezelése (kibocsátás, visszavonás, felfüggesztés, újra aktiválás).

A regisztrált kártya birtokosok (ügyfelek) adatai külső forrásból (LDAP, IDM) származhatnak, vagy a rendszeren belül kerülnek rögzítésre.

A kártyák kezelése a rendszerbe vételétől kezdve, a kártya kibocsátáson át, a kártyaprofil kezeléstől a különböző riportok készítéséig minden olyan funkciót biztosít, melyre egy vállalati környezetben szükség lehet. A Margaréta rendszer működése során nyomon követhetővé teszi a kártyák állapotát, adatokat szolgáltat a kártyakészletről, státuszinformációkat tárol.

A Margaréta rendszer egy hitelesítés-szolgáltató PKI rendszerhez kapcsolódva részelegesen vagy teljes körűen ellátja a kártyákhoz kapcsolódó nyilvános kulcsú tanúsítványok kezelését is, lehetővé téve a tanúsítványok kibocsátását visszavonását, felfüggesztését és újra aktiválását. (Ezáltal a Margaréta rendszer betölti a hitelesítés-szolgáltató (CA, Certification Authority) regisztrációs alrendszerének (RA, Registration Authority) feladatait.)

Egy Identity Management (IDM) és a Margaréta rendszer együttműködése lehetővé teszi az IDM rendszer számára, hogy az alapvető kártya-igénylési funkciókat a többi jogosultsággal együtt, egységes felületen keresztül valósítsa meg. A Margaréta rendszer közreműködése lehetőséget ad szerepkör alapú kártya-igénylésre, vagy kilépés/tartós távollét esetén a kártyákon tárolt tanúsítványokhoz kötődő jogosultságok automatikus visszavonására/ felfüggesztésére.

A Margaréta rendszer számos biztonsági funkciót tartalmaz a bizalmasság, integritás és hitelesség biztosítása érdekében. Legfontosabb biztonsági tulajdonságai az alábbiak:

- A rendszer kizárólag titkosított és hitelesített SSL kapcsolaton keresztül érhető el felhasználói számára.
- A rendszer használói különböző szerepkörökkel ruházhatók fel, az egyes szerepkörök jól elkülönülő jogosultságokkal rendelkeznek a rendszer által biztosított funkciók igénybe vételére.
- A rendszer által biztosított funkciókat csak egy hozzáférés ellenőrzés után, az azonosított és hitelesített szerepkör jogosítványainak megfelelően érhetik el az egyes felhasználók.
- A rendszer megvédi tárolt adatainak integritását.
- A rendszerben történt valamennyi fontos esemény naplózásra kerül, biztosítva az utólagos egyéni felelősségre vonhatóságot. A naplóesemények tartalmazzák az esemény azonosítását, dátumát és időpontját, valamint az eseményért felelős entitást.

A Margaréta rendszer külső környezetének tartalmaznia kell az alábbiakat:

- egy tanúsítványokkal kapcsolatos hitelesítés-szolgáltatást biztosító (a Margaréta rendszerrel kapcsolatot kezelni képes) PKI rendszer,
- kliens platform, kliens böngésző, hardver token és hardver token kezelő a rendszer privilegizált felhasználói számára,
- böngésző a rendszer végfelhasználói számára,
- Syslog szerver (opcionális),
- SMTP szerver.

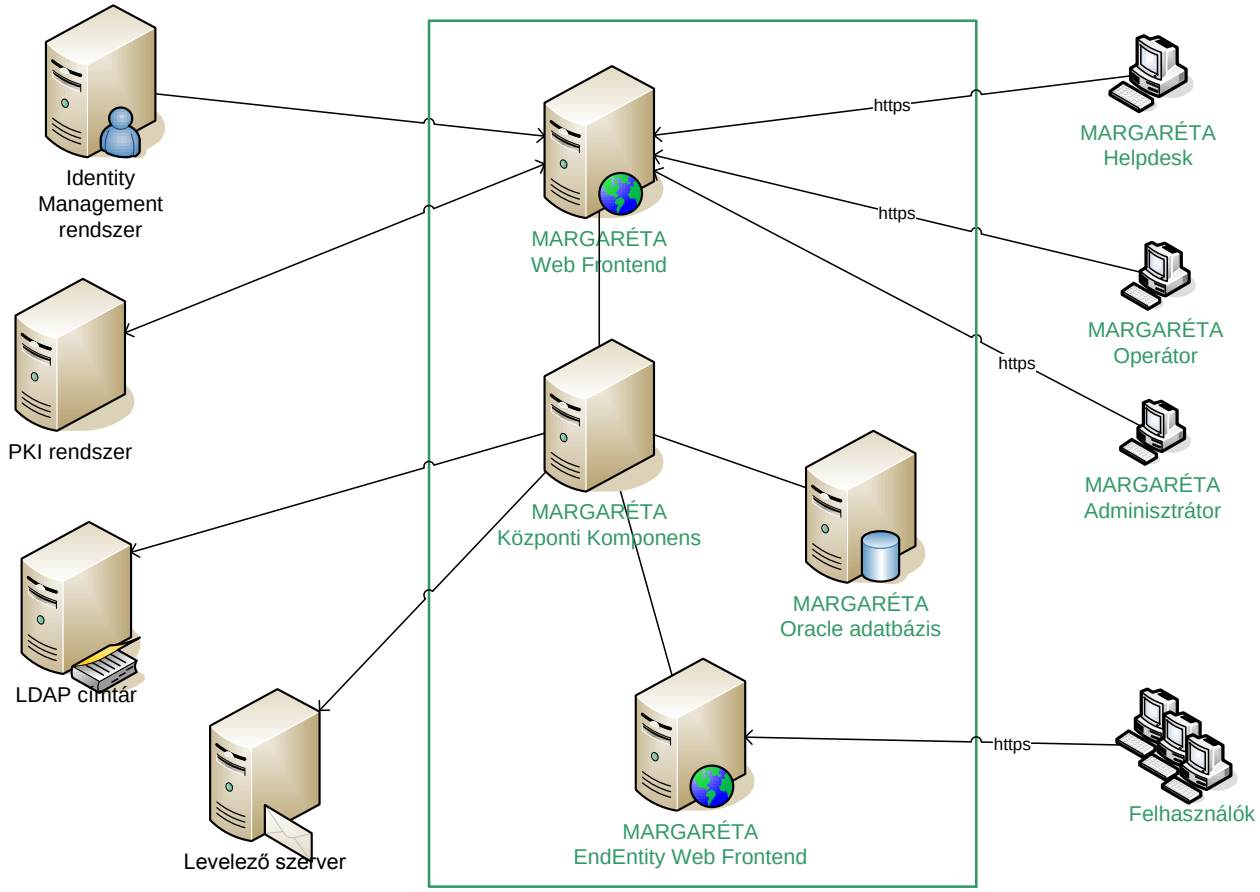
A Margaréta rendszer futtatókörnyezetének tartalmaznia kell az alábbiakat:

- hardverek (a Margaréta komponensek, valamint a futtatókörnyezet számára szükséges hardverek),
- operációs rendszerek (a Margaréta komponensek, valamint az adatbázis kezelő számára szükséges operációs rendszerek),
- adatbázis kezelő (a Margaréta rendszerben tárolt felhasználói és rendszer adatok menedzselését és védelmét megvalósító szoftver),
- alkalmazásszerver (a Margaréta rendszer egyes komponenseinek futtatásához szükséges szoftver),
- Java Development Kit (az alkalmazásszerver futtatásához szükséges szoftver),
- hardver token kezelő (a felhasználók számára készítendő hardver tokenek kezeléséhez szükséges kártyaolvasó és kártya CSP).

A Margaréta rendszer típusa kettős: kártya menedzsment rendszer, egyúttal egy nem minősített hitelesítés-szolgáltató regisztrációs alrendszere is (amely regisztráció, visszavonás kezelés és aláíró eszköz ellátási szolgáltatásokat végez).

1.4. TOE leírás

A Margaréta rendszer fizikai hatókörét, fő összetevőit és a rendszer környezetének fő elemeit az 1.1 ábra szemlélteti, külön (zöld téglalapban) megjelenítve benne az értékelés tárgyát.



1.1. ábra: A Margaréta rendszer fizikai hatóköre

A Margaréta rendszer külső környezetét alkotják az alábbiak:

- **IDM rendszer** (opcionális, a Margaréta rendszer integrálható Identity Management rendszerekkel, mely esetben az IDM saját felhasználói (ügyfelei) számára a Margaréta rendszer különböző regisztrációs, kártya- és tanúsítvány kezelésre vonatkozó szolgáltatásokat nyújt)
- **PKI rendszer** (kötelező, a Margaréta rendszer saját feladatainak elvégzése érdekében egy hitelesítés-szolgáltatótól különböző szolgáltatásokat vesz igénybe)
- **LDAP címtár** (opcionális, a Margaréta rendszer az ügyféltörzs kitöltését LDAP(S) protokollon elérhető címtárból is képes elvégezni)
- **Kliens platform és kliens böngésző** (kötelező, a Margaréta rendszer adminisztratív és végfelhasználói felülete egy kliens oldali platformon futtatott böngészőn keresztül érhető el)
- **Hardver token** (kötelező, a rendszerfelhasználók számára az adminisztratív felület eléréséhez szükséges magánkulcsot tároló hardver)
- **Hardver token kezelő** (kötelező, a rendszerfelhasználók hardver tokenjeinek kezeléséhez szükséges olvasó és CSP)
- **Syslog szerver** (opcionális, a rendszer naplók biztonságos tárolására)
- **SMTP szerver** (kötelező, a Margaréta rendszer által a végfelhasználók számára generált elektronikus levelek továbbítására)

A Margaréta rendszer futtatókörnyezetét alkotják az alábbiak:

- **Hardverek** (kötelező, a Margaréta komponensek, valamint a futtatókörnyezet számára szükséges hardverek)
- **Operációs rendszerek** (kötelező, a Margaréta komponensek**,** valamint az adatbázis kezelő számára szükséges operációs rendszerek)
- **Adatbázis kezelő** (kötelező, a Margaréta rendszerben tárolt felhasználói és rendszer adatok menedzselését és védelmét megvalósító szoftver)
- **Alkalmazásszerver** (kötelező, a Margaréta rendszer Margaréta Web Frontend és Margaréta EndEntity Web Frontend komponenseinek futtatásához szükséges szoftver)
- **Java Development Kit** (kötelező, az alkalmazásszerver futtatásához szükséges szoftver)
- **Hardver token** (kötelező, a rendszerfelhasználók számára készítendő, magánkulcsokkal és tanúsítványokkal ellátott hardver elem)
- **Hardver token kezelő** (kötelező, a rendszerfelhasználók számára készítendő hardver tokenek kezeléséhez szükséges olvasó és CSP)

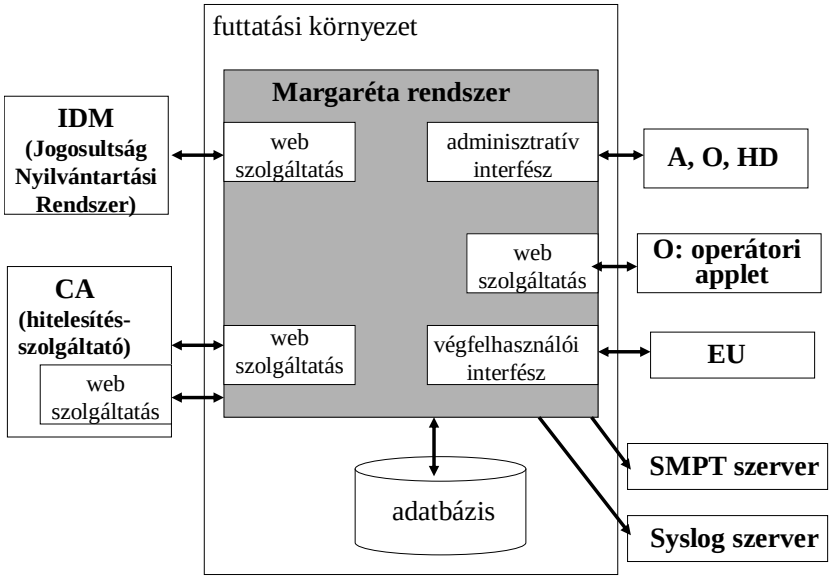
A Margaréta rendszert alkotó szoftver, hardver, förmver és útmutató elemek az alábbiak:
Hardver elemek: ---
Szoftver elemek:

- CAWeb v2.0 (a PKI rendszert kiszolgáló WebService)
- EEWs v2.0 (EndEntity felületet kiszolgáló WebService)
- InfoCaConnector v2.0 (InfoCa konnektor)
- InfoCaWsClient v2.0 (InfoCa WebService kliens)
- Margareta v2.0 (Margaréta Központi Komponens)
- Margareta-EE v2.0 (Margareta EndEntity felület)
- Margareta-EE-WsClient v2.0 (Margareta EndEntity WebService kliens)
- MargaretaUtil v2.0 (Margareta közös szoftver komponensek)
- OperatorApplet v2.0 (Operátori applet)
- PKI_XML v2.0 (InfoCa kommunikáció során használt XML segédosztályok)
- TokenWs v2.0 (a Margaréta Operátori applet (mint kliens) és a Margaréta Központi Komponens (mint szerver) közötti kommunikáció szerver oldali részét megvalósító alkalmazás)

Útmutató elemek:

- Telepítési és konfigurációs dokumentáció
- Operátori kézikönyv
- Végfelhasználói útmutató

A Margaréta rendszer logikai hatókörét, az általa nyújtott logikai biztonsági szolgáltatásokat és külső interfészeit az 1.2 ábra szemlélteti.



1.2. ábra: A Margaréta rendszer logikai hatóköre

A Margaréta rendszer (https protokollon keresztül) egy adminisztratív interfészt biztosít különböző funkciók (http kérések) végrehajtására az azonosított és hitelesített rendszerfelhasználók számára:

- a **Margaréta adminisztrátor (A)** számára a rendszerfelhasználói fiókok kezelését és a rendszer konfigurálását,
- a **Margaréta operátor (O)** számára a végfelhasználói fiókok kezelését és a rendszer napi működtetését (benne a felhasználók kártyáinak és a kártyán tárolt tanúsítványoknak a teljes körű menedzselése)
- a **Margaréta HelpDesk (HD)** számára a napi működtetés részét képező speciális funkciók (benne a kártyák és tanúsítványok felfüggesztése és visszavonása) végrehajtását.

A Margaréta rendszer (https protokollon keresztül) egy végfelhasználói interfészt biztosít az azonosított és hitelesített **végfelhasználók (EU)** számára tanúsítvány igénylésére, majd az elkészült tanúsítvány letöltésére.

A Margaréta rendszer a hitelesített Margaréta operátorok (O) számára egy token applet letöltését is lehetővé teszi, melynek segítségével egy web szolgáltatás igénybevételével az Operátor eszköz ellátási szolgáltatást is végezhet (kulcspárt generáltathat egy hardver tokenen, tanúsítvány kérelmet adhat ki erre, az elkészült tanúsítványt tokenre töltheti).

A Margaréta rendszer (egy https kapcsolaton keresztül elérhető, OASIS SPMLv2 szabványnak megfelelő web szolgáltatással) biztosítja az azonosított és hitelesített **IDM rendszer (IDM)** által kiadott, annak ügyfeleire vonatkozó alábbi parancsok végrehajtását vagy végrehajttatását:

- IDM ügyfelek Margaréta rendszerbe történő regisztrálását, mint végfelhasználók,
- IDM ügyfelek kártyáinak kiadását, illetve visszavonását,
- A Margaréta rendszerben elérhető profilok adatainak lekérdezését,
- IDM ügyfelek kártyáira és az azokon elhelyezett tanúsítványokra vonatkozó adatok lekérdezését.

A Margaréta rendszer és a **PKI rendszer (CA)** (egy-egy https kapcsolaton keresztül elérhető, speciális, XML alapú web szolgáltatáson keresztül) azonosítás és hitelesítés után különböző parancsokat adhatnak egymásnak:

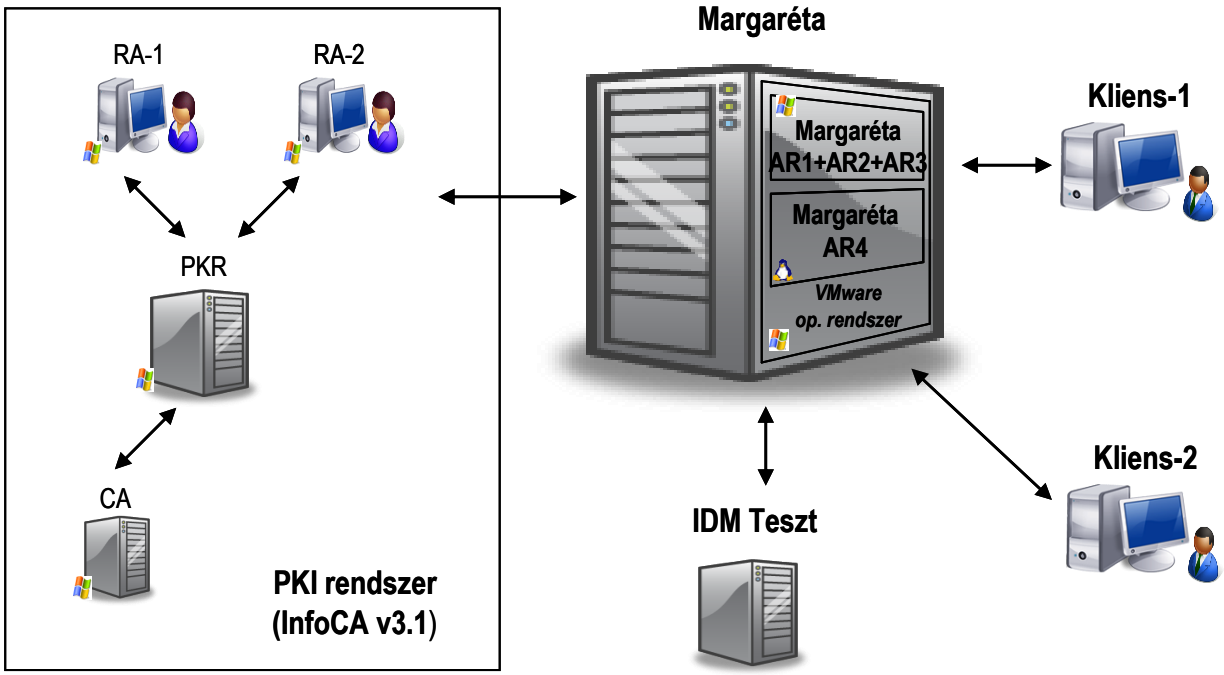
- a Margaréta rendszer oldaláról: tanúsítványok kibocsátására, felfüggesztésére, újra aktiválására, visszavonására, valamint állapotok lekérésére irányuló kérések,
- a PKI rendszer oldaláról: a kérésekre adott válaszok, CRL küldés és tájékoztatás tanúsítvány állapot változásról.

A Margaréta rendszer értékelt konfigurációi az alábbiak voltak:

- értékelt konfiguráció az értékelő helyszínén (egyszerűsített kiépítés)
- értékelt konfiguráció a fejlesztő helyszínén (teljes kiépítés)

Értékelt konfiguráció az értékelő helyszínén

Az 1.3 ábra az egyszerűsített értékelt konfigurációt szemlélteti, melyet az értékelő épített ki saját környezetében.



1.3. ábra: Értékelt konfiguráció az értékelő helyszínén

Külső környezet:

- IDM rendszer: IDMTest.war (egy általános OASIS SPMLv2 szabványt támogató IDM rendszert szimuláló teszt web-alkalmazás)
- PKI rendszer: InfoCA hitelesítés-szolgáltató rendszer v3.1
- LDAP címtár: Windows 2003 ActiveDirectory (a szabványos LDAP(S) protokollt megvalósító alkalmazás, mely az AR1+AR2+AR3 alrendszereket futtató virtuális gép operációs rendszerének a része)
- Levelező szerver: Red Hat Enterprise Linux 5 levelező rendszere (Postfix 2.2.3, mely az AR4 alrendszert futtató megvalósító virtuális gép operációs rendszerének a része)
- Kliens-1 (rendszerfelhasználók /A, O és HD/ számára:
  - operációs rendszer: Microsoft Windows Server 2003 SP2,
  - böngésző: Microsoft Internet Explorer 7
  - hardver token és kezelője: Aladdin eToken 64K, Microsoft Crypto API eTOKCSP.dll
- Kliens-2 (végfelhasználók /EU/ számára):
  - operációs rendszer: Microsoft Windows Server 2003 SP2
  - böngésző: Microsoft Internet Explorer

- Naplózás: az operációs rendszer által védett állományokba.

Futtatókörnyezet - Margaréta Web Frontend, Margaréta Központi Komponens, Margaréta EndEntity Web Frontend:

- Hardver: VMware virtuális gép (Processzor: InteCore i3 M330 2.13 GHZ, Memória: 1,17 GB, Háttértár: 15 GB)
- Operációs rendszer: Windows Server 2003 SP2
- Alkalmazásszerver: SUN Glassfish Enterprise Server v2.1.1 (Sun GlassFish Enterprise Server v2.1)
- Java Development Kit: Java Development Kit 6 Update 14

Futtatókörnyezet - Margaréta Adatbázis:

- Hardver: VMware virtuális gép (Processzor: Intel Core i3 M330 2.13 GHZ, Memória: 1,17 GB, Háttértár: 14 GB)
- Operációs rendszer: Red Hat Enterprise Linux 5
- Adatbázis kezelő: Oracle Database 11g Release 1 (11.1.0.7.0) Enterprise Edition

Értékelt konfiguráció a fejlesztő helyszínén

Az 1.4 ábra a teljes kiépítésű értékelt konfigurációt szemlélteti, melyet a fejlesztő használt saját környezetében.

Külső környezet:

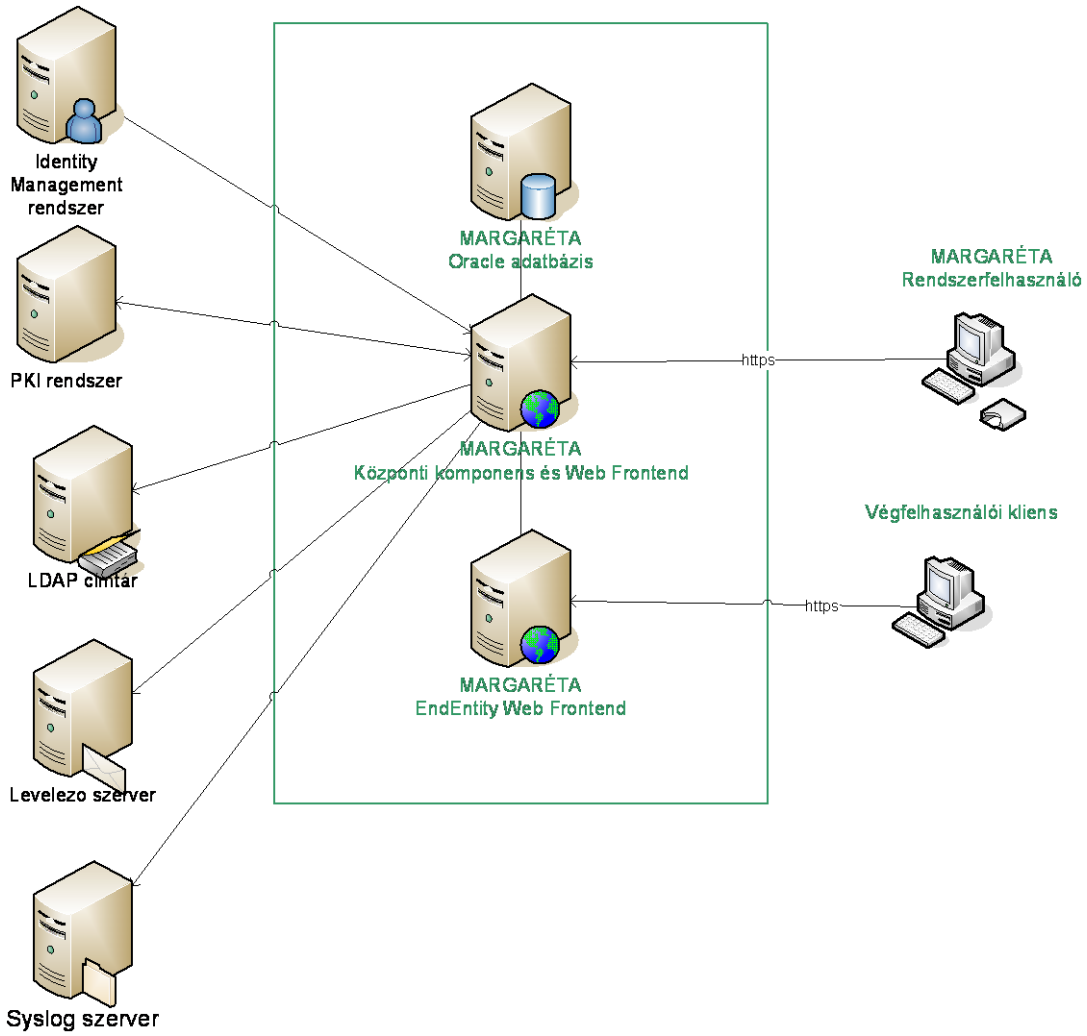
- IDM rendszer: IDMTest.war (egy általános OASIS SPMLv2 szabványt támogató IDM rendszert szimuláló teszt web-alkalmazás)
- PKI rendszer: InfoCA hitelesítés-szolgáltató rendszer v3.1
- LDAP címtár: Windows 2003 ActiveDirectory (a szabványos LDAP(S) protokollt megvalósító alkalmazás
- Levelező szerver: Microsoft Exchange Server 2010
- Kliens oldali (A, O és HD) hardver: HP Compaq 8510p notebook
- Kliens oldali (A, O és HD) operációs rendszer: Microsoft Windows XP SP3
- Kliens oldali (A, O és HD) böngésző: Mozilla Firefox 3.6.9
- Kliens oldali (A, O és HD) hardver token és kezelő: Aladdin eToken 64K, Mozilla NSS, eTPKCS11.dll
- Kliens oldali (EU) hardver: HP Compaq Z400 Workstation
- Kliens oldali (EU) operációs rendszer: Windows 7
- Kliens oldali (EU) böngésző: Mozilla Firefox 3.6.9

Futtatókörnyezet - Margaréta EndEntity Web Frontend

- Hardver: VMware virtuális gép (Processzor: 2*Intel Xeon E5520 2.27 GHZ, Memória: 1 GB, Háttértár: 51 GB)
- Operációs rendszer: Windows Server 2008 R2 Standard
- Alkalmazásszerver: SUN Glassfish Enterprise Server v2.1.1
- Java Development Kit: Java Development Kit 6 Update 21

Futtatókörnyezet - Margaréta Adatbázis

- Hardver: VMware virtuális gép (Processzor: 2*Intel Xeon E5520 2.27 GHZ, Memória: 1,2 GB, Háttértár: 30 GB)
- Operációs rendszer: Red Hat Enterprise Linux 5
- Adatbázis kezelő: Oracle Database 11g Release 1 (11.1.0.7.0) Enterprise Edition



1.4. ábra: Értékelt konfiguráció a fejlesztő helyszínén

2. Megfelelőségi nyilatkozatok

2.1. CC megfelelőség

2.1.1 CC verzió

Jelen biztonsági előirányzat és az alapját képező TOE a CC v3.1-nek felel meg. [1], [2], [3]

Az alkalmazott CC verzió nyelve angol.

2.1.2 ST megfelelőség a CC 2. részéhez képest

Jelen biztonsági előirányzat megfelel a CC v3.1 2. részének.

2.1.3 ST megfelelőség a CC 3. részéhez képest

Jelen biztonsági előirányzat megfelel a CC v3.1 3. részének.

2.2. PP megfelelőség

Jelen biztonsági előirányzat védelmi profil megfelelőséget nem állít.

2.3. Biztonsági követelmény csomag megfelelőség

Jelen biztonsági előirányzat megfelel a CC v3.1 3. rész EAL 4 garanciacsomagnak (a MIBÉTS szerinti kiemelt értékelési garanciaszintnek).

3. Biztonsági probléma meghatározás

3.1 Felhasználók

Operációs rendszer adminisztrátor
A Margaréta rendszer futtatókörnyezetében az operációs rendszerek telepítését és konfigurálását végző, a működő Margaréta rendszerhez közvetlenül hozzá nem férő, bizalmi munkakört (szerepkört) betöltő személy.

Alkalmazásszerver adminisztrátor
A Margaréta rendszer futtatókörnyezetében az alkalmazás szerverek telepítését és konfigurálását végző, a működő Margaréta rendszerhez közvetlenül hozzá nem férő, bizalmi munkakört (szerepkört) betöltő személy.

Adatbázis adminisztrátor
A Margaréta rendszerben az adatbázis kezelő telepítését és konfigurálását végző, egyúttal az adatbázis mentésére és helyreállítására is felhatalmazott, a működő Margaréta rendszerhez közvetlenül hozzá nem férő, bizalmi munkakört (szerepkört) betöltő személy.

Rendszervizsgáló
A Margaréta rendszerben keletkezett, majd egy Syslog szerverre továbbított naplóadatok kezelését (megtekintés, szűrés, átvizsgálás, mentés, törlés) végző, a működő Margaréta rendszerhez közvetlenül hozzá nem férő, bizalmi munkakört (szerepkört) betöltő személy.

(Margaréta) Adminisztrátor (A)
A Margaréta rendszer konfigurációjának elvégzésére és a bizalmi munkakört betöltő felhasználók (A, O, HD) fiókjainak kezelésére (létrehozás, módosítás, törlés) feljogosított, bizalmi munkakört (szerepkört) betöltő személy.

(Margaréta) Operátor (O)
A végfelhasználók (EU) fiókjainak kezelésére (létrehozás, módosítás, törlés), valamint a kártyamenedzsmenttel kapcsolatos összes tevékenységre feljogosított, bizalmi munkakört (szerepkört) betöltő személy.

(Margaréta) HelpDesk (HD)
Végfelhasználók támogatáshoz köthető feladatok (EU számára kártyalétrehozás és visszavonás, kártyák felfüggesztése, visszavonása és újra aktiválása, tanúsítványok letöltése) végrehajtására feljogosított, bizalmi munkakört (szerepkört) betöltő személy.

Végfelhasználó (EU)
Saját RSA kulcspár generálására, erre vonatkozó tanúsítvány kibocsátási kérés kiadására, valamint az elkészült tanúsítvány letöltésére feljogosított személy.

IDM rendszer (IDM)
A Margaréta rendszerhez kapcsolható külső rendszer, melynek ügyfelei számára a Margaréta rendszer különböző regisztrációs, kártya- és tanúsítvány kezelési szolgáltatást nyújt.

PKI rendszer (CA)
A Margaréta rendszerhez kapcsolódó hitelesítés-szolgáltató (CA) PKI rendszer nemcsak végrehajtja a Margaréta rendszer által kiadott, hitelesítés-szolgáltatásra vonatkozó kéréseket, hanem egyben a rendszer egy speciális felhasználója is: az általa visszavont tanúsítványokról és a szóló tájékoztató üzenet következménye pontosan ugyanaz, mint egy O vagy HD által kiadott tanúsítvány visszavonás.

3.2 Szubjektumok

A szubjektumok a különböző felhasználók nevében tevékenykedő aktív komponensek:

- A, O, HD és EU felhasználók esetén a http kéréseket feldolgozó folyamatok,
- IDM és CA felhasználó esetén a web szolgáltatás kéréseket feldolgozó folyamatok.

3.3 Fenyegetések[1]

A Margaréta rendszer által védendő értékek a Margaréta rendszer által fogadott és feldolgozott, valamint a Margaréta rendszer által elküldött információk. „Információ" alatt minden Margaréta rendszeren belüli vagy a Margaréta rendszer részét képező adat értendő. A Margaréta rendszer az információkhoz való jogosulatlan hozzáférés általános fenyegetésével számol, ahol a „hozzáférés" értelmébe beleértendő a felfedés, módosítás és megsemmisítés is.

A **védendő értékek** tehát az alábbiak:

- a Margaréta rendszer által kezelt, adatbázisban tárolt *felhasználói adatok* (a végfelhasználókra, kártyáikra és tanúsítványaikra vonatkozó adatok),
- a felhasználói adatok feldolgozásához szükséges, adatbázisban tárolt *menedzsment adatok* (rendszerfelhasználókra vonatkozó adatok, beállítási paraméterek, profilok, sablonok, sablon fordítók, email sablonok, törzsadat táblák, tábla linkek),
- a Margaréta rendszer működését meghatározó *konfigurációs állományok*,
- *hitelesítési adatok* (jelszavak és magánkulcsok).

A **veszélyforrások** döntő többsége az alábbi két kategóriába sorolható:

- a Margaréta rendszer hitelesített, feljogosított felhasználói (a 3.1 alatt meghatározott A, O, HD, EU, IDM és CA felhasználók), akik miután sikeresen hitelesítették magukat a rendszer felé, a hozzáférés ellenőrzési információk által meghatározott erőforrásokhoz és szolgáltatásokhoz férhetnek hozzá a rendszer külső interfészein keresztül,
- nem hitelesített személyek (külső támadók), akik a Margaréta rendszer számára ismeretlenek, mégis hálózat alapú hozzáférést kísérelnek meg a rendszer kommunikációs interfészeihez,
- a rendszer fejlesztői.

Az alábbiak meghatározzák a Margaréta rendszer vagy annak környezete által kivédendő biztonsági fenyegetéseket.

3.3.1 Jogosult felhasználók által okozott fenyegetések

T.Administrative errors of omission
Egy bizalmi munkakört betöltő felhasználó elmulaszt végrehajtani bizonyos funkciókat, amelyek alapvetően fontosak a biztonság szempontjából.

T.Privileged users commit errors or hostile actions
Egy bizalmi munkakört betöltő felhasználó véletlenül olyan hibát követ el, amely megváltoztatja a Margaréta rendszer célul tűzött biztonsági politikáját, vagy rosszindulatúan módosítja a rendszer konfigurációját, hogy lehetővé tegye a biztonság megsértését.

T.Sender denies sending information
Egy üzenet küldője letagadja az üzenet elküldését, hogy elkerülje az üzenet küldéséért és az ezt követő cselekvés vagy nem cselekvés miatti felelősségre vonhatóságot.

T.User abuses authorization
Egy felhasználó visszaél jogosultságaival abból a célból, hogy nem megengedett módon érzékeny vagy a biztonság szempontjából kritikus adatokat gyűjtsön és/vagy küldjön.

T.User error makes data inaccessible
Egy felhasználó véletlenül felhasználói adatot töröl, amely így hozzáférhetetlenné válik.

[1] A fenyegetésekre T. -tal kezdődő jelölést használunk (T: Threat)

3.3.2 Külső támadók fenyegetései

T.Disclosure or modification of authentication data
Egy külső támadó hitelesítéshez használt magánkulcsot vagy jelszót jogosulatlanul felfed vagy módosít.

T.Hacker gains access
Egy külső támadó jogosult felhasználónak álcázva magát, a hiányzó, gyenge és/vagy nem helyesen implementált hozzáférés ellenőrzés következtében a jogosult felhasználóhoz vagy egy rendszerfolyamathoz kapcsolódó műveletet végez, illetve nem észlelt hozzáférést nyer a rendszerhez, ami a sértetlenség, bizalmasság vagy rendelkezésre állás lehetséges megsértését eredményezi.

T.Hacker physical access
Egy támadó fizikai kölcsönhatásba lép a rendszerrel, hogy kiaknázza a fizikai környezetben meglévő sebezhetőségeket, ami a biztonság kompromittálódását eredményezheti.

T.Message content modification
Egy külső támadó információt módosít, amelyet két gyanútlan entitás közötti kommunikációs kapcsolatból fog el, mielőtt azt a tervezett címzetthez továbbítaná.

3.3.3 Egyéb fenyegetések

T.Flawed code
A rendszer fejlesztői olyan kódot szállítanak le, mely nem a specifikációnak megfelelően működik vagy biztonsági hibákat tartalmaz.

T.Incorrect_certificate_status
A rendszerben kezelt végfelhasználók tanúsítvány állapotai nem egyeznek meg a tanúsítványokat kibocsátó és kezelő CA rendszer állapotaival.

T.Malicious code exploitation
Egy jogosult felhasználó, informatikai rendszer vagy támadó olyan rosszindulatú kódot tölt fel és hajt végre, amely rendellenes folyamatokat okoz, s ezzel megsérti a rendszer értékeinek sértetlenségét, rendelkezésre állását vagy bizalmasságát.

3.4 Szervezeti biztonsági szabályok[2]

P.Authorized use of information
A Margaréta rendszerben tárolt (végfelhasználókra vonatkozó) információ csak az engedélyezett cél(ok)ra használható fel.

P.Adequate profiles
A Margaréta rendszerben tilos olyan tanúsítványprofilt használni, ami személyes megjelenés nélküli elektronikus aláírás célra használható tanúsítványkérelmet generál.

[2] A szervezeti biztonsági szabályokra P. -tal kezdődő jelölést használunk (P: Policy)

3.5 Üzemeltetési környezetre vonatkozó feltételezések[3]

3.5.1 Személyi feltételek

A.Authentication data management
A Margaréta rendszer működési környezetében érvényben van egy olyan hitelesítési adat (jelszó és PIN kód) kezelésre vonatkozó szabályzat, melynek betartásával a felhasználók hitelesítési adataikat megfelelő időközönként, és megfelelő értékekre (azaz megfelelő hosszúsággal, előtörténettel, változatossággal stb. rendelkező értékekre) változtatják.

A.Competent privileged users
A bizalmi munkaköröket betöltő személyek kellőképpen képzettek, megbízhatók és megfelelően ellátják feladataikat.

A.Disposal of authentication data
A hitelesítési adatokat és az ezekhez tartozó jogosultságokat eltávolítják, miután a hozzáférési jogosultság megszűnt (pl. munkahely vagy munkakör változás következtében).

3.5.2 Kapcsolódási feltételek

A.Appliance
A Margaréta rendszer futtatókörnyezete kizárólag a Margaréta rendszerhez szükséges szoftver elemeket tartalmaz, más alkalmazásokat nem.

A.CA
A Margaréta rendszerrel kapcsolatban álló PKI rendszer (CA) megbízható: a sikeresen azonosított és hitelesített CA által küldött adatokat a Margaréta rendszer minden további ellenőrzés nélkül elfogadhatja.

A.Communication protection
A futtatókörnyezet alkalmazásszervere(i) minden esetben védett SSL kapcsolatot épít(enek) ki a Margaréta rendszer és annak külső felhasználói (CA, IDM, A, O, HD, EU) között.
A futtatókörnyezet alkalmazásszervere(i) védett és hitelesített SSL kapcsolatot épít(enek) ki a Margaréta Központi Komponens és a Margaréta EndEntity Web Frontend alrendszerek között.
Amennyiben a Margaréta Központi Komponens és a Margaréta Oracle Adatbázis fizikailag elkülönülnek egymástól, az informatikai környezet (a végpontok hitelesítését garantáló, a továbbított adatok sértetlenségét és bizalmasságát megvédő) védett kommunikációs csatornát biztosít e két alrendszer között (pl. VPN).

A.Digital signature
A Margaréta rendszer futtatókörnyezete (az alkalmazásszerver) biztosítja a PKI rendszer felé küldött üzenetek digitális aláírását, egy kizárólag az alkalmazásszerverben aktivizált magánkulcs segítségével.

A.Hard tokens
A Margaréta rendszer rendszerfelhasználói (A, O, HD) hardver tokenen generálják, tárolják és aktivizálják a hitelesítésükhöz használt magánkulcsukat.

[3] A feltételezésekre A. -tal kezdődő jelölést használunk (A: Assumption)

A.IDM
A Margaréta rendszerrel kapcsolatban álló IDM rendszer megbízható: a sikeresen azonosított és hitelesített IDM által küldött adatokat a Margaréta rendszer jogosultság ellenőrzés után, további vizsgálatok nélkül elfogadhatja.

A.Operating system
Az operációs rendszer(ek) úgy kerül(nek) kiválasztásra, hogy az(ok) rendelkez(ik/nek) a Margaréta rendszer által elvárt azon funkciókkal, melyek a 3.3 alfejezetben meghatározott fenyegetések kivédéséhez szükségesek.

A.Syslog server
A Margaréta rendszer által használt Log4j naplózó könyvár úgy kerül beállításra, hogy a naplóesemények egy külön Syslog szerverre kerüljenek át, TCP protokoll alkalmazásával. A Syslog szerveren informatikai és nem informatikai intézkedések biztosítják az alábbiakat:

- kellő méretű tároló hely (beleértve a naplóbejegyzések automatikusan felülírásának megakadályozásával),
- a tárolt naplóbejegyzések sértetlensége,
- a tárolt naplóbejegyzések módosításának megakadályozása,
- a naplóesemények közötti keresési lehetőség az esemény időpontja, típusa és/vagy a felhasználó személye szerint,
- a naplóbejegyzések megjeleníthetősége ember számára értelmezhető módon,
- a naplóbejegyzésekhez való hozzáférés (beleértve a keresést és megtekintést is) rendszervizsgáló szerepkörre való korlátozása.

3.5.3 Fizikai feltételek

A.Physical protection
A Margaréta rendszer hardver, szoftver és förmver elemei védve vannak a jogosulatlan fizikai módosításokkal szemben.

4. Biztonsági célok

4.1. Az értékelés tárgyára vonatkozó biztonsági célok[4]

O.Correct certificate status
Biztosítani kell, hogy a rendszerben kezelt végfelhasználók tanúsítvány állapotai szinkronban legyenek a tanúsítványokat kibocsátó és kezelő CA rendszer állapotaival.

O.Individual accountability and audit records
Egyéni felelősségre vonhatóságot kell biztosítani a naplózott események vonatkozásában. A naplóeseményeknek tartalmazniuk kell az alábbiakat: az esemény dátuma és időpontja, az eseményért felelős entitás.

O.Limitation of administrative access
Az adminisztratív funkciókat úgy kell megtervezni, hogy a rendszerfelhasználók (adminisztrátorok, operátorok és helpdesk-esek) csak a szükséges mértékig rendelkezzenek hozzáféréssel a végfelhasználói objektumokhoz.

O.Maintain user attributes
Az egyéni felhasználókkal kapcsolatosan kezelni kell egy biztonsági tulajdonság együttest (amely többek között tartalmazza a szerepkörhöz tartozást is). Ez kiegészíti a felhasználói azonosítót.

O.React to detected attacks
Automatizált reagálást kell megvalósítani a TSF által felfedett támadások esetében a támadások azonosítása és elrettentése érdekében.

O.Restrict actions before authentication
Korlátozni kell azokat a tevékenységeket, amelyeket egy felhasználó végrehajthat, mielőtt a Margaréta rendszer hitelesíti felhasználói azonosítóját.

O.Security roles
Biztonsági szerepköröket kell fenntartani, és kezelni kell a felhasználóknak ezen szerepkörökkel való társítását.

O.Security-relevant configuration management
Kezelni és frissíteni kell a rendszer biztonsági szabályzatok adatait és érvényre juttató funkcióit, valamint a biztonság-kritikus konfigurációs adatokat annak biztosítása érdekében, hogy ezek konzisztensek legyenek a szervezeti biztonsági szabályzatokkal.

O.User authorization management
Kezelni kell a felhasználói jogosultság és privilégium adatait annak biztosítása érdekében, hogy ezek konzisztensek legyenek a szervezeti biztonsági és személyzeti szabályzatokkal.

[4] A TOE-ra vonatkozó biztonsági célokra O. –val kezdődő jelölést használunk (O: Objective)

4.2. Az értékelés tárgyának környezetére vonatkozó biztonsági célok[5]

OE.Authentication data management
A környezetnek egy hitelesítési adat kezelésre vonatkozó szabályzat érvényre juttatásával biztosítani kell, hogy a felhasználók hitelesítési adataikat (jelszavaikat, magánkulcsukat aktivizáló PIN kódjaikat) megfelelő időközönként, és megfelelő értékekre (azaz megfelelő hosszúsággal, előtörténettel, változatossággal stb. rendelkező értékekre) változtassák.

OE.Backup and recovery
A környezetnek a Margaréta rendszerre biztosítania kell az alábbiakat:

- álljon rendelkezésre egy rendszer mentési funkció,
- a rendszer mentésében tárolt adatok elegendőek legyenek a rendszer állapotának visszaállítására,
- az adatbázis adminisztrátor szükség esetén képes legyen a mentési funkció meghívására,
- a mentést védeni kell a módosítás ellen,
- a kritikus biztonsági paraméterek és más bizalmas információk csak titkosított formában tárolhatók,
- álljon rendelkezésre egy helyreállítási funkció is, amely képes egy mentésből helyreállítani a rendszert,
- az adatbázis adminisztrátor szükség esetén legyen képes a helyreállítási funkció meghívására.

OE.CA
A Margaréta rendszerrel kapcsolatban álló PKI rendszernek (CA) megbízhatónak kell lennie.

OE.Changing compromised infrastructure key
A Margaréta rendszert a különböző felhasználók felé hitelesítő saját infrastrukturális kulcsainak kompromittálódása esetén biztosítani kell az azonnali cserét.
A CA és IDM rendszereket a Margaréta rendszer felé hitelesítő infrastrukturális kulcsok kompromittálódása esetén biztosítani kell a Margaréta rendszerben tárolt, ezekhez tartozó tanúsítványok azonnali cseréjét. Ilyen esetben az új tanúsítvány subject mezője nem lehet azonos a régivel.
A rendszerfelhasználók (A, O, HD) hitelesítő infrastrukturális kulcsok kompromittálódása esetén biztosítani kell az azonnali cserét.

OE.Communication protection
A környezetnek biztosítania kell a Margaréta rendszer és felhasználói közötti külső, illetve a Margaréta rendszer egyes alrendszerei közötti belső kommunikáció védettségét (a hitelesség, bizalmasság és sértetlenség szempontjából egyaránt).

OE.Competent privileged users
Biztosítani kell a Margaréta rendszer megfelelő kezelését megbízható, hozzáértő és feljogosított adminisztrátorok, operátorok és Helpdesk-esek kijelölésével.
A környezetnek biztosítania kell továbbá a Margaréta rendszerhez közvetlenül hozzá nem férő, ugyanakkor az IT környezetben fontos bizalmi munkakört betöltő személyek (operációs rendszer, alkalmazásszerver és adatbázis adminisztrátorok, valamint a rendszervizsgáló) számára az alábbiakat:

[5] A TOE környezetére vonatkozó biztonsági célokra OE. –vel kezdődő jelölést használunk (OE: Objective for Environment)

- e szerepkörök összerendelése hitelesített felhasználókkal,
- az operációs rendszer és adatbázis adminisztrátor, valamint a rendszervizsgáló szerepköröket betöltő felhasználók kellő biztonságú azonosítása és hitelesítése egyedi hitelesítő adat használatával, kilépés utáni belépésnél újra hitelesítés kikényszerítésével, a hitelesítési kísérletek számának korlátozásával,
- e szerepköröket betöltő felhasználók hozzáféréseinek ellenőrzése és korlátozása szigorú hozzáférés ellenőrzési szabályok érvényre juttatásával,
- e szerepköröket betöltő felhasználók kellőképpen képzettek, megbízhatók, megfelelően ellátják feladataikat.

OE.Configuration management
A környezetben konfiguráció kezelési tervet kell megvalósítani. A konfiguráció kezelés alkalmazásával biztosítani kell a Margaréta rendszer (szoftver, hardver és förmver) összetevőinek azonosítását, valamint a konfiguráció tételekben történő változások ellenőrzését és nyomon követését.

OE.Control keys on hard token
A Margaréta rendszer bizalmi munkakört betöltő rendszerfelhasználóinak (A, O, HD) hitelesítését megalapozó rendszervezérlő magánkulcsait egy hardver kriptográfiai eszközben (pl. Aladdin eToken) kell generálni, tárolni és aktivizálni.

OE.Cryptographic functions
A környezetnek biztosítania kell, hogy jóváhagyott kriptográfiai algoritmusokat alkalmazzanak titkosításra/dekódolásra, hitelesítésre/ellenőrzésre, aláírás létrehozásra /ellenőrzésre, illetve jóváhagyott kulcsgenerálási technikákat használjanak.

OE.Disposal of Authentication Data
A környezetben biztosítani kell a hitelesítési adatok és az ezekhez tartozó jogosultságok megfelelő eltávolítását, miután a hozzáférési jogosultság megszűnt (pl. munkahelyváltozás, vagy munkaköri felelősség megváltozása következtében).

OE.Examine source code for developer flaws
Vizsgálni kell a fejlesztők által a forráskódba véletlenül vagy szándékosan elhelyezett biztonsági hibákat, specifikációtól eltérő működést.

OE.IDM
A Margaréta rendszerrel kapcsolatban álló IDM rendszernek megbízhatónak kell lennie.

OE.Integrity protection of user data and software
A környezetnek megfelelő védelmet kell biztosítania a felhasználói adatok és a szoftverek sértetlenségére.

OE.Non repudiation
A környezetnek biztosítania kell a Margaréta rendszerből a PKI rendszerbe küldött üzenetek digitális aláírását. A digitális aláírásnál alkalmazott infrastrukturális magánkulcsra teljesíteni kell az alábbiak elvárásokat is:

- szabályos időközönként, legalább évente cserélni kell,
- kompromittálódás esetén biztosítani kell az azonnali cseréjét,
- a kulcs cserét biztonságosan kell végrehajtani,

Ezáltal biztosítható a személyes felelősségre vonhatóság egy biztonsági szempontból kritikus üzenet elküldéséért, bizonyítékot szolgáltatva arra, hogy ki küldte az üzenetet.

OE.Operating System
A Margaréta rendszer csak olyan operációs rendszert használhat, mely garantálja számára a tartomány szétválasztást és a biztonsági funkciók megkerülhetetlenségét.

OE.Physical protection
A környezetnek biztosítania kell a Margaréta rendszer hardver, szoftver és förmver elemeinek fizikai védelmét a jogosulatlan módosításokkal szemben.

OE.Protect stored audit records
A futtatókörnyezet biztosítsa a Margaréta rendszer naplózási paramétereit is tartalmazó konfigurációs állomány módosításának és a naplózás tárolási hibájának naplózását.
A környezet biztosítsa a Margaréta rendszerben keletkezett naplóadatok védelmét a jogosulatlan hozzáféréssel, módosítással vagy törléssel szemben, s így biztosítva legyen a felelősségre vonhatóság a felhasználói tevékenységekért. Ennek érdekében biztosítandók az alábbiak:

- megbízható továbbítás egy Syslog szerverre,
- a szükséges tároló hely garantálása a Syslog szerveren, a naplóbejegyzések automatikusan felülírásának megakadályozásával,
- a tárolt naplóbejegyzések sértetlenségének biztosítása,
- a tárolt naplóbejegyzések módosításának megakadályozása,
- a naplóesemények közötti keresési lehetőség biztosítása az esemény időpontja, típusa és/vagy a felhasználó személye szerint,
- a naplóbejegyzések megjeleníthetősége ember számára értelmezhető módon,
- a naplóbejegyzésekhez való hozzáférés (beleértve a keresést és megtekintést is) rendszervizsgáló szerepkörre való korlátozása.

OE.Time stamp
A futtatókörnyezet operációs rendszere(i) megbízható (és szinkronizált) időpontot biztosíts(on/anak) a Margaréta rendszer számára, a naplózott események időpontjának pontos jelzésére, valamint a napló események sorrendjének ellenőrizhetőségéhez.

4.3. A biztonsági célok indoklása

4.3.1 A biztonsági célok szükségessége

A 4.1 táblázatból látható, hogy minden TOE-ra vonatkozó biztonsági cél visszavezethető legalább egy fenyegetésre vagy szervezeti biztonsági szabályra (azaz nincs felesleges TOE-ra vonatkozó biztonsági cél).

TOE-ra vonatkozó biztonsági cél	**Fenyegetés/ szervezeti biztonsági szabály**
O.Correct_certificate_status	T.Incorrect_certificate_status
O.Individual accountability and audit records	T.Administrative errors of omission T.Privileged users commit errors or hostile actions T.User abuses authorization T.Hacker gains access P.Authorized use of information
O.Limitation of administrative access	T.Privileged users commit errors or hostile actions
O.Maintain user attributes	T.Privileged users commit errors or hostile actions P.Authorized use of information
O.React to detected attacks	T.Hacker gains access
O.Restrict actions before authentication	T.Hacker gains access T.Privileged users commit errors or hostile actions P.Authorized use of information
O.Security roles	T.Privileged users commit errors or hostile actions P.Authorized use of information
O.Security-relevant configuration management	T.Administrative errors of omission
O.User authorization management	P.Authorized use of information

4.1. táblázat: A TOE-ra vonatkozó biztonsági célok visszavezetése

A 4.2 táblázatból látható, hogy minden környezetre vonatkozó biztonsági cél visszavezethető legalább egy fenyegetésre, szervezeti biztonsági szabályra vagy feltételezésre (azaz nincs felesleges környezetre vonatkozó biztonsági cél).

Környezetre vonatkozó biztonsági cél	**Fenyegetés/szervezeti biztonsági szabály/feltételezés**
OE.Authentication data management	A.Authentication data management
OE.Backup and recovery	T.Malicious code exploitation T.User error makes data inaccessible
OE.CA	T.Privileged users commit errors or hostile actions T.User abuses authorization A.CA
OE.Changing compromised infrastructure key	T.Privileged users commit errors or hostile actions T.Disclosure or modification of authentication data
OE.Communication protection	T.Message content modification T.Disclosure or modification of authentication data A.Communication protection
OE.Competent privileged users	T.Privileged users commit errors or hostile actions T.Administrative errors of omission T.User abuses authorization A.Competent privileged users P.Adequate profiles
OE.Configuration management	T.Malicious code exploitation
OE.Control keys on hard token	T.Disclosure or modification of authentication data A.Hard tokens
OE.Cryptographic functions	T.Disclosure or modification of authentication data T.Message content modification
OE.Disposal of authentication data	A.Disposal of authentication data
OE.Examine source code for developer flaws	T.Flawed code
OE.IDM	T.Privileged users commit errors or hostile actions T.User abuses authorization A.IDM
OE.Integrity protection of user data and software	T.Malicious code exploitation T.Disclosure or modification of authentication data A.Appliance
OE.Non repudiation	T.Sender denies sending information A.Digital signature
OE.Operating system	A.Operating system
OE.Physical protection	T.Hacker physical access A.Physical protection
OE.Protect stored audit records	T.Administrative errors of omission T.Privileged users commit errors or hostile actions T.User abuses authorization T.Hacker gains access P.Authorized use of information A.Syslog server
OE.Time stamp	T.Privileged users commit errors or hostile actions

4.2. táblázat: A környezetre vonatkozó biztonsági célok visszavezetése

4.3.2 A biztonsági célok elégségessége

Ez az alfejezet kimutatja az alábbiakat:

- az azonosított biztonsági célok hatékony ellenintézkedéseket valósítanak meg a fenyegetésekkel szemben (4.3.2.1),
- az azonosított biztonsági célok teljesen lefedik (érvényre juttatják) valamennyi biztonsági szabályzatot (4.3.2.2),
- az azonosított biztonsági célok teljesítik az összes feltételezést (4.3.2.3).

4.3.2.1 A biztonsági célok elégségessége a fenyegetések kivédésére

A 4.3 táblázat szemlélteti, hogy a biztonsági célok minden fenyegetést lefednek.

Fenyegetés	A fenyegetés kivédésében közreműködő biztonsági cél
T.Administrative errors of omission	OE.Competent privileged users O.Individual accountability and audit records OE.Protect stored audit records O.Security-relevant configuration management
T.Privileged users commit errors or hostile actions	O.Restrict actions before authentication O.Security roles O.Maintain user attributes OE.Competent privileged users O.Limitation of administrative access OE.CA OE.IDM OE.Changing compromised infrastructure key O.Individual accountability and audit records OE.Protect stored audit records
T.Sender denies sending information	OE.Non repudiation
T.User abuses authorization	OE.CA OE.IDM OE.Competent privileged users O.Individual accountability and audit records OE.Protect stored audit records
T.User error makes data inaccessible	OE.Backup and recovery
T.Disclosure or modification of authentication data	OE.Cryptographic functions OE.Integrity protection of user data and software OE_Communication protection OE.Changing compromised infrastructure key OE.Control keys on hard token
T.Hacker gains access	O.Restrict actions before authentication O.Individual accountability and audit records O.React to detected attacks OE.Protect stored audit records
T.Hacker physical access	OE.Physical protection
T.Message content modification	OE_Communication protection OE.Cryptographic functions
T.Flawed code	OE.Examine source code for developer flaws
T.Incorrect_certificate_status	O.Correct_certificate_status
T.Malicious code exploitation	OE.Configuration management OE.Integrity protection of user data and software OE.Backup and recovery

4.3. táblázat: A fenyegetések kivédésében közreműködő biztonsági célok

Jogosult felhasználók által okozott fenyegetések

T.Administrative errors of omission azt a veszélyt fogalmazza meg, hogy egy bizalmi munkakört betöltő felhasználó elmulaszt végrehajtani bizonyos funkciókat, amelyek alapvetően fontosak a biztonság szempontjából. Ezt a veszélyt az alábbiak védik ki:

O.Competent privileged users biztosítja, hogy a Margaréta rendszert hozzáértő és feljogosított adminisztrátorok, operátorok és Helpdesk-esek kezelik.

O.Individual accountability and audit records és **OE.Protect stored audit records** biztosítja az egyéni felelősségre vonhatóságot a naplózott eseményeken keresztül. Minden felhasználó egyedileg azonosított, s így a naplóesemények visszavezethetők egy felhasználóhoz. A naplóesemények egy erre feljogosított személynek információt szolgáltatnak a felhasználók múltbeli viselkedésére nézve. A naplóesemények rögzítése visszatartja a rendszer feljogosított (privilegizált) felhasználóit attól, hogy elmulasszanak végrehajtani egy biztonsági szempontból kritikus funkciót, hiszen ezért utólag felelősségre vonhatók lesznek.

O.Security-relevant configuration management garantálja, hogy a rendszer biztonsági szabályzatok adatait és érvényre juttató funkcióit, valamint a biztonság-kritikus konfigurációs adatokat kezelik és frissítik. Ez biztosítja, hogy ezek konzisztensek lesznek a szervezeti biztonsági szabályzatokkal, s minden változtatás megfelelően nyomon követhető és megvalósítható legyen.

T.Privileged users commit errors or hostile actions arra irányul, hogy egy bizalmi munkakört betöltő felhasználó véletlenül vagy szándékosan megsérti a biztonságot. Ezt a veszélyt az alábbiak védik ki:

O.Restrict actions before authentication biztosítja, hogy a felhasználók csak sikeres hitelesítés után tevékenykedhetnek.

O.Security roles és **O.Maintain user attributes** biztosítja, hogy biztonsági szerepköröket határoznak meg, s az egyes felhasználókat a szerepkörökhöz rendelik. Ez megakadályozza, hogy a felhasználók olyan műveletet hajtsanak végre, melyekre nincs jogosultságuk.

OE.Competent privileged users biztosítja, hogy a Margaréta rendszer privilegizált rendszerfelhasználói képesek a rendszer megfelelő kezelésére. Ez csökkenti annak valószínűségét, hogy hibát követnek el.

O.Limitation of administrative access biztosítja, hogy még a rendszerfelhasználók is csak a szükséges mértékben férhetnek hozzá a végfelhasználók adataihoz, így csökkentve a véletlen hibázás vagy szándékos visszaélés lehetőségét.

OE.CA és **OE.IDM** biztosítja, hogy a Margaréta rendszerrel kapcsolatban álló PKI (CA) és IDM rendszerek megbízhatóak, s így a sikeresen hitelesített CA és IDM rendszerek privilegizált felhasználói nem jelentenek fenyegetést.

OE.Changing compromised infrastructure key biztosítja, hogy a CA és IDM rendszereket hitelesítő kulcsok esetleges kompromittálódása esetén azonnal lecserélik azokat.

Végül **O.Individual accountability and audit records** és **OE.Protect stored audit records** biztosítja az egyéni felelősségre vonhatóságot a naplózáson keresztül.

T.Sender denies sending information arra irányul, hogy egy üzenet küldője letagadja az üzenet elküldését, hogy elkerülje az üzenet küldéséért és az ezt követő cselekvés vagy nem cselekvés miatti felelősségre vonhatóságot. Ezt a veszélyt közvetlenül az alábbi védi ki:

OE.Non repudiation, mely szerint a környezet biztosítja a Margaréta rendszerből a PKI rendszerbe küldött üzenetek digitális aláírását.

T.User abuses authorization arra irányul, hogy egy felhasználó visszaélve jogosultságával érzékeny vagy a biztonság szempontjából kritikus adatokat gyűjt és/vagy küld ki a rendszerből. Ezt a veszélyt az alábbiak védik ki:

OE.CA és **OE.IDM** biztosítja, hogy a Margaréta rendszerrel kapcsolatban álló PKI (CA) és IDM rendszerek megbízhatók, s így a sikeresen hitelesített CA és IDM rendszerek privilegizált felhasználói nem jelentenek fenyegetést.

OE.Competent privileged users biztosítja, hogy a Margaréta rendszer rendszerfelhasználói megbízhatók, s így a sikeresen hitelesített A, O és HD rendszerfelhasználók nem jelentenek fenyegetést.

O.Individual accountability and audit records és **OE.Protect stored audit records** biztosítja, hogy abban az esetben, ha a fenti szereplők mégis visszaélnének jogosultságaikkal, akkor ez utólag a naplóból kimutatható, a felelősség megállapítható.

T.User error makes data inaccessible arra irányul, hogy egy felhasználó véletlenül felhasználói adatot töröl, amely így hozzáférhetetlenné válik. Ezt a veszélyt az alábbi védi ki:

OE.Backup and recovery, mely biztosítja, hogy a Margaréta rendszerben esetlegesen elveszett (törölt) felhasználói adatok a rendszer mentésekből visszaállíthatók.

Külső támadók fenyegetései

T.Disclosure or modification of authentication data arra irányul, hogy egy külső támadó hitelesítéshez használt magánkulcsot vagy jelszót jogosulatlanul felfed vagy módosít. Ezt a veszélyt az alábbiak védik ki:

OE.Control keys on hard token biztosítja, hogy a Margaréta rendszerfelhasználói (A, O, HD) hitelesítésükhöz használt magánkulcsaikat egy hardver kriptográfiai eszközben (pl. Aladdin eToken) generálják, tárolják, aktivizálják.

OE.Changing compromised infrastructure key biztosítja, hogy bármely hitelesítéshez használt magánkulcs kompromittálódása esetén azonnal lecserélik azt.

OE.Communication protection biztosítja, hogy a végfelhasználó hitelesítéséhez használt jelszó védett módon jut el a Margaréta rendszerbe.

OE.Cryptographic functions biztosítja, hogy a jelszó kommunikációs védelme (SSL) megfelelő biztonságú kriptográfiai algoritmusokat alkalmaz.

OE.Integrity protection of user data and software pedig azt biztosítja, hogy egy külső támadó a Margaréta rendszer szoftverének módosításával sem juthat hozzá a hitelesítő magánkulcsokhoz vagy jelszavakhoz.

T.Hacker gains access arra irányul, hogy egy külső támadó jogosult felhasználónak álcázva sérti meg a biztonságot. Ezt a veszélyt az alábbiak védik ki:

O.Restrict actions before authentication biztosítja, hogy a felhasználók sikeres hitelesítése előtt semmilyen érdemi tevékenység nem hajtható végre a rendszerben. Ez megakadályozza a hozzáférés ellenőrzési mechanizmusok megkerülésére képtelen támadót abban, hogy biztonság-kritikus tevékenységeket hajtson végre.

O.React to detected attacks automatizált reagálást biztosít (a végfelhasználói fiók blokkolása) felfedett támadások (meghatározott számú sikertelen belépési kísérlet) esetén.

O.Individual accountability and audit records és **OE.Protect stored audit records** biztosítja, hogy a külső támadási kísérletek (pl. jelszópróbálgatással belépési kísérlet) manipulálhatatlan nyomot hagynak a naplóban.

T.Hacker physical access arra irányul, hogy egy támadó fizikailag hozzáférve a rendszerhez sérti meg a biztonságot (módosítja a hardvert, szoftvert vagy förmvert). Ezt a veszélyt közvetlenül az alábbi védi ki:

OE.Physical protection, mely biztosítja, hogy a fizikai hozzáférés ellenőrzés elegendő a rendszer komponensek fizikai támadásával szemben.

T.Message content modification arra irányul, hogy egy külső támadó információt módosít, amelyet két gyanútlan entitás közötti kommunikációs kapcsolatból fog el, mielőtt azt a tervezett címzetthez továbbítaná. Ezt a veszélyt az alábbiak védik ki:

OE.Communication protection szerint a környezet biztosítja a Margaréta rendszer és felhasználói közötti külső, illetve a Margaréta rendszer egyes alrendszerei közötti belső kommunikáció védettségét, ezen belül a továbbított információk sértetlenségét is.

OE.Cryptographic functions szerint a környezet biztosítja, hogy megbízható (jóváhagyott) kriptográfiai algoritmusokat alkalmaznak a kommunikáció sértetlenségének védelmére.

Egyéb fenyegetések

T.Flawed code arra irányul, hogy a rendszer fejlesztői nem a specifikációnak megfelelően működő, vagy biztonsági hibákat tartalmazó kódot szállítanak le. Ezt a veszélyt közvetlenül az alábbi védi ki:

OE.Examine source code for developer flaws, mely biztosítja, hogy a leszállítandó forráskódot megvizsgálják (értékelik) a véletlenül vagy szándékosan elhelyezett biztonsági hibák és nem tervezett működés szempontjából.

T.Incorrect certificate status arra irányul, hogy a rendszerben kezelt végfelhasználók tanúsítvány állapotai nem egyeznek meg a tanúsítványokat kibocsátó és kezelő CA rendszer állapotaival. Ezt a veszélyt közvetlenül az alábbi védi ki:

O.Correct certificate status, mely biztosítja, hogy a Margaréta rendszerben kezelt végfelhasználók tanúsítvány állapotai szinkronban legyenek a tanúsítványokat kibocsátó és kezelő CA rendszer állapotaival.

T.Malicious code exploitation arra irányul, hogy egy jogosult felhasználó, informatikai rendszer vagy támadó rosszindulatú kódot feltöltve sérti meg a biztonságot. Ezt a veszélyt az alábbiak védik ki:

OE.Configuration management szerint a környezetben megfelelő konfiguráció kezelés biztosítja a Margaréta rendszer (szoftver, hardver és förmver) összetevőinek azonosítását, valamint a konfiguráció tételekben történő változások ellenőrzését és nyomon követését. Ez csökkenti annak veszélyét, hogy a rendszer összetevőkbe rosszindulatú kód kerül.

OE.Integrity protection of user data and software közvetlenül biztosítja a felhasználói adatok és a szoftver sértetlenségét.

Végül **OE.Backup and recovery** azt biztosítja, hogy a Margaréta rendszerben esetlegesen mégis elveszett (törölt) felhasználói adatok a rendszer mentésekből visszaállíthatók.

A fenti igazolásból látható, hogy az azonosított biztonsági célok lefedik (kivédik) az összes fenyegetést.

4.3.2.2 A biztonsági célok elégségessége a biztonsági szabályok érvényre juttatására

A 4.4 táblázatból látható, hogy a biztonsági célok minden biztonsági szabályt érvényre juttatnak.

Szervezeti biztonsági szabály	A biztonsági szabály érvényre juttatásában közreműködő biztonsági cél
P.Authorized use of information	O.Individual accountability and audit records O.Maintain user attributes O.Restrict actions before authentication O.Security roles O.User authorization management OE.Protect stored audit records
P.Adequate profiles	OE.Competent privileged users

4.4. táblázat: A biztonsági szabályok érvényre juttatásában közreműködő biztonsági célok

P.Authorized use of information megállapítja, hogy információ csak az engedélyezett cél(ok)ra használható fel. Ennek a biztonsági szabálynak az érvényre juttatására az alábbi biztonsági célok irányulnak:

> **O.Maintain user attributes, O.User authorization management, O.Restrict actions before authentication és O.Security roles** azt biztosítják, hogy a felhasználókat csak azon tevékenységek végrehajtására jogosítják fel, melyekre munkájuk során szükségük van.
>
> **O.Individual accountability and audit records** és **OE.Protect stored audit records** pedig visszatartja a felhasználókat attól, hogy jogosultságaikkal visszaéljenek (hiszen tevékenységük manipulálhatatlan módon naplózásra kerül).

P.Adequate profiles megállapítja, hogy tilos olyan tanúsítványprofilt használni, ami személyes megjelenés nélküli elektronikus aláírás célra használható tanúsítványkérelmet generál. Ennek a biztonsági szabálynak az érvényre juttatására az alábbi biztonsági cél irányul:

> **OE.Competent privileged users**, mely azt biztosítják, hogy a tanúsítványprofilokat hozzáértő és feljogosított adminisztrátorok kezelik (létrehozásuknál és módosításuknál).

A fenti igazolásból látható, hogy az azonosított biztonsági célok lefedik (érvényre juttatják) az összes szervezeti biztonsági szabályt.

4.4.2.3 A biztonsági célok elégségessége a feltételek alátámasztására

A 4.5 táblázatból látható, hogy a környezetre vonatkozó biztonsági célok minden feltétel alátámasztásához hozzájárulnak.

Feltétel	A feltétel teljesülésében közreműködő, üzemeltetési környezetre vonatkozó biztonsági cél
A.Authentication data management	OE.Authentication data management
A.Competent privileged users	OE.Competent privileged users
A.Disposal of authentication data	OE.Disposal of authentication data
A.Appliance	OE.Integrity protection of user data and software
A.CA	OE.CA
A.Communication protection	OE.Communication protection
A.Digital signature	OE.Non repudiation
A.Hard tokens	OE.Control keys on hard token
A.IDM	OE.IDM
A.Operating system	OE.Operating system
A.Syslog server	OE.Protect stored audit records
A.Physical protection	OE.Physical protection

4.5. táblázat: A feltételek alátámasztásában közreműködő (üzemeltetési környezetre vonatkozó) biztonsági célok

Személyi feltételek

A.Authentication data management feltételezi, hogy a Margaréta rendszer működési környezetében érvényben van egy olyan hitelesítési adat (jelszó és PIN kód) kezelésre vonatkozó szabályzat, melynek betartásával a felhasználók hitelesítési adataikat megfelelő időközönként, és megfelelő értékekre (azaz megfelelő hosszúsággal, előtörténettel, változatossággal stb. rendelkező értékekre) változtatják. Közvetlenül erre a feltételre irányul az alábbi környezeti biztonsági cél:

> **OE.Authentication data management**, mely elvárja a környezettől egy ilyen hitelesítési adat kezelésre vonatkozó szabályzat érvényre juttatását.

A.Competent privileged users feltételezi, hogy a bizalmi munkaköröket betöltő személyek kellőképpen képzettek, megbízhatók és megfelelően ellátják feladataikat. Közvetlenül erre a feltételre irányul az alábbi környezeti biztonsági cél:

- **OE.Competent privileged users**, mely elvárja a környezettől, hogy a különböző bizalmi munkaköröket betöltő felhasználók (Margaréta adminisztrátorok, operátorok és Helpdesk-esek, rendszervizsgálók, valamint operációs rendszer, alkalmazásszerver és adatbázis adminisztrátorok) kellőképpen képzettek, megbízhatók, megfelelően ellátják feladataikat.

A.Disposal of authentication data feltételezi, hogy a hitelesítési adatokat és az ezekhez tartozó jogosultságokat eltávolítják, miután a hozzáférési jogosultság megszűnt (pl. munkahely vagy munkakör változás következtében). Közvetlenül erre a feltételre irányul az alábbi környezeti biztonsági cél:

- **OE.Disposal of Authentication Data**, mely elvárja a környezettől a hitelesítési adatok és az ezekhez tartozó jogosultságok megfelelő eltávolítását a hozzáférési jogosultság megszűnte után.

Kapcsolódási feltételek

A.Appliance feltételezi, hogy a Margaréta rendszer futtatókörnyezete kizárólag a Margaréta rendszerhez szükséges szoftver elemeket tartalmaz, más alkalmazásokat nem. Közvetlenül erre a feltételre irányul az alábbi (általánosabban megfogalmazott) környezeti biztonsági cél:

- **OE.Integrity protection of user data and software**, mely elvárja a környezettől a felhasználói adatok és a szoftverek sértetlenségét (melynek egy lehetséges teljesítési módja az összes nem Margaréta alkalmazás kitiltása a szerverről).

A.CA feltételezi, hogy a Margaréta rendszerrel kapcsolatban álló PKI rendszer (CA) megbízható: a sikeresen azonosított és hitelesített CA által küldött adatokat a Margaréta rendszer minden további ellenőrzés nélkül elfogadhatja. Közvetlenül erre a feltételre irányul az alábbi környezeti biztonsági cél:

- **OE.CA**, mely elvárja a Margaréta rendszerhez kapcsolódó PKI rendszer megbízhatóságát.

A.Communication protection feltételezi az alábbiakat:

- A futtatókörnyezet alkalmazásszervere(i) minden esetben védett SSL kapcsolatot épít(enek) ki a Margaréta rendszer és annak külső felhasználói (CA, IDM, A, O, HD, EU) között.
- A futtatókörnyezet alkalmazásszervere(i) védett és hitelesített SSL kapcsolatot épít(enek) ki a Margaréta Központi Komponens és a Margaréta EndEntity Web Frontend alrendszerek között.
- Amennyiben a Margaréta Központi Komponens és a Margaréta Oracle Adatbázis fizikailag elkülönülnek egymástól, az informatikai környezet (a végpontok hitelesítését garantáló, a továbbított adatok sértetlenségét és bizalmasságát megvédő) védett kommunikációs csatornát biztosít e két alrendszer között (pl. VPN).

Közvetlenül erre a feltételre irányul az alábbi környezeti biztonsági cél:

- **OE.Communication protection**, mely elvárja a környezettől a Margaréta rendszer és felhasználói közötti külső, illetve a Margaréta rendszer egyes alrendszerei közötti belső kommunikáció hitelességének, bizalmasságának és sértetlenségének védelmét.

A.Digital signature feltételezi, hogy a Margaréta rendszer futtatókörnyezete (az alkalmazásszerver) biztosítja a PKI rendszer felé küldött üzenetek digitális aláírását, egy kizárólag az alkalmazásszerverben aktivizált magánkulcs segítségével. Közvetlenül erre a feltételre irányul az alábbi környezeti biztonsági cél:

- **OE.Non repudiation**, mely elvárja a környezettől a Margaréta rendszerből a PKI rendszerbe küldött üzenetek digitális aláírását.

A.Hard tokens feltételezi, hogy a Margaréta rendszer rendszerfelhasználói (A, O, HD) hardver tokenen tárolják a hitelesítésük során aktivizálandó magánkulcsukat. Közvetlenül erre a feltételre irányul az alábbi környezeti biztonsági cél:

- **OE.Control keys on hard token,** mely elvárja a környezettől, hogy a rendszerfelhasználók (A, O, HD) hitelesítő magánkulcsait egy hardver kriptográfiai eszközben generálják, tárolják és aktivizálják.

A.IDM feltételezi, hogy a Margaréta rendszerrel kapcsolatban álló IDM rendszer megbízható: a sikeresen azonosított és hitelesített IDM által küldött adatokat a Margaréta rendszer jogosultság ellenőrzés után, további vizsgálatok nélkül elfogadhatja. Közvetlenül erre a feltételre irányul az alábbi környezeti biztonsági cél:

- **OE.IDM** mely elvárja a Margaréta rendszerhez kapcsolódó IDM rendszer megbízhatóságát.

A.Operating system feltételezi, hogy az operációs rendszer(ek) úgy kerül(nek) kiválasztásra, hogy az(ok) rendelkez(ik/nek) a Margaréta rendszer által elvárt azon funkciókkal, melyek a 3.3 alfejezetben meghatározott fenyegetések kivédéséhez szükségesek. Közvetlenül erre a feltételre irányul az alábbi környezeti biztonsági cél:

- **OE.Operating System**, mely elvárja a környezettől olyan operációs rendszer alkalmazását, mely garantálja a Margaréta rendszer számára a (fenyegetések kivédéséhez szükséges) tartomány szétválasztást és a biztonsági funkciók megkerülhetetlenségét.

A.Syslog server feltételezi, hogy a Margaréta rendszer által használt Log4j naplózó könyvár úgy kerül beállításra, hogy a naplóesemények egy külön Syslog szerverre kerüljenek át, TCP protokoll alkalmazásával, valamint a Syslog szerveren informatikai és nem informatikai intézkedések biztosítják az alábbiakat:

- kellő méretű tároló hely (beleértve a naplóbejegyzések automatikusan felülírásának megakadályozásával),
- a tárolt naplóbejegyzések sértetlensége,
- a tárolt naplóbejegyzések módosításának megakadályozása,
- a naplóesemények közötti keresési lehetőség az esemény időpontja, típusa és/vagy a felhasználó személye szerint,
- a naplóbejegyzések megjeleníthetősége ember számára értelmezhető módon,
- a naplóbejegyzésekhez való hozzáférés (beleértve a keresést és megtekintést is) rendszervizsgáló szerepkörre való korlátozása.

Közvetlenül erre a feltételre irányul az alábbi környezeti biztonsági cél:

- **OE.Protect stored audit records,** mely elvárja a környezettől a Margaréta rendszerben keletkezett naplóadatok védelmét egyrészt egy Syslog szerverre történő biztos továbbítással, másrészt a Syslog szerveren a szükséges védelem és funkcionalitás garantálásával.

Fizikai feltételek

A.Physical protection feltételezi, hogy a Margaréta rendszer hardver, szoftver és förmver elemei védve vannak a jogosulatlan fizikai módosításokkal szemben. Közvetlenül erre a feltételre irányul az alábbi környezeti biztonsági cél:

- **OE.Physical protection,** mely elvárja a környezettől a Margaréta rendszer hardver, szoftver és förmver elemeinek fizikai védelmét a jogosulatlan módosításokkal szemben.

A fenti igazolásból látható, hogy az azonosított, üzemeltetési környezetre vonatkozó biztonsági célok lefedik (teljesítik) az összes feltételezést.

5. Kiterjesztett összetevők meghatározása

5.1 Kiterjesztett funkcionális biztonsági követelmények

A biztonsági előirányzat nem tartalmaz kiterjesztett funkcionális biztonsági követelményeket.

5.2 Kiterjesztett garanciális biztonsági követelmények

A biztonsági előirányzat nem tartalmaz kiterjesztett garanciális biztonsági követelményeket.

6. Biztonsági követelmények

6.1. Funkcionális biztonsági követelmények

A 6.1 táblázat azonosítja a funkcionális biztonsági követelményeket.

Osztály	A funkcionális biztonsági követelmény (SFR) megnevezése	Az SFR jele
Biztonsági naplózás (FAU)	Napló adatok generálása	FAU_GEN.1
	A felhasználói azonosítóval való összekapcsolás	FAU_GEN.2
A felhasználói adatok védelme (FDP)	Részleges hozzáférés ellenőrzés	FDP_ACC.1
	Biztonsági tulajdonság alapú hozzáférés ellenőrzés	FDP_ACF.1
	Felhasználói adatok exportálása biztonsági tulajdonságok nélkül	FDP_ETC.1
	Felhasználói adatok importálása biztonsági tulajdonságok nélkül	FDP_ITC.1
Azonosítás és hitelesítés (FIA)	Hitelesítési hibák kezelése	FIA_AFL.1
	Felhasználói tulajdonságok megadása	FIA_ATD.1
	A felhasználó hitelesítése minden más tevékenység előtt	FIA_UAU.2
	Egyszer használható hitelesítési mechanizmusok	FIA_UAU.4
	Több hitelesítési mechanizmus	FIA_UAU.5
	A felhasználó azonosítása minden más tevékenység előtt	FIA_UID.2
	Felhasználó - szubjektum összerendelése	FIA_USB.1
Biztonsági menedzsment (FMT)	Biztonsági tulajdonságok kezelése	FMT_MSA.1/account
	Biztonsági tulajdonságok kezelése	FMT_MSA.1/unlock
	Biztonsági tulajdonságok kezelése	FMT_MSA.1/manage
	Biztonságos biztonsági tulajdonságok	FMT_MSA.2
	Statikus tulajdonságok kezdeti értékadása	FMT_MSA.3
	TSF adatok kezelése	FMT_MTD.1/attempts
	TSF adatok kezelése	FMT_MTD.1/password
	Menedzsment funkciók megadása	FMT_SMF.1
	Biztonsági szerepkörök	FMT_SMR.1
A TOE biztonsági funkciók védelme (FPT)	TSF-ek közötti TSF adat konzisztencia	FPT_TDC.1

6.1. táblázat: A funkcionális biztonsági követelmények

Az alábbiak a funkcionális biztonsági követelményeket részletezik, a kielégítendő biztonsági funkciók szerinti csoportosításban.

6.1.1 Biztonsági naplózás

FAU_GEN.1 Napló adatok generálása

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: FPT_STM.1 Megbízható időbélyegzés
Naplózandó események (minimális): nincs

FAU_GEN.1.1 A TSF-nek képesnek kell lennie arra, hogy naplóbejegyzést generáljon a következő naplózható eseményekről:

a) **A naplózási funkciók indítása és leállítása;**
b) **A naplózás [alap] szintjére vonatkozó minden naplózható esemény**

FAU_GEN.1.2 A TSF-nek minden naplóbejegyzésben rögzítenie kell legalább a következő információkat:

a) az esemény dátuma és időpontja, az esemény típusa, a szubjektum azonosítója (ha ez alkalmazható) és az esemény kimenetele (siker vagy sikertelenség);
b) minden napló esemény típusra [**Prioritás (DEBUG, INFO, WARN, ERROR és FATAL), küldő komponens, küldő szál**]

FAU_GEN.2 A felhasználói azonosítóval való összekapcsolás

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: FAU_GEN.1 Napló adatok generálása
FIA_UID.1 Az azonosítás időzítése
Naplózandó események (minimális): nincs

FAU_GEN.2.1 A TSF-nek képesnek kell lennie arra, hogy minden naplózható eseményt összekapcsoljon az eseményt kiváltó felhasználó azonosítójával.

6.1.2 A felhasználói adatok védelme

FDP_ACC.1 Részleges hozzáférés ellenőrzés

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: FDP_ACF.1 Biztonsági tulajdonság alapú hozzáférés ellenőrzés
Naplózandó események: nincs

FDP_ACC.1.1 A TSF-nek érvényre kell juttatnia a **[„Margaréta" hozzáférés ellenőrzés szabály SFP-t]** az alábbi szubjektumok és objektumok között, az alábbi műveletekre:
szubjektumok: **a különböző felhasználók nevében indított feldolgozási munkafolyamatok**
objektumok: **felhasználói adatok (lásd 6.2 táblázat)**
műveletek: **(lásd 6.2 táblázat)**

felhasználói adat	műveletek
EndUser	List, detail, create, edit, delete, card_create, card_revoke, set_certificate, find_from_ldap
Card	list, detail, hold, unhold, revoke
Certificate	list, detail, download, request_mail, download_mail, token applet, request

6.2. táblázat: felhasználói adat/ műveletek a „Margaréta" SFP-ben

FDP_ACF.1 Biztonsági tulajdonság alapú hozzáférés ellenőrzés

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: FDP_ACC.1 Részleges hozzáférés ellenőrzés
FMT_MSA.3 Statikus tulajdonságok inicializálása
Naplózandó események: hozzáférésre irányuló összes művelet kérés az SFP által lefedett objektumra

FDP_ACF.1.1 A TSF-nek az objektumokra érvényre kell juttatnia a **[„Margaréta" hozzáférés ellenőrzés szabály SFP-t]** a következők alapján:
szubjektumok:

szubjektum	biztonsági tulajdonság
a felhasználó nevében indított feldolgozási munkafolyamat	szerepkör

objektumok:

felhasználói adat	biztonsági tulajdonság
EndUser	eu _id (egyedi felhasználó azonosító) eu_status (a végfelhasználó státusza, lehetséges értékei: active, locked, deleted) eu_source_system (a végfelhasználó adatrögzítésének forrása, lehetséges értékei: Margaréta, IDM)
Card	cr_id (egyedi kártya azonosító) cr_status (kártya státusz, értéke a következők egyike lehet: init, underprocess, active, onhold, error, revoked, pendingreplace, pendingrevoke, pendingonhold, pendingactivate, underrenewal, renewed, expired)
Certificate	cer_id (egyedi tanúsítvány azonosító) cer_status (tanúsítvány státusz, értéke a következők egyike lehet: init, underprocess, active, onhold, error, revoked, pendingrevoke, pendingonhold, pendingactivate, expired)

FDP_ACF.1.2 A TSF-nek érvényre kell juttatnia a következő szabályokat annak megállapítása érdekében, hogy egy művelet megengedett-e az ellenőrzött szubjektumok és ellenőrzött objektumok között: **[a 6.3 táblázat soraiban meghatározott objektumra az oszlopban meghatározott művelet akkor megengedett, ha a szubjektum „szerepkör" biztonsági tulajdonsága megegyezik a sor/oszlop mezőben jelzett szerepkörök egyikével][6]**

	list	detail	create	edit	delete	card_create	card_revoke	findFromLdap	hold	unhold	revoke	download	request_mail	downloadMail	query_cert	token-applet	request	issue
EndUser	AOH	AOH	AOI	AOI	AOI	O	OH	AO	I	I	-	-	-	-	-	-	-	-
Card	AOHI	AOH	I	-	-	-	-	-	OH	OH	AOHI	-	-	-	-	-	-	-
Certificate	AOH	AOH	-	-	-	-	-	-	IP	IP	IP	AOHE	OH	OH	AOH	O	E	IP

6.3. táblázat: hozzáférés ellenőrzési szabályok a „Margaréta" SFP-ben

FDP_ACF.1.3 A TSF-nek explicit módon meg kell adnia a szubjektumok objektumokhoz való hozzáférési engedélyeit a következő kiegészítő szabályok alapján: **[nincsenek további szabályok].**

FDP_ACF.1.4 A TSF-nek explicit módon le kell tiltania a szubjektumok objektumokhoz való hozzáféréseit a 6.4 táblázatban foglaltak alapján:

felhasználói adat	művelet	feltétel biztonsági tulajdonságra
EndUser Card Certificate	list, detail	amennyiben nincs az adatbázisban a megadott azonosítójú felhasználói adat
EndUser	edit, delete, create, card_revoke,	amennyiben nincs az adatbázisban a megadott azonosítójú felhasználói adat
Card	hold	amennyiben az adatbázisban a megadott „cr_id" azonosítójú kártya státusza nem „active"
Card	unhold	amennyiben az adatbázisban a megadott „cr_id" azonosítójú kártya státusza nem „onhold"
Card	revoke	amennyiben az adatbázisban a megadott „cr_id" azonosítójú kártya státusza nem „active" vagy „onhold"

[6] A: Adminisztrátor, O: Operátor, H: HelpDesk (HD), E: végfelhasználó (EU), I: IDM rendszer, P: PKI rendszer

Certificate	download, request_mail, download_mail	amennyiben nincs az adatbázisban „cer_id” azonosítójú tanúsítvány
EndUser	edit delete card_create	amennyiben az adatbázisban a megadott EndUser adatainak forrása nem a Margaréta (az eu_source_system mező értéke a t_end_user adattáblában nem MARGARETA)
EndUser	edit (ModifyUser_ replace) delete (Deprovisioning) hold (Disable User) unhold (Unable User)	amennyiben az adatbázisban a megadott EndUser adatainak forrása nem az IDM (az eu_source_system mező értéke a t_end_user adattáblában nem IDM)
Card	list (Lookup_Card)	amennyiben az adatbázisban a megadott kártyához tartozó EndUser adatainak forrása nem az IDM (az eu_source_system mező értéke a t_end_user adattáblában nem IDM)
Certificate	hold (Disable User) unhold (Enable User) revoke (Deprovisioning)	amennyiben az adatbázisban a megadott tanúsítványhoz tartozó EndUser adatainak forrása nem az IDM (az eu_source_system mező értéke a t_end_user adattáblában nem IDM)

6.4. táblázat: közvetlen letiltási szabályok a „Margaréta” SFP-ben

FDP_ETC.1 Felhasználói adatok exportálása biztonsági tulajdonságok nélkül

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: [FDP_ACC.1 Részleges hozzáférés ellenőrzés, vagy
FDP_IFC.1 Részleges információ áramlás ellenőrzés]
Naplózandó események: minden információ exportálási kísérlet

FDP_ETC.1.1 A TSF-nek érvényt kell szereznie a **[„Margaréta” hozzáférés ellenőrzés szabály SFP]**-nek, amikor felhasználói adatokat exportál a TOE-n kívülre, az SFP ellenőrzése alatt.

FDP_ETC.1.2 A TSF-nek a felhasználói adatokat a hozzájuk kapcsolódó biztonsági tulajdonságok nélkül kell exportálnia.

FDP_ITC.1 Felhasználói adatok importálása biztonsági tulajdonságok nélkül

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: [FDP_ACC.1 Részleges hozzáférés ellenőrzés, vagy
FDP_IFC.1 Részleges információ áramlás ellenőrzés]
FMT_MSA.3 Statikus tulajdonságok inicializálása
Naplózandó események: minden felhasználó adat importálási kísérlet, akár biztonsági tulajdonságokkal is

FDP_ITC.1.1 A TSF-nek érvényt kell szereznie a **[„Margaréta” hozzáférés ellenőrzés szabály SFP]**-nek, amikor felhasználói adatokat importál a TOE-n kívülről, az SFP ellenőrzése alatt.

FDP_ITC.1.2 A TSF-nek figyelmen kívül kell hagynia az importált felhasználói adatokhoz kapcsolódó biztonsági tulajdonságokat.

6.1.3 Azonosítás és hitelesítés

FIA_AFL.1 Hitelesítési hibák kezelése

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: FIA_UAU.1 A hitelesítés időzítése
Naplózandó események: a sikertelen hitelesítési kísérletek maximális számának elérése és ennek következménye (pl. a felhasználói fiók lezárása)

FIA_AFL.1.1 A TSF-nek észlelnie kell, amikor **[az adminisztrátor által konfigurálható „hitelesítési kísérletek maximális száma (EndUserMaxLoginattempts)" 2-10 közötti elfogadható tartományban]** sikertelen hitelesítési kísérlet történik **[a végfelhasználó legutolsó sikeres hitelesítése óta]**.

FIA_AFL.1.2 Amennyiben a sikertelen hitelesítési kísérletek száma eléri vagy meghaladja a „hitelesítési kísérletek maximális száma"-ban megadott értéket, a TSF-nek az alábbiakat kell végrehajtania: **[az érintett felhasználó fiókját blokkolni kell].**

FIA_ATD.1 Felhasználói tulajdonságok megadása

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: nincs
Naplózandó események: nincs

FIA_ATD.1.1 A TSF-nek az egyedi felhasználókhoz tartozó alábbi biztonsági tulajdonságokat kell kezelnie: **[szerepkör]**.

FIA_UID.2 A felhasználó azonosítása minden más tevékenység előtt

Hierarchikus fölérendeltség más összetevőkhöz képest: FIA_UID.1 Az azonosítás időzítése
Függések: nincs
Naplózandó események: a felhasználó azonosítási mechanizmus minden használata (benne a megadott felhasználó azonosító is).

FIA_UID.2.1 A TSF-nek meg kell követelnie minden felhasználó sikeres azonosítását, mielőtt bármilyen TSF által közvetített más tevékenységet lehetővé tenne az adott felhasználó nevében.

FIA_UAU.2 A felhasználó hitelesítése minden más tevékenység előtt

Hierarchikus fölérendeltség más összetevőkhöz képest: FIA_UAU.1 A hitelesítés időzítése
Függések: FIA_UID.1 Az azonosítás időzítése
Naplózandó események: a hitelesítési mechanizmus minden (sikeres, sikertelen) használata

FIA_UAU.2.1 A TSF-nek meg kell követelnie minden felhasználó sikeres hitelesítését, mielőtt bármilyen TSF által közvetített más tevékenységet lehetővé tenne az adott felhasználó nevében.

FIA_UAU.4 Egyszer használható hitelesítési mechanizmusok

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: nincs
Naplózandó események: a hitelesítési adat ismételt felhasználásának kísérlete

FIA_UAU.4.1 A TSF-nek meg kell akadályoznia a hitelesítési adatok ismételt felhasználását a [**token kezelő appletet aktivizáló felhasználó hitelesítésénél**].

FIA_UAU.5 Több hitelesítési mechanizmus

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: nincs
Naplózandó események: minden aktivizált hitelesítési mechanizmus eredménye, a végső döntéssel együtt

FIA_UAU.5.1 A TSF-nek biztosítani kell az alábbi hitelesítési mechanizmusokat a felhasználó hitelesítésének támogatására:

1. **Hitelesítés tanúsítvánnyal**
2. **Hitelesítés végfelhasználói jelszóval**
3. **Hitelesítés egyszer használható titokkal**

FIA_UAU.5.2 A TSF-nek minden felhasználó állított azonosságát hitelesítenie kell az alábbi szabályok szerint:

1.a A rendszerfelhasználó tanúsítványának szerepelnie kell az Oracle adatbázisban (a t_certificate adattábla cer_cert mezőjében).

1.b Az IDM rendszer tanúsítvány Subject -jének szerepelnie kell egy konfigurációs állományban (IDMTest/web.xml)

1.c A PKI üzenetek esetén a PKI rendszer tanúsítvány Subject-jének szerepelnie kell egy konfigurációs állományban (CAWeb-war/WEB-INF/web.xml)

1.d Az End Entity üzenetek esetén az EE komponens tanúsítvány Subject-jének szerepelnie kell egy konfigurációs állományban (EEWs-war/WEB-INF/web.xml)

2. A végfelhasználó által megadott jelszónak meg kell egyeznie a felhasználói fiókban tárolt jelszóval.

3. A token kezelő appletet használó rendszerfelhasználó (Operátor) által visszaküldött egyszer használható titoknak meg kell egyeznie a korábban részére (hitelesített és védett kommunikációs kapcsolatban) elküldött titokkal.

FIA_USB.1 Felhasználó - szubjektum összerendelése

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: FIA_ATD.1 Felhasználói tulajdonságok megadása
Naplózandó események: a felhasználó biztonsági tulajdonságainak egy szubjektumhoz való sikeres és sikertelen összekapcsolása

FIA_USB.1.1 A TSF-nek össze kell kapcsolnia a felhasználó **[szerepkör]** biztonsági tulajdonságát az adott felhasználó nevében tevékenykedő szubjektumokkal**.**

6.1.4 Biztonsági menedzsment

FMT_SMR.1 Biztonsági szerepkörök

Hierarchikus fölérendeltség más összetevőkhöz képest:nincs
Függések: FIA_UID.1 Az azonosítás időzítése
Naplózandó események: szerepkör felhasználói csoportjának módosítása, egy szerepkör sikertelen felvételi kísérlete

FMT_SMR.1.1 A TSF-nek kezelnie kell az alábbi szerepköröket:

- **[Margaréta Adminisztrátor (A),**
- **Margaréta Operátor (O),**
- **Margaréta HelpDesk (HD),**
- **Margaréta végfelhasználó (EU),**
- **IDM rendszer (IDM) és**
- **PKI rendszer (CA)]**

FMT_SMR.1.2 A TSF-nek össze kell kapcsolnia a felhasználókat a szerepkörökkel.

FMT_SMF.1 Menedzsment funkciók megadása

Hierarchikus alárendeltség más komponensekhez képest: nincs.
Függések: nincs
Naplózandó események: a menedzsment funkciók használata

FMT_SMF.1.1 A TSF-nek képesnek kell lennie a következő biztonság menedzsment funkciók végrehajtására:

- **[rendszerfelhasználói (A, O, HD) fiókok kezelése,**
- **végfelhasználói (EU) fiókok kezelése,**
- **hibás jelszó hitelesítési kísérletre korlát megadása,**
- **blokkolt végfelhasználó újra aktiválása,**
- **rendszer konfiguráció elvégzése (beállítási paraméterek, profilok, sablonok, sablon fordítók, email sablonok, városok, telephelyek, szervezeti egységek kezelése)]**

FMT_MSA.1/account - Biztonsági tulajdonságok kezelése

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: [FDP_ACC.1 Részleges hozzáférés ellenőrzés, vagy
FDP_IFC.1 Részleges információ áramlás ellenőrzés]
FMT_SMR.1 Biztonsági szerepkörök
FMT_SMF.1 Menedzsment funkciók megadása
Naplózandó események: minden változtatás a biztonsági tulajdonságok értékeiben

FMT_MSA.1.1/account A TSF-nek érvényt kell szereznie a **[„Margaréta" hozzáférés ellenőrzés szabály SFP]**-nek, azáltal, hogy a **[szerepkör]** biztonsági tulajdonságra vonatkozó **[6.5 táblázatban meghatározott műveletetek]** végrehajtását a **[6.5 táblázatban meghatározott Margaréta Adminisztrátor (A)]** szerepkörre korlátozza.

művelet	Jogosult szerepkör
A, O vagy HD érték beállítás	Adminisztrátor (A)
EU érték beállítás	Operátor (O), IDM rendszer (IDM)
Érték lekérdezés	Adminisztrátor (A), Operátor (O), HelpDesk (HD)

6.5 táblázat

FMT_MSA.1/unlock - Biztonsági tulajdonságok kezelése

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: [FDP_ACC.1 Részleges hozzáférés ellenőrzés, vagy
FDP_IFC.1 Részleges információ áramlás ellenőrzés]
FMT_SMR.1 Biztonsági szerepkörök
FMT_SMF.1 Menedzsment funkciók megadása
Naplózandó események: minden változtatás a biztonsági tulajdonságok értékeiben

FMT_MSA.1.1 /unlock A TSF-nek érvényt kell szereznie a **[„Margaréta" hozzáférés ellenőrzés szabály SFP]**-nek, azáltal, hogy a **[felhasználó státusza (eu_status)]** biztonsági tulajdonság **[„locked" értékről „active" értékre módosítását]** a **[Margaréta Operátor (O) és HelpDesk (HD)]** szerepkörre korlátozza.

FMT_MSA.1/manage - Biztonsági tulajdonságok kezelése

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: [FDP_ACC.1 Részleges hozzáférés ellenőrzés, vagy
FDP_IFC.1 Részleges információ áramlás ellenőrzés]
FMT_SMR.1 Biztonsági szerepkörök
FMT_SMF.1 Menedzsment funkciók megadása
Naplózandó események: minden változtatás a biztonsági tulajdonságok értékeiben

FMT_MSA.1.1 /manage A TSF-nek érvényt kell szereznie a **[„Margaréta" hozzáférés ellenőrzés szabály SFP]**-nek, azáltal, hogy a **[6.6 táblázatban meghatározott]** biztonsági tulajdonságokra vonatkozó **[6.6 táblázatban meghatározott műveletek létrehozását, módosítását és törlését] végrehajtását** a **[6.6 táblázatban meghatározott]** szerepkörre korlátozza.

biztonsági tulajdonság	művelet	Jogosult szerepkör
profil adatok (pr_*) sablon adatok (pt_*) sablon fordító adatok (ptt_*) email sablon adatok (ptm_*) város adatok (cit_*)	létrehozás (create), módosítás (edit), törlés (delete)	Adminisztrátor (A)
beállítási paraméterek (set_*)	lekérdezés (list, detail) létrehozás (create), módosítás (edit),	Adminisztrátor (A)
sablon adatok (pt_*) sablon fordító adatok (ptt_*) email sablon adatok (ptm_*) város adatok (cit_*)	lekérdezés (list, detail)	Adminisztrátor (A) Operátor (O)
profil adatok (pr_*)	lekérdezés (list, detail)	Adminisztrátor (A) Operátor (O) IDM rendszer (IDM)
telephely adatok (loc_*) szervezet adatok (ouo_*)	lekérdezés (list, detail)	Adminisztrátor (A) Operátor (O) HelpDesk (HD)
telephely adatok (loc_*) szervezet adatok (ouo_*)	létrehozás (create), módosítás (edit), törlés (delete)	Operátor (O)

6.6 táblázat

FMT_MSA.2 - Biztonságos biztonsági tulajdonságok

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: [FDP_ACC.1 Részleges hozzáférés ellenőrzés, vagy
FDP_IFC.1 Részleges információáramlás ellenőrzés]
FMT_MSA.1 Biztonsági tulajdonságok kezelése
FMT_SMR.1 Biztonsági szerepkörök
Naplózandó események: valamennyi, a biztonsági tulajdonságokra felkínált, majd elfogadott vagy visszautasított érték.

FMT_MSA.2.1 A TSF-nek biztosítania kell, hogy csak biztonságos értékek legyenek elfogadva a biztonsági tulajdonságok számára.

FMT_MSA.3 - Statikus tulajdonságok kezdeti értékadása

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: FMT_MSA.1 Biztonsági tulajdonságok kezelése
FMT_SMR.1 Biztonsági szerepkörök
Naplózandó események:
a korlátozó vagy megengedő alapérték szabály megváltoztatása
minden változtatás a biztonsági tulajdonságok kezdeti értékeiben

FMT_MSA.3.1 A TSF-nek érvényt kell szereznie a **[„Margaréta" hozzáférés ellenőrzés szabály SFP]**-nek, **[korlátozó]** alapértékek biztosításával az SFP-t érvényre juttató biztonsági tulajdonságokra.

FMT_MSA.3.2 A TSF-nek lehetővé kell tennie **[senki]** számára, hogy egy objektum létrehozásakor alternatív kezdeti értékeket adhasson meg az alapértelmezett értékek helyett.

FMT_MTD.1/attempts TSF adatok kezelése

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: FMT_SMR.1 Biztonsági szerepkörök
FMT_SMF.1 Menedzsment funkciók megadása
Naplózandó események: minden TSF adat változtatás

FMT_MTD.1.1/attempts A TSF-nek a [**Margaréta Adminisztrátor (A)**] szerepkörre kell korlátoznia a **[végfelhasználók sikertelen belépési kísérleteire vonatkozó korlát (EndUserMaxLoginAttempts)]** TSF adat **[létrehozását és módosítását]**.

FMT_MTD.1/password TSF adatok kezelése

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: FMT_SMR.1 Biztonsági szerepkörök
FMT_SMF.1 Menedzsment funkciók megadása
Naplózandó események: minden TSF adat változtatás

FMT_MTD.1.1/password A TSF-nek a [**Margaréta Operátor (O) és IDM rendszer (IDM)**] szerepkörre kell korlátoznia a **[végfelhasználók belépési jelszava (eu_passw)]** TSF adat **[létrehozását és módosítását]**.

6.1.5 A TOE biztonsági funkciók védelme

FPT_TDC.1 TSF-ek közötti TSF adat konzisztencia

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: nincs
Naplózandó események:
a TSF adat konzisztenciát biztosító mechanizmusok sikeres használata
a TSF adat konzisztenciát biztosító mechanizmusok használata
az érintett TSF adat azonosítása

FPT_TDC.1.1 A TSF-nek képesnek kell lennie konzisztens módon ábrázolni a **[tanúsítvány állapot (cer_status) TSF adatot]**, amikor azokat egy más IT termék között megosztja.

6.2. Garanciális biztonsági követelmények

A 6.7 táblázat áttekinti a garanciális biztonsági követelményeket a választott MIBÉTS kiemelt (EAL4) értékelési garanciaszinten.

Osztály	A garanciális biztonsági követelmény (SAR) megnevezése	A SAR összetevő jelölése
Fejlesztés (ALC)	Biztonsági szerkezet leírás	ADV_ARC.1
	Teljes funkcionális specifikáció	ADV_FSP. 4
	Alap moduláris terv	ADV_TDS.3
	A TSF megvalósítási reprezentációja	ADV_IMP.1
Útmutató dokumentumok (AGD)	Üzemeltetési felhasználói útmutató	AGD_OPE.1
	Előkészítő eljárások	AGD_PRE.1
Életciklus támogatás (ALC)	A TOE előállítás támogatása, átvételi eljárások és automatizálás	ALC_CMC.4
	A probléma követés CM lefedettsége	ALC_CMS.4
	Szállítási eljárások	ALC_DEL.1
	A biztonsági intézkedések azonosítása	ALC_DVS.1
	A fejlesztő által meghatározott életciklus modell	ALC_LCD.1
	Jól meghatározott fejlesztő eszközök	ALC_TAT.1
Tesztelés (ATE)	Funkcionális tesztelés	ATE_FUN.1
	A lefedettség vizsgálata	ATE_COV.2
	A biztonságot érvényre juttató modulok tesztelése	ATE_DPT.2
	Független tesztelés - minta	ATE_IND.2
Sebezhetőség felmérés (AVA)	Célirányos sebezhetőség vizsgálat	AVA_VAN.3

6.7. táblázat– A garanciális biztonsági követelmények

6.3. A funkcionális biztonsági követelmények indoklása

A 6.8 táblázat minden SFR-t visszavezet a TOE biztonsági céljaira (a biztonsági célok és a biztonsági követelmények közötti lefedettség kimutatása)

A TOE-ra vonatkozó funkcionális biztonsági követelmény (SFR)	**A TOE-ra vonatkozó biztonsági cél (O)**
FAU_GEN.1 Napló adatok generálása	O.Individual accountability and audit records
FAU_GEN.2 A felhasználói azonosítóval való összekapcsolás	O.Individual accountability and audit records
FDP_ACC.1 Részleges hozzáférés ellenőrzés	O.Limitation of administrative access
FDP_ACF.1 Biztonsági tulajdonság alapú hozzáférés ellenőrzés	O.Limitation of administrative access
FDP_ETC.1 Felhasználói adatok exportálása biztonsági tulajdonságok nélkül	O.Limitation of administrative access
FDP_ITC.1 Felhasználói adatok importálása biztonsági tulajdonságok nélkül	O.Limitation of administrative access
FIA_AFL.1 Hitelesítési hibák kezelése	O.React to detected attacks
FIA_ATD.1 Felhasználói tulajdonságok megadása	O.Maintain user attributes
FIA_UAU.2 A felhasználó hitelesítése minden más tevékenység előtt	O.Restrict actions before authentication O.Individual accountability and audit records
FIA_UAU.4 Egyszer használható hitelesítési mechanizmusok	O.Individual accountability and audit records
FIA_UAU.5 Több hitelesítési mechanizmus	O.Individual accountability and audit records
FIA_UID.2 A felhasználó azonosítása minden más tevékenység előtt	O.Individual accountability and audit records O.Restrict actions before authentication
FIA_USB.1 Felhasználó - szubjektum összerendelése	O.Maintain user attributes
FMT_MSA.1 / account Biztonsági tulajdonságok kezelése	O.Maintain user attributes, O.User authorization management
FMT_MSA.1 / unlock Biztonsági tulajdonságok kezelése	O.Maintain user attributes O.User authorization management
FMT_MSA.1 / manage Biztonsági tulajdonságok kezelése	O.Maintain user attributes O.User authorization management
FMT_MSA.2 Biztonságos biztonsági tulajdonságok	O.Security-relevant configuration management
FMT_MSA.3 Statikus tulajdonságok kezdeti értékadása	O.Security-relevant configuration management
FMT_MTD.1 / attempts TSF adatok kezelése	O.Security-relevant configuration management O.Individual accountability and audit records
FMT_MTD.1 / password TSF adatok kezelése	O.Security-relevant configuration management O.Individual accountability and audit records
FMT_SMF.1 Menedzsment funkciók megadása	O.Maintain user attributes O.Security-relevant configuration management
FMT_SMR.1 Biztonsági szerepkörök	O.Security roles
FPT_TDC.1 TSF-ek közötti TSF adat konzisztencia	O.Correct_certificate_status

6.8. táblázat: Az SFR-ek hozzájárulása a TOE-ra vonatkozó biztonsági célok eléréséhez

A 6.9 táblázat áttekinti, hogy az egyes TOE-ra vonatkozó biztonsági célok teljesítéséhez mely SFR-ek járulnak hozzá.

A TOE-ra vonatkozó biztonsági cél	Funkcionális biztonsági követelmény (SFR)
O.Correct_certificate_status	FPT_TDC.1
O.Individual accountability and audit records	FAU_GEN.1 FAU_GEN.2 FIA_UAU.2 FIA_UAU.4 FIA_UAU.5 FIA_UID.2
O.Limitation of administrative access	FDP_ACC.1 FDP_ACF.1 FDP_ETC.1 FDP_ITC.1
O.Maintain user attributes	FIA_ATD.1 FIA_USB.1 FMT_MSA.1 / account FMT_MSA.1 / unlock FMT_MSA.1 / manage FMT_SMF.1
O.React to detected attacks	FIA_AFL.1
O.Restrict actions before authentication	FIA_UAU.2 FIA_UID.2
O.Security roles	FMT_SMR.1
O.Security-relevant configuration management	FMT_MSA.2 FMT_MSA.3 FMT_MTD.1 / attempts FMT_MTD.1 / password FMT_SMF.1
O.User authorization management	FMT_MSA.1 / account FMT_MSA.1 / unlock FMT_MSA.1 / manage

6.9 táblázat: A TOE-ra vonatkozó biztonsági célok teljesítése az SFR-ek által

O.Correct certificate status azt a célt fogalmazza meg, hogy a Margaréta rendszerben kezelt végfelhasználók tanúsítvány állapotai szinkronban legyenek a tanúsítványokat kibocsátó és kezelő CA rendszer állapotaival. Ennek a biztonsági célnak az érvényre juttatására az alábbi funkcionális biztonsági követelmény irányul:

> **FPT_TDC.1** közvetlenül biztosítja ezt a szinkront, hiszen azt várja el a TSF-től, hogy az konzisztens módon ábrázolja a tanúsítvány állapotokat (cer_status), amikor azokat egy más IT termékkel (a CA rendszerrel) megosztja.

O.Individual accountability and audit records azt a célt fogalmazza meg, hogy a Margaréta rendszerben biztosított legyen az egyéni felelősségre vonhatóság, olyan napló eseményekre alapulva, melyek tartalmazzák az esemény dátumát és időpontját, valamint az eseményért felelős entitást. Ennek a biztonsági célnak az érvényre juttatására az alábbi funkcionális biztonsági követelmények irányulnak:

> **FAU_GEN.1** és **FAU_GEN.2** azt biztosítják, hogy a felhasználókat csak azon tevékenységek végrehajtására jogosítják fel, melyekre munkájuk során szükségük van.

FIA_UID.2 és **FIA_UAU.2** azt biztosítják, hogy Margaréta rendszer minden felhasználó sikeres azonosítását, majd hitelesítését követeli meg, mielőtt bármilyen funkció aktivizálását megengedné számukra.

FIA_UID.5 és **FIA_UAU.4** a hitelesítésre megvalósított mechanizmusok leírását pontosítják (a Margaréta rendszer több különböző mechanizmust is alkalmaz hitelesítésre: tanúsítványon, jelszón, illetve egyszer használható tokenen alapulót).

O.Limitation of administrative access azt a célt fogalmazza meg, hogy az adminisztratív funkciók csak az elengedhetetlenül szükséges mértékben tegyék lehetővé a rendszerfelhasználók számára a végfelhasználói objektumokhoz való hozzáférést. Ennek a biztonsági célnak az érvényre juttatására az alábbi funkcionális biztonsági követelmények irányulnak:

FDP_ACC.1 megnevezi a hozzáférés ellenőrzési szabályt („Margaréta”), illetve azonosítja a szubjektumokat (felhasználók nevében indított feldolgozási munkafolyamatok), valamint a felhasználói adatok és a műveletek körét.

FDP_ACF.1 konkrétan meghatározza a hozzáférés ellenőrzés szabályait, mely szerepköröknek, milyen felhasználói adatokhoz való milyen hozzáférést (műveletet) enged, illetve ezen belül is mely biztonsági tulajdonságokra vonatkozó milyen feltételek esetén tiltja meg mégis a hozzáférést.

FDP_ETC.1 és **FDP_ITC.1** azt biztosítja, hogy a felhasználói adatok exportálása és importálása során is érvényre jut a hozzáférés ellenőrzés, illetve biztonsági tulajdonságok nélkül kerül erre sor.

O.Maintain user attributes azt a célt fogalmazza meg, hogy a Margaréta rendszer az egyéni felhasználókkal kapcsolatosan kezelje a szerepkörhöz tartozást is. Ennek a biztonsági célnak az érvényre juttatására az alábbi funkcionális biztonsági követelmények irányulnak:

FIA_ATD.1 azt biztosítja, hogy a Margaréta rendszer kezeli az egyedi felhasználókhoz tartozó szerepkör biztonsági tulajdonságot, **FIA_USB.1** pedig azt, hogy ezt a szerepkört összekapcsolja az adott felhasználó nevében tevékenykedő feldolgozó folyamatokkal.

FMT_MSA.1 három ismétlésben (/account, /unlock és /manage) megfogalmazott követelménye azt biztosítja, hogy a szerepkör biztonsági tulajdonságot a rendszer figyelembe veszi a menedzsment adatokhoz való hozzáférések ellenőrzésénél, azon biztonság menedzsment funkciók végrehajtása során, melyet **FMT_SMF.1** nevez meg.

O.React to detected attacks automatizált reagálás megvalósítását várja el a Margaréta rendszer által felfedett támadások esetében, a támadások azonosítása és elrettentése érdekében. Ennek a biztonsági célnak az érvényre juttatására az alábbi funkcionális biztonsági követelmény irányul:

FIA_AFL.1 azt a reagálást várja el, hogy a Margaréta rendszer blokkolja annak a végfelhasználónak a fiókját, akinek a nevében gyanúsan sok (egy konfigurálható, 2-10 közé eső korlátot meghaladó) sikertelen hitelesítési kísérlet történik.

O.Restrict actions before authentication azt a célt fogalmazza meg, hogy korlátozni kell azokat a tevékenységeket, amelyeket egy felhasználó végrehajthat, mielőtt a Margaréta rendszer hitelesíti felhasználói azonosítóját. Ennek a biztonsági célnak az érvényre juttatására az alábbi funkcionális biztonsági követelmények irányulnak:

FIA_UID.2 és FIA_UAU.2 közvetlenül biztosítja ezt, megkövetelve, hogy a Margaréta rendszer minden felhasználót sikeresen azonosítson, majd hitelesítse, mielőtt bármilyen funkció aktivizálását megengedné számukra.

O.Security roles azt a célt fogalmazza meg, hogy biztonsági szerepköröket kell fenntartani, és kezelni kell a felhasználóknak ezen szerepkörökkel való társítását. Ennek a biztonsági célnak az érvényre juttatására az alábbi funkcionális biztonsági követelmény irányul:

FMT_SMR.1 közvetlenül biztosítja ezt, meghatározva az elvárt szerepköröket is.

O.Security-relevant configuration management azt a célt fogalmazza meg, hogy kezelni és frissíteni kell a rendszer biztonsági szabályzatok adatait és érvényre juttató funkcióit, valamint a biztonság-kritikus konfigurációs adatokat annak biztosítása érdekében, hogy ezek konzisztensek legyenek a szervezeti biztonsági szabályzatokkal. Ennek a biztonsági célnak az érvényre juttatására az alábbi funkcionális biztonsági követelmények irányulnak:

FMT_MTD.1 két ismétlésben (/attempts és /password) megfogalmazott követelménye azt biztosítja, hogy kezelni lehet a biztonság-kritikus konfigurációs adatokat (végfelhasználók sikertelen belépési kísérleteire vonatkozó korlát, illetve végfelhasználói jelszó) azon biztonság menedzsment funkciók végrehajtása során, melyet **FMT_SMF.1** nevez meg.

FMT_MSA.2 azt biztosítja, hogy a fenti biztonság-kritikus konfigurációs adatokra csak biztonságos értékek (megfelelő hosszúságú jelszó, illetve 2 és 10 közötti korlát érték) lesznek elfogadva, **FMT_MSA.3** pedig azt, hogy ezen adatokat mindig meg kell határozni.

O.User authorization management azt a célt fogalmazza meg, hogy kezelni kell a felhasználói jogosultság és privilégium adatait annak biztosítása érdekében, hogy ezek konzisztensek legyenek a szervezeti biztonsági és személyzeti szabályzatokkal.

FMT_MSA.1 három ismétlésben (/account, /unlock és /manage) megfogalmazott követelménye azt biztosítja, hogy a rendszer a menedzsment adatokhoz való hozzáféréseknél (szerepkör alapú) ellenőrzést végez.

6.4 A funkcionális követelmények közötti függések teljesülése

A 6.10 táblázat összesíti a funkcionális biztonsági követelményeket, megadva a CC 2. rész szerinti függéseket, a függés teljesülését, illetve az esetleges nem teljesülés indoklását.

SFR	Függés	Teljesülés
FAU_GEN.1	FPT_STM.1 (megbízható időforrás)	nem teljesül, de a követelményt környezeti cél teljesíti: OE.Time stamp
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	Igen Igen
FDP_ACC.1	FDP_ACF.1	Igen
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	Igen Igen
FDP_ETC.1	[FDP_ACC.1 vagy FDP_IFC.1]	Igen (FDP_ACC.1)
FDP_ITC.1	[FDP_ACC.1 vagy FDP_IFC.1] FMT_MSA.3	Igen (FDP_ACC.1) Igen
FIA_AFL.1	FIA_UAU.1	Igen
FIA_ATD.1	-	-
FIA_UAU.2	FIA_UID.1	Igen (FIA_UID.2-en keresztül)
FIA_UAU.4	-	-
FIA_UAU.5	-	-
FIA_UID.2	-	-
FIA_USB.1	FIA_ATD.1	Igen
FMT_MSA.1	[FDP_ACC.1 vagy FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	Igen (FDP_ACC.1) Igen Igen
FMT_MSA2	[FDP_ACC.1 vagy FDP_IFC.1] FMT_MSA.1 FMT_SMR.1	Igen (FDP_ACC.1) Igen Igen
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	Igen Igen
FMT_MTD.1	FMT_SMR.1 FMT_SMF.1	Igen Igen
FMT_SMF.1	-	-
FMT_SMR.1	FIA_UID.1	Igen
FPT_TDC.1	-	-

6.10. táblázat: A funkcionális követelmények közötti függések teljesülése

A táblázatból látható, hogy egy kivételével minden megkövetelt függés teljesül.

A kivétel esetén a megbízható időforrást egy környezeti cél teljesíti (OE.Time stamp), mely a futtatókörnyezet operációs rendszerétől várja el a megbízható (egyben szinkronizált) időpont biztosítását.

6.5. A garanciális biztonsági követelmények indoklása

A TOE értékelés garanciaszintje MIBÉTS kiemelt (EAL4), mely megemelt alapszintű támadási potenciállal rendelkező támadók ellen, mérsékelt kockázati profilú környezetekben nyújt védelmet. Ez megfelel a Margaréta rendszer tervezett üzemeltetési környezetének.

A 6.11 táblázat összesíti a garanciális követelményeket, megadva a CC 3. rész szerinti függéseket, a függés teljesülését, illetve az esetleges nem teljesülés indoklását.

SAR	Függés	Teljesülés
ADV_ARC.1	ADV_FSP.1 ADV_TDS.1	Igen (ADV_FSP.4-en keresztül) Igen (ADV_TDS.3-an keresztül)
ADV_FSP.4	ADV_TDS.1	Igen (ADV_TDS.3-an keresztül)
ADV_TDS.3	ADV_FSP.4	Igen
ADV_IMP.1	ADV_TDS.3 ALC_TAT.1	Igen Igen
AGD_OPE.1	ADV_FSP.1	Igen (ADV_FSP.4-en keresztül)
AGD_PRE.1	-	-
ALC_CMC.4	ALC_CMS.1 ALC_DVS.1 ALC_LCD.1	Igen (ALC_CMS.4-en keresztül) Igen Igen
ALC_CMS.4	-	-
ALC_DEL.1	-	-
ALC_DVS.1	-	-
ALC_LCD.1	-	-
ALC_TAT.1	ADV_IMP.1	Igen
ATE_FUN.1	ATE_COV.1	Igen (ATE_COV.2-n keresztül)
ATE_COV.2	ADV_FSP. 2 ATE_FUN.1	Igen (ADV_FSP.4-en keresztül) Igen
ATE_DPT.2	ADV_ARC.1 ADV_TDS.3 ATE_FUN.1	Igen Igen Igen
ATE_IND.2	ADV_FSP.2 AGD_OPE.1 AGD_PRE.1 ATE_COV.1 ATE_FUN.1	Igen (ADV_FSP.4-en keresztül) Igen Igen Igen (ATE_COV.2-n keresztül) Igen
AVA_VAN.3	ADV_ARC.1 ADV_FSP.2 ADV_TDS.3 ADV_IMP.1 AGD_OPE.1 AGD_PRE.1	Igen Igen (ADV_FSP.4-en keresztül) Igen Igen Igen Igen

6.11. táblázat: A garanciális követelmények közötti függések teljesülése

7. TOE összefoglaló előírás

7.1. A funkcionális biztonsági követelmények teljesítésének módja

Az alábbiak áttekintik, hogy a Margaréta rendszer hogyan teljesíti az egyes funkcionális biztonsági követelményeket (SFR-eket).

7.1.1 Biztonsági naplózás

A Margaréta rendszerre az alábbi, biztonsági naplózással kapcsolatos követelmények vonatkoznak:

FAU_GEN.1 (Napló adatok generálása) megköveteli, hogy:

- az egyes SFR-ekre külön meghatározott esetekben mindig készüljön napló bejegyzés,
- minden naplóbejegyzésbe kerüljenek bele a következő információkat: az esemény dátuma és időpontja, az esemény típusa, a szubjektum azonosítója és az esemény kimenetele (siker vagy sikertelenség), prioritás (DEBUG, INFO, WARN, ERROR és FATAL), küldő komponens, küldő szál.

FAU_GEN.2 (A felhasználói azonosítóval való összekapcsolás) azt várja el, hogy minden naplóesemény összekapcsolódjon az eseményt kiváltó felhasználó azonosítójával.

A Margaréta rendszer a biztonsági naplózással kapcsolatos követelményeket az alábbi módon teljesíti:

FAU_GEN.1
A Margaréta rendszer biztosítja, hogy az SFR-ekre külön meghatározott minden esetben készül napló bejegyzés, egyúttal gondoskodik arról, hogy az egyes naplóbejegyzésekben belekerüljenek az elvárt információk. Logger osztály log metódusát hívja minden esetben, a LogHelper osztály getMessage metódusának információival.

FAU_GEN.2
A Margaréta rendszer a naplóbejegyzésekbe kerülő információkkal biztosítja, hogy minden naplóeseményt közvetlenül (a naplóeseménybe bekerülő felhasználó azonosító), vagy közvetve (az előző naplóeseményekbe bekerülő felhasználó azonosítók, küldő szálak alapján) össze lehessen kapcsolni az eseményt kiváltó felhasználóval.

A környezet az alábbi támogatást biztosítja a biztonsági naplózással kapcsolatban:

- A Margarétra rendszer naplózása a Log4j keretrendszerre épül, mely az Apache Software Foundation által fejlesztett, kiforrott naplózó könyvtár).
- A futtatókörnyezet (Alkalmazásszerver) elérhetővé teszi a Margaréta rendszer számára a felépített SSL session-ök contextus-ait, benne az alábbi adatokkal: SSL kliens authentikációs tanúsítvány teljes tanúsítványlánca.
- A futtatókörnyezet (Alkalmazásszerver) (a Margaréta rendszer megfelelő konfigurálása esetén) az eseményekről készült napló sorokat TCP protokollon keresztül (a Syslog4j könyvtár segítségével) egy Syslog szerverbe továbbítja.
- A Syslog szerver informatikai és nem informatikai környezete biztosítja a Syslog szerverre érkező naplóesemények integritásának, bizalmasságának és hitelességének védelmét, valamint a naplóban található információk rendszeres ellenőrzését, elemzését.

7.1.2 A felhasználói adatok védelme

A Margaréta rendszerre az alábbi, felhasználói adatok védelmével kapcsolatos követelmények vonatkoznak:

A Margaréta rendszer adatbázisában különböző felhasználói adatokat tárol, köztük:
- az egyes végfelhasználókra vonatkozó adatok,
- a végfelhasználók kártyáira vonatkozó adatok,
- a végfelhasználók tanúsítványaira vonatkozó adatok.

A Margaréta rendszer a végfelhasználó adatokra különböző funkciókat biztosít, köztük:
- regisztrációs funkciók (végfelhasználói adatok kezelése),
- kártya kezelési funkciók (kibocsátás, nyilvántartás, állapot kezelés, kártya műveletek végrehajtása),
- a kártyákon tárolt tanúsítványok kezelési funkciói (kibocsátás, visszavonás, felfüggesztés, újra aktiválás).

Az egyes funkciókat a különböző felhasználók eltérő módon érhetik el:
- a rendszerfelhasználók (A, O, HD) egy adminisztratív interfészen keresztül adhatnak ki http kéréseket,
- az operátorok (O) egy appleten keresztül is elérhetnek néhány token gyártáshoz kapcsolódó funkciót,
- a végfelhasználók (EU) egyedi link-kel elérhető végfelhasználói interfészen keresztül adhatnak ki http kéréseket (felhasználó nevük és jelszavuk megadását követően),
- a kapcsolódó IDM rendszer (IDM) a számára biztosított web szolgáltatáson keresztül adhat saját ügyfeleire (mint Margaréta rendszer végfelhasználóra) vonatkozó utasításokat,
- a kapcsolódó PKI rendszer (CA) a számára biztosított web szolgáltatáson keresztül válaszolhat a Margaréta rendszer kéréseire, illetve ugyanígy küldhet CRL-eket és tanúsítvány állapot változásra vonatkozó tájékoztatásokat.

FDP_ACC.1 (Részleges hozzáférés ellenőrzés) megnevezi a rendszerben megvalósítandó, felhasználó adatokra vonatkozó ellenőrzés szabályt („Margaréta”).

FDP_ACF.1 (Biztonsági tulajdonság alapú hozzáférés ellenőrzés) jellemzi a „Margaréta” hozzáférés ellenőrzés szabályt, meghatározva, hogy a különböző felhasználók mely végfelhasználói adatokra vonatkozóan milyen funkciók aktivizálására jogosultak.

FDP_ETC.1 (Felhasználói adatok exportálása biztonsági tulajdonságok nélkül) a „Margaréta” hozzáférés ellenőrzés szabály érvényre juttatását várja el, amikor a Margaréta rendszerfelhasználói adatokat exportál (tehát jogosultság ellenőrzött, biztonsági tulajdonság nélküli adatok kiküldését).

FDP_ITC.1 (Felhasználói adatok importálása biztonsági tulajdonságok nélkül) a „Margaréta” hozzáférés ellenőrzés szabály érvényre juttatását várja el, amikor a Margaréta rendszerfelhasználói adatokat importál (tehát jogosultság ellenőrzött, biztonsági tulajdonság nélküli adatok befogadását).

A Margaréta rendszer a fenti követelményeket az alábbi módon teljesíti:

FDP_ACC.1, FDP_ACF.1

A Margaréta rendszer a kérések beérkezési helye alapján egyértelműen képes elkülöníteni a potenciális rendszerfelhasználókat, végfelhasználókat, IDM és PKI rendszereket. Sikeres hitelesítés után a Margaréta rendszer minden felhasználói adatra vonatkozó kérést szerepkörrel kapcsol össze, majd a részleges hozzáférés ellenőrzést e szerepkör alapján végzi (leprogramozott, változtathatatlan jogosultság ellenőrzési táblákkal), a „Margaréta" hozzáférés ellenőrzés szabály érvényre juttatásával, a 6.2 – 6.4 táblázatokba foglaltaknak megfelelően.

FDP_ETC.1

Felhasználói adatok exportálására a következő esetekben kerülhet sor:

rendszerfelhasználók (A, O, HD) felé:

- **list** és **detail** rendszerfelhasználói kérés végrehajtása az alábbi adatok lekérdezésénél: EndUser , Card, Certificate
- **list** operátori kérés végrehajtása a riport adatok lekérdezésénél
- **download** rendszer kérés végrehajtása a Certificate adatra,

appletet kezelő operátor (O) felé:

- **token_cert_download** (tanúsítvány letöltés)

végfelhasználók felé (EU):

- **request_mail** és **download_mail** rendszerfelhasználói kérés végrehajtása a Certificate adatra (a végfelhasználónak való levélküldésre)
- **download** végfelhasználói kérés végrehajtása a Certificate adatra,

IDM rendszer felé (IDM):

- **list (Lookup/Profile)** IDM parancs végrehajtása a profil adatok lekérdezésénél,
- **list (Lookup/Card)** IDM parancs végrehajtása a kártya adatok lekérdezésénél,

CA rendszer felé (CA)

- **CertificateIssue** (a tanúsítványba foglalandó végfelhasználói adatokkal)
- **StatusChange, StatusQuery** (a végfelhasználó azonosítója, akinek a tanúsítvány állapotának a változtatása vagy lekérése a feladat)

Valamennyi fent felsorolt esetben a Margaréta rendszer hozzáférés ellenőrzés után, csak az arra jogosult szerepkör kérésére exportálja a kért adatokat, az azokhoz tartozó (saját adatbázisában tárolt) biztonsági tulajdonságok nélkül.

FDP_ITC.1

Felhasználói adatok importálására a következő esetekben kerülhet sor:

rendszerfelhasználóktól (A,O):

- az összes **create** és **edit** művelet végrehajtása során

appletet kezelő operátortól (O):

- **token_cert_req** művelet végrehajtása során (token sorszám)

LDAP-ból a rendszerfelhasználók (A, O) felé:

- **find_from_ldap** művelet végrehajtása során az EndUser felhasználói adat módosításánál és létrehozásánál

végfelhasználóktól (EU):

- **EndEntity_cerificate_request**

IDM rendszerből (IDM):

- **create** (Provision/AddUser) és **edit** (Provision/ModifyUser_replace) IDM parancs végrehajtása az EndUser felhasználói adat létrehozásánál és módosításánál

Valamennyi fent felsorolt esetben a Margaréta rendszer hozzáférés ellenőrzés után, csak az arra jogosult szerepkör kérésére importálja a kért adatokat, biztonsági tulajdonságok nélkül (azt a rendszer rendeli hozzá az adatbázisban történő letároláskor).

7.1.3 Azonosítás és hitelesítés

A Margaréta rendszerre az alábbi, azonosítással és hitelesítéssel kapcsolatos követelmények vonatkoznak:

FIA_ATD.1 (Felhasználói tulajdonságok megadása) megköveteli, hogy a Margaréta rendszer az egyedi felhasználókhoz tartozóan kezelje a „szerepkör" biztonsági tulajdonságot.

FIA_UID.2 (A felhasználó azonosítása minden más tevékenység előtt) és **FIA_UAU.2** (A felhasználó hitelesítése minden más tevékenység előtt) azt várja el, hogy csak a felhasználó sikeres azonosítása (és hitelesítése) után tegyen elérhetővé bármely más tevékenységet az adott felhasználó nevében.

FIA_USB.1 (Felhasználó - szubjektum összerendelése) azt várja el, hogy sikeres hitelesítés esetén kapcsolódjék össze a http / web szolgáltatás kérést feldolgozó folyamat (amibe sikeresen belépett a hitelesítéssel) és a felhasználó szerepkör biztonsági tulajdonsága.

FIA_UAU.5 több különböző hitelesítési mechanizmus alkalmazását várja el a felhasználó hitelesítésének támogatására (tanúsítvány, jelszó, illetve egyszer használható titok alapján), ezen belül **FIA_UAU.4** egyszer használható hitelesítési mechanizmus alkalmazását írja elő.

FIA_AFL.1 (Hitelesítési hibák kezelése) a végfelhasználó jelszó alapú hitelesítésére megköveteli az alábbiakat:

- észlelnie kell, ha az adminisztrátor által (a 2-10 közötti elfogadható tartományban) konfigurálható „hitelesítési kísérletek maximális száma (EndUserMaxLoginattempts)" darab sikertelen hitelesítési kísérlet történik a végfelhasználó legutolsó sikeres hitelesítése óta.
- amennyiben a sikertelen hitelesítési kísérletek száma eléri vagy meghaladja az „EndUserMaxLoginattempts"-ban megadott értéket, az érintett felhasználó fiókját blokkolni kell.

A Margaréta rendszer az azonosítással és hitelesítéssel kapcsolatos követelményeket az alábbi módon teljesíti:

FIA_ATD.1

A Margaréta rendszer az egyedi felhasználókhoz több lépésben rendeli hozzá a „szerepkör" biztonsági tulajdonságot:

- a kérések beérkezési helye alapján egyértelműen elkülöníti a potenciális rendszerfelhasználókat, végfelhasználókat, IDM és PKI rendszereket, letöltött appletet használó operátort.
- a potenciális külső rendszerek SSL hitelesítéshez használt tanúsítvány subject-jének konfigurációs állományban (IDMTest/web.xml, EEWs-war/WEB-INF/web.xml illetve CAWeb-war/WEB-INF/web.xml) való megtalálása esetén az azonosított szerepkör: IDM, EE, illetve CA.
- a potenciális rendszerfelhasználók SSL hitelesítéshez használt tanúsítványa alapján az adatbázisból megállapítható a szerepkör: A, O, HD (vagy egyik sem).
- a potenciális végfelhasználó helyes jelszó megadása esetén felveszi az „EU" szerepkört.
- A letöltött applettel a hozzátartozó, hitelesített módon megkapott egyedi elemet visszaküldő felhasználó felveszi az „O" szerepkört.

FIA_UID.2, FIA_UAU.2, FIA_UAU.4, FIA_UAU.5
A Margaréta rendszer alkalmazásszervere(i) helyes konfigurálás esetén kikényszeríti(k) a rendszerfelhasználók, valamint a PKI és IDM rendszerek SSL-beli, tanúsítvány alapú azonosítását és hitelesítését. Közvetlenül a sikeres SSL kapcsolat kiépülése után a Margaréta rendszer is azonosítja és hitelesíti a felhasználókat az SSL-nek megadott tanúsítvány alapján (a konfigurációs állományokban, illetve az adatbázisban szereplő adatok alapján). (FIA_UAU.5.2 /1).

A végfelhasználók azonosítása és hitelesítése másképp történik. A Margaréta rendszer (helyes konfigurálás esetén) e-mail-ben küld egy egyedi, egy műveletre használható kapcsolódási linket, melyre kattintva a Margaréta rendszer és a kliens között kiépül egy SSL kapcsolat, amely a kliens által megadott azonosítót és jelszót védetten megküldi a Margaréta rendszer alkalmazásszerverének. (FIA_UAU.5.2 /2)
Közvetlenül a sikeres SSL kapcsolat kiépülése után a Margaréta rendszer az alkalmazásszervertől kapott azonosítót és jelszót ellenőrzi adatbázisában (az adott nevű végfelhasználó adattáblájában szereplő jelszó és a beküldött jelszó összehasonlításával).

Egy Margaréta operátor egy olyan appletet is letölthet a Margaréta rendszerből, mellyel hard tokent kezelhet (kártya olvasás, kulcspár generálás + tanúsítvány igénylés, tanúsítvány letöltés, tanúsítvány törlés funkciók). Ilyen esetekben az operátor egy olyan AES titkosított karakter sorozattal (tokennel) hitelesíti magát a Margaréta rendszer felé, melyet az applet hitelesített csatornán történő letöltésekor paraméterként kapott a rendszertől. A Margaréta rendszer ezt a titkosított véletlen elemet fogadja el hitelesítésként (FIA_UAU.5.2 /3 és FIA_UAU.4).

FIA_USB.1
A Margaréta rendszer alkalmazásszervere(i) kezelik a kiépített HTTP session contextusát. Ebbe az alkalmazásszerver beírja az alábbiakat: SSL kliens authentikációs tanúsítvány teljes tanúsítványlánca. A Margaréta rendszer e contextusba beírja a hitelesített felhasználó szerepkörét, illetve jogosultság ellenőrzések alkalmával kiolvassa ezt és a még szükséges adatokat.
A futtatókörnyezet és a Margaréta rendszer ezen együttműködése biztosítja a felhasználó és a felhasználó nevében tevékenykedő szubjektum folyamatos összerendeltségét.

FIA_AFL.1
A Margaréta rendszer a végfelhasználók jelszó alapú hitelesítése során:

- sikeres jelszó ellenőrzés esetén 0-ra állítja az adott felhasználóhoz rendelt számláló (eu_err_login) értékét,
- sikertelen jelszó ellenőrzés esetén 1-gyel növeli e számláló értékét,
- amennyiben e számláló eléri (a Margaréta Adminisztrátor által 2-10 között beállítható) korlát (EndUserMaxLoginattempts) értékét, akkor az érintett felhasználó fiókját blokkolja (az érintett felhasználó eu_status értékét „locked”–ra állítja).

7.1.4 Biztonsági menedzsment

A Margaréta rendszerre az alábbi, biztonsági menedzsmenttel kapcsolatos követelmények vonatkoznak:

FMT_SMR.1 (Biztonsági szerepkörök) elvárja az alábbi szerepkörök megkülönböztetését: Margaréta Adminisztrátor (A), Margaréta Operátor (O), Margaréta HelpDesk (HD), Margaréta végfelhasználó (EU), IDM rendszer (IDM) és PKI rendszer (CA), illetve a felhasználók összekapcsolását e szerepkörökkel.

FMT_SMF.1 (Menedzsment funkciók megadása) meghatározza a rendszerben megvalósítandó biztonság menedzsment funkciókat, melyek az alábbiak:

- rendszerfelhasználói (A, O, HD) és végfelhasználói (EU) fiókok kezelése
- blokkolt végfelhasználó újra aktiválása
- rendszer konfiguráció elvégzése

Rendszerfelhasználói fiókot csak Margaréta Adminisztrátor (A) hozhat létre, módosíthat, illetve törölhet. Végfelhasználói fiókot csak a Margaréta Operátor (O) hozhat létre, módosíthat, illetve törölhet. A rendszer és végfelhasználói fiókot lekérdezése csak az A, O és HD jogosult. (**FMT_MSA.1/account**).

Csak a Margaréta Operátor (O) és a HelpDesk (HD) módosíthatja a felhasználó státuszát (eu_status) „locked” értékről „active” értékre, lehetővé téve ezzel egy többszörös hibás jelszó megadás miatt zárolt fiók felszabadítását (**FMT_MSA.1/unlock)**

A rendszer konfigurálását alapvetően A, kisebb részben O, HD és IDM végezheti, a 6.6 táblázatban meghatározott jogosultságok mellett (**FMT_MSA.1/manage**). Ez a konfigurálás magában foglalja a végfelhasználók sikertelen belépési kísérleteire vonatkozó korlát (EndUserMaxLoginAttempts) A általi létrehozását és módosítását (**FMT_MTD.1/attempts**), valamint a végfelhasználók belépési jelszavának (eu_passw) O és IDM általi létrehozását és módosítását is.

FMT_MSA.3 (Statikus tulajdonságok kezdeti értékadása) elvárja minden fiókra és konfigurálható adathalmazra, hogy azok mindig üresen, hozzáférést korlátozó módon jöjjenek létre.

A Margaréta rendszer a biztonsági menedzsmenttel kapcsolatos követelményeket az alábbi módon teljesíti:

FMT_SMR.1

A Margaréta rendszer megkülönbözteti felhasználóit, külön port-on fogadja:

- a rendszerfelhasználók (A, O, HD) http kéréseit,
- a letöltött applet web szolgáltatás kéréseit,
- a vele integrált PKI rendszer (CA) web szolgáltatás kéréseit,
- a vele integrálható egyetlen IDM rendszer (IDM) web szolgáltatás kéréseit.

A Margaréta rendszer feldolgozó folyamata a kérések beérkezési helye alapján egyértelműen képes elkülöníteni a potenciális rendszerfelhasználókat, végfelhasználókat, IDM és PKI rendszereket. A szerepkörökkel való összekapcsolás a következők alapján történik:

- a rendszerfelhasználói porton sikeres (tanúsítvány alapú) hitelesítéssel belépő felhasználó szerepköre: A, O, HD, attól függően, hogy a megadott tanúsítványhoz a rendszer adatbázisában melyik szerepkör van hozzárendelve (egy tanúsítványhoz csak egy szerepkör tartozhat, ismeretlen tanúsítvány pedig visszautasítást eredményez)

- az appletet fogadó porton sikeres (hitelesített módon megkapott egyedi elem visszaküldésén alapuló) hitelesítéssel belépő felhasználó szerepköre: O,
- a végfelhasználói porton sikeres (jelszó alapú) hitelesítéssel belépő felhasználó szerepköre: EU,
- a PKI-t, illetve az IDM-t fogadó porton sikeres (tanúsítvány alapú) hitelesítéssel belépő felhasználó szerepköre: PKI, illetve IDM, amennyiben a megadott tanúsítvány subject-je a rendszer konfigurációs állományában is megtalálható, mint PKI-hoz, illetve IDM-hez tartozó tanúsítvány.

FMT_MSA.1/account, FMT_MSA.1/unlock, FMT_MSA.1/manage, FMT_MTD.1/ attempts)
Sikeres hitelesítés után a Margaréta rendszer minden biztonsági menedzsmenttel kapcsolatos kérést szerepkörrel kapcsol össze, majd hozzáférés ellenőrzést végez e szerepkör alapján a 6.5 – 6.6 táblázatokba foglalt hozzáférés ellenőrzés szabályok érvényre juttatásával.

7.1.5 A TOE biztonsági funkciók védelme

A Margaréta rendszerre az alábbi, a saját biztonsági funkciói védelmével kapcsolatos követelmények vonatkoznak:

FPT_TDC.1 (TSF-ek közötti TSF adat konzisztencia) elvárja, hogy a Margaréta rendszer a vele integrált PKI rendszerrel konzisztens módon ábrázolja az általa kezelt tanúsítványok státuszait.

A Margaréta rendszer ezt a követelményt az alábbi módon teljesíti:
Minden tanúsítvány állapotára egy TSF adatot tárol (a „t_certificate" adattábla „cer_status" mezőjében), mely a következő értékeket veheti fel:

- init (Soft token gyártás inicializálva),
- underprocess (CA-nál van kibocsátás alatt),
- active (kibocsátott, érvényes),
- onhold (felfüggesztett),
- error (hibás),
- revoked (visszavont),
- expired (lejárt),
- pendingrevoke (visszavonási kérés kiadva CA-nak),
- pendingonhold (felfüggesztési kérés kiadva CA-nak),
- pendingactivate (újra aktiválási kérés kiadva CA-nak).

Egy újonnan adatbázisba kerülő tanúsítványra a státusz értéke init vagy underprocess, attól függően, hogy a tanúsítvány létrehozás milyen profil alapján került létrehozásra.
Amennyiben a Margaréta rendszer kezdeményez tanúsítvány állapot változást (kibocsátás, visszavonás, felfüggesztés és újra aktiválás kérés), akkor ezt átmeneti állapotokkal (underprocess, pendingrevoke, pendingonhold, pendingactivate) jelzi az adatbázisban miután a CA elfogadta (ACK) a kérést.
Amennyiben a CA pozitív visszaigazoló választ küld a kérésre, akkor a válasznak megfelelő stabil állapotba billenti (active, revoked, onhold, active).
Amennyiben egy konfigurálható idő elteltéig a CA nem válaszol egy visszavonási, felfüggesztési vagy újra aktiválási kérésre, a Margaréta rendszer ismételten kiadja a kérést a CA-nak.
Amennyiben a CA küld tájékoztatást saját döntése alapján végrehajtott tanúsítvány állapot változásról, akkor a Margaréta rendszer ezt közvetlenül átvezeti adatbázisába.
Amennyiben a Margaréta belső ütemezője (a rendszeres időközönként automatikusan elvégzett ellenőrzése során) azt tapasztalja, hogy egy (active vagy onhold státuszú tanúsítvány érvényességi ideje lejárt, akkor az „expired" státuszba billenti az értéket.

Tartalék megoldásként a Margaréta rendszer tetszőleges tanúsítvány állapotát lekérdezheti a PKI rendszertől. A kapott értékeket automatikusan átvezeti saját adatbázisába.

A fenti eljárásokkal és ellenőrzésekkel biztosítható, hogy a CA és a Margaréta rendszer tanúsítvány státuszai szinkronban legyenek egymással, és egy elfogadható fáziskéséssel a Margaréta rendszer belső stabil állapotai a CA megfelelő tanúsítvány állapotával egyezzenek meg.

7.2. Önvédelem a fizikai és logikai hamisítás ellen

A Margaréta számos biztonsági mechanizmust valósít meg annak érdekében, hogy megvédje magát a fizikai és a logikai hamisítás ellen.

A fizikai és a logikai hamisítás elleni önvédelem többrétegű, egymást kiegészítő védelmi eljárások összessége, az alábbi elemekkel:

1. a hardver/szoftver/förmver elemek fizikai módosításának védelme
2. az operációs rendszer szintjén megvalósított logikai védelem
3. az alkalmazásszerveren megvalósított logikai védelem
4. a Margaréta rendszer (mint speciális alkalmazás) által megvalósított logikai védelem
5. a kliens oldalra letölthető operátor applet hitelességének védelme

A fenti mechanizmusokat a „Biztonsági szerkezet leírás” című dokumentum részletezi.

7.3. Önvédelem a megkerülés ellen

A Margaréta rendszer számos biztonsági mechanizmust valósít meg annak érdekében, hogy megvédje magát a megkerülés ellen.

A „Biztonsági szerkezet leírás” című dokumentum részletesen kimutatja, hogy miért nem lehet megkerülni a különböző biztonsági funkciókat (Azonosítás és hitelesítés, A felhasználói és a menedzsment adatokra vonatkozó hozzáférés ellenőrzés, A tanúsítvány státuszok szinkronizáltságának megkerülhetetlensége).

8. Rövidítések

A	(Margaréta) adminisztrátor
CC	Common Criteria (közös szempontrendszer)
CRL	Certification Revocation List (tanúsítvány visszavonási lista)
EAL	Evaluation Assurance Level (értékelési garanciaszint)
EU	End User (Margaréta végfelhasználó)
EE	End Entity
HD	(Margaréta) HelpDesk
MIBÉTS	Magyar Informatika Biztonsági Értékelési és Tanúsítási Séma
O	(Margaréta) operátor
ST	Security Target (biztonsági előirányzat)
PC	Public Key Certificate (nyilvános kulcsú tanúsítvány)
TOE	Target of Evaluation (az értékelés tárgya)
TSF	TOE Security Functionality (TOE biztonsági funkcionalitás)

9. Hivatkozások

[1] ISO/IEC 15408-1: 2009 Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model

[2] ISO/IEC 15408-2: 2008 Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components

[3] ISO/IEC 15408-3: 2008 Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components