Online backup szolgáltatást biztosító informatikai rendszer (StoreGrid)

Rendszer biztonsági előirányzat

Verzió:	v1.1
Dátum:	2009.10.20.
Megrendelő:	Magyar Archív Zrt.
Fájl:	StoreGrid_SST_v11.doc
Minősítés:	Nyilvános
Oldalak:	38

Tartalomjegyzék

Változás kezelés

Verzió	Dátum	Leírás	Készítette
0.1	2008.07.23.	A szerkezet felállítása	Balázs István
0.2	2008.07.27.	A szerkezet pontosítása a három biztonsági tartomány azonosításával	Balázs István
0.3	2008.07.29.	A szerkezet további pontosítása	Balázs István
0.4	2008.08.04.	A telepítés tapasztalatai alapján kiegészített változat	Balázs István
0.5	2008.08.05.	A kezdeti tesztelés tapasztalatai alapján kiegészített változat	Balázs István
0.6	2008.08.08.	Megbízónak egyeztetésre átadott változat	Balázs István
0.7	2008.08.12.	Megbízó véleményét is figyelembe vevő javított és kiegészített változat	Balázs István
0.8	2008.08.19.	Az e-aláíró és a dokumentum megjelenítő alrendszer kivételével véglegesített változat	Balázs István
0.9	2008.08.20.	Átszerkesztett végleges változat (a 2. és 3. fejezet összevonásra került)	Balázs István
1.0	2008.08.25.	Elfogadott változat (iSave)	Balázs István
1.1	2009.10.20.	Továbbfejlesztett változat (elektronikus aláírás nélküli, StoreGrid v2.5.1-en alapuló rendszer)	Balázs István

1. A rendszer egészének jellemzése

1.1 Bevezetés

1.1.1 SST hivatkozás

Jelen rendszer biztonsági előirányzat (SST) hivatkozása az alábbi:

Cím: **Online backup szolgáltatást biztosító informatikai rendszer** – rendszer biztonsági előirányzat

Verzió: v1.1, 2009.10.20.

1.1.2 STOE hivatkozás

A jelen SST az alábbi rendszer értékelés tárgyára (STOE) vonatkozik:

Cím: **Online backup szolgáltatást biztosító informatikai rendszer** (rövid neve: StoreGrid v2.5.1 rendszer vagy StoreGrid rendszer)

Verzió: 1.1

1.1.3 A StoreGrid rendszer áttekintése

A StoreGrid rendszer egy olyan informatikai rendszer, mely lehetővé teszi törvény által előírt iratok, illetve okiratok megőrzését elektronikus úton, a [4] rendelet elvárásai szerint.

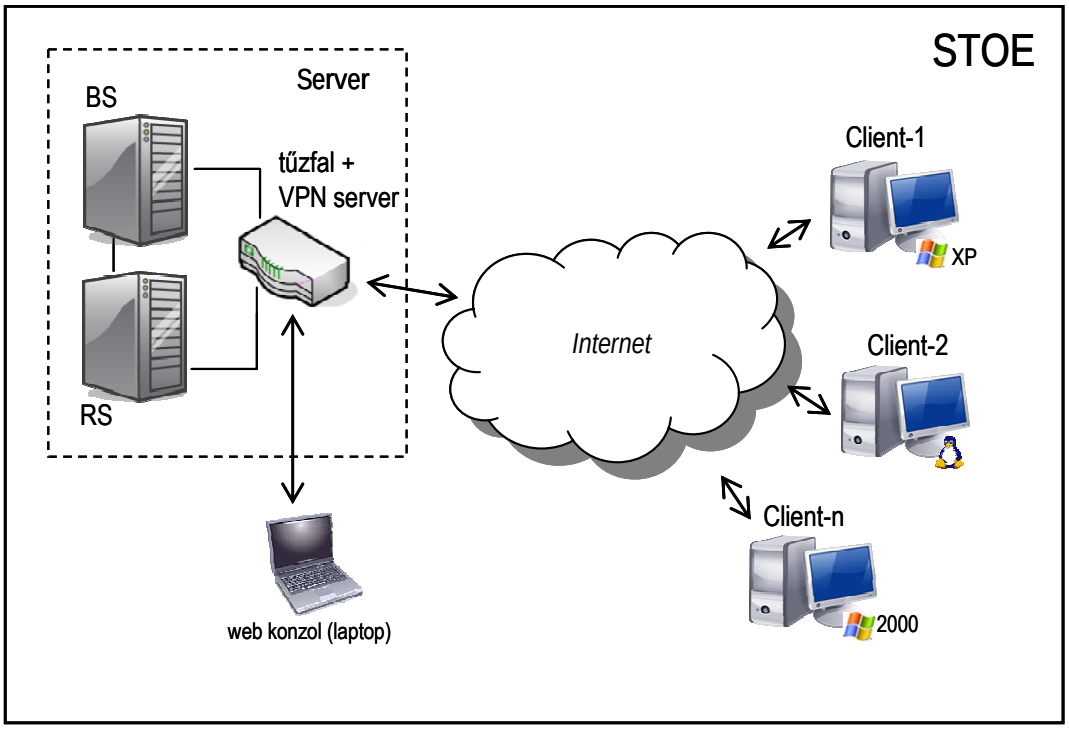
A StoreGrid rendszer egy kliens szerver felépítésű rendszer, melyben a kliens oldalon elektronikus iratok, illetve elektronikus okiratok a szerver oldalon biztonságos mentésre kerülnek, ahonnan szükség esetén, hiteles és jogosult kérésre biztonságosan visszaállíthatók.

A StoreGrid rendszer egy olyan kliens – szerver architektúrájú rendszer, melyben a kliens elektronikus alrendszerét egy valósidejű mentési/helyreállítási szolgáltatást biztosító alrendszer egészíti ki.

1.1.4 A StoreGrid rendszer leírása

1.1.4.1 Rendszer szintű áttekintés

A StoreGrid rendszer rendszerben egy szerver biztonsági tartományhoz (Server) több kliens biztonsági tartomány (Client) csatlakozik az interneten keresztül, ahogyan azt az 1. ábra szemlélteti.

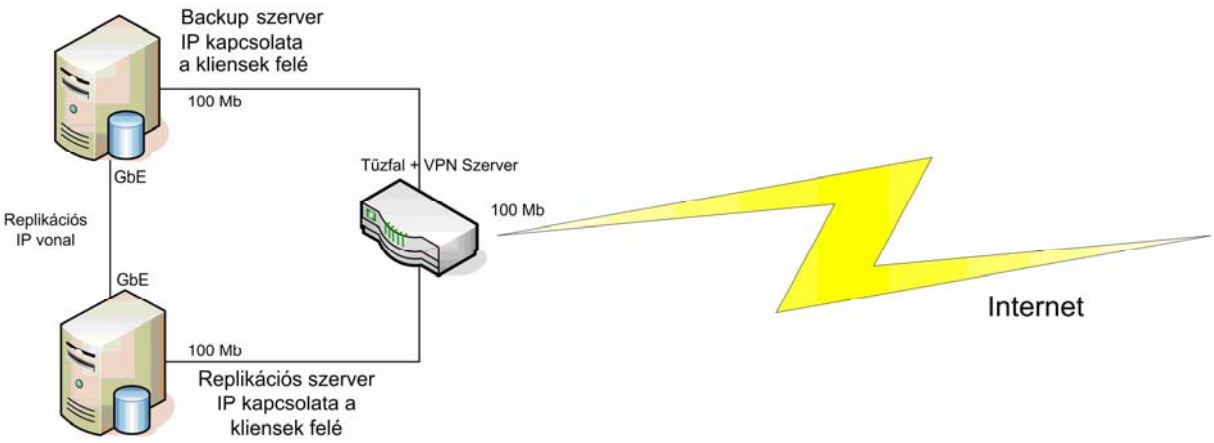


1. ábra: A StoreGrid rendszer fizikai elemei és egymáshoz kapcsolódásuk

1.1.4.2 A fizikai hatókör és határok áttekintése

A Server egy fizikai-környezetbiztonsági, valamint szabályozási-eljárásrendi szempontokból kiemelt védelmet biztosító számítógéptermi környezetben helyezkedik el.

A 2. ábra a szerver biztonsági tartomány legfontosabb fizikai elemeit és ezek kapcsolódásait részletezi.

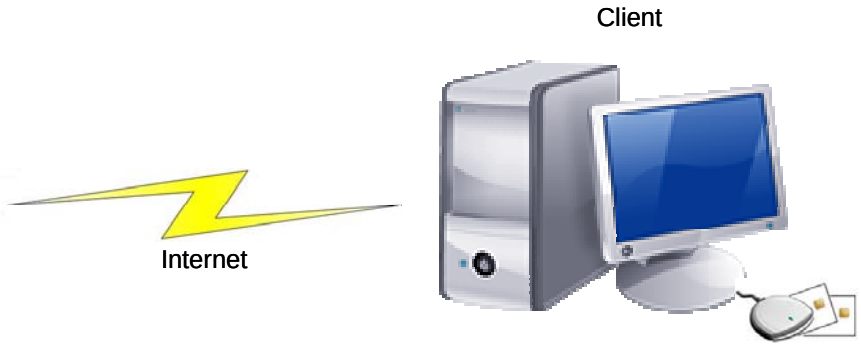


2. ábra: A szerver biztonsági tartomány fizikai elemei és kapcsolódásuk

A szerver biztonsági tartomány legfontosabb fizikai komponensei az alábbiak:

- Egy Backup szerver (az 1. ábrán a BS): melyre a kliens oldalról adatokat lehet menteni, ami szükség esetén az erre jogosultak számára visszatölthet.
- Egy Replikációs szerver (az 1. ábrán az RS): mely a Backup szerver meleg tartalékát képezi, a Backup szerverre kerülő adatok folyamatosan tükröződnek itt, segítségével hiba esetén a Backup szerver teljes tartalma helyreállítható.
- Operációs rendszerek: melyek a különböző szoftver komponenseknek biztosítanak megbízható futtatási környezetet.
- Web konzol (az 1. ábrán a laptop-pal jelzett elem): melyről a szerver biztonsági tartomány távoli menedzselhető.
- Tűzfal és VPN szerver: mely kizárólag a felkínált szolgáltatásokhoz enged hozzáférést, egyúttal biztosítja a szerver biztonsági tartomány távoli menedzselhetőségének védelmét.
- Web szerverek (a szervereken futó alkalmazások: Apache v.2.0.63): melyek a két szerverhez biztosítanak távoli menedzselhetőséget.
- Backup alkalmazások (a szervereken futó alkalmazások: StoreGrid v2.5.1): melyek a két szerveren biztosítják a mentési/helyreállítási funkciókat.
- Böngésző: mely a Web konzolról biztosítja a szerver biztonsági tartomány távoli menedzselhetőségét.
- Útmutatók: melyek segítségével elvégezhetők a fenti hardver és szoftver komponensek biztonságos telepítése, konfigurálása és üzemeltetése.

A 3. ábra a kliens biztonsági tartomány legfontosabb fizikai elemeit és ezek kapcsolódásait tekinti át.



3. ábra: A kliens biztonsági tartomány fizikai elemei és kapcsolódásuk

A kliens biztonsági tartomány legfontosabb fizikai komponensei az alábbiak:

- Egy Internetre kapcsolt PC: mely a hardver alapokat biztosítja, egyúttal betölti a saját Backup alkalmazáshoz tarozó web konzol szerepét is.
- Operációs rendszer: mely a különböző szoftver komponenseknek biztosít megbízható futtatási környezetet.
- Backup alkalmazás /StoreGrid v2.5.1/: mely a kliens oldalon biztosítja a mentési/helyreállítási funkciókat.
- Böngésző: mely a saját Backup alkalmazás lokális menedzselhetőségét biztosítja.

Valamennyi fenti komponens az STOE részét képezi.

A szerver biztonsági tartomány valamennyi fizikai komponensét megadtuk.

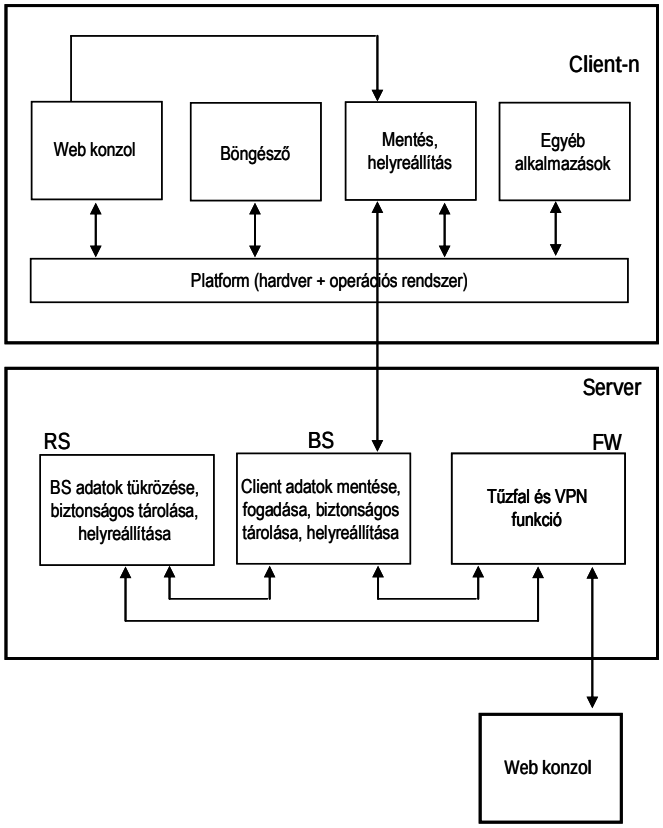
A kliens biztonsági tartomány számos más komponenst is tartalmazhat, köztük különböző dokumentum előállító programokat, adatbázis-kezelőket, dokumentum megjelenítőket és egyéb alkalmazásokat. Ezek azonban nem képezik részét az STOE-nak.

1.1.4.3 A logikai hatókör és határok áttekintése

A StoreGrid rendszerben különböző szolgáltatások nyújtása, illetve igénybe vétele folyik.

A 4. ábra az alábbi logikai alrendszerek egymáshoz kapcsolódását tekinti át:

- kliens oldali online backup alrendszer (komponensei: kliens oldali web konzol, böngésző és Backup (mentés/helyreállítás) alkalmazás /„client only" üzemmódban/),
- backup szerver alrendszer (komponensei: backup szerver, operációs rendszer, web szerver, backup alkalmazás /„server only" üzemmódban/, web konzol, böngésző),
- replikációs szerver alrendszer (komponensei: replikációs szerver, operációs rendszer, web szerver, backup alkalmazás /„replication server only" üzemmódban/, web konzol, böngésző).
- tűzfal alrendszer
- web konzol alrendszer



4. ábra: A StoreGrid rendszer logikai alrendszerei és egymáshoz kapcsolódásuk

A **platform** alrendszer megbízható futtatási környezetet biztosít a kliens oldal többi alrendszere számára. A biztonságos futtatási környezet több dolgot jelent:

- tartomány szétválasztást (a különböző alrendszerek egymást nem befolyásolhatják, egymás erőforrásait nem érik el),
- önvédelem (megvédi a különböző alrendszereket a jogosulatlan logikai hozzáféréstől)
- megkerülhetetlenséget (a többi alrendszer csak akkor éri el erőforrásait, ha az operációs rendszerbe belépő, megfelelő jogosultságú felhasználó elindítja azokat).

A **kliens oldali online backup** alrendszer (a 4. ábrán a Mentés, helyreállítás):

- lehetővé teszi az online backup szolgáltatás hatókörébe eső elektronikus dokumentumok kijelölését, valamint a mentés gyakoriságának és módjának meghatározását,
- továbbítja a kijelölt elektronikus dokumentumokat a szerver biztonsági tartománynak, amely megvédi azokat a törlés, a megsemmisítés, a véletlen megsemmisülés és sérülés ellen.
- a szerver biztonsági tartománytól letölti és helyreállítja a kliens oldalon törölt, megsemmisített, megsemmisült vagy megsérült elektronikus dokumentumokat.

A **backup szerver** alrendszer (a 4. ábrán a BS) az alábbi feladatokat látja el:

- lehetővé teszi a kliensek és a replikációs szerver kijelölését, valamint a (replikációs) mentés gyakoriságának és módjának meghatározását,
- fogadja a kliensektől érkező elektronikus dokumentumokat, s megvédi azokat a törlés, a megsemmisítés, a véletlen megsemmisülés és sérülés ellen,
- a replikációs szerverre is átküldi a kliensektől kapott elektronikus dokumentumokat,
- replikációs szervertől letölti és helyreállítja a nála esetlegesen törölt, megsemmisített, megsemmisült vagy megsérült elektronikus dokumentumokat.

A **replikációs szerver** alrendszer (a 4. ábrán az RS) az alábbi feladatokat látja el:

- lehetővé teszi a backup szerver kijelölését,
- fogadja a backup szervertől érkező elektronikus dokumentumokat, s megvédi azokat a törlés, a megsemmisítés, a véletlen megsemmisülés és sérülés ellen,
- a backup szerverre visszatölti az ott esetlegesen törölt, megsemmisített, megsemmisült vagy megsérült elektronikus dokumentumokat.

A **tűzfal** alrendszer (a 4. ábrán az FW) az alábbi feladatokat látja el:

- VPN kapcsolatot épít ki a web konzolon keresztül bejelentkező felhasználó és saját maga között, mely tanúsítvány alapon hitelesíti mindkét szereplőt, egyúttal megvédi a kommunikáció bizalmasságát, sértetlenségét és hitelesítését.
- IP cím alapú csomagszűrést végez, s csak a backup szerver és a replikációs szerver működéséhez szükséges portokon keresztül engedi be a külső adatforgalmat.

A **web konzol** alrendszer az alábbi feladatokat látja el:

- a tűzfal távoli menedzselése,
- a Backup szerver távoli menedzselése,
- a Replikációs szerver távoli menedzselése.

Valamennyi fenti szolgáltatás az STOE részét képezi.

A szerver biztonsági tartomány valamennyi szolgáltatását megadtuk.

A kliens biztonsági tartomány számos más szolgáltatást is biztosíthat (a 4. ábrán az egyéb alkalmazások). Ezek azonban nem képezik részét az STOE-nak.

1.1.4.4 A StoreGrid rendszer külső rendszerekhez kapcsolódása

A StoreGrid rendszer különböző külső informatikai rendszerekhez is kapcsolódhat, ezek azonban nem képezik részét az STOE-nak.

1.1.5 Tartomány kialakítás specifikáció

A StoreGrid rendszer egy kliens – szerver architektúrájú rendszer. A két oldal eltérő biztonsági tartományt is képvisel (Server és Client biztonsági tartományok), az üzemeltetési környezetükben biztosított jelentős eltérések miatt.

A szerver biztonsági tartomány (Server) biztosítja az online backup szolgáltatást. Fizikailag egy ilyen tartomány van.

A kliens biztonsági tartomány (Client) létrehozza és kezeli az archiválandó elektronikus dokumentumokat, valamint ezek hosszú távú biztonságos megőrzése érdekében igénybe veszi az online backup szolgáltatást. Fizikailag sok ilyen tartomány van (lásd 1. ábra).

1.2 Megfelelőségi nyilatkozatok

Jelen rendszer biztonsági előirányzat, s az általa vizsgált StoreGrid rendszer rendszer az alábbi mértékadó dokumentumhoz való megfelelőséget állít:

- [4] (114/2007. (XII. 29.) GKM rendelet a digitális archiválás szabályairól) 2 § (1).

1.3 Biztonsági célok az üzemeltetési környezetre

A StoreGrid rendszer üzemeltetési környezetére az alábbi általános biztonsági célok vonatkoznak:

1	OE.Configuration	A rendszer valamennyi komponensét úgy kell telepíteni és konfigurálni, hogy biztonságos állapotban kezdjen el üzemelni.
2	OE.Init_Secure_Attr	Az alap értelmezett jelszavakat le kell cserélni.
3	OE.Authorized_Users	Az engedéllyel rendelkező felhasználók megbízhatók a tekintetben, hogy a számukra kijelölt feladatokat biztonsági szempontból korrekt módon hajtják végre.
4	OE.Physical_Security	A környezetnek elfogadható szintű fizikai védelemről kell gondoskodnia, hogy a rendszer komponenseit ne lehessen hamisítani (a különböző alkalmazásokat és ezek konfigurációs állományait ne lehessen módosítani, manipulálni).
5	OE.Trust_Adm	A különböző adminisztrátorok (a kliensek, a szerverek, a tűzfal és a VPN szerver adminisztrátorai) ismerik feladataikat, s ezeket szakképzett módon, lehetőségeikkel nem visszaélve látják el.

1.4 Biztonsági követelmények

1.4.1 A rendszertől elvárt biztonsági funkcionalitás

A rendszertől elvárt biztonsági funkcionalitást a [4] rendelet 2 § (1) alábbi részlete határozza meg:

2 § (1)

A megőrzésre kötelezett a megőrzési kötelezettség lejártáig folyamatosan köteles biztosítani, hogy az elektronikus dokumentumok megőrzése olyan módon történjen, amely .... védi az elektronikus dokumentumokat a törlés, a megsemmisítés, a véletlen megsemmisülés és sérülés, illetve a jogosulatlan hozzáférés ellen.

A fentieknek megfelelően a rendszer egészének az alábbi funkcionális biztonsági követelményeket (SFR) kell kielégítenie:

1.4.1.1 SFR_1 (TrustSave)

SFR_1: A rendszer olyan módon őrizze meg az elektronikus dokumentumokat, amely megvédi az elektronikus dokumentumokat a törlés, a megsemmisítés, a véletlen megsemmisülés és sérülés ellen. (rövid név: TrustSave)

1.4.1.2 SFR_2 (AccessControl)

SFR_2: A rendszer olyan módon őrizze meg az elektronikus dokumentumokat, amely megvédi az elektronikus dokumentumokat a jogosulatlan hozzáférés ellen. (rövid név: AccessControl)

1.4.1.3 SFR_3 (Audit)

SFR_3: A rendszerben kiváltott biztonsági eseményekről napló állományok készüljenek, az ebben található bejegyzéseket a rendszer az erre jogosultak számára jelenítse meg, ugyanakkor védje meg a jogosulatlan hozzáférés ellen (rövid név: Audit).

A StoreGrid rendszer két biztonsági tartománya (Client és Server) a fenti funkcionális biztonsági követelmények teljesítésében különböző szerepet játszik. A biztonsági tartományok leírása a fenti követelményeket tovább bontja, s meghatározza a finomított követelmények teljesítésében játszott szerepeket is (lásd. 2.4 alfejezet).

1.4.2 A rendszerre elvárt garanciák

A rendszer egészére elvárt garancia a [2] által a MIBÉTS módszertan továbbfejlesztéseként meghatározott SAP-A (MIBÉTS_alap) garanciacsomag, pontosabban annak egy megemelt változata.

A StoreGrid rendszer egészére elegendő garanciát nyújt a SAP-A, két kivétellel.

Az első kivételt az okozza, hogy a rendszer osztott rendszer, melynek alrendszerei nyilvános kommunikációs csatornán kapcsolódnak egymáshoz. A nyilvános kommunikációs csatornán megvalósuló adatcserét külön biztonsági mechanizmusok (tömörítés és titkosítás) védik, és ezek megfelelő működésének az egész rendszer szempontjából komoly biztonsági jelentősége van. A SAP-A ellenére nem elég tehát a rendszer architektúrájának megfelelő tesztelési mélység (amit a SAP-A ASTE_DPT.1 összetevője biztosít), szükség van az alrendszerek közötti interfészek tesztelésére is (amit csak az ASTE_DPT.2 összetevő biztosít).

A másik kivételre a mentési szolgáltatás kritikus fontossága miatt van szükség. A StoreGrid mentés/helyreállítás alrendszer alacsony támadó képességű támadókkal szembeni ellenállását nemcsak automatikus eszközökkel végrehajtott behatolás tesztelés, hanem független sebezhetőség vizsgálat is ellenőrizte.

A rendszer egészére elvárt garancia SAP-A+ (megemelt SAP-A), ahol a megemelés az ASTE_DPT.2 és ASVA_VAN.2 garancia-összetevő hozzáadását jelenti (ASTE_DPT.1, illetve ASVA_VAN.1 helyett). SAP-A+ az alábbi garancia-összetevőket tartalmazza:

Rendszer fejlesztés (ASDV)	ASDV_SIS.1	Informális interfész specifikáció
	ASDV_ARC.1	Biztonsági szerkezet leírás
	ASDV_SDS.1	Alrendszer és komponens szintű biztonsági terv
	ASDV_OSC.1	Rendszer-működési biztonsági koncepció
Rendszer útmutató dokumentumok (ASGD)	ASGD_PRE.1	Előkészítő útmutató
	ASGD_OPE.1	Üzemeltetési útmutató
	ASGD_CON.1	Konfigurálási útmutató
Rendszer konfiguráció kezelés (ASCM)	ASCM_SBC.1	Rendszer alap konfiguráció
	ASCM_ECC.1	A tanúsított komponensek felmérése
Rendszer tesztelés (ASTE)	ASTE_FUN.1	Funkcionális tesztelés
	ASTE_COV.1	A teszt lefedettség vizsgálata
	ASTE_DPT.2	Tesztelés: alrendszerek
	ASTE_IND.1	Független tesztelés mintán
Rendszer sebezhetőség felmérés (ASVA)	ASVA_VAN.2	Független sebezhetőség vizsgálat

A Server biztonsági tartományra kiegészítő garanciális elvárások is vonatkoznak, melyeket 2.4.3 határoz meg.

1.4.2.1 Informális interfész specifikáció (ASDV_SIS.1)

ASDV_SIS.1.1D A rendszer integrátornak biztosítania kell egy rendszer interfész specifikációt.

ASDV_SIS.1.1C A rendszer interfész specifikációnak informális stílusban le kell írnia az STOE biztonsági funkcionalitását (SSF) és annak külső interfészeit.

ASDV_SIS.1.2C A rendszer interfész specifikációnak belső ellentmondásoktól mentesnek kell lennie.

ASDV_SIS.1.3C A rendszer interfész specifikációnak le kell írnia az SSF minden külső interfészére a használat célját és módját, részletezve a hatásokat, kivételeket és hibaüzeneteket.

ASDV_SIS.1.4C A rendszer interfész specifikációnak teljes mértékben be kell mutatnia az SSF-et.

ASDV_SIS.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASDV_SIS.1.2E Az értékelőnek meg kell állapítania, hogy a rendszer interfész specifikáció az STOE funkcionális biztonsági követelményeinek pontos és teljes megjelenítése.

1.4.2.2 Biztonsági szerkezet leírás (ASDV_ARC.1)

ASDV_ARC.1.2D A rendszer integrátornak úgy kell megterveznie és megvalósítania a rendszer biztonsági funkcionalitását, hogy az képes legyen megvédeni magát a nem-megbízható aktív egyedek hamisításaitól.

ASDV_ARC.1.3D A rendszer integrátornak biztosítania kell egy leírást az STOE biztonsági architektúrájáról.

ASDV_ARC.1.1C A biztonsági architektúra leírásnak ismertetnie kell az STOE-hez kapcsolódó külső informatikai rendszereket, egymáshoz kapcsolódásukat, valamint a köztük folyó információáramlást.

ASDV_ARC.1.2C A biztonsági architektúra leírásnak ismertetnie kell az STOE biztonsági funkcionalitás szerkezetét, olyan részletességgel, amely összemérhető a rendszer interfész specifikáció és az STOE terv részletességével.

ASDV_ARC.1.3C A biztonsági architektúra leírásnak szemléltetnie kell, hogy az STOE meggátolja a funkcionális biztonsági követelményeket érvényre juttató funkcionalitás megkerülését.

ASDV_ARC.1.4C A biztonsági architektúra leírásnak szemléltetnie kell, hogy a rendszer biztonsági funkcionalitás megvédi magát a hamisítással szemben.

ASDV_ARC.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

1.4.2.3 Alrendszer és komponens szintű biztonsági terv (ASDV_SDS.1)

ASDV_SDS.1.1D A rendszer integrátornak biztosítania kell az STOE rendszer biztonsági tervét (STOE tervét).

ASDV_SDS.1.2D A rendszer integrátornak az STOE tervet vissza kell vezetnie a rendszer architektúra leírásra.

ASDV_SDS.1.1C Az STOE tervnek le kell írnia az STOE szerkezetét alrendszerek szerint.

ASDV_SDS.1.2C Az STOE tervnek azonosítania kell az SSF minden alrendszerét.

ASDV_SDS.1.3C Az STOE tervnek az SSF minden alrendszerére le kell írnia és osztályba kell sorolnia az alrendszer által nyújtott biztonsági funkcionalitást.

ASDV_SDS.1.4C Az STOE tervnek minden alrendszert az alábbi osztályok egyikébe kell sorolnia: SSF-t érvényre juttató, SSF-t támogató, az SSF-be nem beavatkozó (alrendszer).

ASDV_SDS.1.5C Az STOE tervnek azonosítania kell minden alrendszerhez a csatlakozó interfészeket.

ASDV_SDS.1.6C Az STOE tervnek az SSF minden alrendszerére le kell írnia a csatlakozó interfész célját és használati módját, részletezve azok kihatásait, a kivételeket, illetve a hibaüzeneteket.

ASDV_SDS.1.7C Az STOE tervnek az SSF minden alrendszerére azonosítania kell az alrendszert alkotó komponenseket.

ASDV_SDS.1.8C Az STOE tervnek minden azonosított komponensre le kell írnia és osztályba kell sorolnia a komponens által nyújtott biztonsági funkcionalitást.

ASDV_SDS.1.9C Az STOE tervnek minden komponenst az alábbi osztályok egyikébe kell sorolnia: SSF-t érvényre juttató, SSF-t támogató, az SSF-be nem beavatkozó (komponens).

ASDV_SDS.1.10C Az STOE tervnek az SSF minden alrendszerére meg kell határoznia a komponensek közötti belső összefüggéseket.

ASDV_SDS.1.11C Az STOE tervnek az SSF minden alrendszerére azonosítania kell az egyes komponensek által megvalósított, alrendszerhez csatlakozó interfészeket.

ASDV_SDS.1.12C Az STOE tervnek az SSF minden alrendszerére le kell írnia az egyes komponensek által megvalósított, alrendszerhez csatlakozó interfészeket, azok célja és használati módja szempontjából.

ASDV_SDS.1.13C Az STOE tervnek a rendszer architektúra leírásra való visszavezetésének meg kell mutatnia, hogy a rendszer architektúra leírás minden eleme megvan az STOE tervben.

ASDV_SDS.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASDV_SDS.1.2E Az értékelőnek meg kell erősítenie, hogy az STOE terv az összes funkcionális biztonsági követelmény pontos és teljes megjelenítése.

1.4.2.4 Rendszer-működési biztonsági koncepció (ASDV_OSC.1)

ASDV_OSC.1.1D A rendszer integrátornak biztosítania kell a rendszer-működésre vonatkozó biztonsági koncepció leírását.

ASDV_OSC.1.1C A rendszer-működési biztonsági koncepció leírásának meg kell határoznia a rendszer belső (rendszer határain belüli) információ áramlást érvényre juttató képességét.

ASDV_OSC.1.2C A rendszer-működési biztonsági koncepció leírásának meg kell határoznia a rendszer külső (külső rendszerek felé történő) információ áramlást érvényre juttató képességét.

ASDV_OSC1.3C A rendszer-működési biztonsági koncepció leírásának meg kell határoznia a rendszer lokális és távoli hozzáféréseket érvényre juttató képességét.

ASDV_OSC.1.4C A rendszer-működési biztonsági koncepció leírásának meg kell határoznia a rendszer erőforrásokhoz való (hozzáférés közvetítési szabályokon alapuló) hozzáféréseket érvényre juttató képességét.

ASDV_OSC.1.5C A rendszer-működési biztonsági koncepció leírásának meg kell határoznia a rendszer által nyújtott üzemmódokat, az üzemmódok közötti átmenetek feltételeit, és azokat az érvényesítő mechanizmusokat, amelyek minden azonosított rendszer üzemmódban biztonságos működést biztosítanak.

ASDV_OSC.1.6C A rendszer-működési biztonsági koncepció leírásának belső ellentmondástól mentesnek kell lennie.

ASDV_OSC.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASDV_OSC.1.2E Az értékelőnek meg kell állapítania a rendszer architektúra leírásról és az STOE tervről, hogy azok teljesen megvalósítják a rendszer-működési biztonsági koncepciót.

1.4.2.5 Előkészítő útmutató (ASGD_PRE.1)

ASGD_PRE.1.1D A rendszer integrátornak a működőképes STOE mellé biztosítania kell az előkészítő útmutatót.

ASGD_PRE.1.1C Az előkészítő útmutatónak le kell írnia az STOE leszállított komponenseinek biztonságos elfogadásához alkalmazott valamennyi lépést, a komponens szállítójának szállítási eljárásaival összhangban.

ASGD_PRE.1.2C Az előkészítő útmutatónak le kell írnia az STOE komponenseinek biztonságos telepítéséhez, az STOE integrálásához és az üzemeltetési környezethez való biztonságos előkészülethez alkalmazott valamennyi lépést, az SST-ben leírt, üzemeltetési környezetre vonatkozó biztonsági célokkal összhangban.

ASGD_PRE.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

1.4.2.6 Üzemeltetési útmutató (ASGD_OPE.1)

ASGD_OPE.1.1D A rendszer integrátornak üzemeltetési útmutatót kell biztosítania.

ASGD_OPE.1.1C Az üzemeltetési útmutatónak minden felhasználói szerepkörre le kell írnia azokat a felhasználó által elérhető funkciókat és jogosultságokat (beleértve a megfelelő figyelmeztetéseket is), melyeket egy biztonságos üzemeltetési környezetben ellenőrzés alatt kell tartani.

ASGD_OPE.1.2C Az üzemeltetési útmutatónak minden felhasználói szerepkörre le kell írnia, hogy az STOE által biztosított, elérhető interfészeket hogyan kell biztonságos módon használni.

ASGD_OPE.1.3C Az üzemeltetési útmutatónak minden felhasználói szerepkörre le kell írnia az elérhető funkciókat és interfészeket, különösen a felhasználó ellenőrzése alá tartozó minden biztonsági szempontból fontos paramétert, jelezve (ahol ez lehetséges) a biztonságos értékeket.

ASGD_OPE.1.4C Az üzemeltetési útmutatónak minden felhasználói szerepkörre világosan be kell mutatnia a felhasználó által elérhető funkciókkal kapcsolatban végrehajtandó, biztonsági szempontból fontos minden esemény típust, beleértve az SSF ellenőrzése alá eső egyedek biztonsági tulajdonságainak megváltoztatását is.

ASGD_OPE.1.5C Az üzemeltetési útmutatónak azonosítani kell az STOE összes lehetséges üzemmódját (beleértve a karbantartási és a meghibásodás vagy üzemeltetési hiba utáni üzemmódokat is), valamint ezek biztonságos üzemeltetésre gyakorolt következményeit és kihatásait.

ASGD_OPE.1.6C Az üzemeltetési útmutatónak minden felhasználói szerepkörre le kell írnia azokat a betartandó biztonsági intézkedéseket, melyek az SST-ben meghatározott, üzemeltetési környezetre vonatkozó biztonsági célok elérését szolgálják.

ASGD_OPE.1.7C Az üzemeltetési útmutatónak egyértelműnek és megalapozottnak kell lennie.

ASGD_OPE.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

1.4.2.7 Konfigurálási útmutató (ASGD_CON.1)

ASGD_CON.1.1D A rendszer integrátornak biztosítania kell egy konfigurálási útmutatót, amely meghatározza azokat a biztonság-vonzatú konfigurációs paramétereket, amelyek támogatják a rendszer komponenseinek az integrálását, és amelyek lehetővé teszik, hogy a szolgáltató rendszer biztonsági funkciói megvalósítsák és érvényre juttassák a szolgáltató rendszer működésre vonatkozó biztonsági koncepcióját és a kapcsolódó szabályzatokat.

ASGD_CON.1.1C A konfigurálási útmutatónak le kell írnia azokat a biztonsági konfigurációs paramétereket, amelyek a rendszer integrátor vagy az ezzel azonos szerepkörű és felelősségű STOE felhasználók/adminisztrátorok számára elérhetők.

ASGD_CON.1.2C A konfigurálási útmutatónak le kell írnia azoknak a biztonsági paramétereknek a használatát, amelyeket az STOE állíthat be abból a célból, hogy megvalósítsa és érvényre juttassa a rendszer biztonsági szabályzatait.

ASGD_CON.1.3C A konfigurálási útmutatónak figyelmeztetéseket kell tartalmaznia a konfigurálás által hozzáférhető azon funkciókra és privilégiumokra vonatkozóan, amelyeket egy biztonságos feldolgozási környezetben ellenőrizni kell.

ASGD_CON.1.4C A konfigurálási útmutatónak világosan be kell mutatnia az összes konfigurálással kapcsolatos felelősséget, amely az STOE biztonságos működtetéséhez szükséges.

ASGD_CON.1.5C A konfigurálási útmutatónak ellentmondás mentesnek kell lennie az értékeléshez átadott összes többi dokumentumhoz viszonyítva.

ASGD_CON.1.6C A konfigurálási útmutatónak le kell írnia az összes olyan biztonsági követelményt, amely az STOE-ra vonatkozik, beleértve az üzemeltetési környezetet is.

ASGD_CON.1.7C A konfigurálási útmutatónak meg kell mutatnia, hogy az STOE terv megvalósítja az összes olyan komponensre vonatkozó biztonsági paramétert, amelyet a rendszer-működési biztonsági koncepció megkövetel.

ASGD_CON.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

1.4.2.8 Rendszer alap konfiguráció (ASCM_SBC.1)

ASCM_SBC.1.1D A rendszer integrátornak konfiguráció kezelés (CM) rendszert kell használnia a kezdeti/legutolsó értékelt rendszerhez, amelyet „alap konfiguráció”-nak kell nevezni.

ASCM_SBC.1.2D A CM rendszernek nyomon kell követnie és felügyelnie kell minden tervezett és tényleges változtatást a rendszer alap konfigurációján, és ezek értékelési állapotát.

ASCM_SBC.1.3D A rendszer integrátornak vagy rendszer tulajdonosnak CM dokumentációt kell nyújtania a rendszer alap konfigurációjához.

ASCM_SBC.1.1C A CM rendszernek egyedileg azonosítania kell az STOE alap konfigurációt, az alap konfigurációt alkotó összes rendszer komponenst és ezek értékelési állapotát.

ASCM_SBC.1.2C A CM rendszernek nyomon kell követnie az alap konfigurációhoz, illetve az ezt alkotó rendszer komponensekhez kapcsolódó változtatásokat.

ASCM_SBC.1.3C A CM tervnek le kell írnia, hogy a rendszer alap konfigurációját hogyan kezelik, és hogy az alap konfiguráción történő módosításokat hogyan ellenőrzik és hogyan követik nyomon.

ASCM_SBC.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

1.4.2.9 A tanúsított komponensek felmérése (ASCM_ECC.1)

ASCM_ECC.1.1D A rendszer integrátornak az STOE alap konfigurációját alkotó termék-komponensek közül meg kell határoznia az értékelt és tanúsított termék-komponensek listáját, valamint az ezekre vonatkozó garancia csomagokat.

ASCM_ECC.1.2D A rendszer integrátornak specifikálnia kell minden értékelt és tanúsított rendszer komponens termék üzemeltetési paramétereit.

ASCM_ECC.1.1C Az értékelt és tanúsított termék-komponensek listájában le kell írni az értékelt és tanúsított termékek garancia csomagjait.

ASCM_ECC.1.2C Az értékelt és tanúsított termék-komponensek listájának minden termékre azonosítania kell az értékelési eredményekre vonatkozó tanúsítványt, tanúsítási jelentést és az ezek alapjául szolgáló biztonsági előirányzatot.

ASCM_ECC.1.3C Az értékelt és tanúsított termék-komponensek listájának minden termékre le kell írnia az üzemeltetési paramétereit.

ASCM_ECC.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASCM_ECC.1.2E Az értékelőnek meg kell erősítenie, hogy a rendszer üzemeltetési környezete kielégíti az értékelt és tanúsított termékek tanúsítványaiban és tanúsítási jelentéseiben megfogalmazott üzemeltetési feltételeket.

1.4.2.10 Funkcionális tesztelés (ASTE_FUN.1)

ASTE_FUN.1.1D A rendszer integrátornak tesztelnie kell a rendszer biztonsági funkcionalitását (SSF-t), és ennek eredményeit dokumentálnia kell.

ASTE_FUN.1.2D A rendszer integrátornak tesztdokumentációt kell biztosítania.

ASTE_FUN.1.3D A rendszer integrátornak biztosítania kell egy vizsgálatot tesztelése teljességéről.

ASTE_FUN.1.1C A tesztdokumentációnak tartalmaznia kell a teszttterveket, a várt teszteredményeket és a tényleges teszteredményeket.

ASTE_FUN.1.2C A teszttterveknek azonosítaniuk kell a végrehajtandó teszteket, és le kell írniuk minden teszt végrehajtásának forgatókönyvét. Ezen forgatókönyveknek tartalmazniuk kell a más tesztek eredményeitől való minden sorrendbeli függést.

ASTE_FUN.1.3C A várt teszteredményeknek be kell mutatniuk a tesztek sikeres végrehajtásából keletkező várható kimeneteket.

ASTE_FUN.1.4C A tényleges teszteredményeknek összhangban kell állniuk a várt teszteredményekkel.

ASTE_FUN.1.5C A tesztdokumentációnak tartalmaznia kell egy vizsgálatot a teszt eljárás sorrendi függőségeiről.

ASTE_FUN.1.6C A biztonsági intézkedések tesztelésének részletességére vonatkozó vizsgálatának be kell mutatnia, hogy az SST-ben elvárt funkcionális biztonsági követelmények és a tesztdokumentációban megadott tesztek közötti megfeleltetés teljes.

ASTE_FUN.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

1.4.2.11 A teszt lefedettség vizsgálata (ASTE_COV.1)

ASTE_COV.1.1D A rendszer integrátornak biztosítania kell a teszt lefedettség elemzését.

ASTE_COV.1.1C A teszt lefedettség elemzésnek be kell mutatnia a tesztdokumentációban azonosított tesztek és a rendszer biztonsági funkcionalitás (ahogyan azt a rendszer interfész specifikáció a külső interfészeken keresztül leírja) közötti megfeleltetést.

ASTE_COV.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

1.4.2.12 Tesztelés: alrendszerek (ASTE_DPT.2)

ASTE_DPT.22.1D A rendszer integrátornak tesztmélység elemzést kell biztosítania.

ASTE _DPT.2.1C A tesztmélység elemzésnek be kell mutatnia, hogy a tesztdokumentációban azonosított tesztek elegendőek annak bemutatására, hogy a rendszer biztonsági funkcionalitása a rendszer biztonsági architektúra leírással, valamint a rendszer biztonsági terv alrendszerekre vonatkozó leírásával összhangban működik.

ASTE_DPT.2.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

1.4.2.13 Független tesztelés mintán (ASTE_IND.1)

ASTE_IND.1.1D A rendszer integrátornak a teszteléshez biztosítania kell az STOE-t vagy az STOE-hez való hozzáférést.

ASTE_IND.1.1C Az STOE-nek tesztelésre alkalmas állapotban kell lennie.

ASTE_IND.1.2C A rendszer integrátornak biztosítania kell az SSF funkcionális tesztelése során használt erőforrás-készlettel azonos eszközkészletet.

ASTE_IND.1.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASTE_IND.1.2E Az értékelőnek végre kell hajtania a tesztdokumentációban szereplő tesztek valamely részhalmazát (mintáját) a rendszer integrátor teszteredményeinek ellenőrzése érdekében.

ASTE_IND.1.3E Az értékelőnek tesztelnie kell az SSF külső és belső interfészeinek egy részét annak megerősítése érdekében, hogy az SSF a specifikáltaknak megfelelően működik.

1.4.2.14 Független sebezhetőség vizsgálat (ASVA_VAN.2)

ASVA_VAN.2.1C Az STOE-nak alkalmasnak kell lennie tesztelésre.

ASVA_VAN.2.1E: Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASVA_VAN.2.2E: Az értékelőnek egy keresést kell végrehajtania nyilvános forrásokban az STOE lehetséges sebezhetőségeinek azonosítása érdekében.

ASVA_VAN.2.3E Az értékelőnek egy független sebezhetőség vizsgálatot kell végrehajtania az STOE-ra, felhasználva az SST, a biztonsági architektúra leírás, a rendszer interfész specifikáció, az STOE terv, a rendszer-működési biztonsági koncepció és az útmutató dokumentációk által biztosított ismereteket, az STOE lehetséges sebezhetőségeinek azonosítása érdekében.

ASVA_VAN.2.4E Az értékelőnek az azonosított lehetséges sebezhetőségek alapján automatikus eszközöket is felhasználva, behatolás tesztelést kell végrehajtania, annak megállapítása érdekében, hogy az STOE ellenáll egy alap támadó képességgel rendelkező támadó által végrehajtott támadásnak.

1.5 Rendszer összefoglaló előírás

1.5.1 Az SFR_1 teljesítési módja

A rendszer egy online backup szolgáltatás biztosításával védi az elektronikus dokumentumokat a törlés, a megsemmisítés, a véletlen megsemmisülés és sérülés ellen. A Client biztonsági tartomány meghatározott könyvtáraiba kerülő, meghatározott kiterjesztésű elektronikus dokumentumok automatikusan továbbításra kerülnek a Server biztonsági tartományhoz, ahol két különböző, nagy megbízhatóságú tároló szerver garantálja a megőrzését.

Abban az esetben, ha a Client biztonsági tartományban az eredeti dokumentum törlése, megsemmisítése, véletlen megsemmisülése vagy sérülése következne be, mód van (megfelelős jogosultság ellenőrzés után) annak biztonságos visszatöltésére és visszaállítására.

Az online backup szolgáltatást a Client biztonsági tartomány kliens oldali online backup alrendszere és a Server biztonsági tartomány együttesen valósítják meg.

1.5.2 Az SFR_2 teljesítési módja

A StoreGrid rendszer egy kliens szerver felépítésű rendszer, melyben a kliens oldalon az elektronikus dokumentumok (iratok és okiratok) a szerver oldalon biztonságos mentésre kerülnek, ahonnan szükség esetén, hiteles és jogosult kérésre biztonságosan visszaállíthatók.

A Client biztonsági tartományban az operációs rendszer hozzáférés ellenőrzést megvalósító funkciója, s a betartandó környezeti (fizikai, személyi és eljárásrendi) intézkedések védik meg az elektronikus dokumentumokat a jogosulatlan logikai és fizikai hozzáférés ellen.

A Client és Server közötti kommunikáció során a továbbított dokumentumok titkosítása véd a jogosulatlan hozzáférés (pontosabban megismerés) ellen.

A Server biztonsági tartományban operációs rendszer és alkalmazás szintű hozzáférés ellenőrzési és jogosultság kezelési mechanizmusok védenek a távoli illetéktelen logikai hozzáférés ellen. A dokumentumokat kiemelt fizikai, személyi és eljárásrendi védelmet biztosító számítógéptermi környezetben tárolják, ami megvédi ezeket a jogosulatlan fizikai hozzáféréstől.

A dokumentumok tartalmának jogosulatlan megismerést az akadályozza meg, hogy a Server oldalon kizárólag titkosított formában kerülnek tárolásra az oda mentett dokumentumok, a dekódoláshoz szükséges kulcsokat kizárólag a kliens oldal jogosult felhasználója ismeri.

A jogosulatlan hozzáférés elleni védelmet a Client és Server biztonsági tartományok, valamint ezek üzemeltetési környezetei együttesen biztosítják.

1.5.3 Az SFR_3 teljesítési módja

Mindkét biztonsági tartományban a futtatott alkalmazások külön-külön napló állományokat készítenek a kiváltott biztonsági eseményekről, egyúttal az ebben található bejegyzéseket az erre jogosultak számára megjelenítik. Az operációs rendszerek megvédik a napló állományokat a jogosulatlan hozzáférés ellen.

2. A biztonsági tartományok jellemzése

2.1 Bevezetés

2.1.1 Biztonsági tartomány hivatkozások

A szerver oldal biztonsági tartomány neve: Server biztonsági tartomány (Server).

A kliens oldali biztonsági tartomány neve: Client biztonsági tartomány (Client).

2.1.2 A biztonsági tartományok áttekintése

2.1.2.1 A Server biztonsági tartomány áttekintése

A rendszer felhasználója számára a biztonsági tartomány használata automatikus, amennyiben telepítette a kliens oldali online backup alkalmazást.

A biztonsági tartomány legfontosabb biztonsági tulajdonsága, hogy hosszú távon képes folyamatosan biztosítani a fogadott elektronikus dokumentumok sértetlen megőrzését, szükség esetén visszaküldését.

2.1.2.2 A Client biztonsági tartomány áttekintése

A Client biztonsági tartományban dolgoznak azok a felhasználók, akik létrehozzák, megjelenítik és kezelik az elektronikus dokumentumokat.

A hosszú távú biztonságos tárolás érdekében ezek a felhasználók igénybe veszik a Server biztonsági tartomány szolgáltatását, vagyis az elektronikus dokumentumok sértetlen megőrzését, szükség esetén visszaküldését.

A Client biztonsági tartomány legfontosabb biztonsági tulajdonságai az alábbi képességek:

- elektronikus dokumentumok létrehozása, kezelése és megjelenítése (ez a jelen SST hatókörén kívül esik),
- elektronikus dokumentumok titkosítása és átküldése az online backup szolgáltatást biztosító Server biztonsági tartománynak,
- szükség esetén a Server biztonsági tartományban tárolt adatok visszakérése, fogadása és eredeti állapotukra történő visszaállítása.

2.1.3 A biztonsági tartományok leírása

2.1.3.1 A Server biztonsági tartomány leírása

A Server biztonsági tartomány egy fizikai, személyi és eljárásrendi szempontokból kiemelt védelmet biztosító számítógéptermi környezetben helyezkedik el.

A Server biztonsági tartomány az alábbi két alrendszerből áll:

- backup szerver,
- replikációs szerver.

A backup szerver az alábbi komponensekből áll:

- backup szerver hardver: /géptípus: HP DL 320s G2 2U, CPU: 1X Intel Dual-Core Xeon 2,4 GHz, RAM: 4096 MB, Merevlemez: 6 x 750GB 1.5G SATA 7.2K (Raid 6-ban) az adatok számára + 2 x 36GB 3G SAS 15K (Raid 1-ben) az OS számára, 2db betáp csatlakozás/
- backup szerver operációs rendszer: Windows 2003 64 Bit R3 SP2
- web szerver (Apache 2.0.62)
- web konzol (ahonnan a web szerveren keresztül az alkalmazás menedzselhető)
- backup szerver alkalmazás: StoreGrid v2.5.1

A replikációs szerver az alábbi komponensekből áll:

- replikációs szerver hardver: /géptípus: HP DL 320s G2 2U, CPU: 1X Intel Dual-Core Xeon 2,4 GHz, RAM: 4096 MB, Merevlemez: 6 x 750GB 1.5G SATA 7.2K (Raid 6-ban) az adatok számára + 2 x 36GB 3G SAS 15K (Raid 1-ben) az OS számára, 2db betáp csatlakozás/
- replikációs szerver operációs rendszer: Windows 2003 64 Bit R3 SP2
- web szerver (Apache 2.0.62)
- web konzol (ahonnan a web szerveren keresztül az alkalmazás menedzselhető)
- replikációs szerver alkalmazás: StoreGrid v2.5.1

A két biztonsági tartomány között (a helyes konfigurálást követően) egyetlen kapcsolódási lehetőség (interfész) van:

- Backup Server port /alap értelmezés: port 32004, beállítandó érték: 32007 SSL/, ezen az interfészen keresztül egy speciális protokollt használva (mely 32007 esetén SSL védelem alatt is áll) képes a két biztonsági tartomány adatokat (backup vagy restore célból) egymásnak továbbítani. A továbbított adat (helyes konfigurálás esetén) tömörített és titkosított.

2.1.3.2 A Client biztonsági tartomány leírása

A Client biztonsági tartomány egy átlagos irodai elhelyezésű, internetre kapcsolt PC-s környezetben helyezkedik el.

A Client biztonsági tartomány az alábbi alrendszerekből áll:

- platform alrendszer (hardver és operációs rendszer),
- kliens oldali online backup alrendszer,
- egyéb alkalmazások alrendszer.

A platform alrendszer (hardver és operációs rendszer) biztosítja a többi alrendszer futtatásához szükséges környezetet. Tartomány szétválasztást, hozzáférés ellenőrzést és jogosultság kezelést biztosít ezek elkülönítéséhez és védelméhez.

A kliens oldali online backup alrendszer képes a hatókörébe eső dokumentumokat védett módon (tömörített és titkosított formában) a Server biztonsági tartományba továbbítani. Ugyancsak képes a Server biztonsági tartományban tárolt dokumentumok visszatöltésére és eredeti állapotába történő helyreállítására.

Az egyéb alkalmazások alrendszer számos más funkciót biztosít felhasználójának, melyeknek nincs köze a jelen SST által vizsgált rendszer funkcionalitáshoz (pl. elektronikus iratok és

okiratok létrehozása, kezelése, megjelenítése). Ugyanakkor biztosított, hogy ezen az alrendszeren keresztül sem lehet a jelen SST által vizsgált rendszer biztonsági funkcionalitását megkerülni vagy meghamisítani.

A Client biztonsági tartomány az alábbi komponensekből áll:

- internetre kapcsolt PC (hardverre vonatkozó minimális elvárások: 64 MB RAM és 50 MB szabad hely merevlemezen)
- operációs rendszer: Windows, Linux, Mac OS X, FreeBSD (v5.4-től)
- kliens oldali online backup alkalmazás (StoreGrid v2.5.1),
- web szerver (Apache 2.0.62)
- web konzol (ahonnan a web szerveren keresztül az alkalmazás menedzselhető)
- egyéb alkalmazások.

A két biztonsági tartomány között (a helyes konfigurálást követően) egyetlen kapcsolódási lehetőség (interfész) van:

- Backup Server port /alap értelmezés: port 32004, beállítandó érték: 32007 SSL/, ezen az interfészen keresztül egy speciális protokollt használva (mely 32007 esetén SSL védelem alatt is áll) képes a két biztonsági tartomány adatokat (backup vagy restore célból) egymásnak továbbítani. A továbbított adat (helyes konfigurálás esetén) tömörített és titkosított.

2.2 A biztonsági tartományokra vonatkozó megfelelőségi nyilatkozatok

A rendszer egészére megfogalmazott megfelelőségi nyilatkozatot lásd 1.2 alatt.

A Server biztonsági tartomány esetén az SFR_1 funkcionális biztonsági követelmény finomítása figyelembe veszi a [3] által a biztonságos megőrzésre megfogalmazott műszaki biztonsági követelményeket is.

2.3 A biztonsági tartományok üzemeltetési környezetének biztonsági céljai

A rendszer egészének üzemeltetési környezetére vonatkozó biztonsági célokat lásd 1.2 alatt.

Nincsenek tartomány szinten megfogalmazott kiegészítő biztonsági célok.

2.4 A biztonsági tartományok biztonsági követelményei

2.4.1 A Server biztonsági tartománytól elvárt biztonsági funkcionalitás

A Server biztonsági tartomány a rendszer egészére vonatkozó SFR_1 – SFR_3 követelmények teljesítésében különböző szerepet játszik. Az alábbiak finomítják ezeket a követelményeket, egyúttal meghatározzák a Server biztonsági tartománynak a finomított követelmények teljesítésében játszott szerepét is.

SFR_1: A rendszer olyan módon őrizze meg az elektronikus dokumentumokat, amely megvédi az elektronikus dokumentumokat a törlés, a megsemmisítés, a véletlen megsemmisülés és sérülés ellen.

SFR_1-t alapvetően a Server biztonsági tartomány teljesíti, ahhoz a Client biztonsági tartomány csak kis mértékben járul hozzá:

SFR_1a: A Server biztonsági tartomány képes legyen fogadni az elektronikus dokumentumokat a Client biztonsági tartománytól, majd archiválja azokat.

SFR_1b: A Server biztonsági tartomány védje meg az archivált elektronikus dokumentumokat a törlés, a megsemmisítés, a véletlen megsemmisülés és sérülés ellen, az alábbi műszaki biztonsági eljárások alkalmazásával (ahol az alábbi finomítás figyelembe veszi a [3] által a biztonságos megőrzésre megfogalmazott műszaki biztonsági követelményeket is):

SFR_1b_1: A Server biztonsági tartomány az archivált adatok rendelkezésre állásának megőrzése érdekében az alábbi funkciókat kell biztosítania:

- az archiválandó adatok elsődleges adathordozóra (backup szerver) írása,
- az elsődleges adathordozóra rögzített digitális tartalom duplikálása és a másolat fizikailag elkülöníthető tartalék adathordozóra (replikációs szerver) írása,
- az elsődleges adathordozóra rögzített digitális tartalom reprodukálása és a másolat csere adathordozóra írása,
- a digitális tartalom olvasása az elsődleges adathordozóról,
- a digitális tartalom olvasása a tartalék adathordozóról,
- a digitális tartalom olvasása a csere adathordozóról.

SFR_1b_2: A Server biztonsági tartomány az archivált adatok rendelkezésre állásának megőrzése érdekében az alábbi funkciókat kell biztosítania:

- az archiválandó adatokhoz tartozó bizonyíték rekordok, leíró információk és rendszerinformációk adatbázisba írása,
- az archiválandó adatokhoz tartozó bizonyíték rekordok, leíró információk és rendszerinformációk adatbázisból olvasása,
- az adatbázis mentése,
- az adatbázis helyreállítása mentésből.

SFR_1b_3: A Server biztonsági tartomány az archivált adatok sértetlenségének megőrzése érdekében az alábbi funkciókat kell biztosítania:

- az elsődleges adathordozó olvashatóságának rendszeres időközönkénti ellenőrzése,

- az elsődleges adathordozóról beolvasott archivált adatok sértetlenségének ellenőrzése,
- szükség esetén az elsődleges adathordozó cseréje,
- szükség esetén az elsődleges adathordozó tartalmának helyreállítása a másodlagos adathordozón tárolt információ segítségével,
- a tartalék adathordozó olvashatóságának rendszeres időközönkénti ellenőrzése,
- a tartalék adathordozóról beolvasott archivált adatok sértetlenségének ellenőrzése,
- szükség esetén a másodlagos adathordozó cseréje,
- szükség esetén a tartalék adathordozó tartalmának helyreállítása az elsődleges adathordozón tárolt információ megismételt duplikálásával.

SFR_1b_4: A Server biztonsági tartomány az archivált adatok sértetlenségének megőrzése érdekében az alábbi funkciókat kell biztosítania:

- adatbázis adminisztrálás,
- adatbázis frissítés fogadás funkció aktivizálásának jogosultság ellenőrzése,
- rendszer mentése,
- rendszer helyreállítása.

SFR_1b_5: A Server biztonsági tartománynak képesnek kell lennie annak biztosítására, hogy egy jogosultságában ellenőrzött, megőrzés befejezésre (törlésre) irányuló rendelkezés esetén az archivált adatot, visszaállíthatatlan módon törölje informatikai rendszeréből.

SFR_1b_6: A Server biztonsági tartománynak biztosítania kell a következő megőrzéssel kapcsolatos események naplózását:

- minden olyan biztonsági szempontból jelentős esemény, amely az archivált elektronikus adatok rendelkezésre állásának megőrzésével kapcsolatos,
- minden olyan biztonsági szempontból jelentős esemény, amely az archivált elektronikus adatok sértetlenségének megőrzésével kapcsolatos,
- minden olyan esemény, amely az archivált információk törlésével kapcsolatos.

SFR_1c: A Server biztonsági tartomány képes legyen visszaküldeni a letárolt elektronikus dokumentumokat a Client biztonsági tartománynak, erre vonatkozó jogosult kérés esetén.

SFR_2: A rendszer olyan módon őrizze meg az elektronikus dokumentumokat, amely megvédi az elektronikus dokumentumokat a jogosulatlan hozzáférés ellen.

SFR_2-t a Server és a Client biztonsági tartomány közösen teljesíti, de a két tartomány eltérő módon járul a teljesítéshez:

SFR_2a: A Server biztonsági tartománynak (hozzáférés-ellenőrzési és jogosultság-ellenőrzési mechanizmusokkal) meg kell védenie az általa tárolt elektronikus dokumentumokat a jogosulatlan logikai hozzáférés ellen.

SFR_2b: A Server biztonsági tartománynak (fizikai, személyi és eljárásrendi intézkedésekkel) meg kell védenie az általa tárolt elektronikus dokumentumokat a jogosulatlan fizikai hozzáférés ellen.

SFR_3: A rendszerben kiváltott biztonsági eseményekről napló állományok készüljenek, az ebben található bejegyzéseket a rendszer az erre jogosultak számára jelenítse meg, ugyanakkor védje meg a jogosulatlan hozzáférés ellen (rövid név: Audit).

SFR_3-t a Server és a Client biztonsági tartomány közösen teljesíti, és a két tartomány hasonló módon járul a teljesítéshez:

SFR_3a: A Server biztonsági tartomány az itt kiváltott biztonsági eseményekről napló állományokat (biztonsági napló) készítsen, az ebben található bejegyzéseket az erre jogosultak számára jelenítse meg, ugyanakkor védje meg a jogosulatlan hozzáférés ellen.

SFR_3b: A Server biztonsági tartomány tegye lehetővé a replikációs szerver biztonsági naplójának részleges vagy teljes megosztását a backup szerverrel. Megosztás esetén a replikációs szerver a meghatározott bejegyzéseket továbbítsa a backup szerver biztonsági naplójába.

2.4.2 A Client biztonsági tartománytól elvárt biztonsági funkcionalitás

A Client biztonsági tartomány a rendszer egészére vonatkozó SFR_1 – SFR_3 követelmények teljesítésében különböző szerepet játszik. Az alábbiak finomítják ezeket a követelményeket, egyúttal meghatározzák a Client biztonsági tartománynak a finomított követelmények teljesítésében játszott szerepét is.

SFR_1: A rendszer olyan módon őrizze meg az elektronikus dokumentumokat, amely megvédi az elektronikus dokumentumokat a törlés, a megsemmisítés, a véletlen megsemmisülés és sérülés ellen.

SFR_1-t alapvetően a Server biztonsági tartomány teljesíti, ahhoz a Client biztonsági tartomány csak kis mértékben járul hozzá:

SFR_1d: A Client biztonsági tartomány képes legyen továbbítani az elektronikus dokumentumokat a Server biztonsági tartománynak, amely megvédi azokat a törlés, a megsemmisítés, a véletlen megsemmisülés és sérülés ellen.

SFR_1e: A Client biztonsági tartomány képes legyen visszakérni, letölteni és helyreállítani a nála törölt, megsemmisített, megsemmisült vagy megsérült elektronikus dokumentumokat a Server biztonsági tartományból.

SFR_2: A rendszer olyan módon őrizze meg az elektronikus dokumentumokat, amely megvédi az elektronikus dokumentumokat a jogosulatlan hozzáférés ellen.

SFR_2-t a Client és a Server biztonsági tartomány közösen teljesíti, de a két tartomány eltérő módon járul a teljesítéshez:

SFR_2c: A Client biztonsági tartománynak (hozzáférés-ellenőrzési és jogosultság-ellenőrzési mechanizmusokkal) meg kell védenie a rendszerben tárolt elektronikus dokumentumokat a jogosulatlan logikai hozzáférés ellen.

SFR_2d: A Client biztonsági tartománynak (fizikai, személyi és eljárásrendi intézkedésekkel) meg kell védenie az általa tárolt elektronikus dokumentumokat a jogosulatlan fizikai hozzáférés ellen.

SFR_2e: A Client biztonsági tartománynak megfelelő kriptográfiai mechanizmusokat kell alkalmaznia az archiválandó adatok titkosításához, valamint a szükségessé váló dekódolásokhoz. A kriptográfiai mechanizmusok biztonságának feltétele annak garantálása, hogy a titkosító algoritmus bizonyítottan ellenáll minden ismert kripto-analitikai támadási módszernek, megfelelő, a nemzetközi elvárásoknak megfelelő kulcsméret kerül alkalmazásra, valamint biztonságos kulcselőállítási módszereket és kulcskezelési eljárásokat működtetnek.

SFR_3: A rendszerben kiváltott biztonsági eseményekről napló állományok készüljenek, az ebben található bejegyzéseket a rendszer az erre jogosultak számára jelenítse meg, ugyanakkor védje meg a jogosulatlan hozzáférés ellen (rövid név: Audit).

SFR_3-t a Client és a Server biztonsági tartomány közösen teljesíti:

SFR_3c: A Client biztonsági tartomány az itt kiváltott biztonsági eseményekről biztonsági naplót készítsen, az ebben található bejegyzéseket az erre jogosultak számára jelenítse meg, ugyanakkor védje meg a jogosulatlan hozzáférés ellen.

Az alábbi táblázat áttekinti a rendszer egészétől elvárt követelmények biztonsági tartományokra való finomítását.

A rendszer egészétől elvárt biztonsági funkcionalitás	A Server biztonsági tartománytól elvárt biztonsági funkcionalitás	A Client biztonsági tartománytól elvárt biztonsági funkcionalitás
SFR_1 (TrustSave)	SFR_1a (fogadás, archiválás)	SFR_1d (az elektronikus dokumentumok továbbítása a Server biztonsági tartománynak)
	SFR_1b_1 (a tárolt dokumentumok rendelkezésre állásának megőrzése)	
	SFR_1b_2 (a tárolt meta-adatok rendelkezésre állásának megőrzése)	
	SFR_1b_3 (a tárolt dokumentumok sértetlenségének megőrzése)	
	SFR_1b_4 (a tárolt meta-adatok sértetlenségének megőrzése)	SFR_1e (a törölt, megsemmisített, megsemmisült vagy megsérült elektronikus dokumentumok visszakérése, letöltése és helyreállítása a Server biztonsági tartományból)
	SFR_1b_5 (a törlés lehetősége)	
	SFR_1b_6 (a megőrzéssel kapcsolatos események naplózása)	
	SFR_1c (visszaküldés)	
SFR_2 (AccessControl)	SFR_2a (jogosulatlan logikai hozzáférés elleni védelem)	SFR_2c (jogosulatlan logikai hozzáférés elleni védelem)
	SFR_2b (jogosulatlan fizikai hozzáférés elleni védelem)	SFR_2d (jogosulatlan fizikai hozzáférés elleni védelem)
		SFR_2e (a mentendő dokumentumok titkosítása)
SFR_3 (Audit)	SFR_3a (biztonsági napló készítése, megvédése)	SFR_3c (biztonsági napló készítése, megvédése)
	SFR_3b (a replikációs szerver biztonsági naplójának részleges vagy teljes megosztása a backup szerverrel)	

2.4.3 A Server biztonsági tartománytól elvárt garanciák

A rendszer egészére elvárt SAP-A+ garanciacsomag (lásd 2.4.2) értelemszerűen vonatkozik a Server biztonsági tartományra is.

Ugyanakkor a Server biztonsági tartományra az alábbi kiegészítő garancia-összetevő elvárások is vannak:

Rendszer útmutató dokumentumok (ASGD)	ASGD_PRE.**2**	Előkészítő útmutató **igazolása**
	ASGD_OPE.**2**	Üzemeltetési útmutató **igazolása**
	ASGD_CON.**2**	Konfigurálási útmutató **igazolása**

A fenti táblázatból látható, hogy az útmutató dokumentációra szigorúbb elvárások vonatkoznak, mint a rendszer egészére. A szigorítás abban áll, hogy az értékelés a különböző útmutatók tartalmának független ellenőrzésére is kitér (tekintettel arra a tényre, hogy a szerver biztonsági tartomány az értékeléskor már működik, míg a kliens biztonsági tartományok működése a jövőben várható).

2.4.3.1 Az előkészítő útmutató igazolása (ASGD_PRE.2)

ASGD_PRE.2.1D A rendszer integrátornak a működőképes STOE mellé biztosítania kell az előkészítő útmutatót.

ASGD_PRE.2.1C Az előkészítő útmutatónak le kell írnia az STOE leszállított komponenseinek biztonságos elfogadásához alkalmazott valamennyi lépést, a komponens szállítójának szállítási eljárásaival összhangban.

ASGD_PRE.2.2C Az előkészítő útmutatónak le kell írnia az STOE komponenseinek biztonságos telepítéséhez, az STOE integrálásához és az üzemeltetési környezethez való biztonságos előkészülethez alkalmazott valamennyi lépést, az SST-ben leírt, üzemeltetési környezetre vonatkozó biztonsági célokkal összhangban.

ASGD_PRE.2.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASGD_PRE.2.2E **Az értékelőnek független ellenőrzést kell végeznie az előkészítő útmutató tartalmának gyakorlati alkalmazására vonatkozóan, személyi interjúk, az előkészítő útmutató mintavételezése, valamint a telepítés eredményének független vizsgálata útján.**

2.4.3.2 Az üzemeltetési útmutató igazolása (ASGD_OPE.2)

ASGD_OPE.2.1D A rendszer integrátornak üzemeltetési útmutatót kell biztosítania.

ASGD_OPE.2.1C Az üzemeltetési útmutatónak minden felhasználói szerepkörre le kell írnia azokat a felhasználó által elérhető funkciókat és jogosultságokat (beleértve a megfelelő figyelmeztetéseket is), melyeket egy biztonságos üzemeltetési környezetben ellenőrzés alatt kell tartani.

ASGD_OPE.2.2C Az üzemeltetési útmutatónak minden felhasználói szerepkörre le kell írnia, hogy az STOE által biztosított, elérhető interfészeket hogyan kell biztonságos módon használni.

ASGD_OPE.2.3C Az üzemeltetési útmutatónak minden felhasználói szerepkörre le kell írnia az elérhető funkciókat és interfészeket, különösen a felhasználó ellenőrzése alá tartozó minden biztonsági szempontból fontos paramétert, jelezve (ahol ez lehetséges) a biztonságos értékeket.

ASGD_OPE.2.4C Az üzemeltetési útmutatónak minden felhasználói szerepkörre világosan be kell mutatnia a felhasználó által elérhető funkciókkal kapcsolatban végrehajtandó, biztonsági szempontból fontos minden esemény típust, beleértve az SSF ellenőrzése alá eső egyedek biztonsági tulajdonságainak megváltoztatását is.

ASGD_OPE.2.5C Az üzemeltetési útmutatónak azonosítani kell az STOE összes lehetséges üzemmódját (beleértve a karbantartási és a meghibásodás vagy üzemeltetési hiba utáni üzemmódokat is), valamint ezek biztonságos üzemeltetésre gyakorolt következményeit és kihatásait.

ASGD_OPE.2.6C Az üzemeltetési útmutatónak minden felhasználói szerepkörre le kell írnia azokat a betartandó biztonsági intézkedéseket, melyek az SST-ben meghatározott, üzemeltetési környezetre vonatkozó biztonsági célok elérését szolgálják.

ASGD_OPE.2.7C Az üzemeltetési útmutatónak egyértelműnek és megalapozottnak kell lennie.

ASGD_OPE.2.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASGD_OPE.2.2E **Az értékelőnek független ellenőrzést kell végeznie az üzemeltetési útmutató specifikációinak gyakorlati alkalmazását illetően, személyi interjúk, az üzemeltetési útmutató mintavételezése és az üzemeltetés eredményeinek mintavételen alapuló független vizsgálata útján.**

2.4.3.3 A konfigurálási útmutató igazolása (ASGD_CON.2)

ASGD_CON.2.1D A rendszer integrátornak biztosítania kell egy konfigurálási útmutatót, amely meghatározza azokat a biztonság-vonzatú konfigurációs paramétereket, amelyek támogatják a rendszer komponenseinek az integrálását, és amelyek lehetővé teszik, hogy a szolgáltató rendszer biztonsági funkciói megvalósítsák és érvényre juttassák a szolgáltató rendszer működésre vonatkozó biztonsági koncepcióját és a kapcsolódó szabályzatokat.

ASGD_CON.2.1C A konfigurálási útmutatónak le kell írnia azokat a biztonsági konfigurációs paramétereket, amelyek a rendszer integrátor vagy az ezzel azonos szerepkörű és felelősségű STOE felhasználók/adminisztrátorok számára elérhetők.

ASGD_CON.2.2C A konfigurálási útmutatónak le kell írnia azoknak a biztonsági paramétereknek a használatát, amelyeket az STOE állíthat be abból a célból, hogy megvalósítsa és érvényre juttassa a rendszer biztonsági szabályzatait.

ASGD_CON.2.3C A konfigurálási útmutatónak figyelmeztetéseket kell tartalmaznia a konfigurálás által hozzáférhető azon funkciókra és privilégiumokra vonatkozóan, amelyeket egy biztonságos feldolgozási környezetben ellenőrizni kell.

ASGD_CON.2.4C A konfigurálási útmutatónak világosan be kell mutatnia az összes konfigurálással kapcsolatos felelősséget, amely az STOE biztonságos működtetéséhez szükséges.

ASGD_CON.2.5C A konfigurálási útmutatónak ellentmondás mentesnek kell lennie az értékeléshez átadott összes többi dokumentumhoz viszonyítva.

ASGD_CON.2.6C A konfigurálási útmutatónak le kell írnia az összes olyan biztonsági követelményt, amely az STOE-ra vonatkozik, beleértve az üzemeltetési környezetet is.

ASGD_CON.2.7C A konfigurálási útmutatónak meg kell mutatnia, hogy az STOE terv megvalósítja az összes olyan komponensre vonatkozó biztonsági paramétert, amelyet a rendszer-működési biztonsági koncepció megkövetel.

ASGD_CON.2.1E Az értékelőnek meg kell erősítenie, hogy a rendelkezésére bocsátott információk megfelelnek a bizonyítékok tartalmára és bemutatására vonatkozó minden követelménynek.

ASGD_CON.2.2E **Az értékelőnek mintavételezéssel, függetlenül ellenőriznie kell a konfigurálási útmutatóban meghatározott konfigurációs paraméterek gyakorlati alkalmazását.**

2.4.4 A Client biztonsági tartománytól elvárt garanciák

A rendszer egészére elvárt SAP-A garanciacsomag (lásd 2.4.2) értelemszerűen vonatkozik a Client biztonsági tartományra is. /Nincs kiegészítő garancia-összetevő elvárás./

2.5 A biztonsági tartományok összefoglaló előírásai

2.5.1 A Server biztonsági tartomány összefoglaló előírása

2.5.1.1 Az SFR_1 teljesítési módja

Az SFR_1 teljesítését (az elektronikus dokumentumok védelmét törlés, megsemmisítés, véletlen megsemmisülés és sérülés ellen) döntően a Server biztonsági tartomány valósítja meg. A Server biztonsági tartományhoz továbbított elektronikus dokumentumok megőrzését két nagy megbízhatóságú tároló szerver (backup és replikációs szerver) garantálja.

2.5.1.1.1 A mentés és helyreállítás biztosítása (SFR_1a és SFR_1c teljesítési módja)

A backup szerver automatikusan fogadja a mentési célból hozzá küldött elektronikus dokumentumokat a Client biztonsági tartománytól, majd archiválja azokat.

A backup szerver erre vonatkozó hitelesített és jogosultságában is ellenőrzött kérés esetén lehetővé teszi a kliens számára a letárolt elektronikus dokumentumok és meta adatok letöltését (restore, disastery recovery).

A replikációs szerver automatikusan fogadja a mentési célból hozzá küldött elektronikus dokumentumokat a backup szervertől, majd archiválja azokat.

A replikációs szerver erre vonatkozó hitelesített és jogosultságában is ellenőrzött kérés esetén lehetővé teszi a backup szerver számára a letárolt elektronikus dokumentumok és meta adatok letöltését (restore, disastery recovery).

2.5.1.1.2 A mentett adatok rendelkezésre állásának és sértetlenségének biztosítása (SFR_1b_1 - SFR_1b_4 teljesítési módja)

A Client biztonsági tartományból érkező elektronikus dokumentumokat és az ezekre vonatkozó meta adatokat a backup szerver letárolja.

A backup szerver által tárolt dokumentumok és meta adatok duplikált változatai automatikusan a fizikailag elkülönülő replikációs szerverre továbbítódnak, mely a backup szervernek egy meleg tartalékát képezi.

Mindkét szerver RAID technológiát alkalmaz a tárolt adatok rendelkezésre állásának és sértetlenségének biztosítására (lásd 4.2 Fogalom-meghatározások: RAID technológia)

Az operációs rendszer tárolására RAID 1 technológiát (duplikált, tükrözött tárolást) használnak a szerverek.

A mentett adatok tárolására RAID 6 technológiát használnak a szerverek, melyek megvalósítását csak igen speciális alkalmazások esetében szoktak alkalmazni.

Hardver hiba esetén szerződésben biztosított a cseregép (hibás modul) beállítása is.

2.5.1.1.3 A törlés és naplózás biztosítása (SFR_1b_5 teljesítési módja)

A törléssel kapcsolatos elvárásokat az alábbi biztosítják:

- az adminisztrátor törölheti a backup szerveren tárolt dokumentumokat és a hozzá tartozó meta adatokat,
- az adminisztrátor törölheti a replikációs szerveren tárolt dokumentumokat és a hozzá tartozó meta adatokat,
- a kliens oldalról megfelelő hitelesítés után törölhetők a backup és replikációs szerveren tárolt dokumentumok és a hozzá tartozó meta adatok.

2.5.1.1.4 A naplózás biztosítása (SFR_1b_6 teljesítési módja)

A backup szerver naplózza az alábbi eseményeket:

- archivált adatok rendelkezésre állásával kapcsolatos események,
- archivált adatok sértetlenségével kapcsolatos események,
- archivált információk törlésével kapcsolatos események.

2.5.1.2 Az SFR_2 teljesítési módja

Az SFR_2 teljesítését (az elektronikus dokumentumok védelmét jogosulatlan hozzáférés ellen) a Client és Server biztonsági tartományok, valamint ezek üzemeltetési környezetei együttesen biztosítják.

2.5.1.2.1 Az archivált adatok bizalmasságának védelme

A Client és Server közötti kommunikáció során a továbbított dokumentumok titkosítása véd a jogosulatlan megismerés ellen.

A Server oldalon kizárólag titkosított dokumentumok kerülnek tárolásra, így ezek jogosulatlan megismerés elleni védelme is biztosított.

2.5.1.2.2 A jogosulatlan logikai hozzáférés elleni védelem (SFR_2a teljesítési módja)

A Server biztonsági tartomány által biztosított funkciók (Server Management, Customer Management, License Management, Replication Management, Invoice Management, Client Management, Client's Backup Schedule Management) egy távoli web konzolon elérhető felhasználói interfészen, illetve egy web szerveren keresztül érhetők el.

A web konzolról való hozzáférés logikai védelme egy felhasználónév/jelszó azonosítás/hitelesítés mechanizmuson alapul. A felhasználónév/jelszó páros SSL védelem alatt jut át a web szerverhez.

A jogosult hozzáférők köre szabályozott és ellenőrzött.

2.5.1.2.3 A jogosulatlan fizikai hozzáférés elleni védelem (SFR_2b teljesítési módja)

A Server biztonsági tartományban mindkét szerver egy szigorú fizikai, személyi és eljárásrendi intézkedésekkel védett számítógéptermi környezetben, elzárt reck szekrényben van tárolva.

2.5.1.3 Az SFR_3 teljesítési módja

Az SFR_3 teljesítését (a biztonsági napló létrehozását, védelmét és a jogosultak számára való hozzáférés biztosítását) a Server és a Client biztonsági tartományok együttesen biztosítják.

2.5.1.4.1 Biztonsági naplózás (SFR_3a teljesítési módja)

A Server biztonsági tartományban kiváltott (valamint a Client biztonsági tartományból megosztás miatt átküldött) biztonsági eseményekről biztonsági napló készül. Az ebben található bejegyzéseket a web konzolról sikeresen hitelesített felhasználó megtekintheti, a napló eseményeket különböző szempontok (érintett kliens-azonosító, esemény típus, bekövetkezési időszak, bejegyzési szövegrészlet) szerint szűrheti.

2.5.1.4.2 Biztonsági naplózás (SFR_3b teljesítési módja)

A replikációs szerveren a web konzolról sikeresen hitelesített felhasználó megoszthatja a biztonsági napló tartalmát vagy annak egy részét a backup szerverrel. A megosztás a

megosztandó esemény típusoknak és a megosztásra továbbítás időzítésének (gyakoriság vagy bekövetkezett események száma) a meghatározásával történhet. Megosztás esetén a replikációs szerver az érintett bejegyzéseket a meghatározott időzítéssel továbbítja a backup szerver biztonsági naplójába.

2.5.2 A Client biztonsági tartomány összefoglaló előírása

2.5.2.1 Az SFR_1 teljesítési módja

Az SFR_1 teljesítését (az elektronikus dokumentumok védelmét törlés, megsemmisítés, véletlen megsemmisülés és sérülés ellen) döntően a Server biztonsági tartomány valósítja meg.

2.5.2.1.1 A mentés (backup) funkció (SFR_1d teljesítési módja)

A kliens biztonsági tartomány konfigurációs paraméterek által meghatározott gyakorisággal továbbítja a távoli mentés szolgáltatás igénybe vételére kijelölt elektronikus dokumentumokat a szerver biztonsági tartománynak, amely megvédi azokat a törlés, a megsemmisítés, a véletlen megsemmisülés és sérülés ellen.

2.5.2.1.2 A visszaállítás (restore) funkció (SFR_1e teljesítési módja)

A kliens biztonsági tartomány képes visszakérni, letölteni és helyreállítani a nála törölt, megsemmisített, megsemmisült vagy megsérült elektronikus dokumentumokat a szerver biztonsági tartományból.

2.5.2.2 Az SFR_2 teljesítési módja

Az SFR_2 teljesítését (az elektronikus dokumentumok védelmét jogosulatlan hozzáférés ellen) a kliens és szerver biztonsági tartományok, valamint ezek üzemeltetési környezetei együttesen biztosítják.

2.5.2.2.1 A jogosulatlan logikai hozzáférés elleni védelem (SFR_2c teljesítési módja)

A kliens biztonsági tartományban az operációs rendszer a jogosulatlan logikai hozzáférés ellen az alábbi mechanizmusokat biztosítja:

- Csak az operációs rendszeren keresztül indíthatók el az egyes alkalmazások (aláíró, dokumentum megjelenítő kliens oldali online backup).
- Felhasználó név alapján egyedileg azonosít minden felhasználót, és jelszó bekérésével, majd ennek ellenőrzésével hitelesíti azok állítólagos azonosságát, mielőtt egy felhasználónak lehetővé tenné az alkalmazások elindítását.
- Korlátozza az egymás utáni sikertelen hitelesítések számát.
- Nem jelzi ki a hitelesítési információkat (megadott jelszavakat).
- Az alkalmazások futásához megfelelő környezetet biztosít, amely garantálja az alkalmazások biztonságos szétválasztását (hogy az egyik alkalmazásból ne legyen elérhető a többi alkalmazás által kezelt értékek), és megvédi ezeket a külső beavatkozástól, hamisítástól vagy jogosulatlan felfedéstől.

A jogosult felhasználók köre korlátozott és szabályozott.

2.5.2.2.2 A jogosulatlan fizikai hozzáférés elleni védelem (SFR_2d teljesítési módja)

A kliens biztonsági tartományban fizikai, személyi és eljárásrendi intézkedések védik az irodai környezetben elhelyezett PC-t attól, hogy ellopják azt, vagy a gépen tárolt adatokhoz illetéktelen személyek fizikailag hozzáférjenek.

2.5.2.2.3 Az archivált adatok bizalmasságának védelme (SFR_2e teljesítési módja)

A kliens oldali online backup alkalmazás a szerver biztonsági tartományhoz továbbított adatokat előbb tömöríti (a ZLib tömörítő algoritmussal), majd titkosítja (a Blowfish titkosító algoritmussal). A titkosításhoz használt kulcs mérete (helyes konfigurálás esetén) 128 bit.

A tömörítéssel és titkosítással garantálható, hogy sem a kommunikáció, sem a távoli archiválás során senki nem ismerheti meg tartalmukat.

2.5.2.3 Az SFR_3 teljesítési módja

Az SFR_3 teljesítését (a biztonsági napló létrehozását, védelmét és a jogosultak számára való hozzáférés biztosítását) a Client és Server biztonsági tartományok együttesen biztosítják.

2.5.2.3.1 Biztonsági naplózás (SFR_3c teljesítési módja)

A szerver biztonsági tartományban kiváltott (valamint a kliens biztonsági tartományból megosztás miatt átküldött) biztonsági eseményekről biztonsági napló készül. Az ebben található bejegyzéseket a web konzolról sikeresen hitelesített felhasználó megtekintheti, a napló eseményeket különböző szempontok (érintett funkció, érintett kliens-azonosító, esemény típus, bekövetkezési időszak, bejegyzési szövegrészlet) szerint szűrheti.

3. Hivatkozások, fogalmak és rövidítések

3.1 Hivatkozások

A jelen rendszer biztonsági előirányzatban megfogalmazottak az alábbi mértékadó dokumentumokon alapulnak:

[1] Common Criteria for Information Technology Security Evaluation (September 2006 - version 3.1, revision 2) - Part 1: Introduction and general model - Part 2: Security functional components - Part 3: Security assurance components

[2]: Rendszerekre vonatkozó értékelési módszertan (az „e-Közigazgatási Keretrendszer Kialakítása" projekt keretében [5] továbbfejlesztésére kidolgozott dokumentum, mely megtalálható az alábbi helyen: http://kovetelmenytar.complex.hu)

[3]: Nemzeti Hírközlési Hatóság Hivatala – Ajánlás - Elektronikus archiválási szolgáltatások nyújtásához felhasznált megbízható rendszerekre vonatkozó biztonsági követelményekre, 2008. június

[4]: 114/2007. (XII. 29.) GKM rendelet a digitális archiválás szabályairól

[5]: Közigazgatási Informatikai Bizottság 25. számú ajánlása: Magyar Informatikai Biztonsági Ajánlások - Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma 5. számú segédlete: Értékelési módszertan (v1.0, 2008)

3.2 Fogalom-meghatározások

Jelen rendszer biztonsági előirányzat az alábbi fogalmakat az alábbi értelemben használja:

Biztonsági cél: Szándéknyilatkozat azonosított fenyegetések elleni fellépésről és/vagy meghatározott szervezeti biztonsági szabályzatoknak és feltételezésnek való megfelelésről.

Biztonsági követelmények: Az informatikai biztonsági célok lebontása biztonsági funkcionalitásra (SFR) és garanciára (SAR) vonatkozó szakmai követelmények egy összességére, melyek az értékelés tárgyára és annak üzemeltetési környezetére vonatkoznak.

Felhasználó: Az értékelés tárgyán kívüli bármely olyan entitás (humán felhasználó vagy egy külső informatikai entitás), amely kölcsönhatásban áll az értékelés tárgyával.

Garancia: Biztosíték arra nézve, hogy egy egyed megfelel a rá vonatkozó biztonsági céloknak.

Garanciaosztály: Garanciacsaládok egy olyan csoportja, melyek közös feladatokhoz kapcsolódnak. A jelen dokumentumban meghatározott garanciaosztályok az alábbiak: Rendszer biztonsági előirányzat (ASST), Rendszer fejlesztés (ASDV), Rendszer útmutató dokumentumok (ASGD), Rendszer konfiguráció kezelés (ASCM), Rendszer tesztelés (ASTE) és Rendszer sebezhetőség felmérés (ASVA).

Interfész: Különböző informatikai rendszerek közötti, illetve egy informatikai rendszer és felhasználói közötti adatátadást megvalósító rendszerkomponens.

RAID technológia: Több független merevlemez összekapcsolásával egy nagyobb méretű és megbízhatóságú logikai lemez létrehozása.

RAID 1: Alapja az adatok duplikált tárolása, azaz tükrözése. Az eltárolandó információ mindig párhuzamosan két meghajtóra kerül felírásra, s ezt a meghajtó-párost a számítógép egyetlen logikai meghajtónak látja. Az adatok olvasása párhuzamosan történik a két diszkről, bármelyik meghajtó meghibásodása esetén folytatódhat a működés.

RAID 2: A sávokra bontás módszerét használja, emellett egyes meghajtókat hibajavító kód tárolására tartja fenn. A meghajtók egy-egy sávjában a különböző diszkeken azonos pozícióban elhelyezkedő sávokból képzett hibajavító kódot tárolódnak. A módszer esetleges diszkhiba esetén képes annak detektálására, illetve kijavítására.

RAID 3: Felépítése hasonlít a RAID 2-re, viszont nem a teljes hibajavító kód, hanem csak egy diszknyi paritásinformáció tárolódik. Egy adott paritássáv a különböző diszkeken azonos pozícióban elhelyezkedő sávokból XOR művelet segítségével kapható meg. A rendszerben egy meghajtó kiesése nem okoz problémát, mivel a rajta lévő információ a többi meghajtó (a paritást tároló meghajtót is beleértve) XOR-aként megkapható.

RAID 4: Felépítése megegyezik a RAID 3-mal. Az egyetlen különbség, hogy itt nagyméretű sávokat definiálnak, így egy rekord egy meghajtón helyezkedik el, lehetővé téve egyszerre több (különböző meghajtókon elhelyezkedő) rekord párhuzamos írását, illetve olvasását.

RAID 5: A paritás információt nem egy kitüntetett meghajtón, hanem körbeforgó paritás használatával, egyenletesen az összes meghajtón elosztva tárolja, kiküszöbölvén a paritás meghajtó jelentette szűk keresztmetszetet.

RAID 6: A RAID 5 kibővítésének tekinthető. Itt nemcsak soronként, hanem oszloponként is kiszámítják a paritást. A módszer segítségével kétszeres meghajtó meghibásodás is kiküszöbölhetővé válik. A paritássávokat itt is az egyes meghajtók között, egyenletesen elosztva tárolják, de ezek természetesen kétszer annyi helyet foglalnak el, mint a RAID 5 esetében.

Rendszer biztonsági előirányzat (SST): Biztonsági követelmények és előírások olyan összessége, amelyet egy értékelt rendszerre, az értékelés alapjaként használnak.

Rendszer biztonsági funkcionalitás (SSF): Az értékelt rendszer mindazon részei, amelyekre a rendszer biztonsági szabályzatának helyes érvényre juttatásához támaszkodni kell, illetve lehet.

Rendszer biztonsági szabályzat: Egy vagy több biztonsági szabály, eljárás, gyakorlat vagy útmutató, amelyet egy informatikai rendszer biztonságos működtetéséhez a rendszer tulajdonosa állít fel.

Rendszer értékelési garanciacsomag (SAP): Garancia-összetevőkből álló csomag, amelyek egy-egy pontot képviselnek egy előre meghatározott garanciális skálán. A [2] által meghatározott rendszer értékelési módszertan a garanciális skála alábbi három szintjét különbözteti meg: alap (SAP-A), fokozott (SAP-F), kiemelt (SAP-K).

Szervezeti biztonsági szabályzat (OSP): Egy vagy több biztonsági szabály, eljárás, gyakorlat vagy útmutató, amelyet egy szervezet saját biztonságos működtetéséhez állít fel.

Szolgáltató (informatikai) rendszer: Egy konkrét informatikai elrendezés meghatározott céllal és üzemeltetési környezettel.

Támadó képesség: Támadás esetén annak érzékelt lehetősége, hogy a támadás sikeres lesz, a támadó szaktudásával, erőforrásaival és motivációjával kifejezve (Lehetséges szintjei: alap, megemelt-alap, közepes, magas, A [2] által meghatározott rendszer értékelési módszertan szerint lehetséges szintjei: alap, megemelt-alap).

Termék: Informatikai szoftver, förmver és/ vagy hardver által alkotott csomag, amelyek adott használatra vagy különböző szolgáltató rendszerekbe való beépítésre tervezett funkciókészletet biztosítanak.

3.3 Rövidítések

Jelen rendszer biztonsági előirányzat az alábbi táblázatban megadott rövidítéseket használja:

Rövidítés	Angol	Magyar
ASCM	Assurance: System Configuration Management	"Rendszer konfiguráció kezelés" garanciaosztály
ASCM_SBC	ASCM: System Base-Configuration	Rendszer alap konfiguráció garanciacsalád
ASCM_ECC	ASCM: Evaluated and Certified Components	Értékelt és tanúsított komponensek garanciacsalád
ASDV	Assurance: System Development	"Rendszer fejlesztés" garanciaosztály
ASDV_ARC	ASDV: Security Architecture	Biztonsági architektúra garanciacsalád
ASDV_OSC	ASDV: Operational Security Concepts	Rendszer-működési biztonsági koncepció garanciacsalád
ASDV_SDS	ASDV: STOE Design	STOE terv garanciacsalád
ASDV_SIS	ASDV: System Interface specification	Rendszer interfész specifikáció garanciacsalád
ASGD	Assurance: System Guidance documents	"Rendszer útmutató dokumentumok" garanciaosztály
ASGD_CON	ASGD: Configuration guidance	Konfigurálási útmutató garanciacsalád
ASGD_OPE	ASGD: Operational user guidance	Üzemeltetési útmutató garanciacsalád
ASGD_PRE	ASGD: Preparative guidance	Előkészítő útmutató garanciacsalád
ASTE	Assurance: Security Tests	"Rendszer tesztelés" garanciaosztály
ASTE_COV	ASTE: Coverage	Lefedettség garanciacsalád
ASTE_DPT	ASTE: Depth	Mélység garanciacsalád
ASTE_FUN	ASTE: Functional tests	Funkcionális tesztek garanciacsalád
ASTE_IND	ASTE: Independent testing	Független tesztelés garanciacsalád
ASVA	Assurance: System Vulnerability Assessment	"Rendszer sebezhetőség felmérés" garanciaosztály
ASVA_VAN	ASTE: Vulnerability Analysis	Sebezhetőségi elemzés garanciacsalád
BS	Backup server	Backup szerver
CC	Common Criteria	Közös szempontok
CEM	Common Evaluation Methodology	Közös értékelési módszertan
CM	Configuration Management	Konfiguráció kezelés
FW	Firewall	Tűzfal
IT	Information Technology	Információs technológia, informatika
NHH	---	Nemzeti Hírközlési Hatóság
OE	Object for the Environment	(Biztonsági) cél az üzemeltetési környezetre
OSP	Organisational Security Policy	Szervezeti biztonsági szabályzat
RAID	Redundant Array of Independent Disks	Redundáns független merevlemezes tömbök
RS	Replication server	Replikációs szerver
SAP	Security Assurance Package	Rendszer garanciacsomag
SAR	Security Assurance Requirement	Garanciális biztonsági követelmény
SFR	Security Functional Requirement	Funkcionális biztonsági követelmény
SSF	STOE Security Functionality	Rendszer biztonsági funkcionalitás
SST	System Security Target	Rendszer biztonsági előirányzat
STOE	System Target of Evaluation	Rendszer értékelés tárgya
TSA	Time Stamp Authority	Időbélyeg-szolgáltató
TST	Time Stamp Token	Időbélyeg token (válasz)
VPN	Virtual Private Network	Virtuális magánhálózat