Attribútum-szolgáltató szoftver (Info&AA) v1.0

Biztonsági előirányzat

Verzió:	1.0
Dátum:	2010.07.05
Megrendelő:	Infoscope Kft.
Fájl:	InfoAA_v1.0_biztonsagi_eloiranyzat_20100705.doc
Minősítés:	Nyilvános
Oldalak:	63

Tartalomjegyzék

Változás kezelés

Verzió	Dátum	Leírás	Készítette
0.01	2009.01.14	Szerkezeti vázlat	Hunguard
0.02	2009.01.15	CEM v3.1-nek megfelelő szerkezet	Hunguard
0.03	2009.07.08	Első változat (1. – 5. fejezetek, 6.1 alfejezet)	Lengyel Csaba
0.04	2009.07.22	Értékelői kérdésekre pontosított változat	Lengyel Csaba
0.05	2010.06.01	Kiegészített változat (1. – 6 fejezetek)	Lengyel Csaba
0.06	2010.06.11	Első teljes változat	Lengyel Csaba
0.07	2010.06.18	Az értékelők javításait is tartalmazó változat	Lengyel Csaba
0.08	2010.06.26	Az értékelők véleménye alapján véglegesített változat	Lengyel Csaba
0.09	2010.07.01	Az értékelők második véleményezése alapján kiegészített változat	Lengyel Csaba
1.0	2010.07.05	Az Info&AA v1.0 értékeléshez elfogadott változat	Lengyel Csaba

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:	Attribútum-szolgáltató szoftver (Info&AA) - Biztonsági előirányzat
Verzió szám:	1.0
Dátum:	2010.07.05.
Szerző:	Lengyel Csaba

1.2 TOE hivatkozás

Az értékelés tárgya:	Attribútum-szolgáltató szoftver
Az értékelés tárgya rövid neve:	Info&AA
Verzió szám:	1.0
Dátum:	2010 07.05.
Szponzor szervezet:	Infoscope Kft.

1.3. TOE áttekintés

Az Info&AA v1.0 egy olyan speciális elektronikus aláírás termék, amely különböző attribútum-szolgáltatást biztosító funkciókkal rendelkezik.

A szoftver felhasználói az attribútum-szolgáltató operátorai és adminisztrátorai.

Az Info&AA v1.0 az alábbi attribútum-szolgáltatásokat támogatja:

a.) attribútum regisztráció szolgáltatás,
b.) attribútum tanúsítvány igénylés szolgáltatás,
c.) attribútum tanúsítvány előállítás szolgáltatás,
d.) attribútum tanúsítvány szétosztás szolgáltatás,
e.) attribútum visszavonás kezelés szolgáltatás,
f.) attribútum tanúsítvány visszavonás állapot szolgáltatás.

A támogatott szolgáltatásokon belül az alábbiakat valósítja meg:

- attribútum tanúsítvány előállítás (már kiadott PKI tanúsítványokhoz kapcsolódó, X.509 és RFC 3281 szabványoknak megfelelő attribútum tanúsítványok generálása),
- attribútum visszavonás kezelés (már kiadott attribútum tanúsítványok visszavonása, felfüggesztése, újra aktiválása),
- attribútum tanúsítvány visszavonás állapot szolgáltatás (a visszavont és felfüggesztett attribútum tanúsítványokat tartalmazó, X.509 és RFC 5280 szabványoknak megfelelő ACRL-ek előállítása és LDAP-ba publikálása)

Az Info&AA v1.0 típusa: megbízható rendszer hitelesítés-szolgáltatáshoz.

Az Info&AA v1.0 számos külső hardver, szoftver és förmver elemet követel meg.

Az Info&AA v1.0 valamennyi futtatható alkalmazása (InfoAA, InfoAA Setup, Info Policy Manager és InfoRA) számára az alábbi minimum hardver erőforrások szükségesek:

- Processzor: 1 core 2 GHZ
- Memória: 1 GB
- Háttártár: 1 GB

Az Info&AA v1.0 valamennyi futtatható alkalmazása (InfoAA, InfoAA Setup, InfoAA Policy Manager és InfoAA RA) Windows-os, .Net 3.5-ös környezetben működik a következő minimális szoftver környezetben:

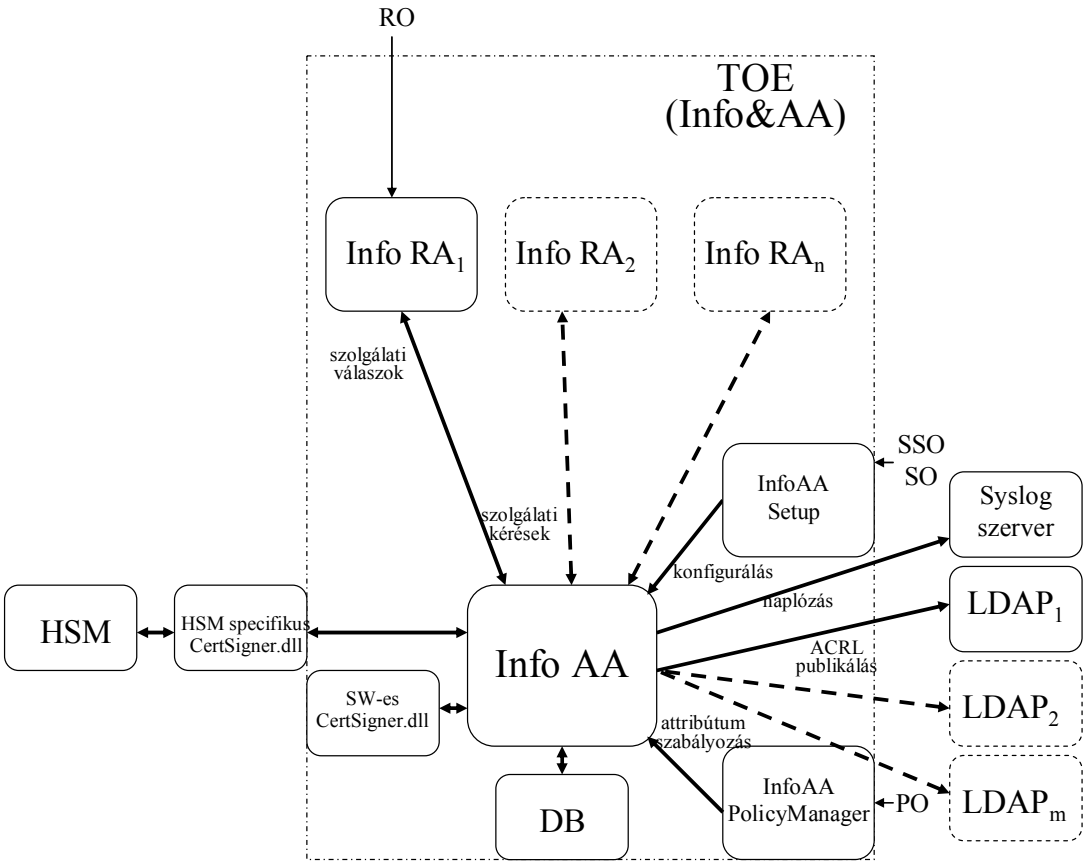
- Windows XP Professional SP3 (további támogatott operációs rendszerek: Vista, Win7, 2003Server, 2008Server)
- .Net 3.5 futtató környezet (.NET Framework 3.5)
- Microsoft Message Queue

Az Info&AA InfoCA alkalmazása a következő környezeti szoftver elemeket is megköveteli:

- adatbázis kezelő (támogatott adatbázis kezelők: tetszőleges szabványos SQL szerver alkalmazható, amelyik támogatja a tranzakciókat, valamint rendelkezik OLDEDB provider-rel, például: MSSQL Desktop Edition, MSSQL 2000, MSSQL 2005, MSSQL 2008)
- Syslog szerver (támogatott napló szerverek: tetszőleges szabványos syslog megoldás.)
- LDAP szerver (támogatott címtárak: tetszőleges szabványos LDAP szerver)
- HSM modul és a hozzá tartozó middleware (támogatott kriptográfiai hardver modul: nCipher nShield + CertSigner.dll)
- hardver token és a hozzátartozó middleware (támogatott eszközök: tetszőleges olyan intelligens kártya vagy token, amely szabványos, Microsoft-os CSP driverrel rendelkezik.)

1.4. TOE leírás

Az Info&AA v1.0 fő összetevőit és fizikai hatókörét az 1.1 ábra szemlélteti, külön megjelenítve benne az értékelés tárgyát.

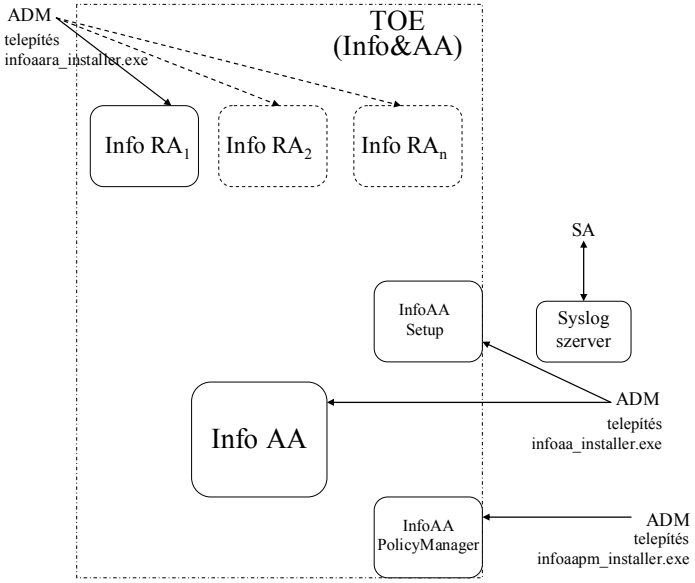


1.1. ábra: Az Info&AA v1.0 fizikai hatóköre

Felhasználók (a működő Info&AA-hoz közvetlenül hozzáférő, bizalmi munkakört betöltő személyek): SSO, SO, RO, PO.

Egyéb felhasználók (a működő Info&AA-hoz közvetlenül hozzá nem férő, bizalmi munkakört betöltő személyek): ADM és SA (lásd 1.2 ábra és 3.2 alfejezetet).

Külső felhasználók az Info&AA-hoz közvetlenül nem férhetnek (csak az RO közvetítésével kérhetnek szolgáltatást, illetve az LDAP-ból tölthetik le az attribútum visszavonási listákat).



1.2. ábra: Az Info&AA egyéb felhasználói

Az Info&AA az alábbi elemekből áll:

Hardver elemek: - (a hardver elemek, köztük az operációs rendszerek hardver alapja, a HSM modul és az SSO, SO, RO, PO felhasználók által használt hardver tokenek az Info&AA informatikai környezetének részei)

Szoftver elemek:

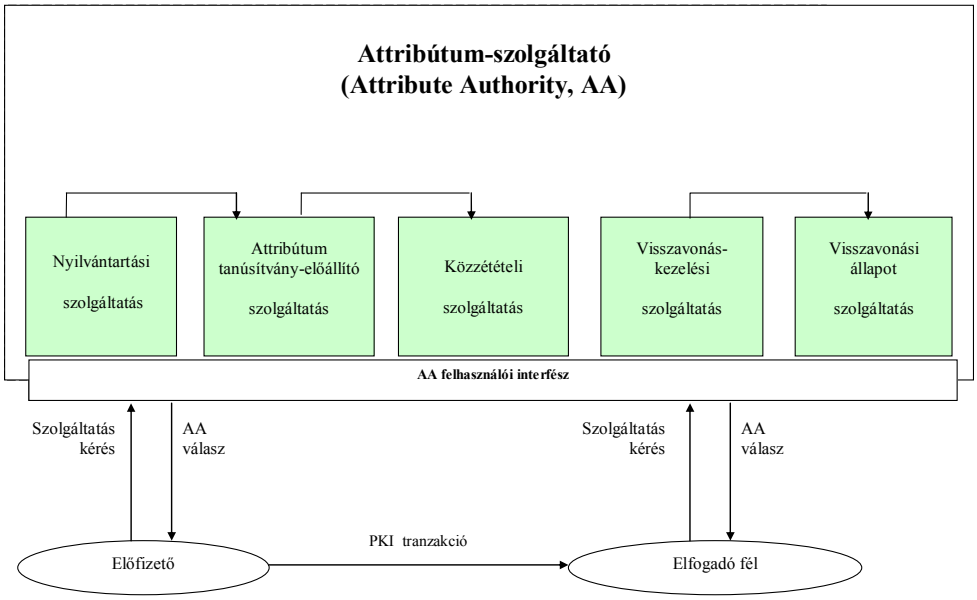
- infoaa_installer.exe (1.0.0.13)- (az InfoAA.exe telepítő alkalmazása)
- infoaara_installer.exe (1.0.0.0) - (az InfoAARA.exe telepítő alkalmazása)
- infoaapm_installer.exe (1.0.0.0) - (az InfoAAPolicyManager.exe telepítő alkalmazása)
- InfoAASsoSetup.exe (2.0.0.3) – (a 3 SSO kezdeti meghatározását, fiókjuk beállítását végző alkalmazás)
- InfoAASetup.exe (1.0.0.0) - az InfoAA.exe beállítását végző alkalmazás
- InfoAARA.exe (1.0.0.0) - regisztrációs alkalmazás
- InfoAA.exe (1.0.0.13) – attribútum tanúsítványokat kezelő szerver oldali alkalmazás
- InfoAAPolicyManager.exe (1.0.0.0) – attribútum kollekciók szerkesztését biztosító alkalmazás
- BusinessEntities.dll (1.0.0.0) - attribútum tanúsítványokhoz kapcsolódó általános segédkönyvtár
- CertSigner.dll (2.0.0.14) - szoftveres aláíró könyvtár (teszt üzemmódhoz)
- PkiMiddleware.dll (1.0.0.0) - a konfigurációs állományok és a szolgáltatói kérések aláírását, valamint a különböző tisztviselők (SSO, SO, RO, PO) beléptetését végző segédkönyvtár
- Repository.dll (1.0.0.0) - a konfigurációs állományok mentését és betöltését támogató segédkönyvtár
- aa.sql - adatbázis generáló script

Förmver elemek: -

Útmutató elemek:

- Telepítési kézikönyv (a teljes Info&AA rendszerre és informatikai környezetére)
- InfoAA Policy Manager kézikönyv
- InfoAA RA kézikönyv
- InfoAA Setup kézikönyv

Az Info&AA attribútum tanúsítványok (AC) kezelését (előállítását, szétosztását, visszavonását, visszavonás állapot kezelését) végző megbízható hitelesítés szolgáltató rendszer, ahogyan azt az 1.3 ábra szemlélteti.



1.3. ábra: Az Info&AA logikai hatóköre

Az **attribútum tanúsítvány** egy olyan adatszerkezet, amelyet az attribútum-szolgáltató (AA) digitálisan aláírt, és amely bizonyos attribútum értékeket birtokosának (előfizető) azonosító információihoz köt.

A **nyilvántartási szolgáltatás** az előfizető azonosságát és egyéb sajátos tulajdonságát vizsgálja. E szolgáltatás eredményeit az attribútum tanúsítvány-előállító szolgáltatásnak továbbítják.

Az **attribútum tanúsítvány-előállító szolgáltatás** a nyilvántartási szolgáltatás által megvizsgált azonosság és más jellemzők alapján attribútum tanúsítványt állít elő és ír alá.

A **közzétételi szolgáltatás** szétosztja az attribútum tanúsítványokat az előfizetők között, és ha az előfizető beleegyezik, az érintett felek között is. Ez a szolgáltatás a Hitelesítés-szolgáltató szabályzataira és gyakorlatára vonatkozó információkat is szétoszt az előfizetők és az érintett felek között.

A **visszavonás-kezelési szolgáltatás** feldolgozza a visszavonással kapcsolatos kérelmeket és jelentéseket a szükséges teendők meghatározása érdekében. E szolgáltatás eredményeit a visszavonási állapot szolgáltatásán keresztül osztják szét.

A **visszavonási állapot szolgáltatás** az attribútum tanúsítványok visszavonási állapotára vonatkozóan nyújt információt az érintett feleknek. Ez a szolgáltatás rendszeres időközönként frissített attribútum tanúsítvány visszavonási állapotinformáción (ACRL) alapul.

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 kiterjeszti a CC v3.1 2. részét[1].

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).

1 A CC 1.rész 10.4 pontja szerint: „Kiterjeszti a 2. részt: a PP vagy a TOE kiterjeszti a 2. részt, ha a funkcionális követelmények a 2. részben nem szereplő funkcionális összetevőket is tartalmaznak.”

3. Biztonsági probléma meghatározás

3.1 Értékek

Az alábbi táblázat áttekinti az értékelés tárgya által védendő értékeket és érzékenységüket (C: Confidentality, bizalmasság), A (Authenticity, hitelesség), I (Integrity, sértetlenség).

érték	**érték leírása**	**C/I/A**
PIN	a különböző felhasználók (SSO,SO,RO,PO) személyes azonosítói, melyekkel hitelesítik magukat a magánkulcsukat tároló és aktivizáló intelligens kártya felé	C
felhasználói magánkulcsok	a különböző felhasználók (SSO,SO,RO,PO) intelligens kártyán tárolt magánkulcsai, melyekkel digitális aláírással hitelesíthetik magukat, illetve az általuk készített szolgálati kéréseket és konfigurációs állományokat	CI
Infrastrukturális titkosító kulcs	a bizalmasság szempontjából érzékeny adatokat titkosító infrastrukturális kulcs	CI
InfoAA.config	az InfoAA.exe konfigurációs állománya	IA
InfoAA.raconfig	az InfoAARA.exe alap konfigurációs állománya	IA
InfoAARA.exe.config	az InfoAARA.exe kiegészítő konfigurációs állománya	IA
InfoAASetup.exe.config	az InfoAASetup.exe konfigurációs állománya	IA
InfoAAPolicyManager. exe.config	az InfoAAPolicyManager.exe konfigurációs állománya	IA
InfoAA.sso	az SSO szerepkört betöltők fiókja (tanúsítványaikat tartalmazó konfigurációs állomány)	CIA
InfoAA.so	az SO szerepkört betöltők fiókja (tanúsítványaikat tartalmazó konfigurációs állomány).	IA
InfoAA.ro	az RO szerepkört betöltők fiókja (tanúsítványaikat és jogosultságaikat tartalmazó konfigurációs állomány).	IA
InfoAA.po	a PO szerepkört betöltők fiókja (tanúsítványaikat és jogosultságaikat tartalmazó konfigurációs állomány).	IA
Attributes/*.attributes	az attribútum kollekciókat tartalmazó konfigurációs állományok	IA
AaProfiles/*.aaprofile	az attribútum tanúsítvány profilokat tartalmazó konfigurációs állományok	IA
CrlProfiles/*.crlprofile	az ACRL profilokat tartalmazó konfigurációs állományok	IA
Szolgálati kérések	a regisztrációs alkalmazás által a szerver oldali alkalmazásnak küldött kérések (AC-re vonatkozó kibocsátás, visszavonás, felfüggesztés, újra aktiválás kérése)	IA
Szolgálati válaszok	a szolgálati kérésekre a szerver oldali alkalmazás által a regisztrációs alkalmazás számára küldött válaszok	IA
Futtatható állományok	valamennyi futtatható állomány (köztük az összes 3.3 alatti) szubjektum	IA
Napló rekordok	a rendszer által generált napló bejegyzések	I
Kibocsátott attribútum visszavonásai listák	a szerver oldali alkalmazás által kiadott (és LDAP szerverhez továbbított) ACRL-ek	IA
AC-ket és ACRL-ket aláíró magánkulcs	HSM-ben (teszt üzemmódban szoftveresen) tárolt aláíró kulcs	CIA
syslog-ra küldött naplósorokat aláíró magánkulcs	HSM-ben (teszt üzemmódban szoftveresen) tárolt aláíró kulcs	CIA

3.2 Felhasználók

Rendszergazda (ADM)
Az Info&AA rendszer telepítését végző, valamint az ehhez szükséges szoftver környezetet (operációs rendszer, Microsoft Message Queue, .Net 3.5 futtató környezet, LDAP szerver, Syslog szerver) biztosító, a működő TOE-hez közvetlenül hozzá nem férő, bizalmi munkakört betöltő személy.

Rendszer auditor (SA)
Az Info&AA rendszerben keletkezett, majd részben a syslog szerverre továbbított naplóadatok kezelését (megtekintés, szűrés, átvizsgálás, mentés, törlés) végző, közvetlenül a TOE-hez hozzá nem férő, bizalmi munkakört betöltő személy.

Rendszer biztonsági tisztviselő (SSO)
A biztonsági tisztviselők (SO) felhasználói fiókjainak kezelésére feljogosított bizalmi munkakört betöltő személy.

Biztonsági tisztviselő (SO)
A regisztrációs tisztviselők (RO) és attribútum-szabályzó tisztviselők (PO) felhasználói fiókjai, az InfoAA.config és az InfoAA.raconfig konfigurációs állományok, valamint az attribútum tanúsítvány és ACRL profilok kezelésére feljogosított bizalmi munkakört betöltő személy.

Regisztrációs tisztviselő (RO)
Attribútum tanúsítványokra vonatkozó különböző szolgáltatási kérések (kibocsátás, visszavonás, felfüggesztés, újra aktiválás) kiadásának, valamint az ezekre kapott válaszok lekérdezésére feljogosított bizalmi munkakört betöltő személy.

Attribútum-szabályzó tisztviselő (PO)
Az egyes attribútum tanúsítványokon belüli attribútum kollekciók kezelésére feljogosított bizalmi munkakört betöltő személy.

Alkalmazói megjegyzés: Az értékelés tárgyának külső (nem bizalmi munkakört betöltő) felhasználói nincsenek. A külső felhasználók az RO-knak küldött kéréseken, vagy az InfoAA rendszer által feltöltött LDAP szerveren keresztül, tehát csak indirekt módon kapcsolódhatnak a rendszerhez.

3.3 Szubjektumok

A szubjektumok az értékelés tárgya aktív komponensei, melyek a felhasználók nevében tevékenykednek.

InfoAASetup.exe	az InfoAA.exe beállítását végző alkalmazás
InfoAARA.exe	regisztrációs alkalmazás
InfoAA.exe	attribútum tanúsítványokat kezelő szerver oldali alkalmazás
InfoAAPolicyManager.exe	attribútumok kollekciók szerkesztését biztosító alkalmazás

3.4 Fenyegetések[2]

A fenyegetések forrásuk szempontjából négy csoportra oszthatók: jogosult felhasználók, rendszer, kriptográfia, illetve külső támadások.

3.4.1 Jogosult felhasználók

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

T.Administrators, Operators, Officers and Auditors commit errors or hostile actions
Egy bizalmi munkakört betöltő személy véletlenül olyan hibát követ el, amely megváltoztatja a rendszer célul tűzött biztonsági szabályzatát, vagy rosszindulatúan módosítja a rendszer konfigurációját, hogy lehetővé tegye a biztonság megsértését.

T.User abuses authorization to collect and/or send data
Egy felhasználó visszaél jogosultságaival abból a célból, hogy helytelen módon gyűjtsön és/vagy küldjön érzékeny vagy a biztonság szempontjából kritikus adatokat.

T.User error makes data inaccessible
Egy felhasználó véletlenül felhasználói adatokat töröl, amellyel felhasználói adatokat hozzáférhetetlenné tesz.

3.4.2 Rendszer

T.Critical system component fails
Egy vagy több rendszer komponens hibája a rendszer kritikus fontosságú funkcionalitásának elvesztését okozza.

T.Flawed code
Egy rendszer vagy alkalmazás fejlesztője olyan kódot ad át, amely nem a specifikációnak megfelelően működik, vagy biztonsági réseket tartalmaz.

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

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

3.4.3 Kriptográfia

T.Disclosure of private and secret keys
Egy magán vagy titkos kulcsot nem megengedett módon felfednek.

T.Modification of private/secret keys
Egy magán vagy titkos kulcs módosítva lesz.

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

3.4.4 Külső támadások

T.Hacker gains access
Egy 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.Social engineering
Egy támadó a "social engineering" technikát alkalmazza arra, hogy információt szerezzen a rendszerbe lépésről, a rendszer felhasználásáról, a rendszer tervéről vagy a rendszer működéséről.

3.5 Szervezeti biztonsági szabályok[3]

P.Authorized use of information
Információ csak az engedélyezett cél(ok)ra használható fel.

P.Cryptography
Jogszabály vagy hatósági ajánlás által jóváhagyott kriptográfiai algoritmusokat kell használni a kriptográfiai műveletek végrehajtásakor.

3.6 Üzemeltetési környezetre vonatkozó feltételezések[4]

3.6.1 Személyi feltételek

A.Auditors Review Audit Logs
A biztonság-kritikus eseményekről naplóbejegyzés készül, s ezeket rendszeresen átvizsgálják.

A.Authentication Data Management
A TOE működési környezetében érvényben van egy olyan hitelesítési adat (jelszó vagy 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 Administrators, Operators, Officers and Auditors
A bizalmi munkakörök betöltésére szakértő személyek lesznek kijelölve a TOE és az általa tartalmazott információk biztonságának kezelésére. Ezen belül bizalmi munkakört betöltő személy gondoskodik a rendszer egyes elemeinek telepítéséről, a konfigurációs állományok szükséges mozgatásáról, valamint az adatbázis rendszeres mentéséről.

A.CPS
Minden bizalmi munkakört betöltő személy jól ismeri azt a hitelesítési rendet (CP) és szolgáltatási szabályzatot (CPS), mely hatálya alatt a TOE-t működtetik.

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

A.Notify Authorities of Security Issues
A bizalmi munkaköröket betöltő személyeknek értesíteniük kell a megfelelő vezetőket a rendszert érintő bármely biztonsági eseményről, a további adatvesztés vagy kompromittálódás lehetőségének minimalizálása érdekében.

A.Social Engineering Training
A bizalmi munkaköröket betöltő személyek képzettek a "social engineering" típusú támadások megakadályozási technikáiban.

A.Cooperative Users
A felhasználóknak néhány olyan feladatot vagy feladatcsoportot is végre kell hajtani, amelyek biztonságos IT környezetet igényelnek. A felhasználóknak a TOE által kezelt információk közül legalább néhányhoz hozzá kell férniük, egyúttal feltételezzük, hogy a felhasználók együttműködő módon tevékenykednek.

3.6.2 Kapcsolódási feltételek

A.Operating System
Az operációs rendszer úgy kerül kiválasztásra, hogy az rendelkezik a 3.4 alfejezetben meghatározott fenyegetések kivédésének támogatásához szükséges, a TOE által elvárt funkciókkal.

3.6.3 Fizikai feltételek

A.Communication Protection
A rendszer megfelelő fizikai védelemmel van ellátva a kommunikáció elvesztésével, azaz a kommunikáció rendelkezésre állásának elvesztésével szemben.

A.Physical Protection
A TOE azon hardver, szoftver és förmver elemei, amelyek létfontosságúak a TOE biztonsági politikája (TSP) érvényre juttatásához, védve vannak a jogosulatlan fizikai módosításokkal szemben.

4. Biztonsági célok

4.1. Az értékelés tárgyára vonatkozó biztonsági célok

O.AttributeCertificates
A TOE biztonsági funkcionalitásának biztosítania kell, hogy az attribútum tanúsítványok, attribútum tanúsítvány visszavonási listák és attribútum tanúsítvány állapot információk érvényesek legyenek.

O.Configuration Management
Konfiguráció kezelési tervet kell megvalósítani. A konfiguráció kezelést abból a célból kell alkalmazni, hogy biztosítva legyen a rendszer csatlakoztatások (szoftver, hardver és förmver) és komponensek (szoftver, hardver és förmver) beazonosítása, a konfigurációs adatok naplózása, valamint a konfiguráció tételekben történő változások ellenőrzése.

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 bizalmi munkakört betöltő személyek automatikusan ne rendelkezzenek hozzáféréssel a felhasználói objektumokhoz, a szükséges kivételeken kívül. Ellenőrizni kell azon bizalmi munkakört betöltő személyek rendszerhez való hozzáférését, akik a rendszer hibák elhárítását, illetve új verziók telepítését végzik.

O.Maintain user attributes
Az egyéni felhasználókkal kapcsolatosan kezelni kell egy biztonsági tulajdonság együttest (amely tartalmazhat szerepkörhöz tartozást, hozzáférési privilégiumokat stb.). Ez kiegészíti a felhasználói azonosítót.

O.Manage behavior of security functions
Menedzsment funkciókat kell biztosítani a biztonsági mechanizmusok konfigurálására, működtetésére és kezelésére.

O.Protect user and TSF data during internal transfer
Biztosítani kell a rendszeren belül átvitt felhasználói és TSF adatok sértetlenségét.

O.Protect stored audit records
A naplórekordokat védeni kell a jogosulatlan módosítással vagy törléssel szemben abból a célból, hogy biztosítva legyen a felelősségre vonhatóság a felhasználói tevékenységekért.

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

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

O.User authorization management

Kezelni és frissíteni kell a felhasználói jogosultság és privilégium adatokat annak biztosítása érdekében, hogy ezek konzisztensek legyenek a szervezeti biztonsági és személyzeti szabályzatokkal.

4.2. Az üzemeltetési környezetre vonatkozó biztonsági célok

OE.Administrators, Operators, Officers and Auditors guidance documentation
Meg kell gátolni a bizalmi munkakört betöltő személyek hibáit azáltal, hogy megfelelő dokumentációt kell számukra biztosítani a TOE biztonságos konfigurálásához és üzemeltetéséhez.

OE.Auditors Review Audit Logs
A biztonság-kritikus eseményeket azonosítani és felügyelni kell, megkövetelve a rendszervizsgálóktól a naplóbejegyzések kellő (kockázatokkal arányban álló) gyakoriságú átvizsgálását.

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

OE.Communication Protection
A rendszert megfelelő fizikai biztonság biztosításával védeni kell a kommunikációs képességekre irányuló fizikai támadásokkal szemben.

OE.Competent Administrators, Operators, Officers and Auditors
Biztosítani kell a TOE megfelelő kezelését a bizalmi munkakörök hozzáértő és feljogosított személyekkel való betöltésével a TOE és az általa tartalmazott információk biztonságának kezelésére.

OE.Cooperative Users
Biztosítani kell, hogy a felhasználók együttműködők legyenek néhány olyan feladat vagy feladatcsoport végrehajtásában, amelyek biztonságos IT környezetet, s a TOE által kezelt információkat igényelnek.

OE.CPS
Minden bizalmi munkakört betöltő személynek jól kell ismernie azt a hitelesítési rendet (CP) és szolgáltatási szabályzatot (CPS), mely alatt a TOE-t működtetik.

OE.Cryptographic functions
Jóváhagyott kriptográfiai algoritmusokat kell megvalósítani a titkosításra/dekódolásra, hitelesítésre és aláírás létrehozására/ellenőrzésére, jóváhagyott kulcsgenerálási technikákat kell alkalmazni, valamint tanúsított kriptográfiai modulokat kell használni.

OE.Data import/export
Az adatok formájában megjelenő értékeket védeni kell a TOE felé vagy a TOE-tól történő átvitel közben, ahol az átvitel akár egy közbeiktatott nem megbízható komponensen keresztül, akár közvetlenül az emberi felhasználókhoz/tól történik.

OE.Detect modifications of firmware, software, and backup data
Sértetlenség védelmet kell biztosítani a förmverek, a szoftverek, valamint a mentett adatok megváltozásának észlelése érdekében.

OE.Disposal of Authentication Data
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.Installation
A TOE-ért felelős személyeknek biztosítaniuk kell, hogy a TOE olyan módon legyen szállítva, telepítve, kezelve és üzemeltetve, amely megőrzi az informatikai biztonságot.

OE.Integrity protection of user data and software
Megfelelő sértetlenség védelmet kell biztosítani a felhasználói adatokra és a szoftverre.

OE.Lifecycle security
A fejlesztési fázisban olyan eszközöket és technikákat kell biztosítani, hogy használatukkal biztosítva legyen a biztonság TOE-ba tervezése. A működtetés során észlelni és javítani kell a hibákat.

OE.Notify Authorities of Security Issues
Értesíteni kell a megfelelő vezetőket a rendszert érintő bármely biztonsági eseményről, az adatvesztés vagy kompromittálódás lehetőségének minimalizálása érdekében.

OE.Object and data recovery free from malicious code
Egy rosszindulatú kód bejutása és károkozása után egy működőképes állapotba kell tudni visszaállni. Ennek az állapotnak mentesnek kell lennie az eredeti rosszindulatú programkódtól.

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

OE.Periodically check integrity
Időszakosan ellenőrizni kell mind a rendszer, mind a szoftver sértetlenségét.

OE.Physical Protection
A TOE-ért felelős személyeknek biztosítaniuk kell, hogy a TOE biztonságkritikus elemei védve legyenek az informatikai biztonságot veszélyeztető fizikai támadásokkal szemben.

OE.Preservation/trusted recovery of secure state
Egy biztonsági komponens hibája esetén meg kell őrizni a rendszer egy biztonságos állapotát, és/vagy helyre kell állítani a rendszert egy biztonságos állapotába.

OE.Procedures for preventing malicious code
A rosszindulatú programkódokat meggátoló beépített eljárásoknak és mechanizmusoknak kell létezniük.

OE.Protect stored audit records
A naplórekordokat védeni kell a jogosulatlan hozzáféréssel szemben abból a célból, hogy biztosítva legyen a felelősségre vonhatóság a felhasználói tevékenységekért.

OE.React to detected attacks
Automatizált értesítést (vagy más reagálásokat) kell megvalósítani a TSF által felfedett támadások esetében a támadások azonosítása és elrettentése érdekében.

OE.Repair identified security flaws
A gyártónak javítani kell a felhasználók által azonosított biztonsági hibákat.

OE.Require inspection for downloads
Meg kell követelni a letöltések/átvitelek felügyeletét.

OE.Respond to possible loss of stored audit records
Amennyiben a napló eseménysor tároló területe megtelt vagy majdnem megtelt, a naplózható események korlátozásával meg kell akadályozni a naplórekordok lehetséges elvesztését.

OE.Social Engineering Training
A bizalmi munkakört betöltő személyek számára képzést kell biztosítani a „social engineering" típusú támadások megakadályozási technikáira.

OE.Sufficient backup storage and effective restoration
Elegendő mentés tárolást és hatékony visszaállítást kell biztosítani a rendszer újra felépíthetősége érdekében.

OE.Time stamps
Pontos időpontot kell biztosítani az időfüggő hitelesítés-szolgáltatásokhoz, valamint a napló események sorrendjének ellenőrizhetőségéhez[5].

OE.Trusted Path
Megbízható útvonalat kell biztosítani a felhasználók és a rendszer között. Megbízható útvonalat kell biztosítani a biztonság-kritikus (TSF) adatok számára, aminek mindkét végpontja megbízhatóan azonosított.

OE.Validation of security function
Funkciók és eljárások alkalmazásával biztosítani kell, hogy a biztonság-kritikus szoftver, hardver és förmver elemek helyesen működnek.

[5] A windows alap network time alapú szinkronizáló szolgáltatását be kell állítania a rendszergazdának az operációs rendszerben.

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.AttributeCertificates	T.Administrators, Operators, Officers and Auditors commit errors or hostile actions
O.Configuration Management	T.Critical system component fails T.Malicious code exploitation
O.Individual accountability and audit records	T.Administrative errors of omission T.Hacker gains access T.Administrators, Operators, Officers and Auditors commit errors or hostile actions T.User abuses authorization to collect and/or send data
O.Limitation of administrative access	T.Disclosure of private and secret keys T.Administrators, Operators, Officers and Auditors commit errors or hostile actions
O.Maintain user attributes	T.Administrators, Operators, Officers and Auditors commit errors or hostile actions
	P.Authorized use of information
O.Manage behavior of security functions	T.Critical system component fails T.Administrators, Operators, Officers and Auditors commit errors or hostile actions
O.Protect user and TSF data during internal transfer	T.Message content modification T.Disclosure of private and secret keys
O.Protect stored audit records	T.Modification of private/secret keys T.Administrators, Operators, Officers and Auditors commit errors or hostile actions
O.Restrict actions before authentication	T.Hacker gains access T.Administrators, Operators, Officers and Auditors commit errors or hostile actions
	P.Authorized use of information
O.Security-relevant configuration management	T.Administrative errors of omission
O.Security roles	T.Administrators, Operators, Officers and Auditors commit errors or hostile actions
	P.Authorized use of information
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.Administrators, Operators, Officers and Auditors guidance documentation	T.Disclosure of private and secret keys T.Administrators, Operators, Officers and Auditors commit errors or hostile actions T.Social engineering
OE.Auditors Review Audit Logs	P.Authorized use of information
	A.Auditors Review Audit Logs

OE.Authentication Data Management	A.Authentication Data Management
OE.Communication Protection	A.Communication Protection
OE.Competent Administrators, Operators, Officers and Auditors	T.Administrators, Operators, Officers and Auditors commit errors or hostile actions
	A.Competent Administrators, Operators, Officers and Auditors
OE.Cooperative Users	A.Cooperative Users
OE.Cryptographic functions	T.Disclosure of private and secret keys T.Modification of private/secret keys
	P.Cryptography
OE.CPS	T.Administrative errors of omission
	A.CPS
OE.Detect modifications of firmware, software, and backup data	T.User error makes data inaccessible T.Administrators, Operators, Officers and Auditors commit errors or hostile actions
OE.Disposal of Authentication Data	A.Disposal of Authentication Data
OE.Installation	T.Critical system component fails
	A.Competent Administrators, Operators, Officers and Auditors
OE.Lifecycle security	T.Critical system component fails T.Malicious code exploitation
OE.Notify Authorities of Security Issues	T.Hacker gains access
	A.Notify Authorities of Security Issues
OE.Object and data recovery free from malicious code	T.Modification of private/secret keys T.Malicious code exploitation
OE.Operating System	A.Operating System
OE.Periodically check integrity	T.Malicious code exploitation
OE.Physical Protection	T.Hacker physical access
	A.Physical Protection
OE.Preservation/trusted recovery of secure state	T.Critical system component fails
OE.Protect stored audit records	T.Modification of private/secret keys T.Administrators, Operators, Officers and Auditors commit errors or hostile actions
OE.React to detected attacks	T.Hacker gains access
OE.Repair identified security flaws	T.Flawed code T.Critical system component fails
OE.Respond to possible loss of stored audit records	T.Administrators, Operators, Officers and Auditors commit errors or hostile actions
OE.Require inspection for downloads	T.Malicious code exploitation
OE.Social Engineering Training	T.Social engineering
	A.Social Engineering Training
OE.Sufficient backup storage and effective restoration	T.Critical system component fails T.User error makes data inaccessible
OE.Time stamps	T.Critical system component fails T.Administrators, Operators, Officers and Auditors commit errors or hostile actions
OE.Validation of security function	T.Malicious code exploitation T.Administrators, Operators, Officers and Auditors commit errors or hostile actions
OE.Trusted Path	T.Hacker gains access T.Message content modification
OE.Data import/export	T.Message content modification
OE.Integrity protection of user data and software	T.Malicious code exploitation
OE.Procedures for preventing malicious code	T.Malicious code exploitation

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 táblázatból látható, hogy a biztonsági célok minden fenyegetést lefednek.

Fenyegetés	A fenyegetés kivédésében közreműködő biztonsági cél
Jogosult felhasználókkal kapcsolatos fenyegetések	
T.Administrative errors of omission	O.Individual accountability and audit records O.Security-relevant configuration management OE.CPS
T.Administrators, Operators, Officers and Auditors commit errors or hostile actions	O.AttributeCertificates O.Individual accountability and audit records O.Limitation of administrative access O.Maintain user attributes O.Manage behavior of security functions O.Protect stored audit records O.Restrict actions before authentication O.Security roles OE.Administrators, Operators, Officers and Auditors guidance documentation OE.Competent Administrators, Operators, Officers and Auditors OE.Detect modifications of firmware, software, and backup data OE.Protect stored audit records OE.Respond to possible loss of stored audit records OE.Time stamps OE.Validation of security function
T.User abuses authorization to collect and/or send data	O.Individual accountability and audit records
T.User error makes data inaccessible	OE.Detect modifications of firmware, software, and backup data OE.Sufficient backup storage and effective restoration
Rendszerrel kapcsolatos fenyegetések	
T.Critical system component fails	O.Configuration Management O.Manage behavior of security functions OE.Installation OE.Lifecycle security OE.Preservation/trusted recovery of secure state OE.Repair identified security flaws OE.Sufficient backup storage and effective restoration OE.Time stamps
T.Flawed code	OE.Repair identified security flaws
T.Malicious code exploitation	O.Configuration Management OE.Integrity protection of user data and software OE.Procedures for preventing malicious code OE.Lifecycle security OE.Object and data recovery free from malicious code OE.Periodically check integrity OE.Require inspection for downloads OE.Validation of security function
T.Message content modification	O.Protect user and TSF data during internal transfer OE.Trusted Path OE.Data import/export

Kriptográfiával kapcsolatos fenyegetések	
T.Disclosure of private and secret keys	O.Limitation of administrative access O.Protect user and TSF data during internal transfer OE.Administrators, Operators, Officers and Auditors guidance documentation OE.Cryptographic functions
T.Modification of private/secret keys	OE.Integrity protection of user data and software O.Protect stored audit records OE.Cryptographic functions OE.Object and data recovery free from malicious code OE.Protect stored audit records
Külső támadások	
T.Hacker gains access	O.Individual accountability and audit records OE.React to detected attacks O.Restrict actions before authentication OE.Notify Authorities of Security Issues OE.Trusted Path
T.Hacker physical access	OE.Physical Protection
T.Social engineering	OE.Procedures for preventing malicious code OE.Social Engineering Training OE.Administrators, Operators, Officers and Auditors guidance documentation

4.3. táblázat: A fenyegetések kivédésében közreműködő biztonsági célok

Jogosult felhasználókkal kapcsolatos fenyegetések

T.Administrative errors of omission fenyegetés azokat a hibákat fogalmazza meg, amelyek közvetlenül kompromittálják a szervezet biztonsági céljait, vagy módosítják a rendszer által érvényre juttatott műszaki biztonsági szabályzatokat. Ezt a fenyegetést az alábbiak védik ki:

O.Individual accountability and audit records biztosítja az egyéni felelősségre vonhatóságot. 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.

OE.CPS biztosítja, hogy minden bizalmi munkakört betöltő személy (SSO, SO, RO, PO és SA) jól ismerje azt a hitelesítési rendet (CP) és szolgáltatási szabályzatot (CPS), mely alatt a TOE-t működtetik. Ezáltal a rendszer feljogosított (privilegizált) felhasználói tisztában vannak felelősségükkel, s ez csökkenti annak valószínűségét, hogy hibásan hajtanak végre egy biztonsági szempontból kritikus funkciót.

T.Administrators, Operators, Officers and Auditors commit errors or hostile actions fenyegetés az alábbiakra irányul:

- a bizalmi munkakört betöltő személyek által elkövetett olyan véletlen hibák, amelyek közvetlenül kompromittálják a szervezet biztonsági céljait, vagy megváltoztatják a rendszer által érvényre juttatandó biztonsági szabályzatot, vagy

- a rendszer konfigurációjának rosszindulatú módosítása a privilegizált felhasználók által, amely lehetővé teszi a biztonság megsértését.

Ezt a fenyegetést az alábbiak védik ki:

OE.Competent Administrators, Operators, Officers and Auditors biztosítja, hogy a a bizalmi munkakört betöltő személyek képesek a TOE megfelelő kezelésére. Ez csökkenti annak valószínűségét, hogy hibát követnek el.

OE.Administrators, Operators, Officers and Auditors guidance documentation megfelelő dokumentáció biztosításával csökkenti a bizalmi munkakört betöltő személyek hiba lehetőségeit.

O.AttributeCertificates biztosítja, hogy az attribútum tanúsítványok és az ezekre vonatkozó visszavonási listák és állapot információk érvényesek. A bizalmi munkakört betöltő személyek által szolgáltatott, tanúsítványokba foglalandó információk érvényesítése segíti annak megakadályozását, hogy az attribútum tanúsítványokba helytelen információ kerüljön.

OE.Detect modifications of firmware, software, and backup data biztosítja, hogy a mentett összetevők esetleges módosulása észlelhető.

O.Individual accountability and audit records biztosítja az egyéni felelősségre vonhatóságot. Minden felhasználó egyedileg azonosított, s így a naplóesemények visszavezethetők egy felhasználóhoz. A naplóesemények egy erre feljogosított személynek információt szolgáltatnak a felhasználók múltbeli viselkedésére. A naplóesemények visszatartják a rendszer felhasználóit attól, hogy hibásan hajtsanak végre egy biztonsági szempontból kritikus funkciót, hiszen ezért utólag felelősségre vonhatók lesznek.

O.Limitation of administrative access: az adminisztratív funkciókat úgy tervezték, hogy a felhasználók automatikusan ne rendelkezzenek hozzáféréssel a felhasználói objektumokhoz, a szükséges kivételeken kívül. A felhasználók által végrehajtható műveletek korlátozása egyben csökkenti az okozható károkat is.

O.Maintain user attributes kezeli az egyéni felhasználókkal kapcsolatos (az adott felhasználó azonosítójához rendelt) biztonsági tulajdonság együttest (amely tartalmazhat szerepkörhöz tartozást, hozzáférési privilégiumokat stb.). Ez megakadályozza, hogy a felhasználók olyan műveletet hajtsanak végre, melyekre nincs jogosultságuk.

O.Manage behavior of security functions menedzsment funkciókat biztosít a biztonsági mechanizmusok konfigurálására. Ez garantálja, hogy a rosszindulatú felhasználók ellen védelmet biztosító biztonsági mechanizmusokat helyesen konfigurálják.

O.Protect stored audit records biztosítja, hogy a naplórekordokat a TOE a hatáskörébe tartozó értékek tekintetében védi a jogosulatlan módosítással és törléssel szemben a felhasználói tevékenységekért való felelősségre vonhatóság érdekében.

OE.Protect stored audit records biztosítja, hogy a naplórekordokat a TOE környezetében védik a jogosulatlan hozzáféréssel szemben a felhasználói tevékenységekért való felelősségre vonhatóság érdekében.

OE.Respond to possible loss of stored audit records biztosítja, hogy amennyiben a napló eseménysor tároló területe megtelt vagy majdnem megtelt, csak a rendszervizsgáló által végrehajtott (naplózandó) eseményekre kerülhessen sor.

Ez garantálja, hogy az egyéb felhasználók nem hajthatnak olyan műveletet végre, melynek nincs biztosítva a naplózása, s ezen keresztül a nyomon követhetősége.

O.Restrict actions before authentication biztosítja, hogy csak korlátozott körű tevékenységek hajthatók végre a felhasználók hitelesítése előtt.

O.Security roles biztosítja, hogy biztonsági szerepköröket határoznak meg, s a felhasználókat egy vagy több ilyen szerepkörhöz rendelik. Ez megakadályozza, hogy a felhasználók olyan műveletet hajtsanak végre, melyekre nincs jogosultságuk.

OE.Time stamps pontos időpontot biztosít az események sorrendjének ellenőrizhetőségéhez. Ez a napló átvizsgálása során lehetővé teszi az események egymásutániságának rekonstruálását.

OE.Validation of security function biztosítja, hogy a biztonság-kritikus szoftver, hardver és förmver elemek helyesen működnek (az alapul szolgáló gép tesztelésére és integritás ellenőrzésére irányuló funkciókon és eljárásokon keresztül).

T.User abuses authorization to collect and/or send data fenyegetés arra az esetre vonatkozik, amikor egy felhasználó visszaélve jogosultságaival fájlokat vizsgál át abból a célból, hogy összegyűjtsön és/vagy jogosulatlan fogadónak elküldjön érzékeny vagy biztonság-kritikus adatokat. Ezt a fenyegetést az alábbiak védik ki:

O.Individual accountability and audit records biztosítja az egyéni felelősségre vonhatóságot. Minden felhasználó egyedileg azonosított, s így a naplóesemények visszavezethetők egy felhasználóhoz. A naplóesemények egy erre feljogosított személynek információt szolgáltatnak a felhasználók múltbeli viselkedésére. A naplóesemények visszatartják a felhasználókat attól, hogy jogosultságaikkal visszaélve adatokat gyűjtsenek és/vagy küldjenek, hiszen ezért utólag felelősségre vonhatók lesznek.

T.User error makes data inaccessible fenyegetés arra irányul, amikor egy felhasználó véletlenül felhasználói adatokat töröl. Következményként a felhasználói adatok hozzáférhetetlenné válnak. Példák erre az alábbiak:

- egy felhasználó véletlenül adatot töröl, rossz billentyű gomb leütéssel, vagy az enter gomb automatikus válaszként történő leütésével,
- egy felhasználó nem érti meg a számára felkínált választás következményeit, s véletlenül olyan választ ad, mely felhasználói adat törléséhez vezet,
- egy felhasználó félreértve egy rendszer parancsot, kiadásával véletlenül felhasználói adatot töröl.

Ezt a fenyegetést az alábbiak védik ki:

OE.Sufficient backup storage and effective restoration elegendő mentés tárolást és szükség esetén hatékony visszaállítást biztosít a rendszer újra felépíthetőségére. Ez biztosítja, hogy a felhasználói adatok elérhetők a mentésből, amennyiben az aktuális példányt véletlenül törölték.

OE.Detect modifications of firmware, software, and backup data biztosítja, hogy amennyiben a mentett összetevőket módosították, ez észlelhető. Ha a mentett összetevők módosítása nem észlelhető, a mentési példány nem tekinthető a felhasználói adatok megbízható visszaállítási forrásának.

Rendszerrel kapcsolatos fenyegetések

T.Critical system component fails fenyegetés egy vagy több rendszer komponens hibájára irányul, mely a rendszer kritikus fontosságú funkcionalitásának elvesztését eredményezi. Ez a fenyegetés akkor lényeges, ha hardver és/vagy szoftver tökéletlenségből adódóan rendszer komponensek hibásodhatnak meg, s a rendszer funkcionális rendelkezésre állása fontos (mint jelen esetben). Ezt a fenyegetés**t** az alábbiak védik ki:

> **O.Configuration Management** biztosítja, hogy egy konfiguráció kezelési terv kerül megvalósításra. Ez magába foglalja a konfiguráció azonosítását és a változások ellenőrzését, valamint garantálja, hogy helytelen konfigurálás miatt nem következik be kritikus rendszer komponens hiba.
>
> **OE.Installation** biztosítja, hogy a TOE-t olyan módon szállítják, telepítik, kezelik és üzemeltetik, amely megőrzi az informatikai biztonságot. Ez garantálja, hogy helytelen telepítés miatt nem következik be kritikus rendszer komponens hiba.
>
> **O.Manage behavior of security functions** menedzsment funkciókat biztosít a biztonsági mechanizmusok konfigurálására. Ez garantálja, hogy a biztonsági mechanizmusok helytelen konfigurálása miatt nem következik be kritikus rendszer komponens hiba.
>
> **OE.Preservation/trusted recovery of secure state** biztosítja, hogy a rendszer egy biztonságos állapotban marad, még akkor is, ha működése során hiba lépett fel, s ezért a rendszert helyre kellett állítani. Ez a cél azért lényeges, mert ha a rendszerhibák nem biztonságos állapotot eredményeznének, akkor a működésre helyreállított (vagy a hiba ellenére tovább működő) rendszer megsérthetné a biztonságot.
>
> **OE.Sufficient backup storage and effective restoration** elegendő mentés tárolást és hatékony visszaállítást biztosít a rendszer újra felépíthetőségére, szükség esetén. Ez biztosítja, hogy az adatok elérhetők a mentésből, amennyiben az aktuális példány elveszett egy rendszer komponens hibája miatt.
>
> **OE.Time stamps** pontos időpontot biztosít az események sorrendjének ellenőrizhetőségéhez. Amennyiben a rendszert helyre kell állítani, szükség lehet különböző tranzakciók sorrendjének a meghatározására, hogy a rendszert a hiba bekövetkezésekor érvényes állapottal konzisztens állapotba lehessen visszaállítani.
>
> **OE.Lifecycle security** a fejlesztési fázisban használt olyan eszközöket és technikákat biztosít, melyek csökkentik a hardver vagy szoftver hibák valószínűségét. Ez a biztonsági cél a működtetés során észlelt olyan hibák kijavítására is irányul, melyek kritikus rendszer komponensek meghibásodásához vezethetnek.
>
> **OE.Repair identified security flaws** biztosítja, hogy a gyártó kijavítja a felhasználók által azonosított biztonsági hibákat. Az ilyen hibák (ha nem javítanák ki ezeket) kritikus rendszer komponensek meghibásodásához vezethetnek.

T.Flawed code fenyegetés a fejlesztő által a kódolás során elkövetett hibákra irányul. A véletlen hibákra példa a technikai részletek hiánya, vagy a rossz tervezés. Ezt a fenyegetést az alábbiak védik ki:

> **OE.Repair identified security flaws** biztosítja, hogy a feltárt biztonsági hibákat kijavítják.

T.Malicious code exploitation fenyegetés arra az esetre irányul, amikor egy jogosult felhasználó, informatikai rendszer vagy támadó olyan rosszindulatú kódot tölt le és hajt végre, amely rendellenes eljárásokat okoz, s ezzel megsérti a rendszer értékeinek sértetlenségét,

rendelkezésre állását vagy bizalmasságát. A rosszindulatú kód végrehajtását egy ezt kiváltó esemény idézi elő. Ezt a fenyegetést az alábbiak védik ki:

O.Configuration Management biztosítja, hogy egy konfiguráció kezelési terv kerül megvalósításra. Ez a terv magába foglalja a konfiguráció azonosítását és a változások ellenőrzését, valamint garantálja, hogy rosszindulatú kód nem jut a rendszerbe a konfigurálási folyamat során.

OE.Integrity protection of user data and software megfelelő sértetlenség védelmet biztosít a felhasználói adatokra és a szoftverre. Ez megakadályozza, hogy a rosszindulatú kód hozzákapcsolódjon a felhasználói adatokhoz vagy szoftverekhez.

OE.Object and data recovery free from malicious code biztosítja, hogy a rendszer egy működőképes állapotba tud visszaállni egy rosszindulatú kód bejutása és károkozása után. A rosszindulatú programkód (pl. vírus vagy féreg) eltávolítása része a visszaállítási folyamatnak.

OE.Periodically check integrity biztosítja mind a rendszer, mind a szoftver sértetlenségének időszakos ellenőrzését. Ha ezek az ellenőrzések hibát találnak, rosszindulatú kód juthatott be a rendszerbe.

OE.Procedures for preventing malicious code eljárásokat és mechanizmusokat biztosít a rosszindulatú programkódok rendszerbe épülésének a megakadályozására.

OE.Require inspection for downloads biztosítja, hogy a letöltött/leszállított szoftvereket megvizsgálják, mielőtt használatba vennék.

OE.Validation of security function biztosítja, hogy a biztonság-kritikus szoftver, hardver és förmver elemek helyesen működnek (az alapul szolgáló gép tesztelésére és integritás ellenőrzésére irányuló funkciókon és eljárásokon keresztül).

OE.Lifecycle security a fejlesztési fázisban használt olyan eszközöket és technikákat biztosít, melyek csökkentik annak valószínűségét, hogy a fejlesztő rosszindulatú programkódot épít a termékbe. Ez a biztonsági cél a működtetés során észlelt olyan hibák kijavítására is irányul, mint a komponensek módosítása rosszindulatú programkódokkal.

T.Message content modification fenyegetés arra az esetre irányul, amikor egy támadó információt módosít, amelyet két gyanútlan entitás közötti kommunikációs kapcsolatból fog el, mielőtt azt a tervezett címzetthez továbbítaná. A módosításnak számos lehetséges módja van: egyetlen üzenet módosítása, kiválasztott üzenetek törlése vagy átrendezése, hamis üzenetek beillesztése, korábbi üzenetek visszajátszása, az üzenetekhez kapcsolódó biztonsági tulajdonságok módosítása. Ezt a fenyegetést az alábbiak védik ki:

O.Protect user and TSF data during internal transfer a rendszeren belül átvitt adatokat védi. A továbbított adatok védelme lehetővé teszi a TOE számára a módosított, visszajátszott vagy hamis üzenetek észlelését.

OE.Trusted Path egy megbízható útvonalat biztosít a felhasználó és a rendszer között. A megbízható útvonal megvédi az üzeneteket a támadók elfogása és módosítása ellen.

OE.Data import/export az adatok formájában megjelenő értékeket védi a TOE felé vagy a TOE-tól történő átvitel közben. A továbbított adatok védelme lehetővé teszi a TOE vagy egy külső felhasználó számára a módosított, visszajátszott vagy hamis üzenetek észlelését.

Kriptográfiával kapcsolatos fenyegetések

T.Disclosure of private and secret keys fenyegetés a magán vagy titkos kulcsok jogosulatlan felfedésére irányul. Ezt a fenyegetést az alábbiak védik ki:

OE.Administrators, Operators, Officers and Auditors guidance documentation megfelelő dokumentáció biztosításával csökkenti a privilegizált felhasználók hiba lehetőségeit.

OE.Cryptographic functions biztosítja, hogy a TOE jóváhagyott kriptográfiai algoritmusokat valósít meg a titkosításra/dekódolásra, hitelesítésre és aláírás létrehozására/ellenőrzésére, jóváhagyott kulcsgenerálási technikákat alkalmaz, valamint tanúsított kriptográfiai modulokat használ. A tanúsított kriptográfiai modulok használata garantálja, hogy a kriptográfiai kulcsokat megfelelően védik a modulokban való tárolás során.

O.Limitation of administrative access biztosítja, hogy az adminisztratív funkciókat úgy tervezték, hogy a bizalmi munkakört betöltő személyek se rendelkezzenek automatikusan hozzáféréssel a felhasználói objektumokhoz, a szükséges kivételeken kívül. A kriptográfiai kulcsokhoz hozzáférő felhasználók számának korlátozása csökkenti a jogosulatlan felfedés valószínűségét.

O.Protect user and TSF data during internal transfer a rendszer különböző részei között átvitt titkos és magánkulcsokat védi a jogosulatlan felfedéssel szemben.

T.Modification of private/secret keys fenyegetés a magán és/vagy titkos kulcsok jogosulatlan módosítására irányul. Ezt a fenyegetés**t** az alábbiak védik ki:

OE.Cryptographic functions biztosítja, hogy a TOE jóváhagyott kriptográfiai algoritmusokat valósít meg a titkosításra/dekódolásra, hitelesítésre és aláírás létrehozására/ellenőrzésére, jóváhagyott kulcsgenerálási technikákat alkalmaz, valamint tanúsított kriptográfiai modulokat használ. A tanúsított kriptográfiai modulok használata garantálja, hogy a kriptográfiai kulcsokat megfelelően védik a modulokban való tárolás során.

OE.Integrity protection of user data and software megfelelő sértetlenség védelmet biztosít a magán és titkos kulcsok számára.

OE.Object and data recovery free from malicious code biztosítja, hogy a rendszer egy működőképes állapotba tud visszaállni egy rosszindulatú kód bejutása és károkozása után. Ha a rosszindulatú programkód jogosulatlanul magán vagy titkos kulcsokat módosít, ez a biztonsági cél garantálja, hogy azok helyes értéke visszaállítható.

O.Protect stored audit records biztosítja, hogy a TOE a hatáskörébe tartozó értékek tekintetében naplórekordokat védik a jogosulatlan módosítással és törléssel szemben a felhasználói tevékenységekért való felelősségre vonhatóság érdekében. Ez a biztonsági cél támogatja, hogy a magán és titkos kulcsok módosítása a naplórekordokból észlelhető lesz.

OE.Protect stored audit records biztosítja, hogy a TOE környezetében a naplórekordokat védik a jogosulatlan hozzáféréssel szemben a felhasználói tevékenységekért való felelősségre vonhatóság érdekében. Ez a biztonsági cél támogatja, hogy a magán és titkos kulcsok módosítása a naplórekordokból észlelhető lesz.

Külső támadások

T.Hacker gains access fenyegetés az alábbiakra irányul:

- gyenge rendszer hozzáférés ellenőrzési mechanizmusok vagy felhasználói tulajdonságok,
- gyengén megvalósított rendszer hozzáférés ellenőrzés,
- a rendszer kódjában talált sebezhetőségek, melyek segítségével egy támadó észrevétlenül betörhet a rendszerbe.

Ezt a fenyegetést az alábbiak védik ki:

O.Restrict actions before authentication biztosítja, hogy csak korlátozott körű tevékenységek hajthatók végre a felhasználók hitelesítése előtt. Ez megakadályozza a hozzáférés ellenőrzési mechanizmusok megkerülésére képtelen támadót abban, hogy biztonság-kritikus tevékenységeket hajtson végre.

O.Individual accountability and audit records biztosítja az egyéni felelősségre vonhatóságot. Minden felhasználó egyedileg azonosított, s így a naplóesemények visszavezethetők egy felhasználóhoz. A naplóesemények egy erre feljogosított személynek információt szolgáltatnak a felhasználók múltbeli viselkedéséről. Ez lehetővé teszi a jogosulatlan tevékenységek észlelését. A már észlelt tevékenységekből származó kár megszüntethető vagy csökkenthető.

OE.Notify Authorities of Security Issues biztosítja, hogy a megfelelő vezetőket értesítik a rendszert érintő bármely biztonsági ügyről. Ez minimalizálja az adatvesztés vagy kompromittálódás lehetőségét.

OE.React to detected attacks automatizált értesítést vagy más reagálásokat biztosít a TSF által felfedett támadások esetében, a támadások azonosítása és elrettentése érdekében. Ez a cél különösen akkor fontos, ha a szervezet által lényegesnek tartott válaszintézkedések is kihasználható támadáshoz vezethetnek.

OE.Trusted Path egy megbízható útvonalat biztosít a felhasználó és a rendszer között. A megbízható útvonalat a hitelesítő adatok megvédésére használják, s ez csökkenti annak a valószínűségét, hogy egy támadó jogosult felhasználónak álcázza magát.

T.Hacker physical access fenyegetés arra az esetre irányul, amikor egy támadó a fizikai környezetben meglévő sebezhetőségeket aknázza ki a rendszer komponensek fizikai ellenőrzésének megszerzése érdekében.. Ezt a fenyegetést az alábbiak védik ki:

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

T.Social engineering fenyegetés arra az esetre irányul, amikor egy támadó a "social engineering" technikát alkalmazza arra, hogy információt szerezzen a rendszerbe lépésről, a rendszer felhasználásáról, a rendszer tervéről vagy a rendszer működéséről. Ezt a fenyegetést az alábbiak védik ki:

OE.Administrators, Operators, Officers and Auditors guidance documentation megfelelő dokumentáció biztosításával csökkenti a privilegizált felhasználók hiba lehetőségeit.

OE.Procedures for preventing malicious code eljárásokat és mechanizmusokat biztosít a rosszindulatú programkódok rendszerbe épülésének a megakadályozására. A rosszindulatú programkódok rendszerbe építése lehet az egyik célja a "social engineering" típusú támadásoknak.

OE.Social Engineering Training biztosítja, hogy az általános felhasználók, a rendszeradminisztrátorok, a rendszerüzemeltetők, a tisztviselők és a rendszervizsgálók képzést kaptak a "social engineering" típusú támadások megakadályozási technikáira.

A fenti igazolásból látható, hogy az azonosított biztonsági célok minden fenyegetéssel szemben hatékony ellenintézkedéseket valósítanak meg.

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.Maintain user attributes O.Restrict actions before authentication O.Security roles O.User authorization management OE.Auditors Review Audit Logs
P.Cryptography	OE.Cryptographic functions

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.Restrict actions before authentication, O.Security roles és **O.User authorization management** azt biztosítják, hogy a felhasználókat csak azon tevékenységek végrehajtására jogosítják fel, melyekre munkájuk során szükségük van.

OE.Auditors Review Audit Logs pedig visszatartja a felhasználókat attól, hogy jogosultságaikkal visszaéljenek.

P.Cryptography megállapítja, hogy jóváhagyott kriptográfiai szabványokat és műveleteket kell alkalmazni a TOE és informatikai környezete tervezése során. Ennek a biztonsági szabálynak az érvényre juttatására az alábbi biztonsági cél irányul:

OE.Cryptographic functions, mely biztosítja, hogy csak szabványokon alapuló megoldásokat használnak.

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

4.3.2.3 A biztonsági célok elégségessége a feltételek teljesüléséhez

A 4.5 táblázatból látható, hogy a biztonsági célok minden feltétel teljesüléséhez hozzájárulnak.

Feltétel	A feltétel teljesülésében közreműködő, üzemeltetési környezetre vonatkozó biztonsági cél
Személyi feltételek	
A.Auditors Review Audit Logs	OE.Auditors Review Audit Logs
A.Authentication Data Management	OE.Authentication Data Management
A.Competent Administrators, Operators, Officers and Auditors	OE.Competent Administrators, Operators, Officers and Auditors OE.Installation
A.Cooperative Users	OE.Cooperative Users
A.CPS	OE.CPS
A.Disposal of Authentication Data	OE.Disposal of Authentication Data
A.Notify Authorities of Security Issues	OE.Notify Authorities of Security Issues
A.Social Engineering Training	OE.Social Engineering Training
Kapcsolódási feltételek	
A.Operating System	OE.Operating System
Fizikai feltételek	
A.Communication Protection	OE.Communication Protection
A.Physical Protection	OE.Physical Protection

4.5. táblázat: A feltételek teljesülésében közreműködő biztonsági célok

Személyi feltételek

A.Auditors Review Audit Logs feltétel megállapítja, hogy a biztonság-kritikus eseményekről naplóbejegyzés szükséges, s ezeket a rendszervizsgálónak át kell vizsgálnia. Ennek a feltételnek a teljesülésére irányul az alábbi biztonsági cél:

> **OE.Auditors Review Audit Logs**, mely biztosítja, hogy a naplózott biztonság-kritikus eseményeket a rendszervizsgáló átvizsgálja.

A.Authentication Data Management feltétel megállapítja, hogy a felhasználói hitelesítési adatok kezelése a TOE-n kívül esik. Ennek a feltételnek a teljesülésére irányul az alábbi biztonsági cél:

> **OE.Authentication Data Management**, mely biztosítja, a felhasználók hitelesítési adataikat megfelelő biztonsági szabályzat szerint módosítják.

A.Competent Administrators, Operators, Officers and Auditors feltétel megállapítja, hogy a TOE biztonsága a TOE-t menedzselőktől függ. Ennek a feltételnek a teljesülésére irányulnak az alábbi biztonsági célok:

> **OE.Competent Administrators, Operators, Officers and Auditors**, mely biztosítja, hogy a rendszert menedzselők szakértők a menedzselésben.
>
> **OE.Installation**, mely biztosítja, hogy a TOE biztonságáért felelős személyek biztosítják, hogy a TOE-t a bitonságot fenntartó módon szállítják, telepítik, kezelik és működtetik.

A.Cooperative Users feltétel megállapítja, hogy biztonságos IT környezet szükséges a TOE biztonságos üzemeltetéséhez, s a felhasználóknak a környezet által támasztott korlátozásoknak megfelelően kell dolgozniuk. Ennek a feltételnek a teljesülésére irányul az alábbi biztonsági cél:

OE.Cooperative Users, mely biztosítja, hogy a felhasználók együttműködő módon, a korlátozásoknak megfelelően tevékenykednek.

A.CPS feltétel megállapítja, hogy a rendszeradminisztrátorok, rendszerüzemeltetők, tisztviselők és rendszervizsgálók jól ismerik azt a hitelesítési rendet (CP) és szolgáltatási szabályzatot (CPS), mely alatt a TOE-t működtetik. Ennek a feltételnek a teljesülésére irányul az alábbi biztonsági cél:

OE.CPS, mely biztosítja, hogy a rendszeradminisztrátorok, rendszerüzemeltetők, tisztviselők és rendszervizsgálók jól ismerik azt a hitelesítési rendet (CP) és szolgáltatási szabályzatot (CPS), mely alatt a TOE-t működtetik.

A.Disposal of Authentication Data feltétel megállapítja, hogy a felhasználóknak nem szabad hozzáférniük a rendszerhez, miután megszűnt az erre vonatkozó jogosultságuk. Ennek a feltételnek a teljesülésére irányul az alábbi biztonsági cél:

OE.Disposal of Authentication Data, mely biztosítja, hogy a rendszerhez való hozzáférést visszautasítják, miután a hozzáférési jogosultság megszűnt.

A.Notify Authorities of Security Issues feltétel megállapítja, hogy a felhasználóknak értesíteniük kell a megfelelő vezetőket a rendszert érintő bármely biztonsági ügyről, a további adatvesztés vagy kompromittálódás lehetőségének minimalizálása érdekében. Ennek a feltételnek a teljesülésére irányul az alábbi biztonsági cél:

OE.Notify Authorities of Security Issues, mely biztosítja, hogy a felhasználók értesítik a megfelelő vezetőket a rendszert érintő bármely biztonsági ügyről.

A.Social Engineering Training feltétel megállapítja, hogy a rendszerhez való hozzáférés érdekében "social engineering" típusú technikát alkalmazhatnak. Ennek a feltételnek a teljesülésére irányul az alábbi biztonsági cél:

OE.Social Engineering Training, mely biztosítja, hogy minden felhasználó képzésben részesül a "social engineering" típusú támadások meghiúsítása érdekében.

Kapcsolódási feltételek

A.Operating System feltétel megállapítja, hogy egy nem biztonságos operációs rendszer kompromittálja a rendszer biztonságát. Ennek a feltételnek a teljesülésére irányul az alábbi biztonsági cél:

OE.Operating System, mely biztosítja, hogy olyan operációs rendszert használnak, mely megfelel az elvárásoknak.

Fizikai feltételek

A.Communication Protection feltétel megállapítja, hogy a kommunikációs infrastruktúra védelme a TOE-n kívül áll. Ennek a feltételnek a teljesülésére irányul az alábbi biztonsági cél:

OE.Communication Protection, mely biztosítja a kommunikációs infrastruktúra megfelelő fizikai védelmét.

A.Physical Protection feltétel megállapítja, hogy a TOE hardver, szoftver és förmver elemeinek fizikai módosítása kompromittálhatja a rendszer biztonságát. Ennek a feltételnek a teljesülésére irányul az alábbi biztonsági cél:

O. Physical Protection, mely biztosítja a TOE hardver, szoftver és förmver elemeinek megfelelő fizikai védelmét.

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

5. Kiterjesztett összetevők meghatározása

5.1 Kiterjesztett funkcionális biztonsági követelmények

Ez a biztonsági előirányzat a CC 2. részét kiterjeszti két családdal: FDP_PKI és FMT_PKI.

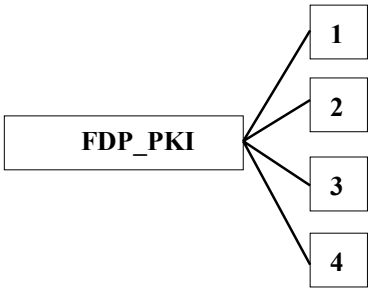
5.1.1 Az FDP_PKI család meghatározása

Az Info&AA funkcionális biztonsági követelményeinek meghatározása érdekében az FDP (A felhasználói adatok védelme) osztályon belül egy további családot (FDP_PKI) határozunk meg az alábbiakban.

FDP_PKI PKI technológia alkalmazása

Családi viselkedés
Ez a család felhasználói adatok X.509 szabványnak megfelelő PKI technikák alkalmazával történő védelmére vonatkozó követelményeket határoz meg.

Összetevő szerkezet



FDP_PKI.1 Tanúsítvány előállítás

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: FMT_PKI.1 Tanúsítvány profil menedzsment
Naplózandó események (minimális): sikeres tanúsítvány létrehozás,
sikertelen tanúsítvány létrehozás

FDP_PKI.1.1 A TSF csak olyan tanúsítványokat állíthat elő, amelyek formátuma megfelel a következőknek: [értékadás: szabványok listája].

FDP_PKI.1.2 A TSF csak olyan tanúsítványokat állíthat elő, amelyekre biztosítja az alábbiakat: [értékadás: kötelezően teljesítendő elvárások listája].

FDP_PKI.1.3 A TSF csak olyan tanúsítványokat állíthat elő, amelyek megfelelnek az aktuálisan meghatározott tanúsítvány profilnak.

FDP_PKI.2 Attribútum tanúsítvány előállítás

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: FMT_PKI.2 Attribútum tanúsítvány profil menedzsment
Naplózandó események (minimális): sikeres attribútum tanúsítvány létrehozás,
sikertelen attribútum tanúsítvány létrehozás

FDP_PKI.2.1 A TSF csak olyan attribútum tanúsítványokat állíthat elő, amelyek formátuma megfelel a következőknek: [értékadás: szabványok listája].

FDP_PKI.2.2 A TSF csak olyan attribútum tanúsítványokat állíthat elő, amelyekre biztosítja az alábbiakat: [értékadás: kötelezően teljesítendő elvárások listája].

FDP_PKI.2.3 A TSF csak olyan attribútum tanúsítványokat állíthat elő, amelyek megfelelnek az aktuálisan meghatározott attribútum tanúsítvány profilnak.

FDP_PKI.3 Tanúsítvány visszavonási lista előállítás

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: FMT_PKI.4 Tanúsítvány visszavonási lista profil menedzsment
Naplózandó események (minimális): sikeres CRL létrehozás,
sikertelen CRL létrehozás

FDP_PKI.3.1 A TSF csak olyan tanúsítvány visszavonási listákat állíthat elő, amelyek formátuma megfelel a következőknek: [értékadás: szabványok listája].

FDP_PKI.3.2 A TSF csak olyan tanúsítvány visszavonási listákat állíthat elő, amelyekre biztosítja az alábbiakat: [értékadás: kötelezően teljesítendő elvárások listája].

FDP_PKI.3.3 A TSF csak olyan tanúsítvány visszavonási listákat állíthat elő, amelyek megfelelnek az aktuálisan meghatározott CRL profilnak.

FDP_PKI.4 Attribútum tanúsítvány visszavonási lista előállítás

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: FMT_PKI.5 Attribútum tanúsítvány visszavonási lista profil menedzsment
Naplózandó események (minimális): sikeres ACRL létrehozás,
sikertelen ACRL létrehozás

FDP_PKI.4.1 A TSF csak olyan attribútum tanúsítvány visszavonási listákat állíthat elő, amelyek formátuma megfelel a következőknek: [értékadás: szabványok listája].

FDP_PKI.4.2 A TSF csak olyan attribútum tanúsítvány visszavonási listákat állíthat elő, amelyekre biztosítja az alábbiakat: [értékadás: kötelezően teljesítendő elvárások listája].

FDP_PKI.4.3 A TSF csak olyan attribútum tanúsítvány visszavonási listákat állíthat elő, amelyek megfelelnek az aktuálisan meghatározott ACRL profilnak.

5.1.2 Az FMT_PKI család meghatározása

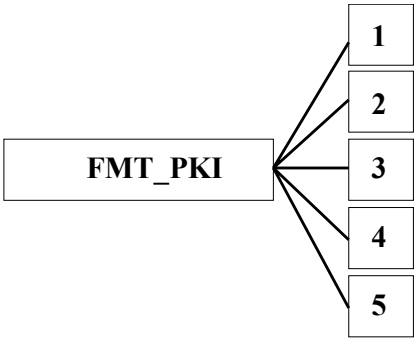
Az Info&AA funkcionális biztonsági követelményeinek meghatározása érdekében az FMT (Biztonsági menedzsment) osztályon belül egy további családot (FMT_PKI) határozunk meg az alábbiakban.

FMT_PKI A PKI technológiát alkalmazó TSF funkciók menedzsmentje

Családi viselkedés

Ez a család az X.509 szabványnak megfelelő PKI technikákat alkalmazó biztonsági funkciók kezelésére vonatkozó követelményeket határoz meg.

Összetevő szerkezet



FMT_PKI.1 Tanúsítvány profil menedzsment

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: FMT_MOF.1 A biztonsági funkciók viselkedésének kezelése
FMT_SMR.1 Biztonsági szerepkörök
FDP_PKI.1 Tanúsítvány előállítás
Naplózandó események (minimális): új tanúsítvány profil sikeres létrehozása,
létező tanúsítvány profil sikeres módosítása,
tanúsítvány profil törlése

FMT_PKI.1.1 A TSF-nek meg kell valósítania legalább egy tanúsítvány profilt, és biztosítania kell, hogy a kiadott tanúsítványok megfelelnek a kijelölt tanúsítvány profilnak.

FMT_PKI.1.2 A TSF-nek biztosítania kell, hogy a [értékadás: feljogosított szerepkörök listája] minden tanúsítvány profilra külön-külön megadhassák a következő mezőkre és kiterjesztésekre vonatkozó elfogadható értékek összességét: [értékadás: mezők/kiterjesztések, illetve az ezekre vonatkozó elfogadható értékek listája].

FMT_PKI.1.3 A TSF-nek meg kell követelnie, hogy az [értékadás: feljogosított szerepkör] által megadott kiterjesztésekre vonatkozóan teljesüljenek az alábbiak: [értékadás: kötelezően teljesítendő elvárások listája].

FMT_PKI.2 Attribútum tanúsítvány profil menedzsment

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: FMT_MOF.1 A biztonsági funkciók viselkedésének kezelése
FMT_SMR.1 Biztonsági szerepkörök
FMT_PKI.3 Attribútum kollekció menedzsment
FDP_PKI.2 Attribútum tanúsítvány előállítás
Naplózandó események (minimális): új attribútum tanúsítvány profil sikeres létrehozása,
létező attribútum tanúsítvány profil sikeres módosítása,
attribútum tanúsítvány profil törlése

FMT_PKI.2.1 A TSF-nek meg kell valósítania legalább egy attribútum tanúsítvány profilt, és biztosítania kell, hogy a kiadott attribútum tanúsítványok megfelelnek a kijelölt attribútum tanúsítvány profilnak.

FMT_PKI.2.2 A TSF-nek biztosítania kell, hogy az [értékadás: feljogosított szerepkörök listája] minden attribútum tanúsítvány profilra külön-külön megadhassák a következő mezőkre és kiterjesztésekre vonatkozó elfogadható értékek összességét: [értékadás: mezők/kiterjesztések, illetve az ezekre vonatkozó elfogadható értékek listája].

FMT_PKI.2.3 A TSF-nek meg kell követelnie, hogy az [értékadás: feljogosított szerepkör] által megadott kiterjesztésekre vonatkozóan teljesüljenek az alábbiak: [értékadás: kötelezően teljesítendő elvárások listája].

FMT_PKI.3 Attribútum kollekció menedzsment

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: FMT_MOF.1 A biztonsági funkciók viselkedésének kezelése
FMT_SMR.1 Biztonsági szerepkörök
FMT_PKI.2 Attribútum tanúsítvány profil menedzsment
FDP_PKI.2 Attribútum tanúsítvány előállítás
Naplózandó események (minimális): új attribútum kollekció sikeres létrehozása,
létező attribútum kollekció sikeres módosítása,
attribútum kollekció törlése,

FMT_PKI.3.1 A TSF-nek meg kell valósítania egy attribútum kollekciót, hozzá kell ezt rendelnie egy létező attribútum tanúsítvány profilhoz, valamint biztosítania kell, hogy a kiadott attribútum tanúsítványok megfelelnek az adott profilnak és kollekciónak.

FMT_PKI.3.2 A TSF-nek biztosítania kell, hogy az [értékadás: feljogosított szerepkörök listája] megadhassák a következő (Attribute Types) kiterjesztésekre vonatkozó elfogadható értékek összességét: [értékadás: az Attribute Types kiterjesztésekre vonatkozó elfogadható értékek listája].

FMT_PKI.3.3 A TSF-nek meg kell követelnie, hogy az [értékadás: feljogosított szerepkörök listája] által megadott kiterjesztésekre vonatkozóan teljesüljenek az alábbiak: [értékadás: kötelezően teljesítendő elvárások listája].

FMT_PKI.4 Tanúsítvány visszavonási lista profil menedzsment

Függések: FMT_MOF.1 A biztonsági funkciók viselkedésének kezelése
FMT_SMR.1 Biztonsági szerepkörök
FDP_PKI.3 Tanúsítvány visszavonási lista előállítás
Naplózandó események (minimális): új CRL profil sikeres létrehozása,
létező CRL profil sikeres módosítása,
CRL profil törlése

FMT_PKI.4.1 A TSF-nek meg kell valósítania legalább egy tanúsítvány visszavonási lista profilt, és biztosítania kell, hogy a kiadott tanúsítvány visszavonási listák megfelelnek a kijelölt tanúsítvány visszavonási lista profilnak.

FMT_PKI.4.2 A TSF-nek biztosítania kell, hogy az [értékadás: feljogosított szerepkörök listája] minden tanúsítvány visszavonási lista profilra külön-külön megadhassák a következő mezőkre és kiterjesztésekre vonatkozó elfogadható értékek összességét: [értékadás: az Attribute Types kiterjesztésekre vonatkozó elfogadható értékek listája].

FMT_PKI.4.3 A TSF-nek meg kell követelnie, hogy az [értékadás: feljogosított szerepkörök listája] által megadott kiterjesztésekre vonatkozóan teljesüljenek az alábbiak: [értékadás: kötelezően teljesítendő elvárások listája].

FMT_PKI.5 Attribútum tanúsítvány visszavonási lista profil menedzsment

Függések: FMT_MOF.1 A biztonsági funkciók viselkedésének kezelése
FMT_SMR.1 Biztonsági szerepkörök
FDP_PKI.4 Attribútum tanúsítvány visszavonási lista előállítás
Naplózandó események (minimális): új ACRL profil sikeres létrehozása,
létező ACRL profi sikeres módosítása,
ACRL profil törlése

FMT_PKI.5.1 A TSF-nek meg kell valósítania legalább egy attribútum tanúsítvány visszavonási lista profilt, és biztosítania kell, hogy a kiadott ACRL-ek megfelelnek a kijelölt ACRL profilnak.

FMT_PKI.5.2 A TSF-nek biztosítania kell, hogy az [értékadás: feljogosított szerepkörök listája] minden ACRL profilra külön-külön megadhassák a következő mezőkre és kiterjesztésekre vonatkozó elfogadható értékek összességét: [értékadás: az Attribute Types kiterjesztésekre vonatkozó elfogadható értékek listája].

FMT_PKI.5.3 A TSF-nek meg kell követelnie, hogy az [értékadás: feljogosított szerepkörök listája] által megadott kiterjesztésekre vonatkozóan teljesüljenek az alábbiak: [értékadás: kötelezően teljesítendő elvárások listája].

5.2 Kiterjesztett garanciális biztonsági követelmények

Jelen 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 (a kiterjesztett összetevőket félkövér betűtípus jelzi).

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
	A belső adatátvitel alapszintű védelme	FDP_ITT.1
	Részleges információ áramlás ellenőrzés	FDP_IFC.1
	Egyszerű biztonsági tulajdonságok	FDP_IFF.1
	Felhasználói adatok exportálása biztonsági tulajdonságokkal	FDP_ETC.2
	Attribútum tanúsítvány előállítás	**FDP_PKI.2**
	Attribútum tanúsítvány visszavonási lista előállítás	**FDP_PKI.4**
Azonosítás és hitelesítés (FIA)	Felhasználói tulajdonságok megadása	FIA_ATD.1
	A hitelesítés időzítése	FIA_UAU.1
	Az azonosítás időzítése	FIA_UID.1
	Felhasználó - szubjektum összerendelése	FIA_USB.1
Biztonsági menedzsment (FMT)	A biztonsági funkciók viselkedésének kezelése	FMT_MOF.1
	Attribútum tanúsítvány profil menedzsment	**FMT_PKI.2**
	Attribútum kollekció menedzsment	**FMT_PKI.3**
	Attribútum tanúsítvány visszavonási lista profil menedzsment	**FMT_PKI.5**
	Biztonsági tulajdonságok kezelése (iteráció 1)	FMT_MSA.1/ SO fiók
	Biztonsági tulajdonságok kezelése (iteráció 2)	FMT_MSA.1/ RO fiók
	Biztonsági tulajdonságok kezelése (iteráció 3)	FMT_MSA.1/ PO fiók
	Statikus tulajdonságok kezdeti értékadása	FMT_MSA.3/ fiókok
	Statikus tulajdonságok kezdeti értékadása	FMT_MSA.3/ LDAP
	Menedzsment funkciók megadása	FMT_SMF.1
	Biztonsági szerepkörök	FMT_SMR.1
A TOE biztonsági funkciók védelme (FPT)	A külső TSF adatátvitel módosításának észlelése	FPT_ITI.1
	A TSF-adatok belső adatátvitelének alapszintű védelme	FPT_ITT.1

6.1. táblázat: A funkcionális biztonsági követelmények

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

6.1.1 Biztonság menedzsment (biztonság menedzsment funkciók)

FMT_SMR.1 Biztonsági szerepkörök

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

FMT_SMR.1.1 A TSF-nek kezelnie kell az alábbi szerepköröket: **[rendszer biztonsági tisztviselő (SSO), biztonsági tisztviselő (SO), regisztrációs tisztviselő (RO), attribútum-szabályzó tisztviselő (PO)]**

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 (minimális): a menedzsment funkciók használata

FMT_SMF.1.1 A TSF-nek képesnek kell lennie a következő biztonság menedzsment funkciók végrehajtására: **[SO fiók kezelés, RO fiók kezelés, PO fiók kezelés, konfigurációs állományok kezelése, Attribútum tanúsítvány profil kezelés, ACRL profil kezelés, Attribútum kollekciók kezelése]**

FMT_MSA.1/ SO fiók - 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 (minimális): nincs

FMT_MSA.1.1 A TSF-nek érvényt kell szereznie az **[„InfoAA" hozzáférés ellenőrzés szabály SFP]**-nek, azáltal, hogy a **[biztonsági tisztviselő (SO) szerepkör]** biztonsági tulajdonság **[meghatározását, módosítását és törlését]** a **[rendszer biztonsági tisztviselő (SSO)]** szerepkörre korlátozza.

FMT_MSA.1/ RO fiók - 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 (minimális): nincs

FMT_MSA.1.1 A TSF-nek érvényt kell szereznie az **[„InfoAA" hozzáférés ellenőrzés szabály SFP]**-nek, azáltal, hogy a **[regisztrációs tisztviselő (RO) szerepkör, valamint a szerepkört betöltő felhasználó jogosultságai (jogosult profilok, illetve profilonként jogosult műveletek /Issue, Revoke, Hold, Activate/]** biztonsági tulajdonságok **[meghatározását, módosítását és törlését]** a **[biztonsági tisztviselő (SO)]** szerepkörre korlátozza.

FMT_MSA.1/ PO fiók - 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 (minimális): nincs

FMT_MSA.1.1 A TSF-nek érvényre kell juttatnia az **[„InfoAA" hozzáférés ellenőrzés szabály SFP-t]** azáltal, hogy az **[attribútum-szabályozó tisztviselő (PO) szerepkör, valamint a szerepkört betöltő felhasználó jogosultságai (jogosult profilok)]** biztonsági tulajdonságok **[meghatározását, módosítását és törlését]** a **[biztonsági tisztviselő (SO)]** szerepkörre korlátozza.

FMT_MSA.3/ fiókok - Statikus tulajdonságok kezdeti értékadása

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: FMT_MSA.1 Biztonsági tulajdonságok kezelése
FMT_SMR.1 Biztonsági szerepkörök
Naplózandó események (minimális): nincs

FMT_MSA.3.1 A TSF-nek érvényt kell szereznie az **[„InfoAA" 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_MSA.3/ LDAP - Statikus tulajdonságok kezdeti értékadása

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: FMT_MSA.1 Biztonsági tulajdonságok kezelése
FMT_SMR.1 Biztonsági szerepkörök
Naplózandó események (minimális): nincs

FMT_MSA.3.1 A TSF-nek érvényre kell juttatnia az **[„ACRL LDAP-ba exportálása" információ áramlás ellenőrzés szabály SFP-t], [korlátozó]** alapértékek biztosításával az SFP-t érvényre juttató biztonsági tulajdonságokra.

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

FMT_MOF.1 A biztonsági funkciók viselkedésének kezelése

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: FMT_SMR.1 Biztonsági szerepkörök
FMT_SMF.1 Menedzsment funkciók megadása
Naplózandó események (minimális): nincs

FMT_MOF.1.1 A TSF-nek a **[6.2 táblázatban szereplő]** szerepkörökre kell korlátoznia a **[6.2 táblázatban szereplő]** biztonság menedzsment funkciók **[viselkedésének módosítását]**.

biztonság menedzsment funkció	Jogosult szerepkör
konfigurációs állományok (InfoAA.config és InfoAA.raconfig) kezelése	SO /két SO együttes aláírása kell/
Attribútum tanúsítvány profil kezelés	SO /két SO együttes aláírása kell/.
ACRL profil kezelés	SO /két SO együttes aláírása kell/
Attribútum kollekciók kezelése	PO /egy erre jogosult PO aláírása kell/

6.2 táblázat: Jogosult szerepkörök a biztonsági funkciók működésének módosítására

6.1.2 Felhasználó adatokra vonatkozó funkciók (hozzáférés ellenőrzés)

Az InfoAA.exe egyes objektumok olvasásakor speciális hozzáférés ellenőrzési szabályokat érvényesít:

FDP_ACC.1 Részleges hozzáférés ellenőrzés

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

FDP_ACC.1.1 A TSF-nek érvényre kell juttatnia az **[„InfoAA"** hozzáférés ellenőrzés szabály SFP-t**]** az alábbi szubjektumok és objektumok között, az alábbi műveletekre:

szubjektum: **InfoAA.exe**
objektumok: **InfoAA.sso,**
InfoAA.so,
InfoAA.ro, InfoAA.po,
AaProfiles/*.aaprofile, CrlProfiles/*.crlprofile,
Attributes/*.attributes
szolgálati kérések (Issue, Revocation, Hold, Activate)
művelet: **olvasás**

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 (minimális): hozzáférésre irányuló sikeres művelet kérés

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

objektum	Az „InfoAA" hozzáférés ellenőrzés szabályban érintett biztonsági tulajdonság
InfoAA.sso	**-**
InfoAA.so	**az objektumot digitálisan aláíró 2 felhasználó által betölthető szerepkör**
InfoAA.ro, InfoAA.po, AaProfiles/*.aaprofile, CrlProfiles/*.crlprofile	**az objektumot digitálisan aláíró 2 felhasználó által betölthető szerepkör**
Attributes/*.attributes	**az objektumot digitálisan aláíró felhasználó által betölthető szerepkör és jogosultság**
szolgálati kérések	**az objektumot digitálisan aláíró felhasználó által betölthető szerepkör és jogosultság**

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:

objektum	érvényre juttatandó szabály
InfoAA.sso	**A tároláshoz használt gépfüggő titkosítás dekódolható-e**
InfoAA.so	**az objektum mindkét digitális aláírása érvényes-e**
InfoAA.ro, InfoAA.po, AaProfiles/*.aaprofile, CrlProfiles/*.crlprofile	**az objektum mindkét digitális aláírása érvényes-e**
Attributes/*.attributes	**az objektum digitális aláírása érvényes-e**
szolgálati kérések	**az objektum digitális aláírása érvényes-e**

FDP_ACF.1.3 A TSF-nek explicit módon kell megadnia a szubjektumok objektumokhoz való hozzáférési engedélyeit a következő kiegészítő szabályok alapján:

objektum	érvényre juttatandó szabály
InfoAA.sso	**-**
InfoAA.so	**a két aláíró különböző személy-e, egyúttal mindketten betölthetnek-e SSO szerepkört**
InfoAA.ro, InfoAA.po, AaProfiles/*.aaprofile, CrlProfiles/*.crlprofile	**a két aláíró különböző személy-e, egyúttal mindketten betölthetnek-e SO szerepkört**
Attributes/*.attributes	**az aláíró betölthet-e PO szerepkört, egyúttal jogosult-e az adott attribútum kollekcióhoz tartozó profilhoz attribútum szabályok meghatározására**
szolgálati kérések	**az aláíró betölthet-e RO szerepkört, egyúttal jogosult-e a kérésben érintett profilra, valamint a kérésben érintett műveletre (Issu, Revoke, Hold, Activate)**

FDP_ACF.1.4 A TSF-nek explicit módon le kell tiltania a szubjektumok objektumokhoz való hozzáféréseit az alábbiak alapján: **[nincsenek további szabályok].**

Az InfoAA.exe a generált ACRL-ek LDAP szerverre továbbításánál speciális információáramlás ellenőrzési szabályokat érvényesít.

FDP_IFC.1 Részleges információ áramlás ellenőrzés

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: FDP_IFF.1 Egyszerű biztonsági tulajdonságok
Naplózandó események (minimális): nincs

FDP_IFC.1.1 A TSF-nek érvényre kell juttatnia az **[„ACRL LDAP-ba exportálása”** információ áramlás ellenőrzés szabály SFP-t**]** az alábbi szubjektumra, információra és műveletre:
szubjektum: **InfoAA.exe**
információ: **generált új ACRL**
művelet: **az információ (ACRL) elküldése**

FDP_IFF.1 Egyszerű biztonsági tulajdonságok

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: FDP_IFC.1 Részleges információ áramlás ellenőrzés
FMT_MSA.3 Statikus tulajdonságok inicializálása
Naplózandó események (minimális): az információ áramlást engedélyező döntések

FDP_IFF.1.1 A TSF-nek érvényre kell juttatnia az **[„ACRL LDAP-ba exportálása”** információ áramlás ellenőrzés szabály SFP-t**]** az alábbi szubjektumra, információra és biztonsági tulajdonságokra:
szubjektum: **InfoAA.exe**
információ: **ACRL**
biztonsági tulajdonságok: **az érintett CRL profilban meghatározott, az LDAP szerver beállítására vonatkozó paraméterek (Address, Port, CRL DN, Delta CRL DN, Username, Password)**

FDP_IFF.1.2 A TSF-nek engedélyeznie kell egy információ áramlást egy ellenőrzött szubjektum és egy ellenőrzött információ között egy ellenőrzött műveleten keresztül, ha teljesülnek az alábbi szabályok:

- **Address értéke egy IP cím (az LDAP szerver IP címe),**
- **Port értéke egy szám (az LDAP szerver portja),**
- **CRL DN értéke egy megkülönböztetett név (az ACRL publikálására szolgáló levélelem az LDAP szerveren),**
- **Delta CRL DN értéke egy megkülönböztetett név (a Delta CRL publikálására szolgáló levélelem az LDAP szerveren),**
- **Username (az LDAP telepítésekor meghatározott, az LDAP hozzáféréséhez szükséges felhasználói név)**
- **Password (a felhasználói névhez tartozó jelszó)**

FDP_IFF.1.3 A TSF-nek érvényre kell juttatnia a következő egyéb szabályokat:

- **Az ACRL-t az RFC 5280 X.509 szabvány CRL formátumának megfelelő üzenetetben kell exportálni a TOE-n kívülre.**

FDP_IFF.1.4 A TSF-nek explicit módon engedélyeznie kell az információ áramlást az alábbi szabályok alapján: [**az információ fogadása az LDAP szerveren sikeresen megtörtént**].

FDP_IFF.1.5 A TSF-nek explicit módon meg kell akadályoznia az információ áramlást az alábbi szabályok alapján: [**nincs szabály**].

6.1.3 Azonosítás és hitelesítés

FIA_ATD.1 Felhasználói tulajdonságok megadása

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: nincs
Naplózandó események (minimális): nincs

FIA_ATD.1.1 A TSF-nek az egyedi felhasználókhoz tartozó alábbi biztonsági tulajdonságokat kell kezelnie: **[a felhasználó által betölthető szerepkörök halmaza (SSO, SO, RO, PO), PO és RO esetén azon tanúsítvány profilok, melyek szabályozására az adott felhasználó fel van hatalmazva, RO esetén az egyes tanúsítvány profilokhoz tartozó külön jogosultságok (Issue, Revoke, Hold, Activate) is].**

FIA_UID.1 Az azonosítás időzítése

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: nincs
Naplózandó események (minimális): a felhasználó azonosítási mechanizmus sikertelen használata (benne a megadott felhasználó azonosító is).

FIA_UID.1.1 A TSF-nek a felhasználó azonosítása előtt lehetővé kell tennie az alábbi tevékenységek felhasználó nevében történő végrehajtását: **[azonosításra használandó saját tanúsítvány kiválasztása az MS tanúsítványtárából, a hitelesítés során aláírandó adat megtekintése, a login-ból való visszalépés].**

FIA_UID.1.2 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.1 A hitelesítés időzítése

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: FIA_UID.1 Az azonosítás időzítése
Naplózandó események (minimális): a hitelesítési mechanizmus sikertelen használata

FIA_UAU.1.1 A TSF-nek a felhasználó hitelesítése előtt lehetővé kell tennie az alábbi tevékenységek felhasználó nevében történő végrehajtását: **[a „login to <alkalmazásnév> <dátum> <időpont>" adat aláírása az azonosítás során kiválasztott magánkulccsal].**

FIA_UAU.1.2 A TSF-nek meg kell követelnie minden felhasználó sikeres hitelesítését, mielőtt bármilyen TSF által közvetített más tevékenységet lehetővé tenne az adott felhasználó nevében.

FIA_USB.1 Felhasználó - szubjektum összerendelése

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: FIA_ATD.1 Felhasználói tulajdonságok megadása
Naplózandó események (minimális): sikertelen összekapcsolás (szubjektum és biztonsági tulajdonságok)

FIA_USB.1.1 A TSF-nek össze kell kapcsolnia a felhasználó alábbi biztonsági tulajdonságait az adott felhasználó nevében tevékenykedő szubjektumokkal: **[a felhasználó által betöltött szerepkör (SSO, SO, RO vagy PO), PO és RO esetén az adott felhasználó jogosultságai /PO: jogosult profilok, RO: jogosult profilok és műveletek (Issue, Hold, Revoke, Activate)/].**

6.1.4 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 [minimális] 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 és az esemény kimenetele (siker vagy sikertelenség);

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.

6.1.5 Külső és belső adatátvitel védelme

FDP_ITT.1 A belső adatátvitel alapszintű védelme

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: [FDP_ACC.1 Részleges hozzáférés ellenőrzés, vagy
FDP_IFC.1 Részleges információ áramlás ellenőrzés]
Naplózandó események (minimális): nincs

FDP_ITT.1.1 A TSF-nek érvényre kell juttatnia az **[„InfoAA" hozzáférés ellenőrzés szabály SFP-t]** a szolgáltatói kérdésekben és válaszokban továbbított felhasználói adatok [**módosítás]** elleni védelme érdekében, a TOE fizikailag elkülönülő részei közötti átvitel közben.

FPT_ITT.1 A TSF-adatok belső adatátvitelének alapszintű védelme

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: nincs
Naplózandó események (minimális): nincs

FPT_ITT.1.1 A TSF-nek az adatátvitel során védenie kell a [**módosítással**] szemben a TSF adatokat, a TOE fizikailag elkülönülő részei közötti átvitel közben.

FDP_ETC.2 Felhasználói adatok exportálása biztonsági tulajdonságokkal

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: [FDP_ACC.1 Részleges hozzáférés ellenőrzés, vagy
FDP_IFC.1 Részleges információ áramlás ellenőrzés]
Naplózandó események (minimális): az információ sikeres exportálása

FDP_ETC.2.1 A TSF-nek érvényre kell juttatnia az [**„ACRL LDAP-ba exportálása"** információ áramlás ellenőrzés szabály SFP-t] amikor az SFP által ellenőrzött LDAP-ba publikált ACRL felhasználói adatot és az ehhez kapcsolódó biztonsági tulajdonságokat exportálja a TOE-n kívülre.

FDP_ETC.2.2 A TSF-nek a felhasználói adatot a hozzá kapcsolódó biztonsági tulajdonságokkal együtt kell exportálnia.

FDP_ETC.2.3 A TSF-nek biztosítania kell, hogy amennyiben biztonsági tulajdonságokat exportál a TOE-n kívülre, akkor azok egyértelműen kapcsolódjanak az exportált felhasználói adatokhoz.

FPT_ITI.1 A külső TSF adatátvitel módosításának észlelése

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: nincs
Naplózandó események (minimális): nincs

FPT_ITI.1.1 A TSF-nek biztosítania kell az összes syslog szervernek küldött naplórekordra a módosítás észlelésének lehetőségét a TSF és a syslog szerver közötti adatátvitel során az alábbi módosítási metrika szerint: [**tetszőleges módosítás a naplórekordok tartalmában vagy sorrendjében (beleértve a kihagyást és beszúrást is) kimutatható legyen**].

6.1.6 Attribútum tanúsítványok

6.1.6.1 Attribútum tanúsítványok létrehozása

A TOE által kibocsátott attribútum tanúsítványoknak meg kell felelniük az ITU-T X.509-2000, RFC 3281 és RFC 4476 szabványoknak. Minden attribútum tanúsítványba kerülő mezőt és kiterjesztést vagy az Info&AA rendszernek kell előállítania a fenti X.509 szabványok szabályainak megfelelően, vagy a megfelelést ellenőriznie kell.

Minden attribútum tanúsítványba kerülő mezőt és kiterjesztést jóvá kell hagyni. Egy tanúsítvány mező vagy kiterjesztés értéke általában a következő négyféle mód valamelyikével hagyható jóvá:

1. Az adatot jóváhagyhatja egy regisztrációs tisztviselő (RO) manuális úton.
2. Egy automatizált eljárás alkalmazható az adatok átvizsgálására és jóváhagyására.
3. A mező vagy kiterjesztés értékét generálhatja automatikusan az Info&AA.
4. A mezőre vagy kiterjesztésre vonatkozó érték származhat egy attribútum kollekció vagy attribútum tanúsítvány profilból.

FDP_PKI.2 Attribútum tanúsítvány előállítás

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: FMT_PKI.2 Attribútum tanúsítvány profil menedzsment
Naplózandó események (minimális): sikeres tanúsítvány létrehozás,
sikertelen tanúsítvány létrehozás

FDP_PKI.2.1 A TSF csak olyan attribútum tanúsítványokat állíthat elő, amelyek formátuma megfelel a következőknek: **[ITU-T X.509-2000, RFC 3281 és RFC 4476 X.509 szabványok].**

FDP_PKI.2.2 A TSF csak olyan attribútum tanúsítványokat állíthat elő, amelyre biztosítja az alábbiakat:

a.) Az AttCertVersion mező a 2 egész számot tartalmazza.
b.) A Holder mezőnek vagy a tulajdonos PKI tanúsítványának azonosítóját (baseCertificateID) vagy a tulajdonos nevét (General Names formátumban) kell tartalmaznia (pontosan az egyiket).
c.) Az AttCertIssuer mező kizárólag az attribútum tanúsítvány kibocsátó nevét (issuerName) tartalmazza GeneralNames formátumban.
d.) A Signature mezőben szereplő algorithm-nak egy FIPS-által jóváhagyott algoritmus OID-jét kell tartalmaznia.
e.) A serialNumber mező értékének egyedinek kell lennie a kibocsátó Attribútum-szolgáltatóra vonatkozóan.
f.) A validity mezőnek specifikálnia kell egy notBefore értéket, amely nem előzheti meg az aktuális időpontot, és egy notAfter értéket, ami nem előzheti meg a notBefore-ban megadott értéket
g.) Az Issuer Unique Identifier akkor és csak akkor használandó, ha az AC kibocsátó PKI tanúsítványában is szerepel.

FDP_PKI.2.3 A TSF csak olyan attribútum tanúsítványokat állíthat elő, amelyek megfelelnek az aktuálisan meghatározott attribútum tanúsítvány profilnak.

6.1.6.2 Attribútum tanúsítvány profil menezsment

Egy attribútum tanúsítvány profil az attribútum tanúsítványokban előforduló mezőkre és kiterjesztésekre (az Attribute Types kiterjesztések kivételével) elfogadható értékek egy összességét határozza meg.

FMT_PKI.2 Attribútum tanúsítvány profil menedzsment

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: FMT_MOF.1 A biztonsági funkciók viselkedésének kezelése
FMT_SMR.1 Biztonsági szerepkörök
FMT_PKI.3 Attribútum kollekció menedzsment
FDP_PKI.2 Attribútum tanúsítvány előállítás
Naplózandó események (minimális): új attribútum tanúsítvány profil sikeres létrehozása,
létező attribútum tanúsítvány profil sikeres módosítása,
attribútum tanúsítvány profil törlése

FMT_PKI.2.1 A TSF-nek meg kell valósítania legalább egy attribútum tanúsítvány profilt, és biztosítania kell, hogy a kiadott attribútum tanúsítványok megfelelnek a kijelölt attribútum tanúsítvány profilnak.

FMT_PKI.2.2 A TSF-nek biztosítania kell, hogy a **[biztonsági tisztviselők (SO)]** mindenattribútum tanúsítvány profilra külön-külön megadhassák a következő mezőkre és kiterjesztésekre vonatkozó elfogadható értékek összességét:

- **Érvényességi idő korlát mezők (az alábbi négy paraméter opcionális meghatározásával: Minimum validity, Maximum validity, Minimum duration, Maximum duration)**
- **Targeting információ (targeting name és targeting group),**
- **Certificate policy,**
- **CRL Distribution Point kiterjesztés,**
- **Info access kiterjesztés,**
- **No revocation available kiterjesztés,**
- **Authority key id kiterjesztés,**
- **Certificate policy kiterjesztés (RFC 4476)**

FMT_PKI.2.3 A TSF-nek meg kell követelnie, hogy a **[biztonsági tisztviselők (SO)]** által megadott kiterjesztésekre vonatkozóan teljesüljenek az alábbiak:

- **Ha van CRL Distribution Point kiterjesztés érték meghatározva, akkor a No revocation available kiterjesztés értékét nem szabad beállítani (0),**
- **Ha nincs CRL Distribution Point kiterjesztés érték meghatározva, akkor a No revocation available kiterjesztés értékét be kell állítani (1).**

Egy attribútum kollekció az attribútum tanúsítványokban előforduló Attribute Types kiterjesztésekre vonatkozóan határozza meg az elfogadható értékek egy összességét. Minden kollekció egy adott tanúsítvány profilhoz tartozik, egy profilhoz több kollekció is megadható.

FMT_PKI.3 Attribútum kollekció menedzsment

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: FMT_MOF.1 A biztonsági funkciók viselkedésének kezelése
FMT_SMR.1 Biztonsági szerepkörök
FMT_PKI.2 Attribútum tanúsítvány profil menedzsment
FDP_PKI.2 Attribútum tanúsítvány előállítás
Naplózandó események (minimális): új attribútum kollekció sikeres létrehozása,
létező attribútum kollekció sikeres módosítása,
attribútum kollekció törlése

FMT_PKI.3.1 A TSF-nek meg kell valósítania egy attribútum kollekciót, hozzá kell ezt rendelnie egy létező attribútum tanúsítvány profilhoz, valamint biztosítania kell, hogy a kiadott attribútum tanúsítványok megfelelnek az adott profilnak és kollekciónak.

FMT_PKI.3.2 A TSF-nek biztosítania kell, hogy az **[attribútum-szabályzó tisztviselők (PO)]** megadhassák a következő (Attribute Types) kiterjesztésekre vonatkozó elfogadható értékek összességét:

- **Service Authentication Information,**
- **Access Identity,**
- **Charging Identity,**
- **Group,**
- **Role,**
- **Clearance,**
- **Custom attributes.**

FMT_PKI.3.3 A TSF-nek meg kell követelnie, hogy az **[attribútum-szabályzó tisztviselők (PO)]** által megadott kiterjesztésekre vonatkozóan teljesüljenek az alábbiak:

- **nincs**

6.1.7 Attribútum tanúsítvány visszavonás kezelés

6.1.7.1 Attribútum tanúsítvány visszavonási listák létrehozása

A TOE által kibocsátott attribútum tanúsítvány visszavonási listáknak (ACRL) meg kell felelniük az X.509 szabványnak. Egy ACRL-be kerülő minden mezőt vagy kiterjesztést a TOE-nek kell előállítania az X.509 szabványnak megfelelően.

FDP_PKI.4 Attribútum tanúsítvány visszavonási lista előállítás

Hierarchikus fölérendeltség más összetevőkhöz képest: nincs
Függések: FMT_PKI.5 Attribútum tanúsítvány visszavonási lista profil menedzsment
Naplózandó események (minimális): sikeres ACRL létrehozás,
sikertelen ACRL létrehozás

FDP_PKI.4.1 A TSF csak olyan attribútum tanúsítvány visszavonási listákat állíthat elő, amelyek formátuma megfelel a következőknek: **[ITU-T X.509-2000 és RFC 5280 szabványok].**

FDP_PKI.4.2 A TSF csak olyan attribútum tanúsítvány visszavonási listákat állíthat elő, amelyre biztosítja az alábbiakat:

1. **Ha a version mező szerepel, akkor annak 1-et kell tartalmaznia.**
2. **Ha az ACRL tartalmaz kritikus kiterjesztést, akkor a version mezőnek szerepelnie kell, s az 1 egész számot kell tartalmaznia.**
3. **Ha az issuer mező egy null Name értéket tartalmaz (pl. nullák sorozatából álló megkülönböztetett neveket), akkor az ACRL-nek tartalmaznia kell egy kritikus issuerAltName kiterjesztést.**
4. **A signature mezőnek és a signatureAlgorithm mezőnek egy FIPS által jóváhagyott algoritmus OID-jét kell tartalmaznia.**
5. **A thisUpdate mezőnek az ACRL kibocsátásának dátumát kell jeleznie.**
6. **A nextUpdate mezőben (ha ki van töltve) megadott idő nem előzheti meg a thisUpdate mezőben megadott időt.**

FDP_PKI.4.3 A TSF csak olyan attribútum tanúsítvány visszavonási listákat állíthat elő, amelyek megfelelnek az aktuálisan meghatározott ACRL profilnak.

6.1.7.2 Attribútum tanúsítvány visszavonási lista profil menedzsment

Egy attribútum tanúsítvány visszavonási lista profil arra szolgál, hogy egy attribútum tanúsítvány visszavonási listában szereplő mezőkre és kiterjesztésekre elfogadható értékeket határozzon meg. Az attribútum tanúsítvány visszavonási lista profilban megadható információkra példák az alábbiak:

- extensions – azon kiterjesztések összessége, amelyeket bele lehet/kell venni egy attribútum tanúsítvány visszavonási listába, és minden kiterjesztés esetében a kritikusságot mutató bit értéke;
- issuer, issuerAltName – az attribútum tanúsítvány visszavonási lista kibocsátójának a neve;
- nextUpdate – egy tanúsítvány visszavonási lista élettartama.

FMT_PKI.5 Attribútum tanúsítvány visszavonási lista profil menedzsment

Függések: FMT_MOF.1 A biztonsági funkciók viselkedésének kezelése
FMT_SMR.1 Biztonsági szerepkörök
FDP_PKI.4 Attribútum tanúsítvány visszavonási lista előállítás

Naplózandó események (minimális): új ACR lista sikeres létrehozása,
létező ACRL lista sikeres módosítása,
ACRL törlése

FMT_PKI.5.1 A TSF-nek meg kell valósítania legalább egy attribútum tanúsítvány visszavonási lista profilt, és biztosítania kell, hogy a kiadott ACRL-ek megfelelnek a kijelölt ACRL profilnak.

FMT_PKI.5.2 A TSF-nek biztosítania kell, hogy a **[biztonsági tisztviselők (SO)]** minden ACRL profilra külön-külön megadhassák a következő mezőkre és kiterjesztésekre vonatkozó elfogadható értékek összességét:

- **Include serial number (azt határozza meg, hogy az ACRL tartalmazzon-e egyedi sorozatszámot),**
- **Include keyid (azt határozza meg, hogy az ACRL tartalmazza-e a kibocsátó keyid mezőt),**
- **Validity period (a CRL érvényességi ideje),**
- **nextUpdate (ezt a mezőt a következő megadható paraméterek befolyásolják: Public at - az első generálás időpontja, Public period - a generálási időköz, Generate at startup – az InfoAA induláskor mindenképp generáljon ACRL-t az adott ACRL profil alapján vagy csak szükség esetén, Create at revocation - az InfoAA függetlenül a generálási időköztől minden visszavonás, felfüggesztés és aktiválás esetén generáljon-e ACRL-t az adott profil alapján)**

FMT_PKI.5.3 A TSF-nek meg kell követelnie, hogy a **[biztonsági tisztviselők (SO)]** által megadott kiterjesztésekre vonatkozóan teljesüljenek az alábbiak:

- **nincs**

A 6.3 táblázat áttekinti a garanciális biztonsági követelményeket a választott MIBÉTS kiemelt (EAL4) értékelési garanciaszinten.

Osztály	A garanciális biztonsági követelmény (SAR) megnevezése	Az 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

6.3. táblázat– A garanciális biztonsági követelmények

6.3. A funkcionális biztonsági követelmények indoklása

A 6.4 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_ITT.1 A belső adatátvitel alapszintű védelme	O.Protect user and TSF data during internal transfer
FDP_IFC.1 Részleges információ áramlás ellenőrzés	O.AttributeCertificates
FDP_IFF.1 Egyszerű biztonsági tulajdonságok	O.AttributeCertificates
FDP_ETC.2 Felhasználói adatok exportálása biztonsági tulajdonságokkal	O.AttributeCertificates
FDP_PKI.2 Attribútum tanúsítvány előállítás	O.AttributeCertificates
FDP_PKI.4 Attribútum tanúsítvány visszavonási lista előállítás	O.AttributeCertificates
FIA_ATD.1 Felhasználói tulajdonságok megadása	O.Maintain user attributes
FIA_UAU.1 A hitelesítés időzítése	O.Limitation of administrative access O.Restrict actions before authentication
FIA_UID.1 Az azonosítás időzítése	O.Individual accountability and audit records O.Limitation of administrative access
FIA_USB.1 Felhasználó - szubjektum összerendelése	O.Maintain user attributes
FMT_MOF.1 A biztonsági funkciók viselkedésének kezelése	O.Configuration Management O.Manage behavior of security functions O.Security-relevant configuration management
FMT_PKI.2 Attribútum tanúsítvány profil menedzsment	O.Configuration Management
FMT_PKI.3 Attribútum kollekció menedzsment	O.Configuration Management
FMT_PKI.5 Attribútum tanúsítvány visszavonási lista profil menedzsment	O.Configuration Management
FMT_MSA.1 /SO fiók Biztonsági tulajdonságok kezelése	O.Maintain user attributes O.User authorization management
FMT_MSA.1 /RO fiók Biztonsági tulajdonságok kezelése	O.Maintain user attributes O.User authorization management
FMT_MSA.1 /PO fiók Biztonsági tulajdonságok kezelése	O.Maintain user attributes O.User authorization management
FMT_MSA.3/ fiókok Statikus tulajdonságok kezdeti értékadása	O.Security-relevant configuration management
FMT_MSA.3/ LDAP Statikus tulajdonságok kezdeti értékadása	O.Security-relevant configuration management
FMT_SMF.1 Menedzsment funkciók megadása	O.Manage behavior of security functions
FMT_SMR.1 Biztonsági szerepkörök	O.Security roles
FPT_ITI.1 A külső TSF adatátvitel módosításának észlelése	O.Protect stored audit records
FPT_ITT.1 A TSF adatok belső adatátvitelének alapszintű védelme	O.Protect user and TSF data during internal transfer

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

A 6.5 táblázat áttekini, 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.AttributeCertificates	FDP_PKI.2 Attribútum tanúsítvány előállítás FDP_PKI.4 Attribútum tanúsítvány visszavonási lista előállítás FDP_IFC.1 Részleges információ áramlás ellenőrzés FDP_IFF.1 Egyszerű biztonsági tulajdonságok FDP_ETC.2 Felhasználói adatok exportálása biztonsági tulajdonságokkal
O.Configuration Management	FMT_MOF.1 A biztonsági funkciók viselkedésének kezelése FMT_PKI.2 Attribútum tanúsítvány profil menedzsment FMT_PKI.3 Attribútum kollekció menedzsment FMT_PKI.5 Attribútum tanúsítvány visszavonási lista profil menedzsment
O.Individual accountability and audit records	FAU_GEN.1 Napló adatok generálása FAU_GEN.2 A felhasználói azonosítóval való összekapcsolás FIA_UID.1 Az azonosítás időzítése
O.Limitation of administrative access	FDP_ACC.1 Részleges hozzáférés ellenőrzés FDP_ACF.1 Biztonsági tulajdonság alapú hozzáférés ellenőrzés FIA_UAU.1 A hitelesítés időzítése FIA_UID.1 Az azonosítás időzítése
O.Maintain user attributes	FIA_ATD.1 Felhasználói tulajdonságok megadása FIA_USB.1 Felhasználó - szubjektum összerendelése FMT_MSA.1 /SO fiók Biztonsági tulajdonságok kezelése FMT_MSA.1 /RO fiók Biztonsági tulajdonságok kezelése FMT_MSA.1 /PO fiók Biztonsági tulajdonságok kezelése
O.Manage behavior of security functions	FMT_SMF.1 Menedzsment funkciók megadása FMT_MOF.1 A biztonsági funkciók viselkedésének kezelése
O.Protect user and TSF data during internal transfer	FDP_ITT.1 A belső adatátvitel alapszintű védelme FPT_ITT.1 A TSF adatok belső adatátvitelének alapszintű védelme
O.Protect stored audit records	FPT_ITI.1 A külső TSF adatátvitel módosításának észlelése
O.Restrict actions before authentication	FIA_UAU.1 A hitelesítés időzítése
O.Security-relevant configuration management	FMT_MOF.1 A biztonsági funkciók viselkedésének kezelése FMT_MSA.3/ fiókok Statikus tulajdonságok kezdeti értékadása FMT_MSA.3/ LDAP Statikus tulajdonságok kezdeti értékadása
O.Security roles	FMT_SMR.1 Biztonsági szerepkörök
O.User authorization management	FMT_MSA.1 /SO fiók Biztonsági tulajdonságok kezelése FMT_MSA.1 /RO fiók Biztonsági tulajdonságok kezelése FMT_MSA.1 /PO fiók Biztonsági tulajdonságok kezelése

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

6.4 A funkcionális követelmények közötti függések teljesülése

A 6.6 táblázat összesíti a funkcionális 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 környzeti cél teljesíti: OE.TImeStamp
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_ITT.1	[FDP_ACC.1 vagy FDP_IFC.1]	Igen (FDP_ACC.1)
FDP_IFC.1	FDP_IFF.1	Igen
FDP_IFF.1	FDP_IFC.1 FMT_MSA.3	Igen Igen
FDP_ETC.2	[FDP_ACC.1 vagy FDP_IFC.1]	Igen (FDP_IFC.1)
FDP_PKI.2	FMT_PKI.2	Igen
FDP_PKI.4	FMT_PKI.5	Igen
FIA_ATD.1	-	-
FIA_UAU.1	FIA_UID.1	Igen
FIA_UID.1	-	-
FIA_USB.1	FIA_ATD.1	Igen
FMT_MOF.1	FMT_SMR.1 FMT_SMF.1	Igen Igen
FMT_PKI.2	FMT_MOF.1 FMT_SMR.1 FMT_PKI.3 FDP_PKI.2	Igen Igen Igen Igen
FMT_PKI.3	FMT_MOF.1 FMT_SMR.1 FMT_PKI.2 FDP_PKI.2	Igen Igen Igen Igen
FMT_PKI.5	FMT_MOF.1 FMT_SMR.1 FDP_PKI.4	Igen Igen Igen
FMT_MSA.1 /SO fiók	[FDP_ACC.1 vagy FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	Igen (FDP_ACC.1) Igen Igen
FMT_MSA.1 /RO fiók	[FDP_ACC.1 vagy FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	Igen (FDP_ACC.1) Igen Igen
FMT_MSA.1 /PO fiók	[FDP_ACC.1 vagy FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	Igen (FDP_ACC.1) Igen Igen
FMT_MSA.3/ fiókok	FMT_MSA.1 FMT_SMR.1	Igen Igen
FMT_MSA.3/ LDAP	FMT_MSA.1 FMT_SMR.1	Igen Igen
FMT_SMF.1	-	-
FMT_SMR.1	FIA_UID.1	Igen
FPT_ITI.1	-	-
FPT_ITT.1	-	-

6.6. táblázat: A funkcionális követelmények közötti függések teljesülése

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.

Az Info&AA alkalmazásának várható környezete legfeljebb mérsékelt kockázati profilú.
A legfeljebb megemelt alapszintű támadási potenciállal rendelkező támadók elleni védelem elvárása egy ár/érték elemzés eredménye volt, melyet a megbízó végzett az értékelés elvárt garanciaszintjének meghatározásakor.

7. TOE összefoglaló előírás

7.1. A funkcionális biztonsági követelmények teljesítésének módja

Az alábbiak áttekintik, hogy az Info&AA hogyan teljesíti az egyes SFR-eket. Az áttekintés a 6.1 alfejezetben is alkalmazott SFR csoportosításokat alkalmazza, mert az egymást feltételező vagy kiegészítő SFR-ek kielégítése együttesen jobban szemléltethető.

7.1.1 SF1 - Biztonság menedzsment (biztonság menedzsment funkciók)

FMT_SMR.1 (Biztonsági szerepkörök) elvárja az SSO, SO, PO és RO szerepkörök megkülönböztetését, illetve a felhasználók összekapcsolását e szerepkörökkel.

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

- SO fiók kezelés,
- RO fiók kezelés, PO fiók kezelés,
- konfigurációs állományok kezelése (InfoAA.config és InfoAA.raconfig),
- AC profil kezelés, ACRL profil kezelés,
- Attribútum kollekciók kezelése.

FMT_MSA.1, FDP_ACC.1 és ACF.1 az első 3 menedzsment funkcióra elvárják, hogy:

- csak SSO kezelheti az SO fiókot, egyúttal 2 különböző SSO kell ehhez,
- csak SO kezelheti a PO és RO fiókot, egyúttal 2 különböző SO kell ehhez.

FMT_MOF.1 a másik 4 menedzsment funkcióra elvárja, hogy:

- csak SO kezelheti a konfigurációs állományokat (InfoAA.config és InfoAA.raconfig), AC és ACRL profilokat, egyúttal 2 különböző SO kell ehhez,
- csak PO kezelheti az attribútum kollekciókat, akinek külön felhatalmazás is kell az érintett AC profilra.

„FMT_MSA.3/ fiókok” elvárja mindhárom fiókra, hogy:

- a fiókok mindig üresen jöjjenek létre és csak a jogosultak kezelhessék

„FMT_MSA.3/ LDAP” elvárja egy másik biztonsági tulajdonságra (LDAP elérés):

- az ACRL publikálás helyét jelentő LDAP címek kezdetben üresek legyenek, s ezt csak a jogosult SO-k kezelhessék.

A fent áttekintett, biztonság menedzsmenthez kapcsolódó SFR-eket az Info&AA az alábbi módon teljesíti:
Az InfoAA.exe program induláskor beolvassa az összes konfigurációs és napló állományt és ellenőrzi azokat. Az ellenőrzés kitér arra, hogy:

- SO fiókot (InfoAA.so állományt) csak két különböző SSO írhat alá
- PO és RO fiókot (InfoAA.po és InfoAA.ro állományt) csak két különböző SO írhat alá
- AC profilokat (AaProfiles/*.aaprofile) és ACRL profilokat (CrlProfiles/*.crlprofile) csak két különböző SO írhat alá.
- egyéb biztonság-kritikus konfigurációs állományokat (InfoAA.config, InfoAA.raconfig) csak két különböző SO írhat alá.
- Attribútum kollekciókat (Attributes/*.attributes) csak jogosult PO írhat alá.

7.1.2 SF2 - Felhasználó adatokra vonatkozó funkciók (hozzáférés ellenőrzés)

Az Info&AA rendszer a felhasználó adatokra alapvetően két funkciót biztosít:

- „AC előállítás kérés”
- „ACRL előállítás kérés”

Az „AC előállítás kérés” egy InfoAA RA oldalon egy jogosult RO által kiadott Issue szolgálati kérelem összeállításával és elküldésével aktivizálható. A kérés átjut az InfoAA oldalra, ahol ellenőrzésre kerül. Sikertelen ellenőrzés hiba válasz üzenetet és napló bejegyzést generál, egyéb feldolgozás nem történik. Sikeres ellenőrzés esetén a kérelem feldolgozásra kerül. A feldolgozás sikertelensége hiba válasz üzenetet és napló bejegyzést generál. Sikeres feldolgozás esetén az előállított új AC adatbázisba kerül, egyúttal továbbítódik a kérelmet kiadó InfoAA RA-nak is, ahol kimenthető a rendszerből.

Az „ACRL előállítás kérés” két féleképp keletkezhet:

Egyrészt ez a funkció egy InfoAA RA oldalon egy jogosult RO által kiadott Revoke, Hold vagy Activate szolgálati kérelem összeállításával és elküldésével aktivizálható. A kérés átjut az InfoAA oldalra, ahol ellenőrzésre kerül. Sikertelen ellenőrzés hiba válasz üzenetet és napló bejegyzést generál, egyéb feldolgozás nem történik. Sikeres ellenőrzés esetén a kérelem feldolgozásra kerül. A feldolgozás sikertelensége hiba válasz üzenetet és napló bejegyzést generál. Sikeres feldolgozás esetén az érintett AC státusza megváltozik az adatbázisban, majd (konfigurációs beállítástól függő módon) új ACRL generálódik. A státusz változás tényéről a kérelmet kiadó InfoAA RA szolgálati választ kap, az esetleg legenerálódó új ACRL pedig a megfelelő LDAP szerverre publikálódik.

Másrészt ez a funkció automatikusan is aktivizálódhat az InfoAA oldalon, a konfigurációs beállítástól függően (a következő generálás időpontját több paraméter is befolyásolja). Az ilyenkor előállított ACRL a megfelelő LDAP szerverre publikálódik, illetve a kiadásnak adatbázis változási következménye is van.

FDP_ACC.1 és FDP_IFC.1 megnevezi a rendszerben megvalósítandó, felhasználó adatokra vonatkozó ellenőrzés szabályokat, melyek az alábbiak:

- „InfoAA” hozzáférés ellenőrzés szabály,
- „ACRL LDAP-ba exportálása” információ áramlás ellenőrzés szabály.

FDP_ACC.1 és FDP_ACF.1 jellemzi az „**InfoAA**” hozzáférés ellenőrzés szabályt:

Az InfoAA.exe minden elinduláskor ellenőrzi az alábbiakat:

- az InfoAA.sso sértetlensége (sikerül-e dekódolni)
- az InfoAA.so sértetlensége és hitelessége (2 különböző SSO aláírásának ellenőrzése)
- az InfoAA.ro, InfoAA.po, *.aaprofile és *.crlprofile sértetlensége és hitelessége (2 különböző SO aláírásának ellenőrzése)
- az *.attributes sértetlensége és hitelessége (egy az érintett profilra is jogosult PO aláírásának ellenőrzése)

Az ellenőrzés sikertelensége naplózódik, és az érintett adatok nem kerülnek elfogadásra.

Az InfoAA.exe minden szolgálati kérés queu-ból történő olvasásakor ellenőrzi az alábbiakat:

- a szolgálati kérések (Issue, Revocation, Hold, Activate) sértetlensége és hitelessége (egy az érintett profilra és műveletre is jogosult RO aláírásának ellenőrzése)

Az ellenőrzés sikertelensége naplózódik, és az érintett kérelem feldolgozása helyett egy hiba válasz továbbítódik az RA-hoz.

FDP_IFC.1 és FDP_IFF.1 jellemzi az „**ACRL LDAP-ba exportálása**” információ áramlás ellenőrzés szabályt.

Új ACRL létrehozása esetén az InfoAA az érintett ACRL profilban meghatározott LDAP-ra exportálja az adatokat.

7.1.3 SF3 - Az azonosítással és hitelesítéssel kapcsolatos SFR-ek

FIA_ATD.1 meghatározza, hogy az Info&AA rendszer az egyedi felhasználókhoz tartozó alábbi biztonsági tulajdonságokat kezeli:

Biztonsági tulajdonság	leírás	Lehetséges értékek
szerepkör	a felhasználó által betölthető szerepkör	SSO, SO, PO, RO
jogosultság	a felhasználó által az adott szerepkörön belül meghatározott speciális jogosultság	SSO esetén: - , SO esetén: - PO esetén (pr_név) lista, ahol a pr_név által meghatározott profilra jogosult a szabály-szerkesztésre RO esetén: (pr_név, jog) párok listája, ahol a pr_név a profilt, a hozzátartozó jog pedig az adott profilon belül kiadható (I,R,H,A) kéréseket határozza meg

FIA_UID.1 azt várja el, hogy egy felhasználó sikeres azonosítása előtt kizárólag az alábbiakat tehesse csak meg:

- saját tanúsítvány kiválasztása az MS tanúsítványtárából
- a hitelesítés során aláírandó adat megtekintése
- a login-ba való visszalépés

FIA_UAU.1 azt várja el, hogy egy felhasználó sikeres hitelesítése előtt kizárólag az alábbiakat tehesse csak még meg (az azonosításon kívül):

- a megnézhető, automatikusan előállított üzenet aláírása a kiválasztott tanúsítványhoz tartozó magánkulccsal („sign” gomb)

FIA_USB.1 azt várja el, hogy sikeres hitelesítés esetén kapcsolódjék össze az alkalmazás (ahova sikeresen belépett a hitelesítéssel) és a felhasználó biztonsági tulajdonságai (szerepkör és jogosultság)

A fent áttekintett, azonosításhoz és hitelesítéhez kapcsolódó SFR-eket az Info&AA az alábbi módon teljesíti:

FIA_UID.1 és FIA_UAU.1: Az Info&AA rendszer valamennyi, felhasználói hozzáférést biztosító alkalmazása (InfoAARA.exe, InfoAASetup.exe, InfoAAPolicyManager.exe) elindításkor egy login ablakot nyit meg. Ebben kizárólag az alábbiak tehetők meg:

- „...” gomb megnyomása: saját tanúsítvány kiválasztása
- „Show data” gomb megnyomása: aláírandó adat megtekintés
- „Cancel” gomb megnyomása: visszalépés a login-ból
- „sign” gomb megnyomása: aláírás

Bármilyen más funkció aktivizálására csak sikeres hitelesítés után kerülhet sor.

FIA_ATD.1: az InfoAASetup.exe által kezelhető konfigurációs fájlokon keresztül:

- az **InfoAA.sso** fájl (titkosítva) tartalmazza az SSO szerepkör betöltésére jogosult felhasználók tanúsítványát,
- az **InfoAA.so** fájl (titkosítva) tartalmazza az SO szerepkör betöltésére jogosult felhasználók tanúsítványát,
- az **InfoAA.ro** fájl (titkosítva) tartalmazza az RO szerepkör betöltésére jogosult felhasználók tanúsítványát, az ezek által szabályozható tanúsítvány profil azonosítókat, valamint az egyes tanúsítvány profilokon belül kiadható szolgálati kéréseket (Issue, Revoke, Hold, Activate)
- az **InfoAA.po** fájl (titkosítva) tartalmazza a PO szerepkör betöltésére jogosult felhasználók tanúsítványát, valamint az ezek által szabályozható tanúsítvány profil azonosítókat.

7.1.4 SF4 - A biztonsági naplózással kapcsolatos SFR-ek

FAU_GEN.1 azt várja el, hogy a minden SFR-re külön meghatározott esetekben készüljön napló bejegyzés.
FAU_GEN.2 azt várja el, hogy minden naplóesemény összekapcsolódjon az eseményt kiváltó felhasználó azonosítójával.

Az Info&AA rendszer szerver alkalmazása (InfoAA.exe) a napló eseményekről készült napló sorokat syslog szerverbe továbbítja. Az SFR-ekre külön meghatározott minden esetben készül napló bejegyzés.

Az Info&AA rendszer másik három alkalmazása (InfoAARA.exe, InfoAA Setup.exe, InfoAAPolicyManager.exe) saját napló file-okat hoz létre, amelyek szöveges állományok. Az SFR-ekre külön meghatározott minden esetben készül napló bejegyzés.
Minden nap új állomány keletkezik minden alkalmazás számára, ha valamilyen esemény történik. Esemény minden felhasználói be és kilépés is.

A fentiek alapján a syslog szerverre kerülő, illetve a 3 alkalmazás által külön generált napló állományok együttes vizsgálata (mely vizsgálatra az Info&AA rendszer hatókörén kívül kerül sor) elvileg alkalmas arra, hogy:

- minden naplóesemény összekapcsolható legyen az eseményt kiváltó felhasználó azonosítójával (FAU_GEN.2),
- minden elvárt esetben készül napló bejegyzés (FAU_GEN.1).

7.1.5 SF5 - A külső és belső adatátvitel védelmével kapcsolatos SFR-ek

FDP_ITT.1 és FPT_ITT.1 azt várja el, hogy a szolgáltatói kérések és válaszok módosítás ellen védve legyenek, a felhasználói adatok, illetve a kapcsolódó TSF adatok vonatkozásában.
Az Info&AA rendszerben az InfoAARA.exe-t működtető RO személyes aláíró magánkulcsával aláírja a szolgáltatói kéréseket, az InfoAA.exe pedig infrastruktúrális aláíró magánkulcsával aláírja az ezekre adott válaszokat.

FDP_ETC.2 az ACRL szabványos LDAP-ba publikálását várja el.
Az InfoAARA.exe a keletkező ACRL-eket szabványos módon publikálja a bekonfigurált LDAP-ba.

FPT_ITI.1 azt várja el, hogy a syslog szervernek küldött naplórekordok módosítás ellen védve legyenek (beleértve a kihagyást és beszúrást is).
Az Info&AA rendszerben a syslog szervernek küldött napló sorok digitálisan aláírt, sorszámozott, láncoltan egymásba fűzött sorok. A napló sorok felépítése (amely a syslog szabványos elemeket nem tartalmazza): <sn: XX> <hash: XX> message <sig: XX>, ahol:

- sn: az aktuális napló sor sorszáma (hexa kódolással)
- hash: az előző napló sor lenyomata (hexa kódolással)
- message: az aktuális napló bejegyzés szövege
- sig: az aktuális napló sor aláírása (hexa kódolással), amely tartalmazza az sn, hash és message elemeket.

Az aláírás véd az egyes bejegyzések módosítása ellen (pontosabban kimutathatóvá teszi a sértetlenség tényét vagy hiányát), a különböző sorok láncolt egymásba fűzése pedig véd a kihagyás és beszúrás ellen.

7.1.6 SF6 - Az attribútum tanúsítvány előállítással kapcsolatos SFR-ek

FDP_PKI.2 Attribútum tanúsítvány előállítás

Az Info&AA rendszer olyan attribútum tanúsítványokat állít elő, amelyek formátuma megfelel az ITU-T X.509-2000, RFC 3281 és RFC 4476 X.509 szabványok elvárásainak.

FMT_PKI.2 Attribútum tanúsítvány profil menedzsment

Az Info&AA rendszer attribútum tanúsítvány profilok kezelésére ad lehetőséget (Az InfoAASetup.exe két különböző SO számára lehetővé teszi ilyen profilok létrehozását, módosítását és törlését.)

Az attribútum tanúsítvány profilok meghatározzák az attribútum tanúsítványokban előforduló mezőkre és kiterjesztésekre (az Attribute Types kiterjesztések kivételével) elfogadható értékek összességét.

FMT_PKI.3 Attribútum kollekció menedzsment

Az Info&AA rendszer attribútum kollekciók kezelésére is lehetőséget biztosít. (Az InfoAAPolicyManagment.exe az errel feljogosított PO számára lehetővé teszi egy létező attribútum tanúsítvány profilhoz kapcsolódóan attribútum kollekciók létrehozását, módosítását és törlését.)

Egy attribútum kollekció az attribútum tanúsítványokban előforduló Attribute Types kiterjesztésekre vonatkozóan határozza meg az elfogadható értékek egy összességét. Minden kollekció egy adott tanúsítvány profilhoz tartozik, egy profilhoz több kollekció is megadható.

7.1.7 SF7 - Az attribútum tanúsítványok visszavonás kezelésével kapcsolatos SFR-ek

FDP_PKI.4 Attribútum tanúsítvány visszavonási lista előállítás

Az Info&AA rendszer által kibocsátott attribútum tanúsítvány visszavonási listák (ACRL) megfelelnek az X.509 szabványnak. Az ACRL-ekbe kerülő minden mezőt vagy kiterjesztést a Info&AA rendszer (InfoAA.exe) állít elő, az X.509 szabványnak megfelelően.

FMT_PKI.5 Attribútum tanúsítvány visszavonási lista profil menedzsment

Az Info&AA rendszer attribútum tanúsítvány visszavonási lista profilok kezelésére is lehetőséget ad. (Az InfoAASetup.exe két különböző SO számára lehetővé teszi ilyen profilok létrehozását, módosítását és törlését.)

7.2. Önvédelem a fizikai és logikai hamisítás ellen

Az Info&AA számos biztonsági mechanizmust valósít meg annak érdekében, hogy megvédje magát a fizikai és a logikai hamisítás ellen.

A fizikai és a logikai hamisítás elleni védelem összetevői az alábbiak:

- Code signing minden futtatható állományra
- minden konfigurációs állomány digitálisan aláírva kerül tárolásra, az alkalmazások pedig olvasáskor ellenőrzik az aláírt állományok sértetlenségét,
- a naplóbejegyzések digitális aláírása biztosítja a beszúrás és kitörlés elleni védelmet,

- az Info&AA rendszernek nincsenek külső, nem bizalmi munkakört betöltő felhasználói (az InfoAA szolgáltatásait igénylő külső felhasználók az RO-knak küldött kéréseken, vagy az InfoAA rendszer által feltöltött LDAP szerveren keresztül, tehát csak indirekt módon vehetik igénybe a rendszer szolgáltatásait).

7.3. Önvédelem a megkerülés ellen

Az Info&AA számos biztonsági mechanizmust valósít meg annak érdekében, hogy megvédje magát a megkerülés ellen.

A (biztonsági funkcionalitás) megkerülése elleni védelem összetevői az alábbiak:
- az Info&AA rendszer nem biztosít távoli elérést (valamennyi felhasználó közvetlenül kapcsolódik a rendszerhez, nincs tehát olyan távoli (pl. web-es) elérés, mely speciális támadási módszerekkel alkalmat adna a biztonsági funkcionalitás megkerülésére),
- az Info&AA rendszerben minden felhasználó számára kényszerpályás belépés (login) van (csak sikeres azonosítás és hitelesítés után nyílnak meg a funkcionalitások aktivizálását felkínáló menük),
- a beolvasott input adatok szintaktikai ellenőrzésre kerülnek (az esetleges túlcsordulásokból adódó jogosultságellenőrzés megkerülés kivédése érdekében).

7.4. SFR – SF megfeleltetés

A 7.1. táblázat megfelelteti a funkcionális biztonsági követelményeket (SFR) és az SFR csoportokat.

Az SFR jele	SF
FAU_GEN.1	4
FAU_GEN.2	4
FDP_ACC.1	2
FDP_ACF.1	2
FDP_ITT.1 FDP_IFC.1 FDP_IFF.1 FDP_ETC.2	5 2 2 5
FDP_PKI.2	6
FDP_PKI.4	7
FIA_ATD.1	3
FIA_UAU.1	3
FIA_UID.1	3
FIA_USB.1	3
FMT_MOF.1	1
FMT_PKI.2	6
FMT_PKI.3	6
FMT_PKI.5	7
FMT_MSA.1/ SO fiók	1
FMT_MSA.1/ RO fiók FMT_MSA.1/ PO fiók	1 1
FMT_MSA.3/ fiókok FMT_MSA.3/ LDAP	1 1
FMT_SMF.1	1
FMT_SMR.1	1
FPT_ITI.1	5
FPT_ITT.1	5

7.1. táblázat: A funkcionális biztonsági követelmények és az SFR csoportok (SF-ek) megfelelése

8. Rövidítések

AA	Attribute Authority (attribútum-szolgáltató)
AC	Attribute Certificate (attribútum tanúsítvány)
ACRL	Attribute Certification Revocation List (attribútum tanúsítvány visszavonási lista)
CC	Common Criteria (közös szempontrendszer)
CRL	Certification Revocation List (tanúsítvány visszavonási lista)
EAL	Evaluation Assurance Level (értékelési garanciaszint)
MIBÉTS	Magyar Informatika Biztonsági Értékelési és Tanúsítási Séma
SA	Security Auditor (rendszervizsgáló)
SSO	System Security Officer (rendszer biztonsági tisztviselő)
SO	Security Officer (biztonsági tisztviselő)
ST	Security Target (biztonsági előirányzat)
RO	Registration Officer (regisztrációs tisztviselő)
PC	Public Key Certificate (nyilvános kulcsú tanúsítvány)
PO	Policy Officer (attribútum-szabályzó tisztviselő)
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