mySigno PDA és Szerver aláírás létrehozó és aláírás ellenőrző rendszer v1.0

Biztonsági előirányzat

Verzió:	1.0
Dátum:	2006. április 30.
Megrendelő:	Argeon Üzleti Szolgáltató Kft.
Fájl:	mySigno_ST_ v10_final.pdf
Minősítés:	Nyilvános
Oldalak:	78

Változás kezelés

Verzió	Dátum	Leírás	Készítette
0.4	2006.01.10.	A 2., 3., 4. és 6. fejez tervezet elkészítése a mySigno for PDA dokumentum alapján	Juhász Judit
0.7	2006.02.19.	Az ST további részeinek elkészítése	Juhász Judit
0.9	2006.04.25.	Az ST pontosítása a fejlesztői bizonyítékok alapján	Juhász Judit
0.98	2006.04.28.	Az ST pontosítása és kiegészítése az értékelés megállapításai és kérdései alapján	Juhász Judit
1.0	2006.04.30.	Az ST véglegesítése a fejlesztők észrevételei alapján	Juhász Judit

Tartalomjegyzék

1 Bevezetés

Ez a fejezet dokumentum-kezelő és áttekintő információkat tartalmaz.
Az "Azonosítás" alfejezet a biztonsági előirányzatok azonosításhoz, katalogizálásához, regisztrációba vételéhez, illetve hivatkozásokhoz szükséges azonosító és leíró információkat tartalmazza.
Az "Áttekintés" alfejezet egy potenciális felhasználó számára ad olyan részletességű áttekintést, melynek alapján eldöntheti a témában való érdekeltségét.
A „Kapcsolódó dokumentumok” alfejezet felsorolja jelen biztonsági előirányzat elkészítéséhez felhasznált szakirodalmat.
„A biztonsági előirányzat szerkezete” alfejezet a 2-9. fejezetek rövid leírását tartalmazza.
A „Common Criteria (Közös szempontok) megfelelőség” alfejezet pedig a CC jelen értékelésnél irányadó verzióját határozza meg.

1.1 Azonosítás

Cím:	mySigno PDA és Szerver - Biztonsági előirányzat
Az értékelés tárgya:	mySigno PDA és Szerver aláírás létrehozó és ellenőrző rendszer
Az értékelés tárgya rövid neve:	mySigno v1.0
Értékelési garancia szint:	MIBÉTS fokozott (CC EAL3+)
A biztonsági funkcióerősség:	SOF-közepes
Verzió szám:	1.0
Dátum:	2006. április 30.
Szerző:	Juhász Judit
Szponzor szervezet:	Argeon Kft.
Felhasznált védelmi profilok:	Profil de protection: Application de création de signature: Elektronikus aláírás létrehozó alkalmazás Védelmi Profil (Trusted Logic for the account of the DCSSI) - Értékelés alatti verzió Profil de protection: Module vérification de signature: Elektronikus aláírás ellenőrzés Védelmi Profil (Trusted Logic for the account of the DCSSI) - Értékelés alatti verzió

1.2 Áttekintés

A **mySigno PDA és Szerver v1.0** (röviden mySigno v1.0 vagy mySigno) zárt rendszerben működő aláírás létrehozó és ellenőrző rendszer fokozott biztonságú elektronikus aláírások létrehozására és ellenőrzésére alkalmas függvénykönyvtár. Kliens és szerver oldali összetevőkkel rendelkezik. A függvénykönyvtár C++ nyelven készült, az aláírás létrehozására és ellenőrzésére tartalmaz függvényhívásokat, és rendelkezik felhasználó (aláíró) által látható képernyőkezelő függvényekkel.

Jelen biztonsági előirányzat tartalmazza mind az elektronikus aláírás létrehozására, mind pedig az elektronikus aláírás ellenőrzésére vonatkozó, továbbá a mySigno v1.0 *rendszer* jellegéből adódó, kommunikációs funkciókra vonatkozó követelményeket.

A mySigno elektronikus aláírás létrehozása olyan egyéb funkcionalitással rendelkező rendszerbe épül, amely kézi aláírások létrehozását és feldolgozását teszi lehetővé a felhasználók számára.

A kézi aláírások létrehozása, azok megbízhatósága kívül esik a mySigno értékelés hatókörén, az értékelés a fokozott biztonságú elektronikus aláírás létrehozására és ellenőrzésére szorítkozik.

1.3 Kapcsolódó dokumentumok

- Profil de protection: Application de création de signature (Trusted Logic for the account of the DCSSI)
- Profil de protection: Module vérification de signature (Trusted Logic for the account of the DCSSI)
- RFC 3161 X.509 Internet Public Key Infrastructure - Time-Stamp Protocol, August 2001
- RFC 3280: X.509 Internet Public Key Infrastructure - Certificate and CRL Profile, April 2002
- International Standard ISO/IEC 15408 Information technology — Security techniques — Evaluation criteria for IT security
- Common Methodology for Information Security Evaluation (CEM) Version 1.0, August 1999

1.4 A biztonsági előirányzat szerkezete

A 2., 3., és 4. fejezetek a mySigno leírását, a biztonsági környezetet (feltételezéseket, fenyegetéseket és szervezeti biztonsági szabályzatokat), illetve a biztonsági célokat adják meg. Az 5.1 alfejezet a funkcionális biztonsági követelményeket tartalmazza.
Az 5.2 alfejezet az emelt szintű EAL 3 (MIBÉTS fokozott garanciaszint) követelményeit írja le.
A 6. fejezet tartalmazza az értékelés tárgya által megvalósítandó/megvalósított biztonsági funkciókat.
A 7. fejezet a PP megfelelőségi nyilatkozatot, a 8. fejezet az indoklásokat, a 9. pedig egy terminológiai áttekintést és a használt rövidítések listáját tartalmazza.

1.5 Common Criteria (Közös szempontok) megfelelőség

Ez a biztonsági előirányzat a CC 2.2 verzióján alapul (ISO/IEC 15408 IT biztonság értékelési követelményei, 1. rész: Bevezetés és általános modell, 2. rész: Funkcionális biztonsági követelmények, 3. rész: Garanciális biztonsági követelmények.), megfelel a kiterjesztett 2. résznek, valamint megfelel a 3-résznek, emelt szintű EAL3-as értékelési garanciaszinten.
/A kiterjesztett 2. rész definíciója a CC 3.rész 5.4 pontja szerint: „Egy PP vagy TOE kiterjesztett, ha a funkcionális követelmények a 2. részben nem szereplő funkcionális összetevőket is tartalmaznak.”/

2 Az értékelés tárgyának (TOE, mySigno) leírása

2.1 Áttekintés

A TOE típusa

Jelen biztonsági előirányzat egy összetett rendszerbe illeszkedő alkalmazás-fejlesztői könyvtár értékeléséhez határozza meg a használati környezetet, a funkcionális és garanciális biztonsági követelményeket és az azokat megvalósító biztonsági funkciókat.

A mySigno v1.0 fokozott biztonságú elektronikus aláírások létrehozására és ellenőrzésére alkalmas függvénykönyvtár és alkalmazás. Kliens és szerver oldali összetevőkkel rendelkezik, a kliens oldal komponens függvénykönyvtár, a szerver oldali pedig egyéb, a TOE hatáskörén kívül eső elemeket is tartalmazó alkalmazás.

Jelen biztonsági előirányzat tartalmazza mind az elektronikus aláírás létrehozására, mind pedig az elektronikus aláírás ellenőrzésére vonatkozó, továbbá a mySigno v1.0 *rendszer* jellegéből adódó kommunikációs funkciókra vonatkozó követelményeket.

A mySigno v1.0 elektronikus aláírás létrehozása olyan egyéb funkcionalitással rendelkező rendszerbe épül, amely kézi aláírások létrehozását és feldolgozását teszi lehetővé a felhasználók számára.

> Megjegyzés: Jelen dokumentumban és az értékelésre átadandó minden dokumentumban a TOE hatáskörbe eső *aláírás* alatt elektronikus aláírás értendő, a kézi aláírás nem tartozik a TOE hatáskörébe.

A mySigno v1.0 mint rendszer által kezelt szerepkörök:

- **Ügynök** Az a szereplő, aki a csomagot a saját elektronikus aláírásával ellátja, biztosítva ezzel a csomag integritását és hitelességét.
- **Ellenőrző fél: E**zt a szerepkört a szerver oldali automatikus ellenőrző folyamat tölti be.

A mySigno v1.0 hatáskörén belül nem kezel adminisztrátor szerepkört.

A mySigno v1.0 hatáskörön kívüli, de a TOE biztonságos működésével összefüggésben lévő szerepkörök:

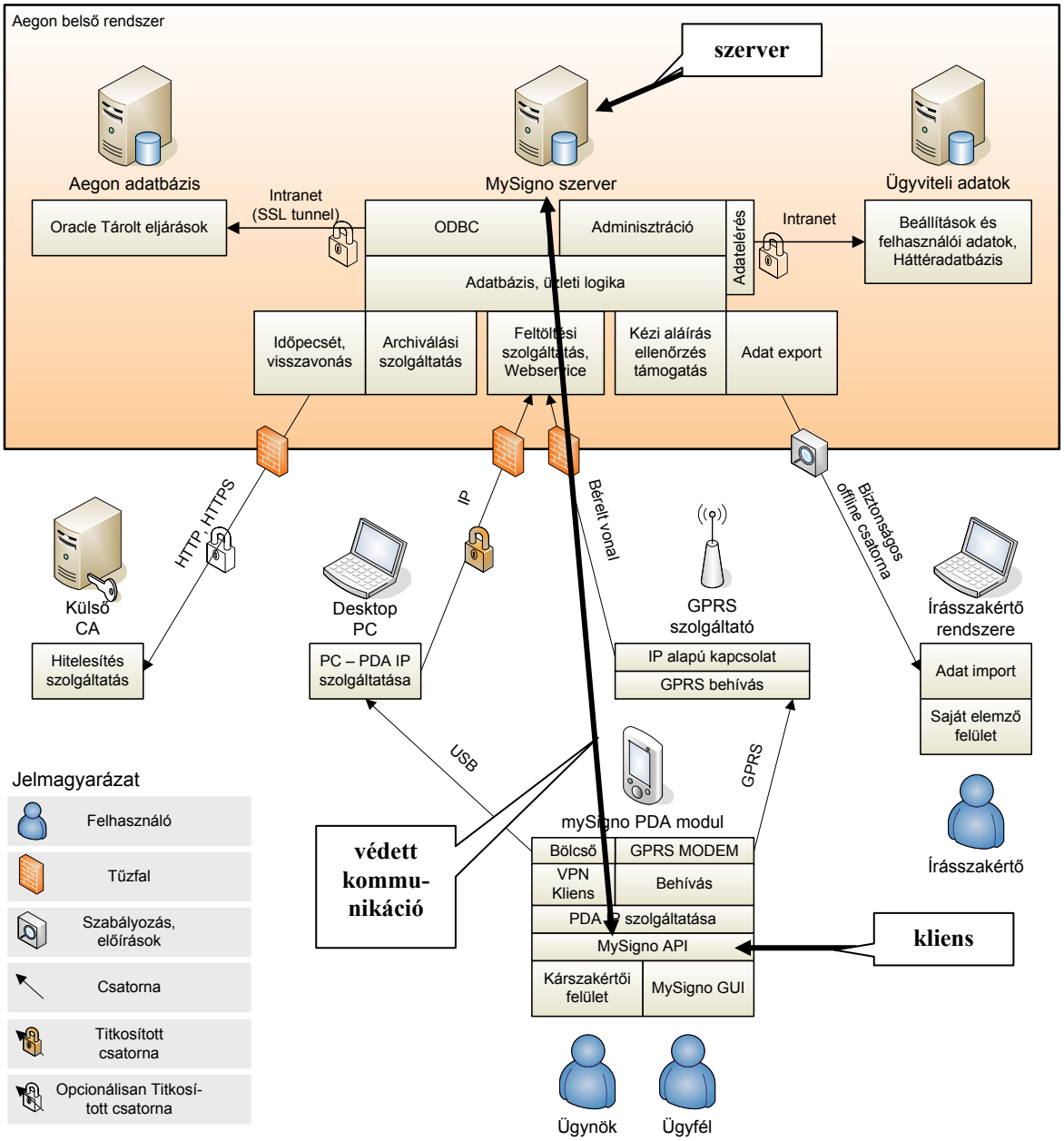
- **Szerver adminisztrátor:** Aki a mySigno szerver karbantartását és beállításait jogosult végezni.
- **PDA adminisztrátor:** Aki a mySigno PDA modul telepítésével, a paraméter fájlok, kulcsok biztonságos PDA-ra juttatásával kapcsolatos feladatokat végzi. Lehetővé teszi az ügynök számára a PIN kód cserét.

A TOE biztonsági funkciói programozói API-n keresztül elérhető DLL-ben megvalósított alkalmazás komponensben kerülnek megvalósításra, kliens oldali fokozott biztonságú aláíró, és ennek szerver oldali ellenőrzését lehetővé tevő funkcionalitással.
A fokozott biztonságú elektronikus aláírás az SHA-1 lenyomatoló és az RSA digitális aláíró algoritmust használja, 1024 bites kulcshosszal. Az aláírás létrehozó környezetben a magánkulcs tárolása PKCS#12 tanúsítványban történik.

A mySigno interfészt biztosít felhasználója, azaz az elektronikus-aláíró által használt hívó alkalmazás számára, aki egy ún. **csomagot** (egy vagy több adat, dokumentum, melyek elektronikus aláírással nem, de kézi aláírással rendelkezhetnek) kíván aláírni.

A mySigno interfészt biztosít az automatikus ellenőrző folyamatok elvégzésére, a hitelesítő adatok begyűjtésére, a hitelesítő adatokkal ellátott aláírt csomagok ellenőrzésére.

Az alábbi ábra a mySigno v1.0 átfogó rendszerbe illeszkedését mutatja.



1. ábra A TOE (mySigno) és környezete

A TOE informatikai környezetének elemei:

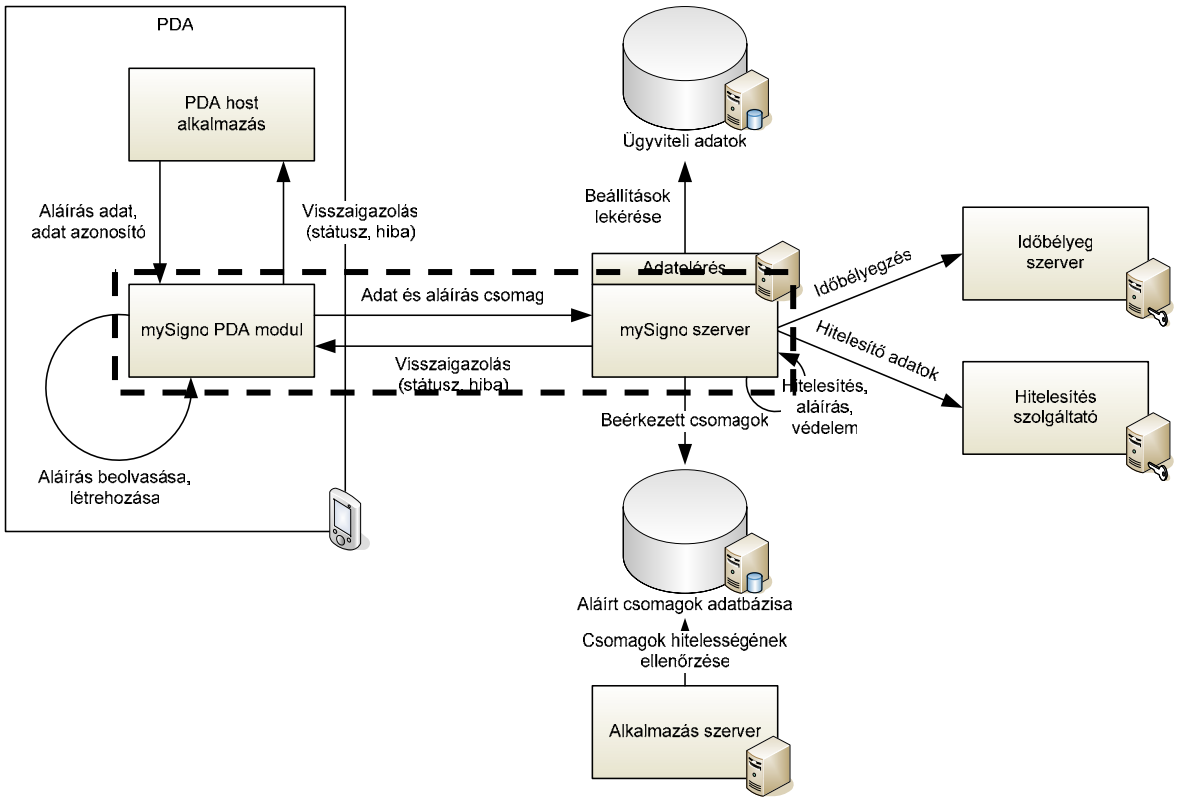
- Gazdagép operációs rendszere:
  - Kliens:
    Operációs rendszer:
    Pocket PC 2003 SE
    Kliens fejlesztőeszközök, telepítéséhez szükséges eszközök:
    Pocket PC 2003 SDK
    Embedded Visual Tools
    ActiveSync (Csak kliens telepítés esetén szükséges a telepítéshez használt számítógépre, üzemeltetéshez csak a nem GPRS alapú IP kapcsolat esetén szükséges a fogadó gépen).

  - Szerver
    Operációs rendszer:
    Windows 2003 Server
    Kommunikáció:
    IP alapú kapcsolatok fogadás az ügynökök PDA-ja felől,
    Szerver oldali kapcsolódás a belső ORACLE adatbázis szerver felé.

- A PKCS#12-ben tárolt adatokhoz való hozzáférést támogató összetevők (kriptográfiai szolgáltatások), melyek kriptográfiai interfészt adnak, amit az aláíró alkalmazás meghív az aláírás létrehozása érdekében.
- Az ügynök számára a dokumentum megjelenítését lehetővé tevő szoftver, illetve jelzés, ha ennek a jellemzői nem teljesen felelnek meg a dokumentum által megkövetelt tulajdonságoknak (színhasználat, a szükséges szabályzatok megléte, …)
- A magánkulcs tárolására szolgáló összetevő:
  - Kliens: PKCS#12 formátumú fájl.
  - Szerver: PKCS#12 formátumú fájl.

2.2 A TOE használata és biztonsági környezete, határai

A 2. ábrán az aláírás létrehozó és ellenőrző környezet látható a TOE interfészekkel.



2. ábra A TOE (mySigno) határai

Az ábrán szaggatott vonallal jelzett elemek képezik a mySigno v1.0 határait.
Azaz a mySigno határain belülre eső funkciók:

- kliens oldali fokozott biztonságú aláírás ügynök által;
- kliens oldali szinkronizálás: az ügynök által elektronikusan aláírt csomag automatikus (eszköz általi) aláírása és titkosítása a kommunikáció sértetlenségének, illetve bizalmasságának biztosítása érdekében;
- szerver oldali üzenet-megoldás, az eszköz általi aláírás ellenőrzése az eredet hitelesség megállapításához;
- fokozott biztonságú ügynök általi aláírás első kezdeti ellenőrzése;
- szerver oldali csomag fogadás után időbélyeg kérés a kapott fokozott biztonságú ügynök aláírásra;
- türelmi idő letelte után az aláírás második kezdeti ellenőrzése;
- szerver oldali aláírás a kapott csomagok archiválása előtt a sértetlenség biztosítása érdekében;
- szerver oldali csomag exportálás kezdeményezés az aláírás adatbázis felé;
- az aláírás utólagos ellenőrzése;
- kliens oldali visszaigazolás fogadás;
- kliens oldali szoftverfrissítés letöltés kezdeményezés;
- szerver oldali szoftverfrissítés letöltés;
- szerver oldali szoftverfrissítés sértetlenségének biztosítása aláírással és bizalmasság védelem titkosítással.

2.3 A TOE kliens oldali funkcionális elemei

1. Az aláírás létrehozásának előkészítése

a) Egy csomag kiválasztása aláírásra vagy a kiválasztás visszavonása

- Jelen TOE terminológiában "aláírandó dokumentum" alatt egy **csomagot** értünk. Az aláírásra való kiválasztás a csomag lezárása funkcióhoz kapcsolódik, amikor kézi és elektronikus aláírás kerül a csomagra.
- Az ügynök már aláírásra kiválasztott csomag esetén dönthet úgy, hogy mégsem kívánja azt aláírni.

b) Az aláírandó csomag tartalmának megjelenítése

Az ügynök számára biztosítani kell azt, hogy közvetlenül az elektronikus aláírás létrehozásának pillanata előtt meg tudja nézni az aláírandó csomag tartalmát.

c) Alkalmazandó aláírási szabályzat

Az aláírási szabályzat azon szabályok összessége, melyek a TOE által létrehozott fokozott biztonságú elektronikus aláírás létrehozására és ellenőrzésére vonatkoznak, és amelyek értelmében egy aláírás érvényesnek tekinthető.

A TOE rögzített szabályok alapján dolgozik.

d) Az aláírási tulajdonságok kiválasztása/megjelenítése.

A TOE eszközt biztosít arra, hogy az aláíró aláírási tulajdonságokat is aláírjon a dokumentummal együtt. A kötelező aláírási tulajdonságokat a csomag aláírása előtt meg kell tudni jeleníteni az ügynök számára.

A kötelezően aláírandó tulajdonságok az alábbiak:

- aláírási szabályzat azonosítója,
- az aláírás feltételezett időpontja,
- aláíró tanúsítványa.

e) Az aláíráshoz használt tanúsítvány (és ezáltal a magánkulcs) kiválasztása

A mySigno lehetőséget biztosít arra, hogy az aláíró megtekintse, mely tanúsítványt (és ezáltal melyik magánkulcsát) használja az aláírás létrehozásához.

f) Az aláírás egyértelmű szándékának kifejezése és az ügynök hitelesítése

Ez biztosítja az ügynök számára, hogy kifejezze egyértelmű aláírási szándékát minden egyes aláírni kívánt csomagra.

Egy csomagra vonatkozó aláírási folyamat elindítása előtt a TOE megállapítja, hogy az ügynök ténylegesen alá akarja-e írni a dokumentumot, hogy az aláírás ne valamilyen véletlen, nem szándékos esemény következménye legyen. Ezért a TOE olyan mechanizmust valósít meg, amellyel az aláírót nem triviális művelet végrehajtására kötelezi az aláírási folyamat folytatásához.

Ebben a fázisban történik meg az ügynök magánkulcsának aktivizálásához szükséges hitelesítő adatnak (PIN kódnak) a bekérése és TOE általi ellenőrzése.

2. Az aláírandó csomagok formázását/lenyomatolását végző összetevő

Ez az összetevő formázza meg az aláírandó dokumentumot és aláírási tulajdonságokat, majd hozza létre az aláírandó formattált tömörített adatlenyomatot, amit ***A fokozott biztonságú elektronikus aláírás létrehozását végző összetevő*** kap meg az aláírás végrehajtásához.

3. A fokozott biztonságú elektronikus aláírás létrehozását végző összetevő

a) Az aláírói magánkulcs aktivizálása.

A magánkulcs aktivizálását lehetővé tevő aláírói hitelesítő adat bekérése és ellenőrzése a modul feladatai közé tartozik. A magánkulcs PKCS#12-es tanúsítványba foglalt. Biztonságos telepítéséről az A.Init_PDA feltételezésnél (lásd 3.2.1 pontot) írtak szerint kell gondoskodni.

A hitelesítő adat paraméterei:

6 hosszúságú betű/szám kombináció

b) Fokozott biztonságú elektronikus aláírás létrehozása

Ez a funkció a bemenetként kapott lenyomat kódolását végzi el.

c) Az elektronikus aláírás visszaadása

Ez a funkció csatolja a csomaghoz az elektronikus aláírást.

4. Csomag szinkronizálás kezdeményezés szerver felé biztonságos csatornán (elektronikus aláírással ellátott csomag importálása)

a) a szerverhez továbbított csomag hitelesítése kliens eszköz aláírással

b) a szerverhez továbbított csomag rejtjelezése

c) a szervertől érkezett szoftverfrissítések fogadása (szerver aláírás ellenőrzése, rejtjelezés megoldása)

A mySigno v1.0 hatáskörön kívüli elemek

A mySigno v1.0 IT környezetéhez tartozó hívó alkalmazás / operációs rendszer kezeli az elfogadott dokumentum formátumok és a megjelenítő alkalmazások közötti kapcsolatot.
Nem tartoznak továbbá a TOE hatáskörébe:

- az ügynök és PDA eszköz elektronikus aláírásának létrehozásához használt magánkulcsok és tanúsítványok telepítése;
- a tanúsítványok PDA eszközön való tárolás közbeni sértetlenség védelme;
- a PDA eszköz és a szerver közötti kommunikáció titkosságát biztosító rejtjelezéshez használt tanúsítványok és kulcsok telepítése.

2.4 A TOE szerver oldali funkcionális elemei

Az ügynöktől, azaz a klienstől beérkezett aláírt adatokat a szerver (**mySigno szerver**) dolgozza fel automatikusan. Így az aláírás ellenőrző fél gépi folyamat, amely:

- fogadja és szintaktikusan ellenőrzi a beérkező csomagokat;
- automatikus szoftver frissítést szolgáltat; és
- felelős az elektronikus aláírások ellenőrzéséért, a hitelesítő adatok összegyűjtéséért.

Az elektronikus aláírások ellenőrzésénél:

- időbélyeget kér a rögzített aláírási szabályzatban meghatározott forrásból az ügynök aláírására;
- ellenőrzi és hitelesíti (azaz ellátja hitelesítő információkkal) a csomagon lévő elektronikus aláírásokat (az ügynök elektronikus aláírását);
- a kliens felé visszaigazolást küld a csomag elfogadásáról.

A mySigno szerver és IT környezete kétféle ellenőrzés megvalósítására ad lehetőséget: kezdeti ellenőrzésre és utólagos ellenőrzésre.

Kezdeti ellenőrzés

A kezdeti ellenőrzés a fogadott csomagban szereplő ügynök aláírás első kezdeti ellenőrzése, melyben megtörténik az ügynök aláírásának ellenőrzése. A nem megfelelt csomagokat a rendszer visszautasítja, a megfelelt csomagokra időbélyeget kér és érkeztető aláírással látja el. A második lépésben (a türelmi idő letelte után) az érvényesítő adatok összegyűjtése történik.

Utólagos ellenőrzés

A mySigno a kezdeti ellenőrzés során összegyűjtött adatok alapján ellenőrzi az elektronikus aláírás érvényességét, egy tetszőleges későbbi időpontban.

Fentiek alapján a mySigno aláírás ellenőrzési összetevői:

1. Az ellenőrzés előkészítését végző összetevő

a) A beérkezett csomag szintaktikai ellenőrzése

b) Aláírási szabályzat alkalmazása

A mySigno rögzített aláírási szabályokkal dolgozik.

2. Az érvényesítő adatok összegyűjtését és kezelését végző összetevő

Az alkalmazott aláírási szabályzattal összhangban ez a komponens az alábbi funkciókat biztosítja:

- az aláírt tulajdonságok megfelelőségének ellenőrzése,
- az aláírás idejének meghatározása,
- érvényes tanúsítvány útvonal felépítése,
- a tanúsítvány útvonal érvényességének ellenőrzése.

Ezek a funkciók ismétlődhetnek, amíg fel nem építhető egy érvényes tanúsítvány útvonal.

Az aláírt tulajdonságok megfelelőségének ellenőrzése

A mySigno az aláírási szabályzat által megkövetelt minden aláírt tulajdonság meglétét és megfelelőségét ellenőrzi. Három ilyen aláírt tulajdonság van: aláírás feltételezett ideje, aláíró tanúsítvány, aláírási szabályzat azonosító.

Az aláírás idejének meghatározása

Az aláíró tanúsítványának érvényességének ellenőrzése és egyéb érvényesítési adatok, következésképp az elektronikus aláírás ellenőrzése érdekében a mySigno-nak meg kell határoznia a beérkezett és tárolásra váró csomag aláírásának időpontját. Az aláírás időbeli meghatározásával kapcsolatos szabályokat az aláírási szabályzat tartalmazza (megbízható időbélyeg szolgáltató, hitelesítési útvonal hossz korlátozásai).

A mySigno működése a használati módok szerint alakul:

- A kezdeti ellenőrzés első indításakor még nem áll rendelkezésre időreferencia, a mySigno az aláírási szabályzatnak megfelelően kér egyet.
- A kezdeti ellenőrzés későbbi indításakor a mySigno az első kezdeti ellenőrzés során csatolt időbélyeget használja, ha talál ilyet. Ellenőrzi, hogy ez megfelel-e az aláírási szabályzatnak. Ha az időbélyeg nem felel meg vagy hiányzik, akkor az aláírást érvénytelennek tekinti. Ha az időbélyeg megfelel, és az aláírási szabályzatban meghatározott türelmi idő letelt az időbélyegben szereplő időponthoz képest, akkor a kezdeti ellenőrzés második lépésre, azaz az érvényesítő adatok összegyűjtésére kerül sor (tanúsítvány útvonal tanúsítványai és visszavonási információk).
- Utólagos ellenőrzés során a kezdeti ellenőrzés során összegyűjtött érvényesítő adatok alapján kerül sor az aláírás (ismételt) ellenőrzésére.

A tanúsítvány megfelelőségének ellenőrzése
Az aláírt tulajdonságokban lévő aláíró tanúsítvány hivatkozásból a mySigno megállapítja, hogy valóban a tanúsítvány útvonal végtanúsítványra mutat-e a hivatkozás.
A tanúsítvány jellemzőinek meg kell felelniük az aláírási szabályzat követelményeinek.

Érvényes tanúsítvány útvonal felépítése
Az aláíró tanúsítványának az aláírás létrehozás pillanatában való érvényességének és hitelességének bizonyításához a mySigno érvényes tanúsítvány útvonalat épít fel az aláíró tanúsítványa és az aláírási szabályzatban rögzített megbízható pont között.

- Kezdeti ellenőrzés esetén
  Ekkor a mySigno az aláírási szabályzatban szereplő szabályok (azonosított megbízható pontok, a visszavonási információk és a CA tanúsítvány ellenőrzésére vonatkozó szabályok) alapján megkövetelt funkciókat valósítja meg az érvényes tanúsítvány útvonal kialakításához. Az útvonal felépítése során a TOE érvényesítési adatokat importál (például hálózatról vagy helyileg), és ellenőrzi, hogy azok megfelelnek-e az alkalmazandó aláírási szabályzatnak.
  Amennyiben nem építhető fel az útvonal vagy a kiépített útvonalak érvénytelenek, akkor a mySigno az elektronikus aláírást érvénytelennek tekinti. Amennyiben az derül ki, hogy az adatok nem hozzáférhetők az útvonal valamely eleme érvényességének (nem visszavont állapotának) bizonyításához, akkor az ellenőrzés befejezetlennek tekintendő és a csomagot visszautasítja a rendszer.

- Utólagos ellenőrzés esetén
  Ekkor a mySigno felépíti az útvonalat és kizárólag a kezdeti ellenőrzés során összegyűjtött adatok alapján ellenőrzi annak érvényességét.
  Amennyiben nem építhető fel az útvonal a rendelkezésre álló adatokból, vagy van érvénytelen elem az útvonalban ezen adatok alapján, akkor az elektronikus aláírás érvénytelennek tekintendő.
  Amennyiben nincs elegendő adat a tanúsítvány útvonal valamely eleme érvényességének (nem visszavont állapotának) a bizonyításához, akkor az elektronikus aláírás érvénytelennek tekintendő.

Az érvényesítési adatok összegyűjtése történhet hálózati protokollon keresztül, vagy egyszerű helyi hozzáféréssel. Az adatok begyűjtéséhez használt eszköz, módszer (hálózati kliensek, merevlemez,…) kívül esik az értékelés tárgya hatáskörén.

A tanúsítványláncban valamely elem érvényességének ellenőrzése az alábbiak ellenőrzéséből áll:
- adott elem sértetlenségének és hitelességének ellenőrzése a kapcsolódó aláírás alapján;
- a csatolt időbélyeg beleesik-e az elem érvényességi idejébe;
- a csatolt időbélyegben szereplő időpontban az elem nem volt-e visszavont státuszú.

A tanúsítványok érvényességének ellenőrzése
A mySigno ellenőrzi, hogy a tanúsítvány érvényes volt-e az aláíráshoz tartozó időbélyeg időpontjában és a tanúsítványban definiált érvényességi ideje nem járt-e le.

3. Aláírásokat ellenőrző összetevő
Ez a kriptográfiai komponens az aláírás ellenőrzési folyamatban az aláírás ellenőrzéséhez alkalmazott algoritmusokat (lenyomatoló és aláírás ellenőrző algoritmusokat) foglalja magába.
Az aláírások ellenőrzéséhez többek között szükség van az alábbiakra:

- a csomagra számolt ügynök elektronikus aláírása;
- az ügynök tanúsítványokhoz tartozó útvonalat alkotó tanúsítványok elektronikus aláírásai;
- az önaláírt gyökér tanúsítvány aláírása (megbízható pont);
- az összegyűjtött érvényesítési adatokon szereplő aláírások (CRL-eken szereplő aláírások).

4. Az ellenőrzés eredményének továbbítása az ellenőrzési folyamat végén
A mySigno felületet biztosít arra, hogy az aláírás ellenőrzésének sikerességét vagy sikertelenségét az IT környezethez tartozó aláírás adatbázis felé továbbítsa, ezáltal lehetővé téve a rendszer többi összetevője számára az ellenőrzés eredményének lekérdezését.
A mySigno v1.0 egyéb funkciói:

- ügynök aláírás ellenőrzés eredmény státusz visszaadása biztonságos kommunikációval a kliens felé;
- ezen adatok (TOE-n kívüli) védett eltárolási lehetőségének a biztosítása a későbbi használathoz. A tárolást az aláírás adatbázis végzi.

A mySigno v1.0 környezet elemei

Kliens oldal:

1. a PDA hosztalkalmazás
2. InfoSigno modul a PKCS#12 tanúsítványban tárolt adatokhoz való hozzáférés biztosításához
3. az ügynök tanúsítványát és magánkulcsát tároló fájlok

Szerver oldal:

1. hitelesítés szolgáltatóval való kommunikáció
2. időbélyeg szolgáltatóval való kapcsolat
3. aláírás adatbázis (aláírt csomagok adatbázisát kezelő adatbázis kezelő rendszer)
4. Oracle adabázis (A mySigno szerver beállításait tartalmazza.)

3 A TOE biztonsági környezete

Az alábbi feltételezések és szervezeti biztonsági szabályok egy része mind a kliens, mind a szerver oldalra vonatkozik. Más szabályok (ezt külön jelezzük) csak a kliens vagy csak a szerver oldalra érvényesek.
Jelen biztonsági előirányzat kizárólag feltételezésekből és szervezeti biztonsági szabályokból jut el a biztonsági célokhoz, így ez a fejezet fenyegetéseket nem tartalmaz. Ennek az az oka, hogy jelen biztonsági előirányzat (az alapjául szolgáló védelmi profiloknak megfelelően) nem egy kockázatelemzésből, hanem két mértékadó követelmény-rendszerből vezeti le biztonsági funkcionális követelményeit (CEN CWA 14170 és CEN CWA 14171).

3.1 Védendő értékek

- **Aláírandó csomag:** egy vagy több adatból álló, kézi aláírást tartalmazó vagy nem tartalmazó adategyüttes, melynek sértetlensége és hitelessége egységesen kezelt az ügynök fokozott biztonságú elektronikus aláírása által.
- **Aláírandó/aláírt adat:** az az információ, melyre az aláírás létrejön, illetve aminek aláírást ellenőrizni kell.
  Ide tartozik:
  - aláírni kívánt csomag **lenyomata**
  - **aláírási tulajdonságok**
    - az aláíró tanúsítványa,
    - az aláírási szabályzat azonosító,
    - az aláírás dátuma és időpontja,
- **elektronikus aláírás:**
    - az aláírandó adat lenyomata,
    - a numerikus aláírás (a digitális aláírás értéke),
- **beérkezett ellenőrizendő csomag**
- **az ellenőrzéshez szükséges érvényesítő adatok:**
    - aláíró tanúsítványa
    - tanúsítvány információk
    - visszavonási információk
    - időbélyeg válasz
- **TOE biztonsági funkciói (a kódolt aláírási szabályzattal)**

3.2 Feltételezések

3.2.1 Közös feltételezések

Az alábbi feltételezések az elektronikus aláírások létrehozására és ellenőrzésére egyaránt vonatkoznak.

A.Init_PDA
Feltételezzük, hogy a mySigno biztonságos működéséhez szükséges infrastrukturális és alapfunkcióhoz tartozó kulcsokat, valamint a mySigno biztonsági funkcióit biztonságos módon telepítették az eszközre.

A.PDA_Physical_Security
A PDA eszközt elektronikus aláírás létrehozására csak feltöltött akkumulátorral lehet használni az adatvesztés elkerülése érdekében.

A.Signer_Only
Feltételezzük, hogy a PDA kliens kizárólag a regisztrált ügynök felügyelete alatt marad. Az eszközt az ügynök felügyelete nélkül más személynek átadni tilos.

A.Host_PDA_Machine
Feltételezzük, hogy az a gazdaszámítógép, melyen a mySigno fut, közvetlenül az aláíró befolyása és a rendszert működtető szervezet felügyelete alatt áll.
A gazdaszámítógép operációs rendszere az általa futtatott alkalmazások számára elkülönített futási környezetet biztosít.
Feltételezzük, hogy az alábbi intézkedések teljesülnek:

- a gazdaszámítógép vírusvédelemmel ellátott;
- a gazdagép adminisztrátori funkcióihoz való hozzáférés kizárólagosan az erre a funkcióhoz hozzárendelt adminisztrátorokra korlátozott (felhasználó és adminisztrátor megkülönböztetése);
- a gazdagép operációs rendszere elutasítja a nem megbízható forrásból letöltött alkalmazások futtatását.

A.Separation_and_Exclusion
Feltételezés, hogy az aláírás létrehozását és ellenőrzését végző IT környezetben a mySigno folyamatok védettek más folyamatok káros beavatkozásai ellen. A mySigno modult csak egy hívó alkalmazás töltheti be egy időben.

A.AccessControl
Feltételezzük, hogy a PDA modul tárolására szolgáló könyvtár tartalmát a kliens eszköz felhasználója nem módosítja.

A.Trusted_Security_Administrator
A mySigno biztonsági adminisztrátoráról felételezzük, hogy megbízható, kiképezték a mySigno használatára és rendelkezik a feladatai ellátáshoz szükséges hozzáférésekkel/jogosultságokkal.

A.Services_Integrity
A mySigno környezetről feltételezzük, hogy a biztonsági adminisztrátor vagy a hívó alkalmazás számára eszközt biztosít, amellyel az ellenőrizheti a mySigno szolgáltatások és paraméterek sértetlenségét.

3.2.2 Az aláírás létrehozásával kapcsolatos feltételezések

A.Signatory_Presence
Az aláírásra kiválasztott egy darab csomag jogosulatlan módosításának elkerülése érdekében feltételezzük, hogy az ügynök végig jelen van attól kezdődően, hogy kifejezte aláírási szándékát, mindaddig, amíg megadja a magánkulcs aktiválásához szükséges hitelesítő adatát.

A.Packet_Viewers
Feltételezzük, hogy a PDA eszköz tartalmaz olyan külső megjelenítő alkalmazásokat, melyek képesek a csomagba foglalható formátumok (melyeket az aláírási szabályzat határoz meg) mindegyikének a megjelenítésére. Az aláírás létrehozó PDA kliens és az aláírás ellenőrző felet jelentő szerver alkalmazás IT környezete pontosan ugyanazon formátumokat ismeri és tudja megjeleníteni, illetve ezen külső alkalmazások a két oldalon egyforma konfigurációs beállításokkal működnek. Ezen külső alkalmazások kívül esnek a TOE hatáskörén.

3.2.3 Az aláírás ellenőrzésével kapcsolatos feltételezések

A.Physical_Security
Feltételezés, hogy az aláírás ellenőrzését végző szerver fizikailag védett a külső támadók közvetlen támadásai ellen.

A.Host_Server_Machine
Az a gazdaszámítógép, melyen a mySigno fut, közvetlenül az ellenőrző (természetes vagy jogi személy) befolyása és felügyelete alatt áll, ami garantálja, hogy a biztonsági intézkedéseket megfelelően alkalmazzák.
A gazdaszámítógép operációs rendszere az általa futtatott alkalmazások számára elkülönített futási környezetet biztosít.
Az alábbi intézkedések teljesülnek:

- a gazdaszámítógép vírusvédelemmel ellátott;
- a gazdaszámítógép és nyílt hálózati kapcsolattal rendelkező egyéb gépek közötti kommunikáció tűzfallal védett és az adatáramlás ellenőrzött,
- a gazdagép adminisztrátori funkcióihoz való hozzáférés kizárólagosan az ehhez a funkcióhoz hozzárendelt adminisztrátorokra korlátozott (felhasználó és adminisztrátor megkülönböztetése);
- a gazdagépen telepítést vagy szoftverfrissítést csak az adminisztrátor végezhet;
- a gazdagép operációs rendszere letiltja a nem megbízható forrásból letöltött alkalmazások futtatását, biztosítva, hogy a mySigno szerver oldali modul csak hitelesített forrásból származó beállításokat, értékeket fogadjon el;
- a mySigno és az aláírás adatbázis a kommunikáció előtt kölcsönösen hitelesíti egymást, a közöttük folyó kommunikáció pedig titkosított;
- Az aláírás adatbázis maga gondoskodik a rajta tárolt adatok sértetlenségéről és hitelességéről.

A.Access_to_Validation_Data
A mySigno-nak hozzáféréssel kell rendelkeznie az aláírás ellenőrzéséhez szükséges összes érvényesítő adathoz.

3.3 Szervezeti biztonsági szabályok

Ez az alfejezet definiálja azokat a biztonsági szabályokat, amelyeket a mySigno modulnak teljesítenie kell.

P.Hash_Algorithm
A mySigno által megvalósított lenyomatoló algoritmusnak meg kell felelnie az alábbi kriptográfiai szabványnak: SHA-1 [FIPS 180-1].

P.Signature_Algorithm
A mySigno által megvalósított kriptográfiai algoritmusnak és kulcshosszának meg kell felelnie az alábbi kriptográfiai szabványnak: RSA Encryption Standard, PKCS#1 v. 1.5, 1024 bit.

P.Signatory_Certificate_Validity
A mySigno-nak ellenőriznie kell, hogy az aláíró tanúsítványa az érvényességi időn belül van-e.

P.Communication

Védeni kell a PDA kliens és a mySigno szerver közötti kommunikációt az alábbi műveletek esetén:
- csomag szinkronizálás,
- programfrissítés,
- ellenőrzési státuszinformációk visszaadása PDA kliensnek,

az adatok sértetlenségének és bizalmasságának biztosítása érdekében.

P.Fix_Signature_Policy
A mySigno zárt (PDA eszközök-mySigno szerver) rendszerében az implementáció tartalmazza az aláírási szabályzatot, aminek a TOE aláírás létrehozási és aláírás ellenőrzési oldalán meg kell egyeznie.

3.4.1 Az aláírás létrehozásával kapcsolatos szervezeti biztonsági szabályok

P.Key_Cert_Storage
A mySigno az alábbi adatokat tárolja és használja biztonságos módon:
- az aláírás létrehozásához használt adatok:
  - az aláíróhoz tartozó kulcs(ok); bizalmasságukat és sértetlenségüket kell megőrizni;
  - az aláíró tanúsítványa(i), sértetlenségüket kell megőrizni;
  - a magánkulcs/tanúsítvány összetartozása, a sértetlenségét kell fenntartani;
- az aláíró hitelesítésével kapcsolatos adatok
  - az aláíró hitelesítő adatának sértetlenségét és bizalmasságát kell megőrizni;
  - a megadott hitelesítő adat és a magánkulcs/tanúsítvány-pár összetartozása, ennek a sértetlenségét kell megőrizni.

P.Signature_Certificate_Conformance
Az aláírás létrehozás érvényességének biztosításához a mySigno-nak ellenőriznie kell, hogy az aláíráshoz használni kívánt tanúsítvány megfelel-e a beépített aláírási szabályzatnak.

P.Signing_Certificate_Validity
Az aláírás létrehozás érvényességének biztosításához a mySigno-nak ellenőriznie kell, hogy az aláíráshoz használni kívánt tanúsítványt az érvényességi idején belül kívánják-e használni.

P.Signature_Attributes_Conformance
Az aláírás létrehozás érvényességének biztosításához a TOE-nek ellenőriznie kell az alábbiakat:

- szerepelnek-e az aláírási szabályzat által megkövetelt aláírási tulajdonságok.

P.Document_Presentation_Possibility
A mySigno-nak lehetővé kell tennie, hogy az aláíró hozzáférjen az aláírandó dokumentum pontos reprezentációjához.
A mySigno-nak csak az aláíró közvetlen jóváhagyása esetén szabad megengednie a dokumentum aláírását, ha az nem felel meg a csatolt dokumentum kiterjesztésére vonatkozó követelményeknek.

P.Signature_Attributes_Presentation
A mySigno-nak lehetővé kell tennie az aláírási tulajdonságok megjelenítését az aláíró számára.

P.Signature_Process_Cancel
Az aláírónak képesnek kell lennie arra, hogy az aláírás létrehozó adat aktivizálása előtt bármely pillanatban le tudja állítani az aláírási folyamatot.

P.Explicit_Consent
A mySigno-nak biztosítania kell az aláírási folyamat elindítása előtt, hogy az aláírónak valamilyen nem nyilvánvaló műveletet kelljen végrehajtania annak kifejezésére, hogy valóban aláírást kíván létrehozni.
A közvetlen jóváhagyás után a mySigno-nak biztosítania kell, hogy valóban a megjelenített dokumentum kerül aláírásra.

P.Certificate_Privatekey_Association
A mySigno-nak kezelnie kell az ügynök tanúsítványához tartozó magánkulcs aktivizálást.

P.Electronic_Signature_Export
Az aláírási folyamatból való visszatéréskor a mySigno-nak el kell helyeznie a csomagban az elektronikus aláírást legalább az alábbi adatokkal:

- a csomag elektronikus aláírása;
- az aláírás időpontja;
- az aláíró tanúsítványa;
- hivatkozás a vonatkozó aláírási szabályzatra.

3.4.2 Az aláírás ellenőrzésével kapcsolatos szervezeti biztonsági szabályok

P.Signature_Attributes_Conformance
A mySigno-nak ellenőriznie kell, hogy:

- az aláírt tulajdonságok összhangban vannak-e az alkalmazandó aláírási szabályzattal,
- az aláírási szabályzat által megkövetelt minden aláírási tulajdonság szerepel-e.

P.Signatory_Certificate_Conformance
A mySigno-nak ellenőriznie kell, hogy a tanúsítvány útvonal minden tanúsítványa (beleértve az aláíró tanúsítványát is) megfelel-e az alkalmazandó aláírási szabályzatnak.

P.Authentic_Signatory_Certificate
A mySigno-nak ellenőriznie kell, hogy érvényes tanúsítvány útvonal építhető ki az aláíró tanúsítványa és a megbízható pont között. Egy ilyen útvonal megléte az aláíró tanúsítványának egy tanúsítási gyökérhez (megbízható ponthoz) viszonyított hitelességét bizonyítja.

P.Validation_Data_Authenticity_Integrity
A mySigno-nak ellenőriznie kell az érvényesítő adatok eredetének hitelességét és sértetlenségét.

P.Communication_Signing_Attributes
A mySigno-nak biztosítani kell olyan lehetőséget, mellyel az aláírt tulajdonságokat közvetíti az ellenőrző félnek.

P.Validation_Data_Export
A mySigno-nak lehetővé kell tennie, hogy az ellenőrző fél (folyamat) az ellenőrzés során a szükséges érvényesítő adatokat exportálni tudja.

4 Biztonsági célok

4.1 Általános IT biztonsági célok

O.Cryptographic_Support
A mySigno-nak az alábbi kriptográfiai tulajdonságokkal rendelkező kriptográfiai algoritmusokat kell alkalmazni:

- A lenyomatoló algoritmus(ok)nak olyannak kell lennie, hogy két dokumentumhoz ne forduljon elő ugyanazon lenyomat érték.
- A mySigno által megvalósított kriptográfiai algoritmusoknak és azok kulcshosszainak a megfelelő nyilvános kulcsok tanúsítványaiban szereplő érvényességi idő alatt ellen kell állni a kriptográfiai támadásoknak.

  Az algoritmusoknak meg kell felelniük a vonatkozó kriptográfiai szabványoknak:
  RSA Encryption Standard, PKCS#1 v. 1.5, 1024 bit
  SHA-1 FIPS-180-1

O.Fix_Signature_Policy
A mySigno zárt (PDA eszközök-mySigno szerver) rendszerében az implementációnak kell tartalmaznia az aláírási szabályzatot, aminek a TOE aláírás létrehozási és aláírás ellenőrzési oldalán meg kell egyeznie.

O.Communication

Védeni kell a PDA kliens és a mySigno szerver közötti kommunikációt az alábbi műveletek esetén:
- csomag szinkronizálás,
- programfrissítés,
- ellenőrzési státuszinformációk visszaadása PDA kliensnek,

az adatok sértetlenségének és bizalmasságának biztosítása érdekében.

4.2 Általános környezeti biztonsági célok

OE.Trusted_Security_Admin
A mySigno használata előtti, a TOE hatáskörön kívülre eső telepítési feladatokat végző adminisztrátorok megbízhatóak, a mySigno használatára kiképezték őket, rendelkeznek a szükséges eszközökkel a feladataik ellátáshoz.

OE.UserGuide
A PDA klienst használó ügynököt az eszköz használatára kiképezték, ismeri az eszköz fizikai paramétereiből következő, és annak biztonságos alkalmazását garantáló használati szabályokat.

OE.Trusted_EnvCode
A mySigno biztonsági funkcióit hívó alkalmazás és a mySigno által hívott funkciókat megvalósító függvénykönyvtár megbízható a tekintetben, hogy teljesíti a jelen biztonsági előirányzatban IT környezeti feltételezésként előírt, a TOE biztonságos használatát feltételező biztonsági követelményeket.

OE.Packet_Viewers
A PDA eszköz, mind pedig a szerver oldali IT környezet tartalmaz olyan külső megjelenítő alkalmazásokat, melyek képesek a csomagba foglalható formátumok (melyeket az aláírási szabályzat határoz meg) mindegyikének a megjelenítésére. Az aláírás létrehozó PDA kliens és az aláírás ellenőrző felet jelentő szerver alkalmazás IT környezete pontosan ugyanazon formátumokat ismeri és tudja megjeleníteni, illetve ezen külső alkalmazások a két oldalon egyforma konfigurációs beállításokkal működnek. Ezen külső alkalmazások kívül esnek a TOE hatáskörén.

OE.Separation_and_Exclusion
Az aláírás létrehozását és ellenőrzését végző IT környezetben a TOE folyamatok védettek más folyamatok káros beavatkozásai ellen. A mySigno v1.0 modult csak egy hosztalkalmazás töltheti be egy időben.

OE.Services_Integrity
A mySigno környezetének (hívó hosztalkalmazásnak, operációs rendszernek) biztosítania kell a számára olyan eszközöket, mellyel azok ellenőrizni tudják a mySigno szolgáltatások és paraméterek sértetlenségét.

OE.Physical_Security
Feltételezés, hogy az aláírás ellenőrzését végző szerver fizikailag védett a külső támadók közvetlen támadásai ellen.

4.3 Az elektronikus aláírás létrehozására vonatkozó biztonsági célok

4.3.1 A TOE által teljesítendő IT biztonsági célok

O.Association_Certificate_and_PrivateKey
A mySigno-nak gondoskodnia kell arról, hogy a megfelelő hitelesítési adatok alapján aktivizálni tudja az aláíráshoz használni kívánt tanúsítványhoz tartozó aláírás létrehozó adatot (magánkulcsot).

O.Presentation_Conformance_Attributes
A mySigno-nak biztosítania kell az aláíró számára az aláírandó tulajdonságokkal összhangban lévő aláírási tulajdonságok megjelenítését.

O.Explicit_Consent
A mySigno-nak biztosítania kell az aláíró számára olyan eszközt, mely által közvetlen módon ki tudja fejezni (egyértelműen és nem véletlenül) egy aláírandó csomag kiválasztásának szándékát és a kiválasztott dokumentumokra az aláírási folyamat elindítását.

O.Signer_Document
Miután az aláíró kifejezte aláírási szándékát, a mySigno-nak gondoskodnia kell arról, hogy a ténylegesen kezelt csomag (azaz amire az aláírás létrehozás meghívódik) pontosan megegyezik az ügynök számára képernyőn látható, elektronikus aláírásra kiválasztott csomaggal.

O.Conform_Certificate
A mySigno-nak ellenőriznie kell, hogy az aláíráshoz használni kívánt tanúsítvány megfelel-e az alkalmazandó aláírási szabályzat követelményeinek.

O.Valid_Signing_Certificate
A TOE-nak ellenőriznie kell, hogy az aláíró által kiválasztott tanúsítvány érvényes-e.
Alkalmazási megjegyzés
Ezen biztonsági cél teljesítésekor az ellenőrzéshez használt időt a PDA eszköz operációs rendszere szolgáltatja.

O.Conform_Attributes
A mySigno-nak ellenőriznie kell az aláírási tulajdonságok meglétét és aláírási szabályzatnak való megfelelését.

O.Electronic_Signature_Export
Az aláírási folyamatból való visszatéréskor a mySigno-nak csatolnia kell a csomaghoz a csomag elektronikus aláírását legalább az alábbi adatokkal:
- a dokumentum elektronikus aláírása;
- az aláírás időpontja;
- az aláíró tanúsítványa;
- hivatkozás a vonatkozó aláírási szabályzatra.

O.Packet_Content_Presentation
A mySigno-nak képesnek kell lennie egy külső alkalmazás elindítására, ami lehetővé teszi az aláíró (ügynök) számára az aláírandó csomagba foglalt adatok/dokumentumok megjelenítését.

> *Annak meghatározása érdekében, hogy melyik megjelenítő alkalmazást kell elindítani, a TOE IT környezetének (a hosztalkalmazásnak) kezelnie kell* a mySigno *által engedélyezett formátumok és a külső megjelenítő alkalmazások közötti megfeleltetést.*
> *A mySigno-nak meg kell akadályozni egy dokumentum aláírását, ha nem lehetett megállapítani, melyik megjelenítő alkalmazást kell elindítani hozzá, illetve ha nem tudta megjeleníteni az adatokat az ügynök kérésére. (OE.Packet_Viewers)*

O.Signature_Creation
A mySigno rendelkezik olyan funkcionalitással, mely fokozott biztonságú elektronikus aláírást hoz létre. Ezen kívül felel az aláíró hitelesítéséért is, azaz ellenőrizi, hogy a kiválasztott tanúsítványhoz tartozó magánkulcsot használhatja-e az aláírást kérő egyén.
A mySigno az alábbi adatokat tárolja és használja biztonságos módon:
az aláírás létrehozásához használt adatok:
- az aláíróhoz tartozó kulcs(ok); bizalmasságukat és sértetlenségüket kell megőrizni (magánkulcs törlése használat után közvetlenül);
- az aláíró tanúsítványa(i), sértetlenségüket kell megőrizni;
- a magánkulcs/tanúsítvány összetartozása, a sértetlenségét kell fenntartani.

az aláíró hitelesítésével kapcsolatos adatok:
- az aláíró hitelesítő adata, sértetlenségét és bizalmasságát kell megőrizni;
- a megadott hitelesítő adat és a magánkulcs/tanúsítvány-pár összetartozása, ennek a sértetlenségét kell megőrizni;

4.3.2 Környezeti biztonsági célok

OE.Host_PDA_Machine
Az a gazdaszámítógép, melyen a mySigno fut, közvetlenül az aláíró (ügynök) befolyása és a rendszert működtető szervezet felügyelete alatt áll.
A gazdaszámítógép operációs rendszere az általa futtatott alkalmazások számára elkülönített futási környezetet biztosít.
A TOE-nak az alábbi intézkedéseket kell érvényre juttatnia:

- a gazdaszámítógép vírusvédelemmel ellátott;
- a gazdagép adminisztrátori funkcióihoz való hozzáférés kizárólagosan az ehhez a funkcióhoz hozzárendelt adminisztrátorokra korlátozott (felhasználó és adminisztrátor megkülönböztetése);
- a gazdagép operációs rendszere elutasítja a nem megbízható forrásból letöltött alkalmazások futtatását.

OE.Signatory_Presence
Az elektronikus aláírás létrehozójának (ügynöknek) végig jelen kell lennie attól kezdődően, hogy kifejezte aláírási szándékát, addig, amíg megadja a magánkulcs aktivizálásához szükséges hitelesítő adatát.

4.4 Az aláírás ellenőrzésére vonatkozó biztonsági célok

4.4.1 TOE IT biztonsági célok

O.Time_Stamp
Az alkalmazott aláírási szabályzattal összhangban, a mySigno-nak megbízható időforrásról kell gondoskodnia, ami lehetővé teszi az ügynök elektronikus aláírás egy adott időpillanatban való meglétének bizonyítását.
Alkalmazási megjegyzés

A PDA eszközön az időforrást a rendszeridő biztosítja. Szerver oldalon a lehetséges időbélyeg szolgáltatók által szolgáltatott időbélyeg.

O.Certificate_Path
A mySigno-nak ellenőriznie kell, hogy érvényes tanúsítvány útvonal létezik

- az aláíró tanúsítvány, aminek a hivatkozása az aláírt tulajdonságok között szerepel, és
- a megbízható pont között.

O.Conform_Certificates
A mySigno-nak ellenőriznie kell, hogy a tanúsítvány útvonal minden tanúsítványa (beleértve az aláíró tanúsítványát is) megfelel az alkalmazandó aláírási szabályzat követelményeinek.

O.Valid_Certificates
A tanúsítvány útvonal minden tanúsítványa (ideértve az aláíró tanúsítványát) esetén a mySigno-nak ellenőriznie kell:

- a tanúsítvány sértetlenségét és eredetének hitelességét,
- azt, hogy a tanúsítvány érvényességi idején belül volt-e az aláírás létrehozásakor,
- a megbízható pontok tanúsítványai kivételével azt, hogy a tanúsítvány nem volt-e visszavont státuszú az aláírás létrehozásakor.

O.Conform_Validation_Data
A mySigno-nak ellenőriznie kell, hogy az aláírás ellenőrzéséhez összegyűjtött érvényesítő adatok megfelelnek-e az alkalmazott aláírási szabályzatnak, különös tekintettel arra, hogy a kibocsátójuk aláírta-e ezen adatokat (a sértetlenségük és eredet hitelesség biztosítása érdekében).

Alkalmazási megjegyzés
Az érvényesítő adatok aláírása egyúttal ezen adatok sértetlenségét és eredetének hitelességét is garantálja.

O.Conform_Signing_Attributes
A mySigno-nak ellenőriznie kell az aláírt tulajdonságok meglétét és az aláírási szabályzat előírásainak való megfeleltetését.

O.Communication_Signing_Attributes
A mySigno-nak továbbítani kell tudni az aláírt tulajdonságokat az ellenőrző fél számára.

O.Validation_Data_Export
A mySigno-nak lehetővé kell tennie a használandó érvényesítő adatok ellenőrző számára történő összegyűjtését az ellenőrzés során.

4.4.2 Környezeti biztonsági célok

OE.Host_Server_Machine
Az a gazdaszámítógép, melyen a mySignofut, közvetlenül az ellenőrző (természetes vagy jogi személy) befolyása és felügyelete alatt áll, ami garantálja, hogy a biztonsági intézkedéseket megfelelően alkalmazzák.
A gazdaszámítógép operációs rendszere az általa futtatott alkalmazások számára elkülönített futási környezetet biztosít.
Az alábbi intézkedések teljesülnek:

- a gazdaszámítógép vírusvédelemmel ellátott;
- a gazdaszámítógép és nyílt hálózati kapcsolattal rendelkező egyéb gépek közötti kommunikáció tűzfallal védett és az adatáramlás ellenőrzött,
- a gazdagép adminisztrátori funkcióihoz való hozzáférés kizárólagosan az ehhez a funkcióhoz hozzárendelt adminisztrátorokra korlátozott (felhasználó és adminisztrátor megkülönböztetése);
- a gazdagépen telepítést vagy szoftverfrissítést csak az adminisztrátor végezhet;
- a gazdagép operációs rendszere letiltja a nem megbízható forrásból letöltött alkalmazások futtatását.

OE.Validation_Data_Provision
A mySigno környezetének biztosítani kell a mySigno számára az aláírás ellenőrzéséhez szükséges adatokhoz való hozzáférést.

Alkalmazási megjegyzés:
A mySigno által végrehajtott ellenőrzés céljából ezen környezeti célt az alábbi három interfészen keresztül teljesíti:
- időbélyeg szolgáltatóval való kommunikáció;
- fogadott csomagok tárolására szolgáló adatbázis szerver;
- hitelesítés szolgáltatóval való kommunikáció.

Ezen kapcsolódások konkrétumai a mySigno-t felhasználó alkalmazás hatáskörébe esnek.

5 IT biztonsági követelmények

Ez a fejezet a mySigno funkcionális és garanciális biztonsági követelményeit írja le. A követelmények a CC 2. és 3. részéből származnak, illetve a 2. rész kiterjesztései. A jelölések a CC-nek megfelelnek.
Az alábbi táblázat azonosítja azokat a követelményeket, amelyek nem a CC 2. részéből származnak.

5.1 táblázat– Kiterjesztett 2. vagy 3. rész követelmények

Követelmény	
FDP_MRU.1 Kötelező szabályok	Kiterjesztett 2. rész

5.1 A TOE funkcionális biztonsági követelményei

5.1.1 Az aláírás létrehozására vonatkozó funkcionális biztonsági követelmények

5.1.1.1 A csomag adatok importálása TOE hatáskörbe

FDP_IFC.1/Csomag jóváhagyás – Részleges információ áramlás ellenőrzés
FDP_IFC.1.1/Csomag jóváhagyás
A TSF-nek érvényre kell juttatnia a „**csomag jóváhagyás" információ áramlási szabály**t az alábbiakra:

- szubjektumok: **aláíró**,
- információ: **az aláírandó csomag (dokumentumok, adatok, kézi aláírások stb.)**
- művelet: **a csomag importálása a TSC-be**.

FDP_IFF.1/Csomag jóváhagyás – Egyszerű biztonsági tulajdonságok
FDP_IFF.1.1/ Csomag jóváhagyás
A TSF-nek végre kell hajtania a „**csomag jóváhagyás" információ áramlási szabályt**, ami az alábbi szubjektum és információ biztonsági tulajdonságokon alapul:

- szubjektumok: **aláíró [aláírói tulajdonságok: aláírási szabályzat, aláíró tanúsítványa]**,
- információ: **aláírandó csomag [csomag tulajdonságok: csomag azonosító (képernyőn látható, aktuális nyitott csomag)]**;
- művelet: **csomag importálása**.

FDP_IFF.1.2/Csomag jóváhagyás
A TSF-nek lehetővé kell tennie az információ áramlást egy ellenőrzött szubjektum és ellenőrzött információ között ellenőrzött művelet révén, ha az alábbi szabályok teljesülnek:
Dokumentum importálás:

- **A csomag csatolt dokumentumainak kiterjesztése az aláírási szabályzatban megadott formátumok egyike.**

FDP_IFF.1.3/Csomag jóváhagyás
A TSF-nek érvényre kell juttatnia a következőket: nincsenek további szabályok.

FDP_IFF.1.4/ Csomag jóváhagyás
A TSF-nek az alábbi egyéb képességeket kell biztosítania:

- **A dokumentum hozzáadásának elutasítása, ha valamelyik csatolandó dokumentum kiterjesztése nem egyezik meg az aláírási szabályzatban meghatározott formátumok egyikével sem;**
- **Külső dokumentum megtekintő elindításának lehetősége az ügynök által választott csomag-elemre;**
- **A TSF-nek biztosítania kell, hogy a tényleges aláírás létrehozás számára átadott aláírandó adat megegyezik az aláíró által megtekintett adatokkal.**

FDP_IFF.1.5/ Csomag jóváhagyás
A TSF-nek explicit módon engedélyeznie kell az információ áramlást az alábbi szabályok alapján: nincsenek egyéb szabályok.
FDP_IFF.1.6/ Csomag jóváhagyás
A TSF-nek explicit módon le kell tiltania az információ áramlást az alábbi szabályok alapján: nincsenek egyéb szabályok.

FDP_ITC.1/ Csomag jóváhagyás – Felhasználói adatok importálása biztonsági tulajdonságok nélkül
FDP_ITC.1.1/ Csomag jóváhagyás
A TSF-nek érvényre kell juttatnia a „**csomag jóváhagyás" információ áramlási szabályt** a TSC-n kívülről érkező, SFP által ellenőrzött felhasználói adatok importálásakor.
FDP_ITC.1.2/ Csomag jóváhagyás
A TSF-nek figyelmen kívül kell hagynia a felhasználó adatokhoz rendelt bármilyen biztonsági tulajdonságot amikor azokat a TSC-n kívülről importálja.
FDP_ITC.1.3/ Csomag jóváhagyás
A TSF-nek érvényre kell juttatnia az alábbi szabályokat amikor az SFP felügyelete alá tartozó, TSC-n kívülről importál felhasználói adatokat:

- **Meg kell állapítania a csatolt dokumentumok kiterjesztését az automatikus importáláshoz, vagy jóváhagyást kell kérnie az importáláshoz.**

FMT_MSA.3/ Csomag jóváhagyás – Statikus tulajdonság inicializálás
FMT_MSA.3.1/ Csomag jóváhagyás
A TSF-nek érvényre kell juttatnia a „**csomag jóváhagyás" információ áramlási szabályt**, hogy **korlátozó** alapértékeket adjon az SFP-t megvalósító biztonsági tulajdonságoknak.

FMT_MSA.3.2/ Csomag jóváhagyás
A TSF-nek **senki** számára sem szabad lehetővé tennie az alapértékek alternatív kezdeti értékekkel való felülírását egy objektum vagy információ létrehozásakor.

FMT_MSA.1/Csomag jóváhagyás – A biztonsági tulajdonságok menedzsmentje
FMT_MSA.1.1/Csomag jóváhagyás
A TSF-nek érvényre kell juttatnia a „**csomag jóváhagyás" információ áramlási szabályt**, annak érdekében, hogy az **aláíróra** korlátozza az **aláírandó csomag elfogadása státusz** biztonsági tulajdonság **módosítását**.

FMT_SMF.1/Csomag kiválasztása aláírásra – Menedzsment funkciók meghatározása
FMT_SMF.1.1/Csomag kiválasztása aláírásra
A TSF-nek képesnek kell lennie az alábbi biztonsági menedzsment funkciók végrehajtására:

- **aláírandó csomag kiválasztása.**

5.1.1.2 Az aláírási tulajdonságokra és aláíró tanúsítványra vonatkozó szabályok

Aláírási tulajdonságok
FMT_MSA.1/Aláírási tulajdonságok – A biztonsági tulajdonságok menedzsmentje
FMT_MSA.1.1/Aláírási tulajdonságok
A TSF-nek érvényre kell juttatnia az „**aláírás létrehozás"** információ áramlási szabályt annak **érdekében, hogy az aláíróra korlátozza az aláíró tanúsítvány, aláírási szabályzat azonosító, aláírási idő biztonsági tulajdonság megtekintés képességét.**

Aláíró (ügynök) tanúsítványa
FMT_SMF.1/Aláírói tanúsítvány megtekintése – Menedzsment funkciók meghatározása
FMT_SMF.1.1/ Aláírói tanúsítvány kiválasztása
A TSF-nek képesnek kell lennie az alábbi biztonsági menedzsment funkciók végrehajtására:

- **lehetővé kell tenni az aláíró számára az aláírói tanúsítvány megtekintését.**

FPT_TDC.1/Aláíró tanúsítványa – TSF-ek közötti alapvető TSF adat konzisztencia
FPT_TDC.1.1/Aláíró tanúsítványa
A TSF-nek gondoskodnia kell olyan képességről, amely segítségével konzisztens módon értelmezhetők a **nyilvános kulcs tanúsítványok,** amikor a TSF és más megbízható IT termék között megosztásra kerül.

FPT_TDC.1.2/Aláíró tanúsítványa
A TSF-nek az **RFC 3280-ban definiált (X509v3) tanúsítvány formátumokat** kell használnia, amikor más megbízható IT terméktől származó TSF adatot értelmez.

5.1.1.3 Az elektronikus aláírás létrehozása

FDP_ACC.1/Aláírás létrehozása – Részleges hozzáférés ellenőrzés
FDP_ACC.1.1 A TSF-nek érvényre kell juttatnia az „**aláírás létrehozás" hozzáférés ellenőrzési szabályt** az alábbiakra:
- szubjektumok: **az aláíró (ügynök)**
- objektumok:
    - **formázott aláírandó adat (lenyomat);**
    - **ügynök PKCS#12 fájlban tárolt magánkulcsa.**

- műveletek:

1. **A rögzített aláírási szabályzat értelmében az aláíróhoz tartozó aláírói tanúsítvány felhasználásával megengedett, hogy az aláíró elektronikus aláírást hozzon létre a mySigno által elkészített csomag lenyomat értékre az aláíró tanúsítványának megfelelő magánkulcs felhasználásával.**
2. **Az aláírás létrehozás előtt az aláírási tulajdonságok megmutatása megengedett az aláírónak (ügynöknek).**

3. **A csomagba foglalt adatok és dokumentumok megjelenítését lehetővé tevő felület szolgáltatása (külső alkalmazás indítása az operációs rendszerben beállított fájlformátum társítás alapján) megengedett az aláíró (ügynök) számára.**

FDP_ACF.1/Aláírás létrehozás – Biztonsági tulajdonság alapú hozzáférés ellenőrzés
FDP_ACF.1.1/Aláírás létrehozás
A TSF-nek érvényre kell juttatnia az „**aláírás létrehozás" hozzáférés ellenőrzési szabályt** az objektumokra az alábbi biztonsági tulajdonságok alapján:
- szubjektumok: **az aláíró** (biztonsági tulajdonságai: **alkalmazott aláírási szabályzat, aláírói tanúsítvány**);
- objektum: **a formázott aláírandó adat** (**aláírási tulajdonságok: aláírási szabályzat azonosító, aláírói tanúsítvány, aláírás ideje)**

FDP_ACF.1.2/ Aláírás létrehozás
A TSF-nek érvényre kell juttatnia az alábbi szabályokat annak meghatározása érdekében, hogy egy művelet megengedett-e az ellenőrzött szubjektumok és objektumok között:
1. **az „aláírási szabályzat azonosító" (SignaturePolicyIdentifier) aláírási tulajdonságnak szerepelnie kell;**
2. **az „aláírás ideje" aláírási tulajdonság szerepeltetése kötelező;**
3. **az "aláíró tanúsítvány" aláírási tulajdonság szerepeltetése kötelező;**
4. **a kiválasztott aláírói tanúsítvány „kulcshasználata" (`keyUsage`) jelzi, hogy a tanúsítvány használható letagadhatatlanságot bizonyító célokra. A keyUsage mezőben a non-repudiation bitnek beállítva kell lennie, és ezen kívül legfeljebb a digitalSignature bit lehet beállítva).**

FDP_ACF.1.3/ Aláírás létrehozás
A TSF-nek explicit módon engedélyeznie kell szubjektumok objektumokhoz való hozzáférését az alábbi egyéb szabályok alapján**: nincsenek további szabályok**.
FDP_ACF.1.4/ Aláírás létrehozás
A TSF-nek explicit módon le kell tiltania szubjektumok objektumokhoz való hozzáférését az alábbi szabályok alapján: **nulla hosszú dokumentum beszúrása a csomagba**

FMT_MSA.3/Aláírás létrehozás – Statikus tulajdonság inicializálás
FMT_MSA.3.1/ Aláírás létrehozás
A TSF-nek érvényre kell juttatnia az **aláírás létrehozás hozzáférés ellenőrzési** szabályt annak érdekében, hogy **korlátozó** alapértékekről gondoskodjon az SFP megvalósításához használt biztonsági tulajdonságokra.
FMT_MSA.3.2/ Aláírás létrehozás
A TSF-nek **senki** számára sem szabad lehetővé tennie az alapértékek alternatív kezdeti értékekkel való felülírását egy objektum vagy információ létrehozásakor.

FDP_ITC.1/Explicit aláírói jóváhagyás – Felhasználói adatok importálása biztonsági tulajdonságok nélkül
FDP_ITC.1.1/ Explicit aláírói jóváhagyás
A TSF-nek érvényre kell juttatnia az **aláírás létrehozás hozzáférés ellenőrzési szabályt** a TSC-n kívülről érkező, SFP által ellenőrzött felhasználói adatok importálásakor.
FDP_ITC.1.2/ Explicit aláírói jóváhagyás
A TSF-nek figyelmen kívül kell hagynia a felhasználó adatokhoz rendelt bármilyen biztonsági tulajdonságot, amikor azokat a TSC-n kívülről importálja.
FDP_ITC.1.3/ Explicit aláírói jóváhagyás

TSF-nek érvényre kell juttatnia az alábbi szabályokat amikor az SFP felügyelete alá tartozó, TSC-n kívülről importál felhasználói adatokat:

- **az ügynöknek (aláírónak) egyértelműen ki kell fejeznie aláírási szándékát, amit a TOE által megjelenített kérdésre adott aláírás létrehozásra vonatkozó *pozitív* válasz jelent.**

5.1.1.4 Az elkészült elektronikus aláírás csatolása

FDP_ACC.1/Elektronikus aláírás csatolása – Részleges hozzáférés ellenőrzés

FDP_ACC.1.1 A TSF-nek érvényre kell juttatnia az **elektronikus aláírás csatolása hozzáférés ellenőrzési szabályt** az alábbiakra:

- szubjektumok: **az aláíró (ügynök)**
- objektumok:
  - **a létrehozott numerikus aláírás,**
  - **dokumentum lenyomat**,
  - **aláírási szabályzat azonosító,**
  - **aláírás ideje,**
  - **aláíró tanúsítvány.**
- művelet:
  - **adat és aláírás csomaghoz fűzése és a csomag lezárása.**

FDP_AFC.1/ Elektronikus aláírás csatolása – Biztonsági tulajdonság alapú hozzáférés ellenőrzés

FDP_ACF.1.1/Elektronikus aláírás csatolása

A TSF-nek érvényre kell juttatnia az „**elektronikus aláírás csatolása" hozzáférés ellenőrzési szabályt** az objektumokra az alábbi biztonsági tulajdonságok alapján:

- szubjektumok:
  - **aláíró (**biztonsági tulajdonságai: **alkalmazott aláírási szabályzat, aláírói tanúsítvány),**
- objektum:
  - **csomag**
  - **az elektronikus aláírás (a létrehozott numerikus aláírás, az aláírt csomag lenyomata, az aláírói tanúsítvány hivatkozása, az alkalmazott aláírási szabályzat hivatkozása, aláírás ideje).**

FDP_ACF.1.2/ Elektronikus aláírás csatolása

A TSF-nek érvényre kell juttatnia az alábbi szabályokat annak meghatározása érdekében, hogy egy művelet megengedett-e az ellenőrzött szubjektumok és objektumok között:

az elektronikus aláírás csomaghoz fűzése és a csomag lezárása megengedett, ha az aláírás létrehozás sikeres volt. (aláírás létrehozási státusz értéke *sikeres*)

FDP_ACF.1.3/ Elektronikus aláírás csatolása

A TSF-nek explicit módon engedélyeznie kell szubjektumok objektumokhoz való hozzáférését az alábbi egyéb szabályok alapján: **nincsenek további szabályok.**

FDP_ACF.1.4/ Elektronikus aláírás csatolása

A TSF-nek explicit módon le kell tiltania szubjektumok objektumokhoz való hozzáférését az alábbi szabályok alapján:

- **a magánkulcshoz való hozzáféréshez szükséges hitelesítő adat sikertelen megadása;**
- **az aláíró ügynök explicit jóváhagyásának hiánya.**

FMT_MSA.3/ Elektronikus aláírás csatolása – Statikus tulajdonság inicializálás
FMT_MSA.3.1/ Elektronikus aláírás csatolása
A TSF-nek érvényre kell juttatnia az „**elektronikus aláírás csatolása" hozzáférés ellenőrzési** szabályt annak érdekében, hogy **korlátozó** alapértékekről gondoskodjon az SFP megvalósításához használt biztonsági tulajdonságokra.
FMT_MSA.3.2/ Elektronikus aláírás csatolása
A TSF-nek **senki** számára sem szabad lehetővé tennie az alapértékek alternatív kezdeti értékekkel való felülírását egy objektum vagy információ létrehozásakor.

FMT_MSA.1/Aláírás létrehozási státusz – A biztonsági tulajdonságok menedzsmentje
FMT_MSA.1.1/Aláírás létrehozási státusz
A TSF-nek érvényre kell juttatnia **az „elektronikus aláírás csatolása" információ áramlás ellenőrzési szabályt**, hogy **senki** ne tudja **módosítani** az **aláírás létrehozási státusz** biztonsági tulajdonságot.

FMT_SMF.1/Az aláírás létrehozási státusz megállapítása – Menedzsment funkciók meghatározása
FMT_SMF.1.1/ Az aláírás létrehozási státusz megállapítása
A TSF-nek képesnek kell lennie az alábbi biztonsági menedzsment funkciók végrehajtására:

- **az aláírás létrehozási állapot megállapítása (annak megkülönböztetése, hogy az aláírás létrehozási folyamat sikeresen befejeződött vagy sikertelenül szakadt meg).**

5.1.2 Az aláírás ellenőrzésére vonatkozó funkcionális biztonsági követelmények

5.1.2.1 Az elektronikus aláírás és az aláírási tulajdonságok importálása

FDP_IFC.1/Elektronikus aláírás importálása - Részleges információ áramlás ellenőrzés
FDP_IFC.1.1/Elektronikus aláírás importálása
A TSF-nek érvényre kell juttatnia az **elektronikus aláírás importálása információ áramlás ellenőrzési szabályt** az alábbiakra:

- szubjektumok: **ellenőrző fél,**
- információ: **az aláírás és a kapcsolódó aláírt tulajdonságok, valamint az aláírt dokumentum**
- művelet: **importálás (azaz az aláírt tulajdonságok: "aláírás ideje", "aláíró tanúsítványa", "aláírási szabályzat azonosító" elfogadása).**

Alkalmazási megjegyzés:
Az elektronikus aláírás és kapcsolódó aláírási tulajdonságok importálásának engedélyezése (elfogadása) azt jelenti, hogy az aláírt tulajdonságok megfelelnek az alkalmazott, programban implementált aláírási szabályzat szabályainak.

FDP_IFF.1/Elektronikus aláírás importálása - Egyszerű biztonsági tulajdonságok
FDP_IFF.1.1/ Elektronikus aláírás importálása
A TSF-nek érvényre kell juttatnia az elektronikus aláírás **importálása** információ áramlás ellenőrzési szabályt az alábbi szubjektum- és információ biztonsági tulajdonságokra:

- szubjektumok**: ellenőrző fél (biztonsági tulajdonság: alkalmazott aláírási szabályzat),**
- információ**:**
    - **elektronikus aláírás (az aláírt tulajdonságok: "aláírás ideje", "aláíró tanúsítványa", "aláírási szabályzat azonosító")**
    - **aláírt dokumentum (az aláírt dokumentum formátuma: szabványos XML formátum).**

FDP_IFF.1.2/Elektronikus aláírás importálása
A TSF-nek lehetővé kell tennie az információ áramlást egy ellenőrzött szubjektum és ellenőrzött információ között ellenőrzött művelet révén, ha az alábbi szabályok teljesülnek:
Aláírás importálása:

- **az„aláírási szabályzat azonosító” aláírt tulajdonságnak szerepelnie kell az elektronikus aláírásban és az értékének meg kell felelni az ellenőrző fix aláírási szabályzatának;**
- **az „aláírás ideje” aláírt tulajdonságnak szerepelnie kell az elektronikus aláírásban;**
- **az "aláíró tanúsítvány" aláírt tulajdonságnak szerepelnie kell az elektronikus aláírásban, valamint ennek egy ügynök aláírói tanúsítványának kell lennie.**

FDP_IFF.1.3/Elektronikus aláírás importálása
A TSF-nek érvényre kell juttatnia: **nincsenek további szabályok**.
FDP_IFF.1.4/ Elektronikus aláírás importálása
A TSF-nek gondoskodnia kell az alábbiakról:

- **az ellenőrző fél tájékoztatása arról, ha a hivatkozott aláírási szabályzat nem egyezik meg az ellenőrző által alkalmazandó/alkalmazott aláírási szabályzattal;**

- **az ellenőrző fél tájékoztatása arról, ha a tényleges időrés nagyobb a megengedettnél.**

FDP_IFF.1.5/ Elektronikus aláírás importálása
A TSF-nek explicit módon engedélyeznie kell az információ áramlást az alábbi szabályok alapján: **nincsenek egyéb szabályok.**
FDP_IFF.1.6/ Elektronikus aláírás importálása
A TSF-nek explicit módon le kell tiltania az információ áramlást az alábbi szabályok alapján: **nincsenek egyéb szabályok.**

FMT_MSA.3/Elektronikus aláírás importálása Statikus tulajdonság inicializálása
FMT_MSA.3.1/Elektronikus aláírás importálása
A TSF-nek érvényre kell juttatnia az **„elektronikus aláírás importálása"** információ áramlás ellenőrzési szabályt, hogy **korlátozó** alapértékeket adjon az SFP-t megvalósító biztonsági tulajdonságoknak.
FMT_MSA.3.2/ Elektronikus aláírás importálása
A TSF-nek **senki** számára sem szabad lehetővé tennie az alapértékek alternatív kezdeti értékekkel való felülírását egy objektum vagy információ létrehozásakor.

FMT_MSA.1/ Elektronikus aláírás importálása A biztonsági tulajdonságok menedzselése
FMT_MSA.1.1/ Elektronikus aláírás
A TSF-nek érvényre kell juttatnia az „**elektronikus aláírás importálása"** információ áramlás ellenőrzési szabályt annak érdekében, hogy **senki** se legyen képes **módosítani** az **"aláírás" és a hozzá tartozó "aláírt tulajdonság"** biztonsági tulajdonságokat.

5.1.2.2 Érvényes időbélyeg importálása

FDP_IFC.1/Időbélyeg - Részleges információ áramlás ellenőrzés
FDP_IFC.1.1/ Időbélyeg
A TSF-nek érvényre kell juttatnia az „**időbélyeg elfogadása"** áramlás ellenőrzési szabályt az alábbiakra:

- szubjektumok**: ellenőrző fél,**
- információ**: az aláírásra alkalmazott időbélyeg,**
- művelet**: az időbélyeg importálása.**

Alkalmazási megjegyzés:
Az időbélyeg importálásnak engedélyezése (elfogadása) azt jelenti, hogy az időbélyeg elfogadott az aláírási szabályzat értelmében.

FDP_IFF.1/ Időbélyeg Egyszerű biztonsági tulajdonságok
FDP_IFF.1.1/ Időbélyeg
A TSF-nek érvényre kell juttatnia az **„időbélyeg elfogadása”** információ áramlás ellenőrzési szabályt, ami az alábbi szubjektum típusokon és információ biztonsági tulajdonságokon alapul:

- szubjektumok**:**
  - **ellenőrző fél**
    - **biztonsági tulajdonság: alkalmazott fix aláírási szabályzat**
- információ**:**
  - **az ügynök aláírására vonatkozó időbélyeg**
    - **tulajdonságok: az időbélyeg tokenek ellenőrzéséhez használható megbízható pontok tanúsítványai, időbélyeg végtanúsítvány, bármilyen szükséges közbenső tanúsítvány a tanúsítvány és a megbízható pont között.**

FDP_IFF.1.2/ Időbélyeg
A TSF-nek lehetővé kell tennie az információ áramlást egy ellenőrzött szubjektum és ellenőrzött információ között, ellenőrzött művelet révén, ha az alábbi szabályok teljesülnek:
Művelet: az aláíró aláírására vonatkozó időbélyeg importálása:

- **az időbélyeg végtanúsítványának kulcshasználata jelöli, hogy a szóban forgó tanúsítvány csak időbélyegzési célokra használható;**
- **tanúsítási útvonal létezik az időbélyeg végtanúsítvány és az aláírási szabályzatban rögzített megbízható időbélyeg szolgáltató között;**
- **az FDP_MRU.1/Tanúsítási útvonal követelményben definiált, előbbiekben említett tanúsítási útvonalra vonatkozó minden szabály teljesül az időreferenciában szereplő dátum/időre, kivéve azokat, amelyekre nincs explicit hivatkozás az alkalmazott aláírási szabályzatban.**

FDP_IFF.1.3/ Időbélyeg
A TSF-nek érvényre kell juttatnia: nincsenek további szabályok.
FDP_IFF.1.4/ Időbélyeg
A TSF-nek biztosítania kell az alábbi egyéb képességeket: nincsenek további szabályok.
FDP_IFF.1.5/ Időbélyeg
A TSF-nek explicit módon engedélyeznie kell az információ áramlást az alábbi szabályok alapján: nincsenek további szabályok.
FDP_IFF.1.6/ Időbélyeg
A TSF-nek explicit módon le kell tiltania az információ áramlást az alábbi szabályok alapján: nincsenek további szabályok.

FMT_MSA.3/ Időbélyeg Statikus tulajdonság inicializálás
FMT_MSA.3.1/ Időbélyeg
A TSF-nek érvényre kell juttatnia az **„időbélyeg elfogadása”** információ áramlás ellenőrzési szabályt **korlátozó** alapértékeket adva az SFP-t megvalósító biztonsági tulajdonságoknak.
FMT_MSA.3.2/ Időbélyeg [szerkesztői finomítás]
A TSF-nek **senki** számára sem szabad lehetővé tennie az alapértékek alternatív kezdeti értékekkel való felülírását egy objektum vagy információ létrehozásakor.

FMT_MSA.1/ Időbélyeg A biztonsági tulajdonságok menedzselése
FMT_MSA.1.1/ Időbélyeg

A TSF-nek érvényre kell juttatnia az „**időbélyeg elfogadása”** információ áramlás ellenőrzési szabályt, hogy **senki** ne tudja **módosítani** az **időbélyeg** biztonsági tulajdonságot.

FDP_ITC.2/ Időbélyeg A felhasználói adatok importálása biztonsági tulajdonságokkal
FDP_ITC.2.1/ Időbélyeg
A TSF-nek érvényre kell juttatnia az **„időbélyeg elfogadása”** információ áramlás ellenőrzési szabályt, amikor az SFP ellenőrzése alatt a TSC-n kívülről felhasználói adatokat importál.
FDP_ITC.2.2/ Időbélyeg
A TSF-nek használnia kell az importált felhasználói adatokhoz kapcsolódó biztonsági tulajdonságokat.
FDP_ITC.2.3/ Időbélyeg
A TSF-nek biztosítania kell, hogy az alkalmazott protokoll egyértelműen összekapcsolja a biztonsági tulajdonságokat és a kapott felhasználói adatokat.
FDP_ITC.2.4/ Időbélyeg
A TSF-nek biztosítania kell, hogy az importált felhasználói adatok biztonsági tulajdonságának értelmezése olyan, amilyennek azt az adatok forrása szándékozta.
FDP_ITC.2.5/ Időbélyeg
A TSF-nek érvényre kell juttatnia az alábbi szabályokat amikor az SFP ellenőrzése alatt a TSC-n kívülről felhasználói adatot importál: nincsenek további szabályok.

5.1.2.3 Érvényes tanúsítási útvonal importálása

Az alábbi követelmények a tanúsítási útvonal tanúsítványaira vonatkozó ellenőrzési szabályokat tartalmazzák, továbbá azon szabályokat, melyek alapján az alkalmazás képes eldönteni, hogy érvényes-e az útvonal vagy sem.

Tanúsítványok

FMT_MSA.1/Tanúsítványok - A biztonsági tulajdonságok menedzselése
FMT_MSA.1.1/ Tanúsítványok
A TSF-nek érvényre kell juttatnia a „**tanúsítási útvonal elfogadása”** információ áramlás ellenőrzési szabályt, hogy **senki** ne tudja **módosítani** az **importált tanúsítványok** biztonsági tulajdonságot.

Tanúsítványok érvényesítő adatai

FMT_MSA.1/Tanúsítványok érvényesítő adatai - A biztonsági tulajdonságok menedzselése
FMT_MSA.1.1/ Tanúsítványok érvényesítő adatai
A TSF-nek érvényre kell juttatnia a „**tanúsítási útvonal elfogadása”** információ áramlás ellenőrzési szabályt, hogy **senki** ne tudja **módosítani** a **tanúsítványok visszavonási adatai** biztonsági tulajdonságot.

Tanúsítási útvonal felépítése

FDP_IFC.1/Tanúsítási útvonal Részleges információ áramlás ellenőrzés
FDP_IFC.1.1/ Tanúsítási útvonal
A TSF-nek érvényre kell juttatnia a „**tanúsítási útvonal elfogadása"** információ áramlás ellenőrzési szabályt az alábbiakra:

- szubjektumok**:**
  - **ellenőrző fél,**
- információ**:**
  - **a tanúsítási útvonalhoz tartozó tanúsítványok,**
  - **a tanúsítási útvonal érvényesség ellenőrzéséhez szükséges visszavonási adatok.**
- művelet**:**
  - **az információk importálása (azaz az útvonal a használt aláírási szabályzat értelmében érvényes tanúsítási útvonalnak fogadható el).**

Alkalmazási megjegyzés:
A tanúsítványok és kapcsolódó érvényesítő adatok importálásának engedélyezése azt jelenti, hogy az útvonal érvényes tanúsítási útvonalnak elfogadott az aláírási szabályzat értelmében.

FDP_IFF.1/ Tanúsítási útvonal Egyszerű biztonsági tulajdonságok
FDP_IFF.1.1/Tanúsítási útvonal
A TSF-nek érvényre kell juttatnia **a „tanúsítási útvonal elfogadása"** információ áramlás ellenőrzési szabályt, ami az alábbi szubjektum típusokon és információ biztonsági tulajdonságokon alapul:

- szubjektumok**:**
  - **ellenőrző fél (mySigno-ba épített fix aláírási szabályzat)**
- információ**:**
  - **tanúsítási útvonal érvényesítő adatai, beleértve az alábbiakat:**
    - **a tanúsítási útvonalhoz tartozó összes tanúsítvány,**
    - **a tanúsítási útvonalban szereplő minden egyes tanúsítvány visszavonási információk.**

FDP_IFF.1.2/ Tanúsítási útvonal
A TSF-nek lehetővé kell tennie az információ áramlást egy ellenőrzött szubjektum és ellenőrzött információ között, ellenőrzött művelet révén, ha az alábbi szabályok teljesülnek:
A tanúsítási útvonal elemeinek és a kapcsolódó érvényesítő adatok importálása:

- **a tanúsítási útvonal összeköti az aláíró (ügynök) tanúsítványát a rögzített aláírási szabályzatban szereplő megbízható pont valamelyikével;**
- **az FDP_MRU.1/Tanúsítási útvonal követelményben definiált minden szabály teljesül az importált időreferenciában (azaz az időbélyegben) szereplő dátumra/időre, kivéve azokat, amelyekre nincs explicit hivatkozás az alkalmazott aláírási szabályzatban;**
- **a kiválasztott aláírói tanúsítvány „kulcshasználata" (`keyUsage`) jelzi, hogy a tanúsítvány használható letagadhatatlanságot bizonyító célokra (alkalmazási megjegyzés: a keyUsage mezőben a nonRepudiation bit be van állítva, és ezen kívül legfeljebb a digitalSignature lehet beállítva);**

FDP_IFF.1.3/ Tanúsítási útvonal
A TSF-nek érvényre kell juttatnia a következő szabályokat:-.
FDP_IFF.1.4/ Tanúsítási útvonal
A TSF-nek biztosítania kell az alábbi egyéb képességeket: -

FDP_IFF.1.5/ Tanúsítási útvonal
A TSF-nek explicit módon engedélyeznie kell az információ áramlást az alábbi szabályok alapján: nincsenek további szabályok.
FDP_IFF.1.6/ Tanúsítási útvonal
A TSF-nek explicit módon le kell tiltania az információ áramlást az alábbi szabályok alapján: nincsenek további szabályok.

FDP_MRU.1/Tanúsítási útvonal Kötelező szabályok
FDP_MRU.1.1/ Tanúsítási útvonal
A TSF-nek képesnek kell lennie adott szabálykészlet alkalmazására a „**tanúsítási útvonal elfogadása”** információ áramlás ellenőrzési szabály és az **„időbélyeg elfogadása”** információ áramlás ellenőrzési szabály teljesítése érdekében.

FDP_MRU.1.2/ Tanúsítási útvonal
A TSF-nek képesnek kell lennie az alábbi szabálykészlet alkalmazására:
1. **a tanúsítási útvonal minden egyes tanúsítványára a tanúsítványon lévő aláírás érvényes;**
2. **a tanúsítási útvonal minden egyes tanúsítványára a tanúsítvány érvényességi idejébe beleesik az időbélyegben szereplő dátum;**
3. **az aláírói és az időbélyegző végtanúsítványok ellenőrzése során az aktuális CRL-t kell használni;**
4. **a CRL-elek aktualizálása a paraméteresen megadható "türelmi idő" biztonsági tulajdonság által meghatározott idő alapján történik;**
5. **a megbízható pontok, hitelesítés-szolgáltatók és időbélyegzés szolgáltatók tanúsítványai esetén nincs CRL ellenőrzés;**
6. **minden egyes visszavonási adatra az adaton lévő aláírás érvényes;**
7. **a tanúsítási útvonal - 3. és 4. pont figyelembe vételével - minden egyes tanúsítványára a tanúsítvány nem volt visszavont az időbélyeg által meghatározott időpontban;**
8. **a tanúsítási útvonal minden egyes tanúsítványára -a végtanúsítvány kivételével- a kulcshasználat jelöli, hogy a tanúsítvány CA tanúsítvány;**
9. **az időbélyegzői végtanúsítvány és a megbízható időbélyegző szolgáltató között a tanúsítvány útvonal hossza max. 1.**
10. **a tanúsítási útvonal minden egyes tanúsítványára a tanúsítványban megnevezett hitelesítési rend megfelel az alkalmazott rögzített aláírási szabályzatnak.**

FMT_MSA.3/Tanúsítási útvonal Statikus tulajdonság inicializálás
FMT_MSA.3.1/ Tanúsítási útvonal
A TSF-nek érvényre kell juttatnia a **tanúsítási útvonal elfogadása információ áramlás ellenőrzési szabályt**, hogy **korlátozó** alapértékeket adjon az SFP-t megvalósító biztonsági tulajdonságoknak.

FMT_MSA.3.2/ Tanúsítási útvonal
A TSF-nek **senki** számára sem szabad lehetővé tennie az alapértékek alternatív kezdeti értékekkel való felülírását egy objektum vagy információ létrehozásakor.

FDP_ITC.2/Tanúsítási útvonal A felhasználói adatok importálása biztonsági tulajdonságokkal
FDP_ITC.2.1/ Tanúsítási útvonal

A TSF-nek érvényre kell juttatnia **a tanúsítási útvonal elfogadása információ áramlás ellenőrzési szabályt,** amikor az SFP ellenőrzése alatt a TSC-n kívülről felhasználói adatokat importál.

FDP_ITC.2.2/ Tanúsítási útvonal

A TSF-nek használnia kell az importált felhasználói adatokhoz kapcsolódó biztonsági tulajdonságokat.

FDP_ITC.2.3/ Tanúsítási útvonal

A TSF-nek biztosítania kell, hogy az alkalmazott protokoll egyértelműen összekapcsolja a biztonsági tulajdonságokat és a kapott felhasználói adatokat.

FDP_ITC.2.4/ Tanúsítási útvonal

A TSF-nek biztosítania kell, hogy az importált felhasználói adatok biztonsági tulajdonságának értelmezése olyan, amilyennek azt az adatok forrása szándékozta.

FDP_ITC.2.5/ Tanúsítási útvonal

A TSF-nek érvényre kell juttatnia az alábbi szabályokat amikor az SFP ellenőrzése alatt a TSC-n kívülről felhasználói adatot importál:

- **érvényes időbélyeg került importálásra (lásd FDP_IFC.1/Időbélyeg és kapcsolódó követelményeket, megbízható időbélyegzés szolgáltató elérés, időbélyeg tanúsítási útvonal hossz korlátozások);**
- **a tanúsítványok letagadhatatlanságának ellenőrzéséhez szükséges minden adat importálásra került a rögzített aláírási szabályzatnak megfelelően.**

5.1.2.4 Az importált adatok értelmezése

FPT_TDC.1/Elektronikus aláírás – TSF-ek közötti alapvető TSF adat konzisztencia

FPT_TDC.1.1/Elektronikus aláírás

A TSF-nek gondoskodnia kell olyan képességről, amely segítségével konzisztens módon értelmezhető az **elektronikus aláírás** amikor a TSF és más megbízható IT termék között megosztásra kerül.

FPT_TDC.1.2/ Elektronikus aláírás

A TSF-nek **XAdES-C TS 101 903 v1.2.formátumot** kell használni, amikor más megbízható IT terméktől származó TSF adatot értelmez.

FPT_TDC.1/Időbélyeg – TSF-ek közötti alapvető TSF adat konzisztencia

FPT_TDC.1.1/ Időbélyeg

A TSF-nek gondoskodnia kell olyan képességről, amely segítségével konzisztens módon értelmezhető az **időbélyeg** amikor a TSF és más megbízható IT termék között megosztásra kerül.

FPT_TDC.1.2/ Időbélyeg

A TSF-nek az **RFC 3161 szabványnak megfelelő formátumot** kell használnia, amikor más megbízható IT terméktől származó TSF adatot értelmez.

FPT_TDC.1/Tanúsítványok – TSF-ek közötti alapvető TSF adat konzisztencia

FPT_TDC.1.1/ Tanúsítványok

A TSF-nek gondoskodnia kell olyan képességről, amely segítségével konzisztens módon értelmezhetők a **tanúsítványok,** amikor a TSF és más megbízható IT termék között megosztásra kerül.

FPT_TDC.1.2/ Tanúsítványok
A TSF-nek az **RFC 3280-ban definiált (X509v3) tanúsítvány formátumokat** kell használnia, amikor más megbízható IT terméktől származó TSF adatot értelmez.

FPT_TDC.1/ Tanúsítvány visszavonási adatok – TSF-ek közötti alapvető TSF adat konzisztencia
FPT_TDC.1.1/ Tanúsítvány visszavonási adatok
A TSF-nek gondoskodnia kell olyan képességről, amely segítségével konzisztens módon értelmezhetők a **tanúsítvány visszavonási adatok,** amikor a TSF és más megbízható IT termék között megosztásra kerül.

FPT_TDC.1.2/ Tanúsítvány visszavonási adatok
A TSF-nek használnia **kell az RFC 3280-ban definiált CRL formátumot (X509v2**) amikor más megbízható IT terméktől származó TSF adatot értelmez.

5.1.2.5 Az ellenőrzés eredményének visszaadása

FDP_IFC.1/Elektronikus aláírás érvényesség ellenőrzése - Részleges információ áramlás ellenőrzés
FDP_IFC.1.1/Elektronikus aláírás érvényesség ellenőrzése
A TSF-nek érvényre kell juttatnia az **elektronikus aláírás érvényességének ellenőrzése információ áramlás ellenőrzési szabályt** az alábbiakra:
- szubjektumok**: ellenőrző fél,**
- információ**: „érvényes aláírás" ellenőrzési státusz**
- művelet**: a státusz közlése az ellenőrző fél számára.**

FDP_IFF.1/ Elektronikus aláírás érvényesség ellenőrzése - Egyszerű biztonsági tulajdonságok
FDP_IFF.1.1/ Elektronikus aláírás érvényesség ellenőrzése
A TSF-nek érvényre kell juttatnia **az elektronikus aláírás érvényességének ellenőrzése információ áramlás ellenőrzési szabályt**, mi az alábbi szubjektum típusokon és információ biztonsági tulajdonságokon alapul:
- szubjektumok**: ellenőrző fél (alkalmazott aláírási szabályzat, [értékadás: ellenőrzői tulajdonságok];**
- információ**: „érvényes aláírás" érvényességi státusz (aláíró nyilvános kulcsa, csomag lenyomat, csomag aláírása).**

FDP_IFF.1.2/ Elektronikus aláírás érvényesség ellenőrzése
A TSF-nek lehetővé kell tennie az információ áramlást egy ellenőrzött szubjektum és ellenőrzött információ között, ellenőrzött művelet révén, ha az alábbi szabályok teljesülnek:
Az ellenőrzés eredményének közvetítése az ellenőrző fél számára:
- **létezik érvényes tanúsítási útvonal az aláíró tanúsítványa és egy megbízható pont tanúsítványa között, mely utóbbira hivatkozás szerepel az aláírási szabályzatban, ami hitelessé teszi az aláíró nyilvános kulcsát;**
- **az aláíró nyilvános kulcsával ellenőrizve a dokumentum aláírása helyes (érvényes).**

FDP_IFF.1.3/ Elektronikus aláírás érvényesség ellenőrzése
A TSF-nek érvényre kell juttatnia a következő szabályokat: -.

FDP_IFF.1.4/ Elektronikus aláírás érvényesség ellenőrzése
A TSF-nek biztosítania kell az alábbi képességeket:
- **az „érvénytelen aláírás" státusz közlésének képessége, amennyiben legalább egy információ áramlás ellenőrzési szabály nem teljesül.**

FDP_IFF.1.5/ Elektronikus aláírás érvényesség ellenőrzése
A TSF-nek explicit módon engedélyeznie kell az információ áramlást az alábbi szabályok alapján: -.
FDP_IFF.1.6/ Elektronikus aláírás érvényesség ellenőrzése
A TSF-nek explicit módon le kell tiltania az információ áramlást az alábbi szabályok alapján: -.

FMT_MSA.3/Aláírás érvényesség ellenőrzés státusz Statikus tulajdonság inicializálása
FMT_MSA.3.1/ Aláírás érvényesség ellenőrzés státusz
A TSF-nek érvényre kell juttatnia az **elektronikus aláírás érvényesség ellenőrzése információ áramlás ellenőrzési szabályt**, hogy **korlátozó** alapértékeket adjon az SFP-t megvalósító biztonsági tulajdonságoknak.

FMT_MSA.3.2/ Aláírás érvényesség ellenőrzés státusz
A TSF-nek **senki** számára sem szabad lehetővé tennie az alapértékek alternatív kezdeti értékekkel való felülírását egy objektum vagy információ létrehozásakor.

FMT_MSA.1/ Aláírás érvényesség ellenőrzés státusz A biztonsági tulajdonságok menedzselése
FMT_MSA.1.1/ Aláírás érvényesség ellenőrzés státusz
A TSF-nek érvényre kell juttatnia az **elektronikus aláírás érvényesség ellenőrzése információ áramlás ellenőrzési** szabályt, hogy **senki** ne tudja **módosítani** az **aláírás érvényesség státusz** biztonsági tulajdonságot.

FDP_ETC.2/Ellenőrzési státusz - A felhasználói adatok exportálása biztonsági tulajdonságokkal
FDP_ETC.2.1/ Ellenőrzési státusz
A TSF-nek érvényre kell juttatnia az **elektronikus aláírás érvényesség ellenőrzése információ áramlás ellenőrzési szabályt**, amikor az SFP ellenőrzése alatt a TSC-ből felhasználói adatokat exportál.
FDP_ETC.2.2/ Ellenőrzési státusz
A TSF-nek a felhasználói adatokat a hozzájuk kapcsolódó biztonsági tulajdonságokkal együtt kell exportálnia.
FDP_ETC.2.3/ Ellenőrzési státusz
A TSF-nek biztosítania kell, hogy a biztonsági tulajdonságok – azok TSC-n kívülre történő exportálása során-, egyértelműen hozzárendelődnek az exportált felhasználói adatokhoz.
FDP_ETC.2.4/ Ellenőrzési státusz
A TSF-nek érvényre kell juttatnia az alábbi szabályokat amikor az SFP ellenőrzése alatt a TSC-ből felhasználói adatot exportál:
az ellenőrzési státusz biztonsági tulajdonságaiként exportált adatok:
- **az ellenőrzési státusz helyessége ellenőrzésének bizonyítását segítő érvényesítő adatok;**
- **az aláírt tulajdonságok,**
- **érvényesítő adatok.**

Alkalmazási megjegyzés:

Az érvényesítő adatok újra felhasználhatóak az utólagos ellenőrzés során.

5.1.3 Általános funkcionális biztonsági követelmények

5.1.3.1 Kriptográfiai támogatás

FCS_COP.1/Aláírás létrehozás - Kriptográfiai műveletek
FCS_COP.1.1/Aláírás létrehozás
A TSF-nek
digitális aláírás létrehozást
kell végrehajtania az alábbi kriptográfiai algoritmus, kulcsméret és szabvány alapján:
RSA Encryption Standard, PKCS#1 v. 1.5, 1024 bit

FCS_COP.1/Aláírás ellenőrzés – Kriptográfiai műveletek
FCS_COP.1.1/ Aláírás ellenőrzés
A TSF-nek
digitális aláírás ellenőrzést
kell végrehajtania az alábbi kriptográfiai algoritmus és kulcsméret és szabvány alapján:
RSA Encryption Standard, PKCS#1 v. 1.5, 1024 bit

FCS_COP.1/Lenyomat – Kriptográfiai műveletek
FCS_COP.1.1/Lenyomat
A TSF-nek
csomag lenyomat létrehozást
kell végrehajtania egy megadott kriptográfiai algoritmus és kulcsméret és szabvány alapján:
SHA-1 [FIPS 180-1]
Globális finomítás:
Az SHA-1 megfelel azon követelménynek, hogy nem hoz létre azonos üzenet-lenyomatot két különböző dokumentumhoz.

5.1.3.2 A felhasználó azonosítása és hitelesítése

FIA_UID.1/Aláíró Az azonosítás időzítése
FIA_UID.1.1 A TSF-nek lehetővé kell tennie
- aláírandó csomag és aláírási tulajdonságok kiválasztása, megtekintése;
amiket a felhasználóra kötelezően végre kell hajtani, mielőtt a felhasználót azonosítva lesz.
FIA_UID.1.2 A TSF-nek meg kell követelnie, hogy minden felhasználó sikeresen azonosítva legyen, mielőtt bármilyen TSF-által közvetített tevékenység történne a felhasználó nevében.
Alkalmazási megjegyzés:
Az ügynöknek a fokozott biztonságú aláírás létrehozása előtt kell megadnia a PIN-kódját.
PDA-szerver kommunikáció PDA oldali kezdeményezése esetén PDA eszköz PIN kód megadása.

FIA_UAU.1/Aláíró A hitelesítés időzítése
FIA_UAU.1.1 A TSF-nek lehetővé kell tennie, hogy
- a FIA_UID.1/Aláíró által megkövetelt TSF eszközökkel a felhasználó azonosítása,
- az aláíró magánkulcshoz tartozó PIN-kód kiválasztása
a felhasználóra kötelezően végrehajtódjon, mielőtt a felhasználó hitelesítődik.

FIA_UAU.1.2 A TSF-nek meg kell követelnie, hogy a felhasználó sikeresen hitelesítve legyen, mielőtt bármilyen TSF-által közvetített tevékenység történne a felhasználó nevében.

FIA_AFL.1 Hitelesítési hibák kezelése
FIA_AFL.1.1 A TSF-nek észlelnie kell, amikor **három** sikertelen hitelesítési kísérlet történik **egymást követően.**
FIA_AFL.1.2 Amikor megadott számú sikertelen hitelesítési kísérlet történik, a TSF-nek
- **zárolnia kell az aláíró (ügynök) magánkulcs hitelesítő adatát;**

FIA_ATD.1 Felhasználói tulajdonságok megadása
FIA_ATD.1.1 A TSF-nek az alábbi, egyedi felhasználókhoz tartozó biztonsági tulajdonságokat kell megőriznie: **hitelesítő adat (PIN kód).**

FMT_MSA.2 Biztonságos biztonsági tulajdonságok
FMT_MSA.2.1 A TSF-nek biztosítania kell, hogy csak biztonságos értékeket fogad el biztonsági tulajdonságként.
Vonatkozó biztonsági tulajdonságok:
magánkulcshoz tartozó PIN kód hossza és formája: számjegyekből álló 6 hosszú karaktersorozat

FMT_MSA.3Statikus tulajdonság-inicializálás
FMT_MSA.3.1 A TSF-nek érvényre kell juttatnia **az aláírás létrehozás hozzáférés ellenőrzési szabály**t, hogy **korlátozó** kezdeti értékekről gondoskodjanak az SFP-t végrehajtását támogató biztonsági tulajdonságokra.
FMT_MSA.3.2 A TSF-nek lehetővé kell tennie, hogy **senki** ne tudja alternatív kezdeti értékkel felülírni az alapértelmezettet egy objektum vagy információ létrehozásakor.

5.1.3.3 Maradványinformációk védelme

FDP_RIP.1 Részleges maradványinformáció védelem
FDP_RIP.1.1 A TSF-nek gondoskodni kell arról, hogy egy erőforrás korábbi információtartalma hozzáférhetetlenné válik **az erőforrás** deallokációja után az alábbi objektumok esetén: **aláíró magánkulcsa, PDA eszköz magánkulcsa, aláíró hitelesítő adat (eszköz PIN kód, ügynök PIN kód), szerver aláíró és rejtjelező kulcsok)**.

5.1.3.4 A kommunikáció védelme

Kriptográfiai műveletek

FCS_COP.1/SecMsg_PDA
FCS_COP.1.1/SecMsg_PDA A TSF-nek **biztonságos csatornát** kell kiépítenie a TOE által küldött és fogadott üzenetek továbbítására az alábbi algoritmusokkal és kulcshossz:
a) RSA Encryption Standard, PKCS#1 v. 1.5, kulcshossz: 1024 bit
- kulcsegyeztetésre;
b) AES Advanced Encryption Standard FIPS-197, kulcshossz: 256 bit
- üzenet rejtjelezésre;
c) RSA Encryption Standard, PKCS#1 v. 1.5, kulcshossz: 1024 bit
- aláírásra.

FCS_COP.1/SecMsg_MySignoServer
FCS_COP.1.1/SecMsg_MySignoServer A TSF-nek **biztonságos csatornát** kell kiépítenie a TOE által küldött és fogadott üzenetek továbbítására az alábbi algoritmusokkal és kulcshossz:

a) RSA Encryption Standard, PKCS#1 v. 1.5, kulcshossz: 1024 bit
- kulcsegyeztetésre;
b) AES Advanced Encryption Standard FIPS-197, kulcshossz: 256 bit
- üzenet rejtjelezésre;
c) RSA Encryption Standard, PKCS#1 v. 1.5, kulcshossz: 1024 bit
- aláírásra.

FTP_ITC.1 TSF-ek közötti megbízható csatorna
FTP_ITC.1.1/PDA-MySignoServer_Comm
A TSF-nek biztonságos kommunikációs csatornáról kell gondoskodnia önmaga és egy távoli megbízható IT termék között, mely csatorna logikailag különbözik más átviteli csatornáktól és végpontjainak garantált azonosítását, valamint a csatornán átmenő adatok módosítással vagy felfedéssel szembeni védelmét biztosítja.
FTP_ITC.1.2/PDA-MySignoServer_Comm
A TSF-nek lehetővé kell tennie, hogy **a TSF** kommunikációt kezdeményezzen a megbízható csatornán keresztül.
FTP_ITC.1.3/ PDA-MySignoServer_Comm
A **TSF-nek és a TOE-nek** kommunikációt kell tudni kezdeményezni a megbízható csatornán keresztül az

- **aláírt csomagok szinkronizálása,**
- **a szerver oldali ellenőrzés eredményének PDA kliens felé való továbbítása, és**
- **a PDA kliens szoftverfrissítés letöltés**

végrehajtására.

5.2 A TOE környezetre vonatkozó IT biztonsági követelmények

FPT_RVM.1 A TSP megkerülhetetlensége
Hierarchikus alárendeltség más komponensekhez képest: nincs.

FPT_RVM.1.1 A TSF-nek biztosítania kell, hogy a TSP-t érvényre juttató funkciók valóban meghívódnak, és befejeződnek, mielőtt a TSF hatáskörén belülre eső egyes funkciók futása lehetővé válik.
Függések: nincsenek.

FPT_SEP.1 TSF tartomány szétválasztás
Hierarchikus alárendeltség más komponensekhez képest: nincs.

FPT_SEP.1.1 A TSF-nek biztonsági tartományt kell kezelnie a saját futásához, ami megvédi a nem megbízható egyedek általi beavatkozástól és hamisítástól.
FPT_SEP.1.2 A TSF-nek érvényre kell juttatnia szétválasztást a szubjektumok biztonsági tartománya között a TSC-ben.
Függések: nincsenek.

5.3 A TOE garanciális biztonsági követelményei: fokozott garanciaszint

Jelen biztonsági előirányzat a fokozott értékelési garanciaszintet követeli meg.

A fokozott garanciaszint garanciaösszetevői alapvetően megegyeznek a Közös szempontokban (CC) meghatározott 3-as garanciaszint (EAL3) garanciaösszetevőivel.
Az egyetlen különbség: AVA_VLA.1 helyett az erősebb AVA_VLA.1+ az elvárt.
Az így emelt szintű (EAL 3+) garanciaszint összetevőit az alábbi táblázat tekinti át.

Garancia-osztály	**Garancia-család**	**Fokozott garanciaszint**	
		garanciaösszetevők sorszáma és elnevezése	
Konfiguráció menedzselés	**ACM_CAP**	3	ACM_CAP.3 A jogosultságok ellenőrzése
	ACM_SCP	1	ACM_SCP.1 Az értékelés tárgya konfiguráció menedzselésének lefedettsége
Kiszállítás és működtetés	**ADO_DEL**	1	ADO_DEL.1 A szállítás eljárásai
	ADO_IGS	1	ADO_IGS.1 Hardver telepítés, szoftver telepítés, a beindítás eljárásai
Fejlesztés	**ADV_FSP**	1	ADV_FSP.1 Informális funkcionális specifikáció
	ADV_HLD	**2**	ADV_HLD.2 Biztonságot érvényre juttató magas szintű tervezés
	ADV_RCR	1	ADV_RCR.1 A kölcsönös megfelelés informális szemléltetése
Útmutató dokumentumok	**AGD_ADM**	1	AGD_ADM.1 Az adminisztrátori útmutató
	AGD_USR	1	AGD_USR.1 A felhasználói útmutató
Az életciklus támogatása	**ALC_DVS**	**1**	ALC_DVS.1 A biztonsági intézkedések azonosítása
Tesztelés	**ATE_COV**	**2**	ATE_COV.2 A teszt lefedettség elemzése
	ATE_DPT	**1**	ATE_DPT.1 A magas szintű terv tesztelése
	ATE_FUN	1	ATE_FUN.1 Funkcionális tesztelés
	ATE_IND	2	ATE_IND.2 Független tesztelés - mintán
A sebezhetőség felmérése	**AVA_MSU**	**1**	AVA_MSU.1 Az útmutatók vizsgálata
	AVA_SOF	1	AVA_SOF.1 Az értékelés tárgya biztonsági funkcióinak erősségértékelése
	AVA_VLA	**1+**	AVA_VLA.1+ A sebezhetőség független elemzése

1. táblázat – A fokozott értékelési garanciaszint összefoglalása

A konfiguráció menedzselése

ACM_CAP.3 A jogosultságok ellenőrzése

Fejlesztői feladatok:

- ACM_CAP.3.1D A fejlesztőnek meg kell adnia az értékelés tárgya hivatkozást.
- ACM_CAP.3.2D A fejlesztőnek egy konfiguráció menedzselés rendszert kell használnia.
- ACM_CAP.3.3D A fejlesztőnek egy konfiguráció menedzselés dokumentációt kell átadnia.

A bizonyíték elemek tartalma és bemutatása:

- ACM_CAP.3.1C Az értékelés tárgya hivatkozásnak egyedi módon kell azonosítania az értékelés tárgya verzióit.
- ACM_CAP.3.2C Az értékelés tárgyát meg kell jelölni ezzel a hivatkozással.
- ACM_CAP.3.3C A konfiguráció menedzselés dokumentációnak tartalmaznia kell egy konfiguráció listát és egy konfiguráció menedzselés tervet.
- ACM_CAP.3.4C A konfiguráció listának le kell írnia az értékelés tárgyát alkotó konfiguráció elemeket.
- ACM_CAP.3.5C A konfiguráció menedzselés dokumentációnak le kell írnia a konfiguráció elemek egyedi azonosításához használt módszert.
- ACM_CAP.3.6C A konfiguráció menedzselés rendszernek egyedi módon kell azonosítania minden konfiguráció elemet.
- ACM_CAP.3.7C A konfiguráció menedzselés tervnek le kell írnia a konfiguráció menedzselés rendszer használatát.
- ACM_CAP.3.8C Bizonyítékoknak kell kimutatniuk, hogy a konfiguráció menedzselés rendszer a konfiguráció menedzselés tervnek megfelelően működik.
- ACM_CAP.3.9C A konfiguráció menedzselés dokumentációnak bizonyítékot kell adnia arra, hogy minden konfiguráció elemet megfelelően kezeltek és kezelnek a konfiguráció menedzselés rendszer alapján.
- ACM_CAP.3.10C A konfiguráció menedzselés rendszernek biztosítania kell , hogy csak jogosult változtatások történhessenek a konfiguráció elemekben.

Értékelői feladatelemek:

- ACM_CAP.3.1E Az értékelőnek meg kell győződnie arról, hogy a rendelkezésére bocsátott információk megfelelnek-e a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ACM_SCP.1 Az értékelés tárgya konfiguráció menedzselésének lefedettsége

Fejlesztői feladatok:

- ACM_SCP.1.1D A fejlesztőnek konfiguráció menedzselés dokumentációt kell készítenie.

A bizonyíték elemek tartalma és bemutatása:

- ACM_SCP.1.1C A konfiguráció menedzselés dokumentációnak meg kell mutatnia, hogy a konfiguráció menedzselés rendszer nyomon követi legalább a következő konfiguráció elemeket: a TOE megvalósítási reprezentációja, tervezési dokumentációk, tesztelési dokumentáció, felhasználói és adminisztrátori dokumentációk, valamint a konfiguráció menedzselés dokumentáció.
- ACM_SCP.1.1C A konfiguráció menedzselés dokumentációnak le kell írnia, hogyan követi nyomon a konfiguráció menedzselés rendszer a különböző konfiguráció elemeket.

Értékelői feladatelemek:

- ACM_SCP.1.1E Az értékelőnek meg kell győződnie arról, hogy a rendelkezésére bocsátott információk megfelelnek-e a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

A szállítás és működtetés értékelése

ADO_DEL.1 A szállítás eljárásai

Fejlesztői feladatok:

- ADO_DEL.1.1D A fejlesztőnek dokumentálnia kell az értékelés tárgya vagy annak részei felhasználóhoz való szállításának eljárásait.
- ADO_DEL.1.2D A fejlesztőnek használnia kell a szállítási eljárásokat.

A bizonyítékelemek tartalma és megjelenésmódja:

- ADO_DEL.1.1C A szállítási dokumentációnak le kell írnia minden olyan eljárást, amely az értékelés tárgyának a felhasználó telephelyére történő szállítása során a biztonság fenntartásához szükséges.

Értékelői tevékenységelemek:

- ADO_DEL.1.1E Az értékelőnek meg kell arról győződnie, hogy a rendelkezésére bocsátott információk megfelelnek-e a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek

ADO_IGS.1 Hardver telepítés, szoftver telepítés, a beindítás eljárásai

Fejlesztői feladatok:

- ADO_IGS.1.1D A fejlesztőnek dokumentálnia kell a biztonságos hardver és szoftver telepítéshez, valamint az indításhoz szükséges eljárásokat.

A bizonyítékelemek tartalma és megjelenésmódja:

- ADO_IGS.1.1C A dokumentációnak le kell írnia a biztonságos hardver és szoftver telepítéshez, valamint az indításhoz szükséges lépéseket.

Értékelői tevékenységelemek:

- ADO_IGS.1.1E Az értékelőnek meg kell arról győződnie, hogy a rendelkezésére bocsátott információk megfelelnek-e a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek
- ADO_IGS.1.2E Az értékelőnek meg kell állapítania a hardver és szoftver telepítés, valamint az indítás eljárásairól, hogy azok biztonságos konfigurációt eredményeznek-e.

A fejlesztés értékelése

ADV_FSP.1 Informális funkcionális specifikáció

Fejlesztői feladatok:

- ADV_FSP.1.1D A fejlesztőnek funkcionális specifikációt kell átadnia.

A bizonyíték elemek tartalma és bemutatása:

- ADV_FSP.1.1C A funkcionális specifikációnak informális stílusban le kell írnia a TSF-t (az értékelés tárgya biztonsági funkcióit) és annak külső interfészeit.
- ADV_FSP.1.2C A funkcionális specifikációnak belsőleg konzisztensnek (ellentmondásmentesnek) kell lennie.
- ADV_FSP.1.3C A funkcionális specifikációnak le kell írnia minden külső TSF interfész használatának célját és módját, részletezve a hatásokat, kivételeket és hibaüzeneteket, amennyiben ezekre szükség van.
- ADV_FSP.1.4C A funkcionális specifikációnak teljes mértékben reprezentálnia kell a TSF-et.

Értékelői feladatelemek:

- ADV_FSP.1.1E Az értékelőnek meg kell győződnie arról, hogy a rendelkezésére bocsátott információk megfelelnek-e a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.
- ADV_FSP.1.2E Az értékelőnek meg kell állapítania, hogy a funkcionális specifikáció a TOE funkcionális biztonsági követelményeinek pontos és teljes megvalósulása-e.

ADV_HLD.2 Biztonságot érvényre juttató magas szintű tervezés

Fejlesztői feladatok:

- ADV_HLD.2.1D A fejlesztőnek magas szintű tervet kell átadnia.

A bizonyíték elemek tartalma és bemutatása:

- ADV_HLD.2.1C A magas szintű terv bemutatásának informálisnak kell lennie.
- ADV_HLD.2.2C A magas szintű tervnek belsőleg konzisztensnek kell lennie.
- ADV_HLD.2.3C A magas szintű tervnek le kell írnia a TSF struktúráját alrendszerek szerint.
- ADV_HLD.2.4C A magas szintű tervnek le kell írnia minden egyes TSF alrendszer által nyújtott biztonsági funkcionalitást.
- ADV_HLD.2.5C A magas szintű tervnek azonosítania kell a TSF által megkövetelt minden alapul szolgáló hardvert, förmvert és/vagy szoftvert, az ezekkel megvalósított kiegészítő védelmi mechanizmus által biztosított funkciók bemutatásával.
- ADV_HLD.2.6C A magas szintű tervnek azonosítania kell minden TSF alrendszer interfészt.
- ADV_HLD.2.7C A magas szintű tervnek azonosítania kell, hogy a TSF alrendszerek interfészei közül melyek láthatók kívülről.
- ADV_HLD.2.8C A magas szintű tervnek le kell írnia minden TSF alrendszer interfész használatának célját és módját, azok hatásával, kivételekkel és hibaüzenetekkel, amennyiben ez utóbbiak lényegesek.
- ADV_HLD.2.9C A magas szintű tervnek le kell írnia a TOE felosztását TSP-t érvényre juttató és egyéb alrendszerekre.

Értékelői feladatelemek:

- ADV_HLD.2.1E Az értékelőnek meg kell győződnie arról, hogy a rendelkezésére bocsátott információk megfelelnek-e a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

- ADV_HLD.2.2E Az értékelőnek meg kell állapítania, hogy a magas szintű terv pontos és teljes megjelenítése a TOE funkcionális biztonsági követelményeinek.

ADV_RCR.1 A kölcsönös megfelelés informális szemléltetése

Fejlesztői feladatok:

- ADV_RCR.1.1D A fejlesztőnek át kell adnia a biztosított TSF reprezentációk minden egymásnak megfelelő párjának megfeleltetés-elemzését.

A bizonyíték elemek tartalma és bemutatása:

- ADV_RCR.1.1C A megfeleltetés-elemzésnek be kell mutatnia, hogy az absztraktabb TSF reprezentáció minden lényeges biztonsági funkcionalitását helyesen és teljes mértékben finomítja tovább a kevésbé absztrakt TSF reprezentáció.

Értékelői feladatelemek:

- ADV_RCR.1.1E Az értékelőnek meg kell győződnie arról, hogy a rendelkezésére bocsátott információk megfelelnek-e a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

Az útmutató dokumentumok értékelése

AGD_ADM.1 Adminisztrátori útmutató

Fejlesztői feladatok:

- AGD_ADM.1.1D A fejlesztőnek a TOE adminisztrátorai számára adminisztrátori útmutatót kell készítenie és beadnia.

A bizonyíték elemek tartalma és bemutatása:

- AGD_ADM.1.1C Az adminisztrátori útmutatónak le kell írnia a TOE adminisztrátora rendelkezésére álló adminisztrátori funkciókat és interfészeket.
- AGD_ADM.1.2C Az adminisztrátori útmutatónak le kell írnia, hogy hogyan kell a TOE-t biztonságos módon adminisztrálni.
- AGD_ADM.1.3C Az adminisztrátori útmutatónak tartalmaznia kell azon funkciókkal és jogosultságokkal kapcsolatos figyelmeztetéseket, melyeket egy biztonságos üzemeltetési környezetben ellenőrzés alatt kell tartani.
- AGD_ADM.1.4C Az adminisztrátori útmutatónak le kell írnia a felhasználói viselkedéssel kapcsolatos minden feltételezést, mely a TOE biztonságos üzemelése szempontjából lényeges.
- AGD_ADM.1.5C Az adminisztrátori útmutatónak le kell írnia minden biztonsági szempontból fontos paramétert, mely az adminisztrátor ellenőrzése alá tartozik, jelezve (ahol ez lehetséges) a biztonságos értékeket.
- AGD_ADM.1.6C Az adminisztrátori útmutatónak le kell írnia minden adminisztratív funkcióval kapcsolatban végrehajtandó, biztonsági szempontból fontos esemény típusát, ideértve a TSF ellenőrzése alá eső egyedek biztonsági tulajdonságait.
- AGD_ADM.1.7C Az adminisztrátori útmutatónak konzisztensnek kell lennie minden más, értékeléshez beadott dokumentációval.
- AGD_ADM.1.8C Az adminisztrátori útmutatónak le kell írnia minden olyan, az informatikai környezetre vonatkozó biztonsági követelményt, mely az adminisztrátor számára fontos.

Értékelői feladatelemek:

- AGD_ADM.1.1E Az értékelőnek meg kell győződnie arról, hogy a rendelkezésére bocsátott információk megfelelnek-e a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

AGD_USR.1 Felhasználói útmutató

Fejlesztői feladatok:

- AGD_USR.1.1D A fejlesztőnek a TOE felhasználói számára felhasználói útmutatót kell készítenie és átadnia.

A bizonyíték elemek tartalma és bemutatása:

- AGD_USR.1.1C A felhasználói útmutatónak le kell írnia a TOE nem adminisztrátor felhasználói rendelkezésére álló funkciókat és interfészeket.
- AGD_USR.1.2C A felhasználói útmutatónak le kell írnia, hogy a TOE által a felhasználók számára hozzáférhető biztonsági funkciókat hogyan kell biztonságosan használni.
- AGD_USR.1.3C A felhasználói útmutatónak tartalmaznia kell azon felhasználók által hozzáférhető funkciókkal és jogosultságokkal kapcsolatos figyelmeztetéseket, melyeket egy biztonságos üzemeltetési környezetben ellenőrzés alatt kell tartani.
- AGD_USR.1.4C A felhasználói útmutatónak egyértelműen be kell mutatnia minden felhasználói feladatot, mely a TOE biztonságos üzemeltetéséhez szükséges, ideértve azokat, melyek a TOE biztonsági környezetére vonatkozó leírásban található feltételezésekhez kapcsolódnak és a felhasználói viselkedést írják le.
- AGD_USR.1.5C A felhasználói útmutatónak konzisztensnek kell lennie minden más, értékeléshez beadott dokumentációval.
- AGD_USR.1.6C A felhasználói útmutatónak le kell írnia minden olyan, az informatikai környezetre vonatkozó biztonsági követelményt, mely a felhasználó számára fontos.

Értékelői feladatelemek:

- AGD_USR.1.1E Az értékelőnek meg kell győződnie arról, hogy a rendelkezésére bocsátott információk megfelelnek-e a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

Az életciklus támogatás értékelése

ALC_DVS.1 A biztonsági intézkedések azonosítása

Fejlesztői feladatok:

- ALC_DVS.1.1D A fejlesztőnek a fejlesztés biztonságáról dokumentációt kell készítenie.

A bizonyíték elemek tartalma és bemutatása:

- ALC_DVS.1.1C A fejlesztés biztonságáról szóló dokumentációnak le kell írnia minden olyan fizikai, eljárásbeli, személyi és egyéb biztonsági intézkedést, mely a TOE bizalmasságának és sértetlenségének a védelméhez szükséges, annak tervezési, megvalósítási és fejlesztési környezetében.
- ALC_DVS.1.2C A fejlesztési biztonságról szóló dokumentációnak bizonyítékot kell szolgáltatnia arról, hogy ezeket az intézkedéseket betartják a TOE fejlesztése és támogatása során.

Értékelői feladatelemek:

- ALC_DVS.1.1E Az értékelőnek meg kell győződnie arról, hogy a rendelkezésére bocsátott információk megfelelnek-e a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.
- ALC_DVS.1.2E Az értékelőnek meg kell győződnie arról, hogy a biztonsági intézkedéseket betartják.

A tesztelés értékelése

ATE_COV.2 A teszt lefedettség elemzése

Fejlesztői feladatok:

- ATE_COV.2.1D A fejlesztőnek a teszt lefedettségére vonatkozó elemzést kell szolgáltatnia.

A bizonyíték elemek tartalma és bemutatása:

- ATE_COV.2.1C A teszt lefedettség elemzése mutassa be a tesztelési dokumentációban azonosított tesztek és a funkcionális specifikációban leírt TOE biztonsági funkciók közötti megfeleltetést.
- ATE_COV.2.2C A teszt lefedettség elemzésének be kell mutatnia, hogy a funkcionális specifikációban leírt TOE biztonsági funkciók és a tesztelési dokumentációban azonosított tesztek közötti megfeleltetés teljes.

Értékelői feladatelemek:

- ATE_COV.2.1E Az értékelőnek meg kell győződnie arról, hogy a rendelkezésére bocsátott információk megfelelnek-e a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ATE_DPT.1 A magas szintű terv tesztelése

Fejlesztői feladatok:

- ATE_DPT.1.1D A fejlesztőnek gondoskodnia kell a tesztelés mélységének elemzéséről.

A bizonyítékok tartalma és bemutatása:

- ATE_DPT.1.1C A tesztelés mélység elemzése mutassa be, hogy a tesztelési dokumentációban azonosított tesztek elegendőek a biztonsági funkciók magas szintű tervnek megfelelő működésének a demonstrálásához.

Értékelői feladatelemek:

- ATE_DPT.1.1E Az értékelőnek meg kell győződnie arról, hogy a rendelkezésére bocsátott információk megfelelnek-e a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ATE_FUN.1 Funkcionális tesztelés

Fejlesztői feladatok:

- ATE_FUN.1.1D A fejlesztőnek le kell tesztelnie a TOE biztonsági funkcióit, és dokumentálnia kell az eredményeket.
- ATE_FUN.1.2D A fejlesztőnek el kell készítenie, és át kell adnia a tesztelési dokumentációt.

A bizonyítékok tartalma és bemutatása:

- ATE_FUN.1.1C A tesztelési dokumentációnak tartalmaznia kell a tesztelési terveket, a teszt eljárások leírását, a várt teszteredményeket és a tényleges tesztelési eredményeket.
- ATE_FUN.1.2C A tesztelési terveknek azonosítaniuk kell a tesztelendő biztonsági funkciókat, és le kell írniuk a végrehajtandó tesztek célját.
- ATE_FUN.1.3C A teszt eljárások leírásának azonosítania kell a végrehajtandó teszteket, és le kell írnia a tesztelési forgatókönyvet minden biztonsági funkcióra. A forgatókönyveknek tartalmazniuk kell minden, a tesztek sorrendiségére vonatkozó függőséget.
- ATE_FUN.1.4C A várt teszteredményeknek meg kell mutatniuk a tesztek sikeres végrehajtásából keletkező várható kimenteket.
- ATE_FUN.1.5C A fejlesztő által elvégzett tesztelés eredményeinek be kell mutatniuk, hogy minden tesztelt biztonsági funkció a specifikált módon működött.

Értékelői feladatelemek:

- ATE_FUN.1.1E Az értékelőnek meg kell győződnie arról, hogy a rendelkezésére bocsátott információk megfelelnek-e a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ATE_IND.2 Független tesztelés - mintavételezés

Fejlesztői feladatok:

- ATE_IND.2.1D A fejlesztőnek át kell adnia a TOE-t tesztelésre.

A bizonyítékok tartalma és bemutatása:

- ATE_IND.2.1C A TOE-nek tesztelésre alkalmas állapotban kell lennie.
- ATE_IND.2.2C A fejlesztőnek biztosítania kell a TSF fejlesztői funkcionális tesztelése során használt erőforrás-készlettel ekvivalens eszközkészletet.

Értékelői feladatelemek:

- ATE_IND.2.1E Az értékelőnek meg kell győződnie arról, hogy a rendelkezésére bocsátott információk megfelelnek-e a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.
- ATE_IND.2.2E Az értékelőnek tesztelnie kell a TSF megfelelő részeit annak megállapításához, hogy a TOE a specifikáltnak megfelelően működik-e.
- ATE_IND.2.3E Az értékelőnek végre kell hajtania a tesztelési dokumentációban szereplő tesztek valamely részhalmazát (mintáját) a fejlesztői teszt eredmények ellenőrzése érdekében.

A sebezhetőség felmérése

AVA_MSU.1 Útmutatók vizsgálata

Fejlesztői feladatok:

- AVA_MSU.1.1D A fejlesztőnek el kell készítenie az útmutató dokumentációkat.

A bizonyíték elemek tartalma és bemutatása:

- AVA_MSU.1.1C Az útmutatónak azonosítani kell a TOE összes lehetséges üzemmódját (beleértve a meghibásodás vagy üzemhiba utáni műveleteket), és azok biztonságos üzemeltetésre gyakorolt kihatásait és következményeit.
- AVA_MSU.1.2C Az útmutatónak teljesnek, egyértelműnek, következetesnek és megalapozottnak kell lennie.
- AVA_MSU.1.3C Az útmutatónak fel kell sorolnia minden feltételezést a leendő üzemi környezetről.
- AVA_MSU.1.4C Az útmutatónak számba kell vennie a külső biztonsági intézkedésekkel kapcsolatos minden követelményt (ideértve a külső eljárásbeli, fizikai és személyi intézkedéseket).

Értékelői feladatelemek:

- AVA_MSU.1.1E Az értékelőnek meg kell győződnie arról, hogy a rendelkezésére bocsátott információk megfelelnek-e a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.
- AVA_MSU.1.2E Az értékelőnek meg kell ismételnie minden konfigurációs és telepítési eljárást, annak megállapítása érdekében, hogy a TOE kizárólag az átadott útmutató dokumentáció alapján biztonságosan konfigurálható és használható.
- AVA_MSU.1.3E Az értékelőnek meg kell határoznia, hogy az útmutató dokumentáció használatával észrevehető-e minden nem biztonságos állapot.

AVA_SOF.1 Az értékelés tárgya biztonsági funkcióinak erősségértékelése

Fejlesztői feladatok:

- AVA_SOF.1.1D A fejlesztőnek a biztonsági előirányzatban definiált minden funkcióerősségi követelménnyel rendelkező mechanizmusra el kell végeznie egy biztonsági funkcióerősség elemzést.

A bizonyíték elemek tartalma és bemutatása:

- AVA_SOF.1.1C Minden TOE biztonsági funkcióerősségi követelménnyel rendelkező mechanizmus esetén az elemzésnek meg kell mutatnia, hogy a funkció erőssége azonos vagy magasabb szintű annál, amely a védelmi profilban / biztonsági előirányzatban minimális erősségi szintként szerepel.
- AVA_SOF.1.2C Minden TOE biztonsági funkcióerősségi követelménnyel rendelkező mechanizmus esetén az elemzésnek meg kell mutatnia, hogy a funkció erőssége azonos vagy magasabb szintű, mint a védelmi profilban / biztonsági előirányzatban megadott minimális erősségi mérték.

Értékelői feladatelemek:

- AVA_SOF.1.1E Az értékelőnek meg kell győződnie arról, hogy a rendelkezésére bocsátott információk megfelelnek-e a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.
- AVA_SOF.1.2E Az értékelőnek meg kell győződni arról, hogy az erősségi követelmények helyesek.

A MIBÉTS séma fokozott garanciaszintjén elvárt (szigorított) AVA_VLA.1 garanciaösszetevőt a továbbiakban AVA_VLA.1+ -gyel jelöljük.

AVA_VLA.1+ A sebezhetőség független elemzése

Fejlesztői feladatok*:*

- AVA_VLA.1+.1D A fejlesztőnek végre kell hajtania és dokumentálnia kell a TOE anyagok elemzését, olyan nyilvánvaló módszerek után kutatva, melyekkel egy felhasználó megsértheti a TSP-t.
- AVA_VLA.1+.2D A fejlesztőnek dokumentálnia kell a nyilvánvaló sebezhetőségek kiküszöbölését.

A bizonyíték elemek tartalma és bemutatása:

- AVA_VLA.1+.1C A dokumentációnak meg kell mutatnia minden azonosított sebezhetőség esetén, hogy azzal a TOE célkörnyezetben nem lehet visszaélni

Értékelői feladatelemek:

- AVA_VLA.1+.1E Az értékelőnek meg kell győződnie arról, hogy a rendelkezésére bocsátott információk megfelelnek-e a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.
- AVA_VLA.1+.2E Az értékelőnek a fejlesztői sebezhetőségi elemzés alapján le kell folytatnia az áthatolás tesztelést, annak biztosítása érdekében, hogy a nyilvánvaló sebezhetőségeket valóban kivédték.
- AVA_VLA.1+.3E Az értékelőnek a rendelkezésére bocsátott értékelési bizonyítékok alapján végre kell hajtania a független sebezhetőségi elemzést.
- AVA_VLA.1+.4E Az értékelőnek független áthatolás tesztelést kell elvégeznie a független sebezhetőségi elemzés alapján, a célkörnyezetben feltételezhető további azonosított sebezhetőségek kihasználhatóságának meghatározása céljából.
- AVA_VLA.1+.5E Az értékelőnek meg kell határoznia, hogy a TOE ellenáll-e egy alacsony támadási képességgel bíró támadó által végrehajtott áthatolási támadásnak.

6 TOE összefoglaló előírás

6.1 Biztonsági funkciók

A TOE összefoglaló előírás a mySigno biztonsági követelményeit teljesítő biztonsági funkciókat tartalmazza. Leírja a mySigno összes biztonsági funkcióját és garanciális intézkedését, amelyek a TOE biztonsági követelményeinek a kielégítéséhez járulnak hozzá.

6.1 A TOE biztonsági funkciói

A biztonsági követelmények teljesítése érdekében a TOE az alábbi biztonsági funkciókat valósítja meg:

BF1 A felhasználó azonosítása és hitelesítése
BF2 Aláírás létrehozása
BF3 Digitális aláírás ellenőrzése
BF4 Biztonságos üzenetváltás
BF5 Elektronikus aláírás kezdeti ellenőrzése
BF6 Elektronikus aláírás utólagos ellenőrzése
BF7 A TSF védelme

BF1 A felhasználó azonosítása és hitelesítése

A magánkulcshoz való hozzáférés érdekében az aláíró félnek azonosítania/hitelesítenie kell magát.
Kliens oldalon az értékelés hatáskörébe eső életciklus során a TOE felhasználó:

- az ügynök (aláíró);

A szerver oldalon az értékelés hatáskörébe eső életciklus során a TOE felhasználó:

- az ellenőrző felet reprezentáló automatikus folyamat.

BF1.1 Felhasználó azonosítása és hitelesítése
PDA kliensen aláíró (ügynök) azonosítása/hitelesítése:

- kliens oldalon a magánkulcshoz való hozzáféréshez szükséges PIN kód megadásával.

Szerver oldalon az ellenőrző felet reprezentáló automatikus folyamat azonosítása/hitelesítése az IT környezetet biztosító operációs rendszerhez szükséges azonosítás és hitelesítés valósítja meg.

BF1.2 Magánkulcshoz való hozzáférés korlátozása és menedzsmentje
Ügynök magánkulcs védelme:
A TOE hatáskörén kívül, telepítéskor megadott, a magánkulcshoz való hozzáféréshez szükséges 6 hosszú betű/szám kombinációjú PIN kód három egymást követő sikertelen megadási kísérlete esetén a mySigno v1.0 törli a magánkulcsot.

BF2 Aláírás létrehozása

Ez a biztonsági funkció hozza létre az ügynök által kiválasztott csomagra az elektronikus aláírást. Ehhez elkészíti a lenyomatot, amire az aláírást készíti, az aláírás létrehozás számára elfogadható formátumra hozza.
Az aláírás létrehozása során az aláírandó adatokra alkalmazott lenyomatoló algoritmus: SHA-1 [FIPS 180-1].
A lenyomatkészítés előtt a mySigno v1.0 egyértelműen jelzi az ügynöknek, hogy a PDA eszköz kijelzőjén látható csomagra fokozott biztonságú aláírás készül, amely jelzésre az ügynöknek pozitív választ kell adnia.

A mySigno v1.0 lehetőséget biztosít a hatáskörén kívül eső életciklus fázisban telepített külső megjelenítő alkalmazások meghívására.
A mySigno v1.0 aláírás előtt megvizsgálja a kapott dokumentum kiterjesztését, és amennyiben az aláírási szabályzatban meghatározott formátumok közül egyikkel sem egyezik, akkor nem hajtja végre az aláírandó dokumentumokhoz való hozzáadását.

A mySigno v1.0 az aláírás előtt lehetőséget ad az aláíró tanúsítvány adatainak (név, kibocsátó, érvényességi idő) megtekintésére.

Az ügynöknek az aláírás létrehozására adott pozitív válasza és a **BF1** biztonsági funkcióban specifikált hitelesítése után a TOE elektronikus aláírást hoz létre a számított lenyomatra az RSA kriptográfiai algoritmussal, 1024 bit kulcshosszal, a PKCS#1 v1.5-nek megfelelően.
Az aláírást a mySigno v1.0 az alábbi szabályok alapján készíti el:

- Az elektronikus aláírásban csak az **aláíró tanúsítvány azonosítója** szükséges.
- A [keyinfo] elemben csak az **aláíró tanúsítvány**t kell megadni.
- A kötelező aláírási tulajdonságok:
  - **Aláírás ideje**
  - **Aláírási szabályzat azonosítója**
  - **Aláírói tanúsítvány**

BF3 Digitális aláírás ellenőrzése

A mySigno v1.0 képes a **„BF2 Aláírás létrehozás”** alatt meghatározottak szerint létrehozott digitális aláírás ellenőrzésére. A folyamat kiszámítja az aláírt adat lenyomatát, majd az ügynök nyilvános kulcs tanúsítványában található nyilvános kulcs és az RSA/1024 algoritmus felhasználásával ellenőrzi a digitális aláírás értéket, valamint a nyilvános kulcs tanúsítvány érvényességi idejét. Amennyiben a kiszámított lenyomat és a digitális aláírás ellenőrzése során kapott érték megegyezik és a tanúsítvány érvényességi idejébe beleesik a PDA eszköz által szolgáltatott idő, akkor a digitális aláírás érték helyes.
A funkció további ellenőrzéseket nem végez.

BF4 Biztonságos üzenetváltás

A kliens a szerverrel kommunikál az 1. ábrán látható kommunikációs csatornán. Ez a biztonsági funkció a kliens és a szerver közötti kommunikáció bizalmasságáról, sértetlenségéről és hitelességéről gondoskodik.

Csomag szinkronizálás ((kliens)

BF4.1 Üzenet aláírása (PDA kliens hitelesítése)

- elektronikus aláírás RSA/1024 algoritmussal és kulcshosszal a továbbított csomag sértetlenségének biztosításához és a PDA eszköz azonosításához (Ehhez az eszközön tárolt magánkulcsra van szükség. Az aláírás ellenőrzése a szerver oldalon történik, ott az eszköz nyilvános kulcsához kell hozzáférni a csomag feldolgozó folyamatnak.)

BF4.2 Üzenet rejtjelezése (PDA kliens oldalon)

- RSA/1024 algoritmus és kulcshossz a TOE által titkosítandó csomag szimmetrikus kulcsának rejtjelezéséhez
- AES/256 titkosító kulcs a továbbítandó csomag rejtjelezéséhez

Frissítés letöltése és visszaigazolás küldése

BF4.3 Üzenet aláírása (szerver hitelesítése)

- elektronikus aláírás RSA/1024 algoritmussal és kulcshosszal a továbbított csomag sértetlenségének biztosításához és a szerver azonosításához (Ehhez az eszközön tárolt magánkulcsra van szükség. Az aláírás ellenőrzése a kliens oldalon történik, ott a szerver nyilvános kulcsához kell hozzáférni a csomag feldolgozó folyamatnak.)

BF4.4 Üzenet rejtjelezése (szerver oldalon)

- RSA/1024 algoritmus és kulcshossz a TOE által titkosítandó csomag szimmetrikus kulcsának rejtjelezéséhez
- AES/256 titkosító kulcs a továbbítandó csomag rejtjelezéséhez

BF4.5 Kliens üzenet megoldása és hitelesítése

A **mySigno szerver** a rajta tárolt magánkulccsal megoldja a kommunikációs kulcsot RSA/1024 algoritmussal, majd a kommunikációs kulccsal a kapott üzenetet (AES/256).

A **mySigno szerver** a PDA kliens nyilvános kulcsával ellenőrzi az üzenet hitelességét.

A szerver a PDA kliens nyilvános kulcsához a TOE IT környezetéhez tartozó, a beérkezett csomagok és egyéb ellenőrzéshez szükséges információkat tartalmazó adatbázis felé való kommunikációt biztosító interfészen fér hozzá.

BF4.6 Szerver üzenet megoldása és hitelesítése

A **PDA kliens** a rajta tárolt eszköz magánkulccsal megoldja a kommunikációs kulcsot RSA/1024 algoritmussal, majd a kommunikációs kulccsal a kapott üzenetet (AES/256).

A PDA kliens a szerver nyilvános kulcsával ellenőrzi az üzenet hitelességét.

A szerver nyilvános kulcsához való hozzáféréshez a PDA kliens telepítése során a szerver üzenet hitelesítéshez használt kulcspárjának nyilvános kulcs tanúsítványát importálni kell.

BF5 Aláírás kezdeti ellenőrzése

A kezdeti ellenőrzés a TOE szerver oldali összetevője köré épülő IT környezet (hosztalkalmazás) által fogadott csomagban szereplő aláírás első ellenőrzése, melyet a csomag fogadása után a lehető leghamarabb végre kell hajtani.
A TOE ellenőrzi, hogy szerepelnek-e a kötelező aláírási tulajdonságok, majd –amennyiben nem talál–, **időbélyeget kér** az aláírási szabályzat által kijelölt időbélyegzés szolgáltatótól az ügynök aláírás adott időben való meglétének bizonyításához.
Az időbélyeg válasz érvényesítése esetén az időbélyeget a TOE a csomagba foglalja.

Amennyiben a funkció talál érvényes időbélyeget, akkor a biztonsági funkció a kezdeti ellenőrzés második lépését hajtja végre, azaz összegyűjti az aláírás ellenőrzéséhez szükséges érvényesítő adatokat.
Az összegyűjtendő érvényesítő adatok:

- visszavonási információk;
- tanúsítványlánc információk.

A TOE végrehajtja az aláírás ellenőrzését a rendelkezésre álló érvényesítő adatok alapján, aminek a lehetséges kimenetele: sikeres, sikertelen, befejezetlen.
Befejezetlen státusz esetén a türelmi idő (amely paraméterként adható meg) eltelte után megismétli az adatok összegyűjtését az időbélyeghez képest legfrissebb visszavonási információk begyűjtése érdekében.

A funkció részeként a szerver oldali alkalmazás az aláírt PDA felől érkező csomagok tárolására szolgáló adatbázis felé küldés előtt ún. érkeztető aláírással látja el a csomagokat.

BF6 Aláírás utólagos ellenőrzése

Ez a biztonsági funkció hajtja végre a kezdeti ellenőrzés során összegyűjtött adatok alapján az aláírás utólagos ellenőrzését. Ehhez csak a már korábban összegyűjtött információkat használja. A funkció két állapottal tér vissza: sikeres vagy sikertelen (ez utóbbi akkor, ha nem építhető fel az útvonal a rendelkezésre álló adatokból, vagy van érvénytelen elem az útvonalban ezen adatok alapján).

BF7 A TSF védelme

A mySigno v1.0 a PIN kódot annak felhasználása után azonnal törli a memóriából, annak biztosítása érdekében, hogy más folyamatok még véletlenül se férhessenek hozzá.

6.1.12 SOF nyilatkozat

Egy biztonsági előirányzatnak azonosítania kell minden olyan mechanizmust, amelyet az AVA_SOF.1 garanciális követelmény szerint értékelni lehet.
A biztonsági funkciókhoz az alábbi olyan mechanizmusok járulnak hozzá, amelyeket valószínűségi vagy permutációs tulajdonságok alapján vizsgálni lehet:

- ügynök PIN kódja: 6 hosszú, betű és szám

A mySigno v1.0 esetén az elvárás: közepes SOF.

6.2 Garanciális intézkedések

A TOE az alábbi dokumentációkban megnevezett és leírt garanciális intézkedéseket valósítja meg:

Cím	verzió	fájl név
Biztonsági előirányzat	v1.0	mySigno_ST_v10.pdf
Aláírási szabályzat	v1.0	mySigno_A_Signature_Policy.doc
Funkcionális specifikáció	v1.0	mySigno_FS_v10.doc
Magas szintű terv	v1.0	mySigno _HLD_v10.doc
Megfeleltetés elemzések	v1.0	mySigno_RCR_v10.doc
Tesztelési dokumentáció - Adminisztrátori felület	v1.0	mySigno_Admin_Test_Documentation_v10.doc
Tesztelési dokumentáció - PDA modul	v1.0	mySigno_PDA_Test_Documentation_v10.doc
Tesztelési dokumentáció - szerver modul	v1.1	mySigno_Server_Test_Documentation.doc
Teszt lefedettség elemzés	v1.0	mySigno_Test_Coverage_Analysis_v10.doc
Teszt mélység elemzés	v1.0	mySigno_Test_Depth_Analysis_v10.doc
Adminisztrátori útmutató	v1.0	mySigno_Admin_v10.doc
A konfiguráció menedzselés dokumentációja	v1.0	mySigno_ACM_v10.doc
A fejlesztési biztonság dokumentációja	v1.0	mySigno_DVS_v10.doc
Biztonsági funkcióerősség elemzés	v1.0	mySigno _SOF_Analysis_v10.doc
Sebezhetőség elemzés	v1.0	mySigno_Vulnerability_Analysis_v10.doc
mySigno for PDA Specifikáció		Specification_final

7 Megfelelőségi nyilatkozat

Jelen biztonsági előirányzat PP megfelelőségi nyilatkozatot nem tesz.

8 Indoklások

8.1 A biztonsági célok indoklása

8.1.1 A feltételezések leképezése a környezet biztonsági céljaira

Az alábbi három táblázat bemutatja, hogy minden feltételezéshez tartozik környezeti biztonsági cél.

8.1 táblázat
Az általános feltételezések leképezése a környezeti biztonsági célokra

Feltételezés	**Környezeti biztonsági cél**	**Teljesítő követelmény**
A.Init_PDA	**OE.Trusted_Security_Admin** **OE.Trusted_EnvCode**	ADO_IGS.1 AGD_ADM.1
A.PDA_Physical_Security	**OE.UserGuide**	AGD_USR.1
A.Signer_Only	**OE.UserGuide**	AGD_USR.1
A.Host_PDA_Machine	**OE.Host_PDA_Machine**	ADO_IGS.1 ADO_ADM.1 ADO_USR.1
A.Separation_and_Exclusion	**OE.Separation_and_Exclusion**	FPT_RVM.1 FPT_SEP.1 ADO_IGS.1
A.AccessControl	**OE.UserGuide**	AGD_USR.1
A.Trusted_Security_Administrator	**OE.Trusted_Security_Admin**	AGD_ADM.1
A.Services_Integrity	**OE.Services_Integrity**	ADO_IGS.1 AGD_ADM.1 (ehelyett: fejlesztői útmutató)
A.Packet_Viewers	**OE.Packet_Viewers**	ADO_IGS.1 AGD_ADM.1

8.2 táblázat
Az aláírás létrehozásával kapcsolatos feltételezések leképezése a környezeti biztonsági célokra

Feltételezés	Környezeti biztonsági cél	Teljesítő követelmény
A.Signatory_Presence	**OE.Signatory_Presence**	AGD_USR.1
A.Physical_Security	**OE.Physical_Security**	AGD_USR.1 ADO_IGS.1

8.3 táblázat
Az aláírás ellenőrzésével kapcsolatos feltételezések leképezése a környezeti biztonsági célokra

Feltételezés	Környezeti biztonsági cél	Teljesítő követelmény
A.Host_Server_Machine	**OE.Host_Server_Machine**	AGD_ADM.1
A.Access_to_Validation_Data	**OE.Validation_Data_Provisio n**	

8.1.2 A szervezeti biztonsági szabályok leképezése a biztonsági célokra

Az alábbi három táblázat bemutatja, hogy minden szervezeti biztonsági szabályhoz tartozik környezeti biztonsági cél.

8.4 táblázat
Az általános szervezeti biztonsági szabályok leképezése a biztonsági célokra

Szervezeti biztonsági szabály	Biztonsági cél
P.Hash_Algorithm	**O.Cryptographic_Support**
P.Signature_Algorithm	**O.Cryptographic_Support**
P.Fix_Signature_Policy	**O.Fix_Signature_Policy**
P.Communication	**O.Communication**

8.5 táblázat
Az aláírás létrehozására vonatkozó szervezeti biztonsági szabályok leképezése a biztonsági célokra

P.Key_Cert_Storage	**O.Signature_Creation**
P.Signature_Certificate_Conformance	**O.Conform_Certificate**
P.Signing_Certificate_Validity	**O.Valid_Signing_Certificate**
P.Signature_Attributes_Conformance	**O.Conform_Attributes**
P.Document_Presentation_Possibility	**O.Packet_Content_Presentation**
P.Signature_Attributes_Presentation	**O.Presentation_Conformance_Attributes**
P.Explicit_Consent	**O.Explicit_Consent** **O.Signer_Document**
P.Certificate_Privatekey_Association	**O.Association_Certificate_and_PrivateKey**
P.Electronic_Signature_Export	**O.Electronic_Signature_Export**

8.6 táblázat
Az aláírás ellenőrzésére vonatkozó szervezeti biztonsági szabályok leképezése a biztonsági célokra

P.Signatory_Certificate_Validity	**O.Time_Stamp** **O.Valid_Certificates**
P.Signature_Attributes_Conformance	**O.Conform_Signing_Attributes**
P.Signatory_Certificate_Conformance	**O.Conform_Certificates**
P.Authentic_Signatory_Certificate	**O.Certificate_Path**
P.Validation_Data_Authenticity_Integrity	**O.Conform_Validation_Data**
P.Communication_Signing_Attributes	**O.Communication_Signing_Attributes**
P.Validation_Data_Export	**O.Validation_Data_Export**

8.2 A funkcionális biztonsági követelmények indoklása

Ezen alfejezet táblázatai a biztonsági célokat feleltetik meg a funkcionális követelményeknek. A táblázatból látható, hogy minden biztonsági cél teljesítéséhez hozzájárul egy vagy több biztonsági cél.

8.7 táblázat
Az általános biztonsági célok és a funkcionális követelmények megfeleltetése

Biztonsági cél	**Funkcionális követelmény**
O.Cryptographic_Support	**FCS_COP.1/Aláírás létrehozás** **FCS_COP.1/Aláírás ellenőrzés** **FCS_COP.1.1/Lenyomat**
O.Fix_Signature_Policy	**FDP_ACC.1/Aláírás létrehozása** **FDP_ACF.1/Aláírás létrehozása** **FDP_IFF.1.1/Tanúsítási útvonal** **FDP_MRU.1/Tanúsítási útvonal** **FDP_IFF.1/ Időbélyeg** **FDP_IFF.1/Elektronikus aláírás importálása**
O.Communication	**FCS_COP.1/SecMsg_PDA** **FCS_COP.1/SecMsg_MySignoServer** **FTP_ITC.1 TSF-ek közötti megbízható csatorna**

8.8 táblázat
Az aláírás létrehozásával kapcsolatos biztonsági célok és funkcionális követelmények megfeleltetése

Biztonsági cél	Funkcionális követelmény
O.Association_Certificate_and_PrivateKey	FDP_ACC.1/Aláírás létrehozása FDP_ACF.1/Aláírás létrehozása FIA_UID.1/Aláíró FIA_UAU.Aláíró FIA_AFL. Hitelesítési hibák kezelése
O.Presentation_Conformance_Attributes	FDP_ACC.1/Aláírás létrehozása FDP_ACF.1/Aláírás létrehozása
O.Explicit_Consent	FDP_ITC.1/Explicit aláírói jóváhagyás
O.Signer_Document	FDP_IFF.1/Csomag jóváhagyás – Egyszerű biztonsági tulajdonságok
O.Conform_Certificate	FDP_ACC.1/Aláírás létrehozása FDP_ACF.1/Aláírás létrehozása FPT_TDC.1/Aláíró tanúsítványa FMT_SMF.1/Aláírói tanúsítvány megtekintése
O.Valid_Signing_Certificate	FDP_ACC.1/Aláírás létrehozása FDP_ACF.1/Aláírás létrehozása FPT_TDC.1/Aláíró tanúsítványa FMT_SMF.1/Aláírói tanúsítvány megtekintése
O.Conform_Attributes	FDP_ACC.1/Aláírás létrehozása FDP_ACF.1/Aláírás létrehozása FMT_MSA.3/Aláírás létrehozás FMT_MSA.1/Aláírási tulajdonságok
O.Electronic_Signature_Export	FDP_ACC.1/Elektronikus aláírás csatolása FDP_ACF.1/Elektronikus aláírás csatolása FMT_MSA.3/ Elektronikus aláírás csatolása FMT_MSA.1/Aláírás létrehozási státusz FMT_SMF.1/Az aláírás létrehozási státusz megállapítása
O.Packet_Content_Presentation	FDP_ACC.1/Aláírás létrehozása FDP_ACF.1/Aláírás létrehozása FDP_IFC.1/Csomag jóváhagyás FDP_IFC.1/Csomag jóváhagyás
O.Signature_Creation	FDP_ACC.1/Aláírás létrehozása FDP_ACF.1/Aláírás létrehozása FIA_UID.1/Aláíró Az azonosítás időzítése FIA_UAU.1/Aláíró A hitelesítés időzítése FIA_ATD.1 Felhasználói tulajdonságok megadása

8.9 táblázat
Az aláírás létrehozásával kapcsolatos biztonsági célok és funkcionális követelmények megfeleltetése

Biztonsági cél	Funkcionális követelmény
O.Time_Stamp	**FDP_IFC.1/Időbélyeg** **FDP_IFF.1/Időbélyeg** **FMT_MSA.3/ Időbélyeg** **FMT_MSA.1/ Időbélyeg** **FDP_ITC.2/ Időbélyeg** **FPT_TDC.1/Időbélyeg**
O.Valid_Certificates	**FDP_IFC.1/Tanúsítási útvonal** **FDP_IFF.1/Tanúsítási útvonal** **FDP_MRU.1/Tanúsítási útvonal** **FMT_MSA.3/Tanúsítási útvonal** **FDP_ITC.2/Tanúsítási útvonal** **FPT_TDC.1/ Tanúsítvány visszavonási adatok** **FMT_MSA.1/Tanúsítványok** **FMT_MSA.1/Tanúsítványok érvényesítő adatai**
O.Conform_Signing_Attributes	**FDP_IFC.1/Elektronikus aláírás importálása** **FDP_IFF.1/Elektronikus aláírás importálása** **FMT_MSA.3/Elektronikus aláírás importálása** **FMT_MSA.1/Elektronikus aláírás importálása** **FPT_TDC.1/Elektronikus aláírás**
O.Conform_Certificates	**FDP_IFC.1/Tanúsítási útvonal** **FDP_IFF.1/Tanúsítási útvonal** **FDP_MRU.1/Tanúsítási útvonal** **FMT_MSA.3/Tanúsítási útvonal** **FDP_ITC.2/Tanúsítási útvonal** **FPT_TDC.1/ Tanúsítvány visszavonási adatok** **FPT_TDC.1/ Tanúsítványok**
O.Certificate_Path	**FDP_IFC.1/Tanúsítási útvonal** **FDP_IFF.1/Tanúsítási útvonal** **FDP_MRU.1/Tanúsítási útvonal** **FMT_MSA.3/Tanúsítási útvonal** **FDP_ITC.2/Tanúsítási útvonal** **FPT_TDC.1/ Tanúsítvány visszavonási adatok**

O.Conform_Validation_Data	**FDP_IFC.1/Tanúsítási útvonal** **FDP_IFF.1/Tanúsítási útvonal** **FDP_MRU.1/Tanúsítási útvonal** **FMT_MSA.3/Tanúsítási útvonal** **FDP_ITC.2/Tanúsítási útvonal** **FPT_TDC.1/ Tanúsítvány visszavonási adatok**
O.Communication_Signing_Attributes	**FDP_IFF.1/ Elektronikus aláírás importálása**
O.Validation_Data_Export	**FDP_IFC.1/Elektronikus aláírás érvényesség ellenőrzése** **FDP_IFF.1/Elektronikus aláírás érvényesség ellenőrzése** **FMT_MSA.3/Aláírás érvényesség ellenőrzés státusz** **FMT_MSA.1/ Aláírás érvényesség ellenőrzés státusz** **FDP_ETC.2/Ellenőrzési státusz**

8.10 táblázat – A funkcionális követelmények közötti függések

Követelmény	**CC által megkövetelt függések és teljesülésük, illetve a nem teljesülés indoklása**
Aláírás létrehozása	
FDP_IFC.1/Csomag jóváhagyás	FDP_IFF.1/Csomag jóváhagyás - teljesül
FDP_IFF.1/Csomag jóváhagyás	FDP_IFC.1/Csomag jóváhagyás – teljesül FMT_MSA.3/Csomag jóváhagyás – teljesül
FMT_MSA.3/Csomag jóváhagyás	FMT_MSA.1/Csomag jóváhagyás – teljesül FMT_SMR.1- lásd 1. sz. megjegyzést
FMT_MSA.1/Csomag jóváhagyás	FDP_IFC.1/Csomag jóváhagyás – teljesül FMT_SMR.1- lásd 1. sz. megjegyzést FMT_SMF.1.1/Csomag kiválasztása aláírásra – teljesül
FMT_SMF.1.1/Csomag kiválasztása aláírásra – teljesül	Nincs
FMT_MSA.1/Aláírási tulajdonságok	FDP_ACC.1/Aláírás létrehozása - teljesül FMT_SMF.1/Aláírói tanúsítvány kiválasztása/megtekintése - teljesül FMT_SMR.1- lásd 1. sz. megjegyzést
FMT_SMF.1/Aláírói tanúsítvány kiválasztása/megtekintése	Nincs
FPT_TDC.1/Aláíró tanúsítványa	Nincs
FDP_ACC.1/Aláírás létrehozása	FDP_ACF.1/Aláírás létrehozása - teljesül
FDP_ACF.1/Aláírás létrehozása	FDP_ACC.1/Aláírás létrehozása - teljesül FMT_MSA.3/Aláírás létrehozás – teljesül
FMT_MSA.3/Aláírás létrehozás	FMT_MSA.1/Aláírási tulajdonságok – teljesül FMT_SMR.1- lásd 1. sz. megjegyzést
FDP_ITC.1/Explicit aláírói jóváhagyás	FDP_ACC.1/Aláírás létrehozása - teljesül FMT_MSA.3/Aláírás létrehozás – teljesül

FDP_ACC.1/Elektronikus aláírás csatolása	FDP_ACF.1/Elektronikus aláírás csatolása – teljesül
FDP_ACF.1/Elektronikus aláírás csatolása	FDP_ACC.1/Elektronikus aláírás csatolása - teljesül FMT_MSA.3/ Elektronikus aláírás csatolása – teljesül
FMT_MSA.3/ Elektronikus aláírás csatolása	FMT_MSA.1/Aláírás létrehozási státusz - teljesül FMT_SMR.1- lásd 1. sz. megjegyzést
FMT_MSA.1/Aláírás létrehozási státusz	FDP_ACC.1/Elektronikus aláírás csatolása - teljesül FMT_SMF.1/Az aláírás létrehozási státusz megállapítása - teljesül FMT_SMR.1- lásd 1. sz. megjegyzést
FMT_SMF.1/Az aláírás létrehozási státusz megállapítása	Nincs
Aláírás ellenőrzése	
FDP_IFC.1/Elektronikus aláírás importálása	FDP_IFF.1/Elektronikus aláírás importálása – teljesül
FDP_IFF.1/Elektronikus aláírás importálása	FDP_IFC.1/Elektronikus aláírás importálása - teljesül FMT_MSA.3/Elektronikus aláírás importálása – teljesül
FMT_MSA.3/Elektronikus aláírás importálása	FMT_MSA.1/ Elektronikus aláírás importálása- teljesül FMT_SMR.1- lásd 1. sz. megjegyzést
FMT_MSA.1/Elektronikus aláírás importálása	FDP_IFC.1/Elektronikus aláírás importálása – teljesül FMT_SMF.1/ - nem teljesül, itt az ST nem követel meg biztonsági menedzsment funkciót. FMT_SMR.1- lásd 1. sz. megjegyzést
FDP_IFC.1/Időbélyeg	FDP_IFF.1/Időbélyeg – teljesül
FDP_IFF.1/Időbélyeg	FDP_IFC.1/Időbélyeg - teljesül FMT_MSA.3/ Időbélyeg – teljesül
FMT_MSA.3/Időbélyeg	FMT_MSA.1/ Időbélyeg - teljesül FMT_SMR.1- lásd 1. sz. megjegyzést FMT_MSA.1/Tanúsítványok - teljesül FMT_MSA.1/Tanúsítványok érvényesítő adatai - teljesül
FMT_MSA.1/Időbélyeg	FDP_IFC.1/Időbélyeg- teljesül FMT_SMF.1/ - nem teljesül, itt az ST nem követel meg biztonsági menedzsment funkciót. FMT_SMR.1- lásd 1. sz. megjegyzést
FDP_ITC.2/Időbélyeg	FDP_IFC.1/Időbélyeg - teljesül FPT_TDC.1/Időbélyeg – teljesül FPT_TDC.1/Tanúsítványok - teljesül FPT_TDC.1/Tanúsítvány visszavonási adatok – teljesül
FMT_MSA.1/Tanúsítványok	FDP_IFC.1/Tanúsítási útvonal - teljesül FMT_SMF.1/ - nem teljesül, itt az ST nem követel meg biztonsági menedzsment funkciót. FMT_SMR.1- lásd 1. sz. megjegyzést
FMT_MSA.1/Tanúsítványok érvényesítő adatai	FDP_IFC.1/Tanúsítási útvonal - teljesül FMT_SMF.1/ - nem teljesül, itt az ST nem követel meg biztonsági menedzsment funkciót. FMT_SMR.1- lásd 1. sz. megjegyzést
FDP_IFC.1/Tanúsítási útvonal	FDP_IFF.1/Tanúsítási útvonal – teljesül
FDP_IFF.1/Tanúsítási útvonal	FDP_IFC.1/Tanúsítási útvonal - teljesül FMT_MSA.3/Tanúsítási útvonal - teljesül

FDP_MRU.1/Tanúsítási útvonal Lásd még 3. sz. megjegyzést	FDP_IFC.1/Időbélyeg – teljesül FMT_MSA.3/ Időbélyeg – teljesül FDP_IFC.1/Tanúsítási útvonal - teljesül FMT_MSA.3/Tanúsítási útvonal - teljesül
FMT_MSA.3/Tanúsítási útvonal	FMT_MSA.1/Tanúsítványok - teljesül FMT_MSA.1/Tanúsítványok érvényesítő adatai - teljesül FMT_SMR.1- lásd 1. sz. megjegyzést
FDP_ITC.2/Tanúsítási útvonal	FDP_IFC.1/Tanúsítási útvonal - teljesül FPT_TDC.1/Tanúsítványok - teljesül FPT_TDC.1/ Tanúsítvány visszavonási adatok - teljesül
FPT_TDC.1/Elektronikus aláírás	Nincs
FPT_TDC.1/Időbélyeg	Nincs
FPT_TDC.1/Tanúsítványok	Nincs
FPT_TDC.1/ Tanúsítvány visszavonási adatok	Nincs
FDP_IFC.1/Elektronikus aláírás érvényesség ellenőrzése	FDP_IFF.1/Elektronikus aláírás érvényesség ellenőrzése – teljesül
FDP_IFF.1/Elektronikus aláírás érvényesség ellenőrzése	FDP_IFC.1/Elektronikus aláírás érvényesség ellenőrzése – teljesül FMT_MSA.3/Aláírás érvényesség ellenőrzés státusz – teljesül
FMT_MSA.3/Aláírás érvényesség ellenőrzés státusz	FMT_MSA.1/Aláírás érvényesség ellenőrzés státusz – teljesül FMT_SMR.1- lásd 1. sz. megjegyzést
FMT_MSA.1/ Aláírás érvényesség ellenőrzés státusz	FDP_IFC.1/Elektronikus aláírás érvényesség ellenőrzése – teljesül FMT_SMF.1/ - nem teljesül, itt az ST nem követel meg biztonsági menedzsment funkciót. FMT_SMR.1- lásd 1. sz. megjegyzést
FDP_ETC.2/Ellenőrzési státusz	FDP_IFC.1/Elektronikus aláírás érvényesség ellenőrzése - teljesül
Általános követelmények	
FCS_COP.1/Aláírás létrehozás	FCS_CKM.1 vagy FDP_ITC.1: Lásd 2. sz. megjegyzést FCS_CKM.4: Lásd 2. sz. megjegyzést FMT_MSA.2: Lásd 2. sz. megjegyzést
FCS_COP.1/Aláírás ellenőrzés	FCS_CKM.1 vagy FDP_ITC.1: Lásd 2. sz. megjegyzést FCS_CKM.4: Lásd 2. sz. megjegyzést FMT_MSA.2: Lásd 2. sz. megjegyzést
FCS_COP.1/Lenyomat	FCS_CKM.1 vagy FDP_ITC.1: Lásd 2. sz. megjegyzést FCS_CKM.4: Lásd 2. sz. megjegyzést FMT_MSA.2: Lásd 2. sz. megjegyzést
FIA_UID.1/Aláíró Az azonosítás időzítése	Nincs
FIA_UAU.1/Aláíró A hitelesítés időzítése	FIA_UID.1/Aláíró Az azonosítás időzítése – teljesül
FIA_AFL.1 Hitelesítési hibák kezelése	FIA_UAU.1/Aláíró A hitelesítés időzítése - teljesül
FIA_ATD.1 Felhasználói tulajdonságok megadása	Nincs
FDP_RIP.1 Részleges maradványinformáció védelem	Nincs
FCS_COP.1/SecMsg_PDA	FCS_CKM.1 vagy FDP_ITC.1: Lásd 2. sz. megjegyzést FCS_CKM.4: Lásd 2. sz. megjegyzést FMT_MSA.2: Lásd 2. sz. megjegyzést

FCS_COP.1/SecMsg_MySignoServer	FCS_CKM.1 vagy FDP_ITC.1: Lásd 2. sz. megjegyzést FCS_CKM.4: Lásd 2. sz. megjegyzést FMT_MSA.2: Lásd 2. sz. megjegyzést
FTP_ITC.1 TSF-ek közötti megbízható csatorna	Nincs

1. sz. megjegyzés: FMT_SMR.1 Biztonsági szerepkörök függés indokoltan nem teljesül, mert a mySigno v1.0 nem különböztet meg szerepköröket a hatáskörében. A ráépülő alkalmazásnak és a TOE életciklus előtti telepítési, konfigurálási eljárásoknak kell kezelnie az adminisztrátori feladatok elkülönítését.

2. sz. megjegyzés: Az FCS_COP.1 követelménnyel kapcsolatos függések kielégítése azért mellőzhető, mert a mySigno v1.0 ezen kriptográfiai műveleteknek a meghívását végzi, a függéseket jelentő követelmények teljesítésére akkor lenne szükség, ha ezen kriptográfiai funkcióknak a megvalósítása is a TOE hatáskörébe esne.

3. sz. megjegyzés: Az FDP_MRU.1 követelmény a CC v2.2 katalógusban nem szereplő explicit biztonsági követelmény, amelyre a TOE-vel kapcsolatos adatok biztonsági tulajdonságainak pontosabb specifikálása érdekében volt szükség, megfelelvén az alapul felhasznált védelmi profilnak.

8.3A garanciális biztonsági követelmények indoklása

A mySigno v1.0 számára választott fokozott (EAL 3+) értékelési garancia szint azt jelenti, hogy a fejlesztők a függetlenül garantált biztonság közepes szintjét követelik meg, a termék és a fejlesztői környezet mélyreható vizsgálatával.

A fokozott értékelési garancia szint a biztonsági viselkedésmódról következő bizonyítékokat szolgáltatja:

- Biztonsági funkciók analízise (Funkcionális Specifikáció)
- Útmutatók
- A TOE magas-szintű terve (HLD)
- A TOE biztonsági funkcióinak független tesztelése
- A fejlesztői tesztelés
- A fejlesztői teszteredmények független megerősítése
- A biztonsági funkciók erejének értékelése
- Fejlesztői sebezhetőség elemzés

8.4 Az összefoglaló előírás indoklása

A funkcionális biztonsági követelmények leképezése a biztonsági funkciókra

Az alábbi táblázat felsorolja a mySigno v1.0 összes biztonsági követelményét, és megmutatja, hogy minden követelményt teljesíti egy vagy több biztonsági funkció, illetve egy biztonsági funkció visszavezethető egy vagy több biztonsági követelményre.

	BF1 A felhasználó azonosítása és hitelesítése	**BF2 Aláírás létrehozása**	**BF3 Digitális aláírás ellenőrzése**	**BF4 Biztonságos üzenetváltás**	**BF5 Elektronikus aláírás kezdeti ellenőrzése**	**BF6 Elektronikus aláírás utólagos ellenőrzése**	**BF7 A TSF védelme**
FDP_IFC.1/Csomag jóváhagyás		**x**					
FDP_IFF.1/Csomag jóváhagyás		**x**					
FMT_MSA.3 Csomag jóváhagyás		**x**					
FMT_MSA.1 Csomag jóváhagyás		**x**					
FMT_MSA.1/Aláírási tulajdonságok		**x**					
FMT_SMF.1/Aláírói tanúsítvány kiválasztása/megtekintése		**x**					

FPT_TDC.1/Aláíró tanúsítványa		**x**	**x**				
FDP_ACC.1/Aláírás létrehozása		**x**					
FDP_ACF.1/Aláírás létrehozása		**x**					
FMT_MSA.3/Aláírás létrehozás		**x**					
FDP_ITC.1/Explicit aláírói jóváhagyás		**x**					
FDP_ACC.1/Elektronikus aláírás csatolása		**x**					
FDP_ACF.1/Elektronikus aláírás csatolása		**x**					
FMT_MSA.3/ Elektronikus aláírás csatolása		**x**					
FMT_MSA.1/Aláírás létrehozási státusz		**x**					
FMT_SMF.1/Az aláírás létrehozási státusz megállapítása		**x**					
FDP_IFC.1/Elektronikus aláírás importálása					**x**		
FDP_IFF.1/Elektronikus aláírás importálása					**x**		
FMT_MSA.3/Elektronikus aláírás importálása					**x**		
FMT_MSA.1/ Elektronikus aláírás importálása					**x**		
FDP_IFC.1/Időbélyeg					**x**		
FDP_IFF.1/Időbélyeg					**x**		
FMT_MSA.3/ Időbélyeg					**x**		
FMT_MSA.1/ Időbélyeg					**x**		
FDP_ITC.2/ Időbélyeg					**x**		
FMT_MSA.1/Tanúsítványok					**x**	**x**	
FMT_MSA.1/Tanúsítványok érvényesítő adatai					**x**	**x**	
FDP_IFC.1/Tanúsítási útvonal					**x**		
FDP_IFF.1/Tanúsítási útvonal					**x**		
FDP_MRU.1/Tanúsítási útvonal					**x**		
FMT_MSA.3/Tanúsítási útvonal					**x**		
FDP_ITC.2/Tanúsítási útvonal					**x**		
FPT_TDC.1/Elektronikus aláírás					**x**	**x**	
FPT_TDC.1/Időbélyeg					**x**	**x**	
FPT_TDC.1/Tanúsítványok					**x**	**x**	
FPT_TDC.1/ Tanúsítvány visszavonási adatok					**x**	**x**	
FDP_IFC.1/Elektronikus aláírás érvényesség ellenőrzése					**x**	**x**	
FDP_IFF.1/Elektronikus aláírás érvényesség ellenőrzése					**x**	**x**	
FMT_MSA.3/Aláírás érvényesség ellenőrzés státusz					**x**	**x**	
FMT_MSA.1/ Aláírás érvényesség ellenőrzés státusz					**x**	**x**	
FDP_ETC.2/Ellenőrzési státusz					**x**		
FCS_COP.1/Aláírás létrehozás		**x**					
FCS_COP.1/Aláírás ellenőrzés			**x**				

FCS_COP.1/Lenyomat		**x**	**x**		**x**	**x**	
FIA_UID.1/Aláíró Az azonosítás időzítése	**x**	**x**					
FIA_UAU.1/Aláíró A hitelesítés időzítése	**x**	**x**					
FIA_AFL.1 Hitelesítési hibák kezelése	**x**						
FIA_ATD.1 Felhasználói tulajdonságok megadása	**x**						
FMT_MSA.2 Biztonságos biztonsági tulajdonságok	**x**						
FMT_MSA.3Statikus tulajdonság-inicializálás	**x**						
FDP_RIP.1 Részleges maradványinformáció védelem							**x**
FCS_COP.1/SecMsg_PDA				**x**			
FCS_COP.1/SecMsg_MySignoServer				**x**			
FTP_ITC.1 TSF-ek közötti megbízható csatorna				**x**			

8.5 A TOE funkcióerősség indoklása

A biztonsági funkciókhoz az alábbi olyan mechanizmusok járulnak hozzá, amelyeket valószínűségi vagy permutációs tulajdonságok alapján vizsgálni lehet:

- ügynök PIN kód: 6 hosszú, betű és szám

Jelen TOE esetén az elvárás a közepes SOF. A PKCS#12-es tanúsítványban tárolt magánkulcshoz való hozzáféréshez szükséges 6 hosszúságú, betű és szám kombinációból álló hitelesítő adat (PIN) bonyolultsága (véletlenszerű PIN választást feltételezve) elegendő a közepes támadási potenciállal rendelkező támadókkal szemben.

9 Fogalmak

Aláírás dátuma
A digitális aláírás létrehozásának dátuma. A dátum tartalmazza a naptári dátumot és az időpontot. Az elfogadó félnek meg kell bíznia az aláírás dátumának pontosságában. A dátum lehet a tényleges dátum vagy egy feltételezett dátum. Az elfogadó fél feltételezheti, hogy az aláírás dátuma a dokumentum vételének a dátuma. Az elfogadó fél tudatában van, hogy az aláírásnak a vételt megelőzően kellett történnie.

Aláírás ellenőrzés
Az a folyamat, mely során egy aláírást ellenőriznek, és a következő lépésekből áll: 1. Tanúsítási útvonal érvényesség ellenőrzése az aláíró nyilvános kulcsa iránti bizalom megalapozásához; 2. Az ellenőrzendő üzenet hash értékének kiszámítása; és 3. Az első lépésben ellenőrzött aláíró nyilvános kulcsának, és a második lépésben számított hash értéknek, illetve az aláírásnak a segítségével megfelelő kriptográfiai algoritmus alkalmazása az aláírás érvényességének megállapítása céljából.

Aszimmetrikus kulcsok
Olyan kulcspár, mely két tagját (az úgynevezett magánkulcsot és az ennek megfelelő nyilvános kulcsot) egyszerre generálják, különböző értéket vesznek fel, és az egyikkel titkosított információt a másikkal lehet dekódolni, vagy az egyikkel digitálisan aláírt információt a másikkal lehet ellenőrizni. A magánkulcsot nem lehet a nyilvános kulcsból származtatni, csak igen nagy —gyakorlati szempontból kivitelezhetetlen— számítási komplexitás révén.

Digitális boríték
Egy szimmetrikus session (munkaszakasz) kulccsal titkosított adatokból álló adathalmaz, ahol a session kulcsot az egyes fogadók számára a fogadó nyilvános kulcsával titkosították.

Digitálisan aláírt adatok
Adatok összessége (az aláírt adatok) és egy érték (a digitális aláírás), melyet az adatokból számítottak. Az aláírás az adatokon (vagy az adatokból származtatott közbenső értéken) elvégzett aszimmetrikus kriptográfiai algoritmus alkalmazásának eredménye. Az adathalmaz tartalmazhat olyan információkat, melyek segítik az adatot aláíró egyed hitelességének ellenőrzését.

Digitális aláírás (Aláírás)
Olyan érték, mely úgy képződik, hogy az aláírandó adatból először egy hash értéket számítanak, majd egy kriptográfiai funkciót (az aláírási algoritmust) alkalmaznak a hash értékre az aláíró magánkulcsa segítségével.

Elfogadó fél
Olyan egyed vagy szervezet, amely megbízik egy tanúsítványban (azaz felhasználja a tanúsítványban lévő nyilvános kulcsot digitális aláíráshoz és/vagy rejtjelezéshez), valamint megbízik a tanúsítványban szereplő előfizető azonosságának (alany neve) és nyilvános kulcsának összetartozásában.

Előfizető
Az az egyed (például személy), aki egy tanúsítványban szereplő nyilvános kulcshoz tartozó magánkulcsot birtokol. A tanúsítvány alany mezője nevezi meg az előfizetőt.

Gyökér tanúsítvány
A hitelesítő szervezet hierarchiájának tetején szereplő tanúsítvány. Ez egy önaláírt tanúsítvány, ami azt jelenti, hogy a tanúsítvány kibocsátója és az alany ugyanaz az egyed, jelen esetben a gyökér CA. A tanúsítvány általában egy megbízható pont. Mivel az önaláírt tanúsítványokban nem bíznak meg, ezért a gyökér tanúsítványt vagy bármilyen más önaláírt tanúsítványt biztonságos módszerek segítségével kell szétosztani.

Hash algoritmus

Olyan algoritmus, amely változó hosszú bemenetet képez le rögzített hosszúságú eredményre, melyet "digest"-nek vagy "hash"-nek neveznek. Az algoritmus N:1 típusú függvény, elvileg több bemenet is ugyanazt az értéket produkálhatja, de egy kívánt vagy rendelkezésre álló eredményhez a bemeneti érték kiszámítása gyakorlatilag nem kivitelezhető.

Kulcspár
Két összetartozó kulcs, melyeket az aszimmetrikus kriptográfia használ. A kulcsokat egy kulcsgenerálási algoritmus hozza létre.

Lejárt tanúsítvány
Olyan tanúsítvány, melyben az érvényességi mező **not after** eleme korábbi értéket tartalmaz, mint az aktuális dátum. A lejáratuk után az ilyen tanúsítványok vagy megjelennek a CRL-ekben vagy nem.

Letagadhatatlanság
Egy tevékenység végrehajtásának letagadását megakadályozó tulajdonság. A letagadhatatlanság egy üzenet aláírója azonosságának és az üzenet integritásának bizonyítéka, amely elegendő ahhoz, hogy meggátolja azt, hogy valamely fél letagadja egy üzenet eredetét, kibocsátását vagy továbbítását, valamint biztosítja az üzenettartalom sértetlenségét.

Magánkulcs
Kizárólag egy adott egyed számára ismert szám, mely egyedet a kulcs tulajdonosának nevezünk (a tulajdonos gondoskodik a titkosságról). A tulajdonosok a magánkulcsot az általuk elküldött adatok aláírásának számítására, illetve a nekik továbbított üzenetek dekódolására használják.

Megbízható harmadik fél
Olyan egyed, akit vagy amelyet más entitások megbízhatónak tartanak, hiteles és feddhetetlennek ítélt bizonyos szolgáltatás elvégzése tekintetében. A megbízható harmadik fél rendszerint nem részrehajló, és semleges a szolgáltatás elvégzése szempontjából.

Megbízható időpecsét
Digitálisan aláírt adathalmaz vagy más olyan eszköz, amely bizonyítékul szolgál arra, hogy egy dokumentum egy bizonyos időpont előtt már létezett. Az adathalmaz tartalmazza a dátumot és időpontot, valamint a dokumentumot vagy annak hash értékét. Gyakran egy megbízható harmadik fél biztosítja az időpecsét szolgáltatást.

Megbízható pont
Olyan tanúsítvány, melyben az ellenőrző fél közvetlenül megbízik. A tanúsítvány tartozhat CA-hoz vagy végentitáshoz. A tanúsítvány megbízható, mert az aláírás ellenőrző fél a PKI-n kívüli megbízható eszközökkel jutott a tanúsítvány birtokába, és elhiszi, hogy a tanúsítvány pontosan köti össze az előfizető egyed nevét annak nyilvános kulcsával. Amennyiben a megbízható pont egy CA tanúsítvány, akkor az ellenőrző félnek meg kell bíznia minden, a CA által kibocsátott tanúsítványban. Ez a bizalom tranzitív, az X.509 tanúsítvány kiterjesztés által megengedett mértékig; ha a CA egy másik CA-nak bocsát ki tanúsítványt, az ellenőrző fél ebben a másik CA-ban is megbízik, ha az X.509 útvonal érvényesség ellenőrzési logika teljesül.

Nyilvános kulcs
Olyan szám, mely egy adott egyedhez tartozik, és mindenki számára ismertté tehető. A nyilvános kulcs szolgál egy aláírás ellenőrzésére és/vagy olyan információk rejtjelezésére, melyeket csak ezen egyed tud dekódolni.

Nyilvános kulcsú infrastruktúra
Azon erőforrások (emberek, rendszerek, folyamatok és eljárások), melyek új tanúsítványok tulajdonosait regisztrálják és azonosítják, visszakeresik a tanúsítványokat és meghatározzák azok érvényességét.

Nyilvános kulcsú szolgáltatásokat tartalmazó alkalmazás
Olyan szoftver alkalmazás, amely nyilvános kulcs technológiát használ a következőkhöz: felhasználók (emberek, rendszerek és eszközök) hitelesítése, információ módosítás megakadályozása átvitel vagy tárolás során, felhasználók felelősségre vonhatóságának és elszámoltathatóságának biztosítása (azaz felelősség letagadás kivédése), információ rejtjelezése, akik között az előzetes egyeztetés nem lehetséges vagy nem kivitelezhető. A nyilvános kulcs szolgáltatásokat tartalmazó alkalmazások a PKI-ra épülnek a tanúsítványok létrehozása (mely eredményeként korrekt módon összekapcsolják a magánkulcs tulajdonosának nevét és nyilvános kulcsát), tanúsítványok visszanyerése és a tanúsítványok érvényességének meghatározása (például CRL lehívása) céljából.

10 Rövidítések

CA	**Certification Authority**	**Hitelesítés-szolgáltató**
CC	**Common Criteria**	**Közös szempontok**
EAL	**Evaluation Assurance Level**	**Értékelési garanciaszint** /A CC 3. rész olyan garanciális összetevőiből álló csomag, amely a CC előre meghatározott garanciális skáláján egy szintet képvisel./
PDA	**Personal Digital Assistant**	**Digitális személyi asszisztens**
PP	**Protection Profile**	**Védelmi profil** /Megvalósítástól független, olyan biztonsági követelményrendszer az értékelés tárgyainak (TOE-k) egy kategóriájára, amely adott fogyasztói igényeket elégít ki./
SF	**Security Function**	**Biztonsági funkció** /Az értékelés tárgyának (TOE) olyan része vagy részei, amelyekben meg kell bízni ahhoz, hogy a vonatkozó biztonsági szabályzatból (TSP) egy szorosan összefüggő szabályhalmaznak érvényt lehessen szerezni./
SFP	**Security Function Policy**	**Biztonsági funkció szabályzata** /A biztonsági funkció (SF) által érvényre juttatott biztonsági szabályzat./
ST	**Security Target**	**Biztonsági előirányzat** /Biztonsági követelmények és előírások olyan összessége, amelyet egy adott értékelés tárgyának (TOE) értékelésének alapjaként használnak./
SOF	**Strength of Function**	**Funkcióerősség** /Az értékelés tárgya (TOE) valamelyik biztonsági funkciójának minősítése, amely azt fejezi ki, hogy minimálisan mekkora erőkifejtést tartanak szükségesnek az elvárt biztonsági működés legyőzéséhez a mögöttes biztonsági mechanizmusok közvetlen megtámadása esetén./
TOE	**Target of Evaluation**	**Az értékelés tárgya** /Az az informatikai termék vagy rendszer, valamint a hozzákapcsolódó (rendszer) adminisztrátori és felhasználói útmutatók, amelyre az értékelés irányul./
TSF	**TOE Security Functions**	**TOE biztonsági funkciói** /Az értékelés tárgyát (TOE) képező minden olyan hardver, szoftver és förmver összessége, amelyben meg kell bízni ahhoz, hogy a vonatkozó biztonságpolitikát (TSP-t) megfelelő módon érvényre lehessen juttatni./
TSP	**TOE Security Policy**	**TOE biztonsági szabályzata** /Szabályok olyan összessége, amely szabályozza a vagyontárgyak kezelését, védelmét, elosztását az értékelés tárgyán (TOE-n) belül./
TSF data	**TSF data**	**TSF adat** /Az értékelés tárgya (TOE) által és részére létrehozott adat, amely befolyásolhatja annak (TOE) működését./
TSC	**TSF Scope of Control**	**TSF ellenőrzési kör** /Azon kölcsönhatások összessége, amelyek az értékelés tárgyán (TOE-n) belül vagy azzal kapcsolatban felléphetnek, és amelyeknek a vonatkozó biztonsági szabályzat (TSP) szabályait be kell tartaniuk./