MEGFELELÉS
ÉRTÉKELÉSI JELENTÉS

az iSave
online backup szolgáltatást biztosító
informatikai rendszerről

Verzió:	1.0
Fájl:	CER_iSave_v10.pdf
Minősítés:	Nyilvános
Oldalak:	48

Változáskezelés

Verzió	Dátum	A változás leírása
v0.9	2008.09.02.	A bizalmas minősítésű rendszer értékelés jelentésből készített első változat.
v1.0	2008.09.08.	Véglegesített változat.

A rendszer értékelési jelentést készítette:

dr. Balázs István

Digitally signed by dr. Balázs István
DN: CN = dr. Balázs István, C = HU, L = Budapest, O = HUNGUARD Kft., OU = értékelési divízió, T = értékelési divízió vezető
Reason: I am the author of this document
Location: Budapest
Date: 2008.09.10 17:21:33 +02'00'

dr. Balázs István

Hunguard Kft.

értékelési divízió vezető

Dr. Szabó István

Digitally signed by Dr. Szabó István
DN: CN = Dr. Szabó István, C = HU, L = Budapest, O = Hunguard Kft.
Reason: I am approving this document
Location: Budapest
Date: 2008.09.10 17:23:47 +02'00'

Tartalomjegyzék

1. Bevezetés

Jelen értékelési jelentés célja, hogy bemutassa az értékelés során végrehajtott tevékenységekből származó határozatokat, ezek indokolását, és minden ténymegállapítást, beleértve a rendszer integrálása során elkövetett esetleges hibákat és az értékelés során feltárt kiaknázható sebezhetőségeket is.

1.1 Azonosító adatok

A rendszer neve és verziója	Az iSave Informatika Kft. online backup szolgáltatását biztosító informatikai rendszer /rövid név: **iSave v2.3** vagy **iSave rendszer**/ Verzió: 2.3 [2302008080819]
Az értékelő szervezet adatai	Hunguard Kft 1125 Budapest, Kékgolyó u. 6.
A megbízó adatai	L-Sys Kft 1149 Budapest, Kövér Lajos u. 54.
A rendszer integrátor adatai	L-Sys Kft 1149 Budapest, Kövér Lajos u. 54.

1.2 Az értékelés mérföldkövei (tények)

Az előkészítési szakasz kezdési dátuma	2008.06.02.
Az előkészítési szakasz befejezési dátuma	2008.07.21.
Az értékelési szakasz kezdés dátuma	2008.07.23.
Az értékelési szakasz befejezési dátuma	2008.09.07.
A szerver oldali (éles) konfigurálás ellenőrzésének dátuma	2008.08.31.
Az üzemeltetési helyszín látogatásának dátuma	2008.09.05.
A rendszer biztonsági tesztelésének dátuma	2008.08.20. 2008.08.24. 2008.08.29. 2008.09.05.
A behatolás tesztelés dátuma automatikus (gyári) eszközökkel: saját eszközökkel:	 2008.08.18. 2008.08.31.
Rendszer értékelési jelentés tervezet elkészítésének dátuma	2008.08.28.
Rendszer értékelési jelentés (végleges) elkészítésének dátuma	2008.09.08.

1.3 Az értékelő adatai

Az értékelő munkacsoport vezetője	dr. Balázs István
Az értékelő munkacsoport tagjai	Farkas Gábor Badari Csaba Staub Klára

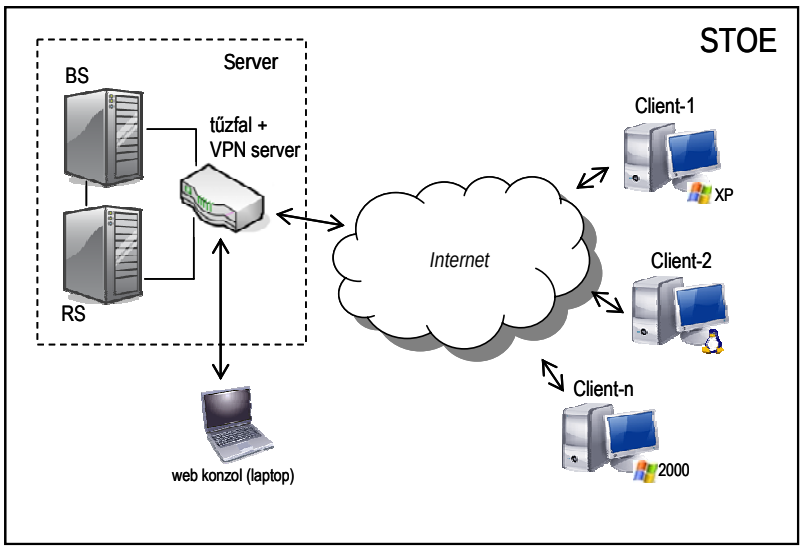
2. A rendszer szerkezeti leírása

2.1 A rendszer elhelyezése egy tágabb rendszerben

Az iSave rendszer értékelését egy tágabb rendszer keretében vizsgáljuk meg először.

A tágabb rendszer egy elektronikus aláírásra és online backup szolgáltatásra épülő digitális archiváló rendszer (rövid neve: DAR). A DAR egy olyan informatikai rendszer, mely lehetővé teszi törvény által előírt iratok, okiratok, illetve eredeti példányok megőrzését elektronikus úton, a 114/2007. GKM rendelet (a digitális archiválás szabályairól) elvárásai szerint.

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

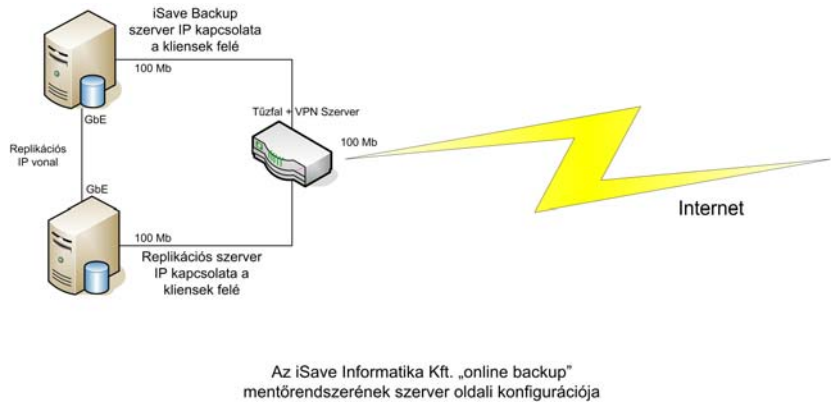


1. ábra: A DAR rendszer fizikai elemei és egymáshoz kapcsolódásuk

2.1.1 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.

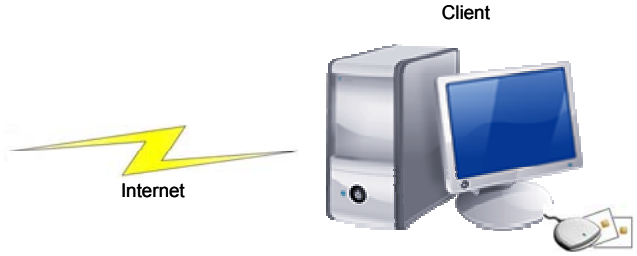


2. ábra: A szerver biztonsági tartomány fizikai elemei és kapcsolódásuk

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 visszatölthető.
- 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 távolról 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.2.0.59): melyek a két szerverhez biztosítanak távoli menedzselhetőséget.
- Backup alkalmazások (a szervereken futó alkalmazások: iSave_ugyfel v2.3): melyek a két szerveren biztosítják a mentési/helyreállítási funkciókat.
- Böngésző: mely a Web konzolról biztosítja a szerver biztonsági tartomány távoli menedzselhetőségét.
- Útmutatók: melyek segítségével elvégezhető 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:

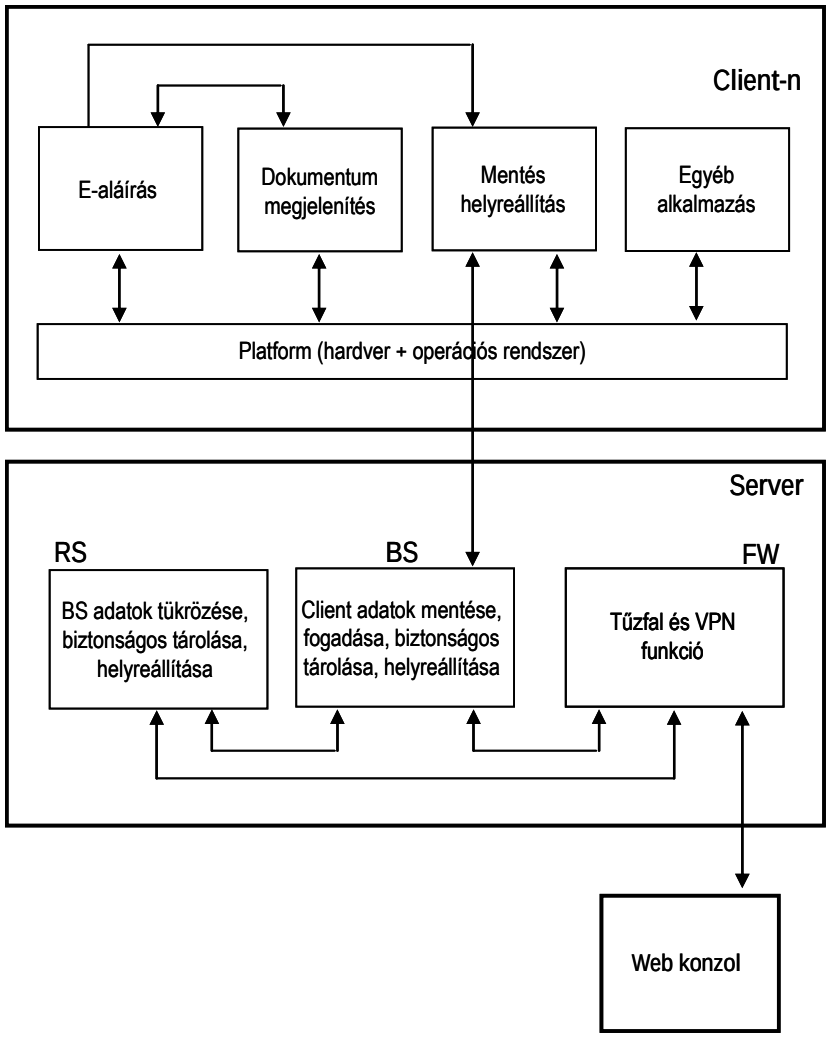
- Egy Internetre kapcsolt PC: mely a hardver alapokat biztosítja, egyúttal betölti a saját Backup alkalmazáshoz tartozó web konzol szerepét is.
- Operációs rendszer: mely a különböző szoftver komponenseknek biztosít megbízható futtatási környezetet.
- Elektronikus aláíró alkalmazás: mely az elektronikus aláírással kapcsolatos szolgáltatásokat biztosítja.
- Aláíró eszköz (pl. BALE), olvasó egység, ezekhez szükséges meghajtó: melyek az elektronikus aláírás létrehozását teszik lehetővé.
- Megjelenítő alkalmazások: melyek a dokumentumok és aláírások megjelenítésével kapcsolatos szolgáltatásokat biztosítják.
- Backup alkalmazás /iSave_ugyfel v2.3/: mely a kliens oldalon biztosítja a mentési/helyreállítási funkciókat.
- Böngésző: mely a saját Backup alkalmazás lokális menedzselhetőségét biztosítja.

2.1.2 A logikai hatókör és határok áttekintése

A DAR rendszerben különböző szolgáltatások nyújtása, illetve igénybevétele folyik.

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

- kliens biztonsági tartomány:
  - platform alrendszer (komponensei: hardver, operációs rendszer),
  - e-aláíró alrendszer (komponensei: elektronikus aláíró alkalmazás, aláíró eszköz, olvasó egység, meghajtó),
  - dokumentum megjelenítő alrendszer (komponensei: megjelenítő alkalmazások),
  - kliens oldali online backup alrendszer (komponensei: kliens oldali web konzol, böngésző és Backup alkalmazás /önálló telepítő programmal/),
- szerver biztonsági tartomány:
  - tűzfal alrendszer (komponensei: tűzfal, VPN szerver),
  - 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” üzemmódban/, web konzol, böngésző),
- web konzol.



4. ábra: A DAR 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),
- önvédelmet (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).

Az **e-aláírás** alrendszer:

- legalább fokozott biztonságú elektronikus aláírással lát el különböző elektronikus dokumentumokat,
- az elektronikus aláírás során minősített szolgáltató által kibocsátott időbélyegzőt helyez el az elektronikus aláírásban,
- ellenőrzi az elektronikus aláírások érvényességét,
- az aláírás ellenőrzés keretében az elektronikus aláírás hosszú távú érvényesítéséhez szükséges információkat (az érvényességi láncot) beszerzi és az aláírásba illeszti,
- az aláírás ellenőrzés keretében minősített szolgáltató által kibocsátott időbélyegzőt helyez el az érvényességi láncon,

- amennyiben a korábban elhelyezett időbélyegző kriptográfiai algoritmusa az elektronikus aláírás törvény szabályai szerint már nem biztonságos, minősített szolgáltató által kibocsátott időbélyegzőt helyez el ismételten az érvényességi láncon.

A **dokumentum megjelenítés** alrendszer:
- megjeleníti az aláírandó elektronikus dokumentumokat,
- megjeleníti az aláírt elektronikus dokumentumokat,
- megjeleníti az elektronikus aláírások különböző mezőit.

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 **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 jelszó 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 **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,
- a 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 **web konzol** alrendszer az alábbi feladatokat látja el:
- a tűzfal távoli menedzselése,
- a Backup szerver távoli menedzselése,
- a Replikációs szerver távoli menedzselése.

2.2 A rendszer értékelés tárgyának (iSave v2.3) hatóköre és határai

Az iSave v2.3 rendszer a DAR rendszerből úgy származtatható, hogy elhagyjuk belőle az e-aláíró és dokumentum megjelenítő alrendszereket.

Az iSave rendszer alap szolgáltatása, hogy központosított, on-line mentési és helyreállítási lehetőséget biztosít a kliensek számára.

Ez egy önálló szolgáltatás, de tekinthető a 114/2007. GKM rendelet (a digitális archiválás szabályairól) elvárásaiból a hosszú távú biztonságos megőrzésre vonatkozó követelmények támogatását biztosító rendszer egy alrendszerének is.

A továbbiakban ez az értékelési jelentés az iSave rendszert önálló szolgáltatásként vizsgálja.

2.2.1 Az iSave rendszer fizikai hatóköre és határai

Az 1. ábra az iSave rendszer fizikai hatókörét és határait is pontosan leírja.

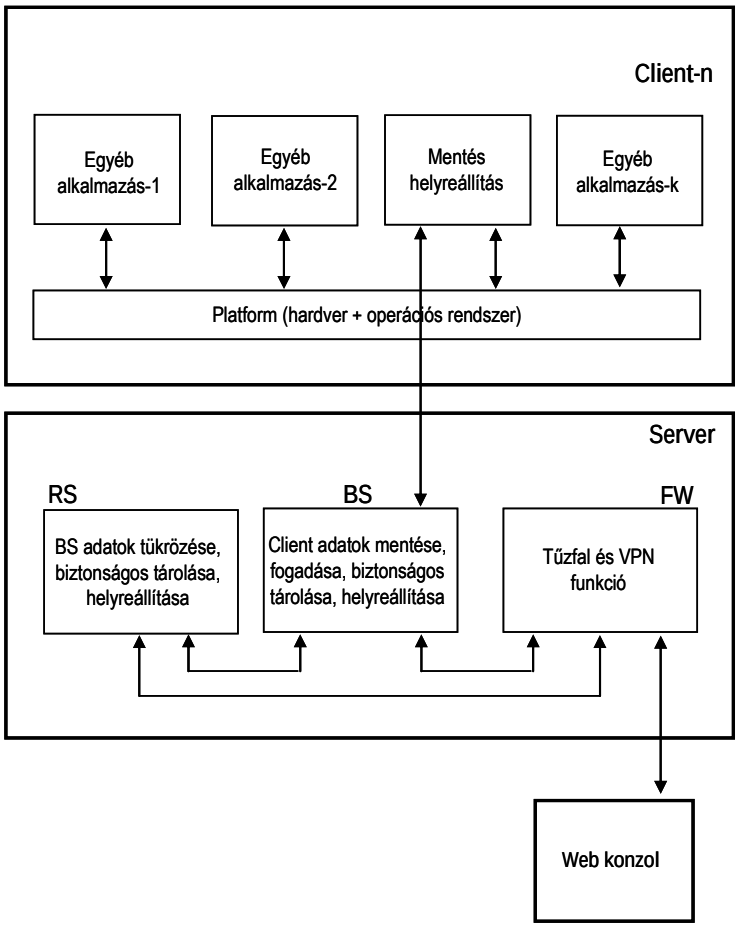
A szerver biztonsági tartomány fizikai komponensei megegyeznek a DAR rendszernél felsoroltakkal.

A kliens biztonsági tartomány fizikai komponensei annyiban térnek el a DAR rendszernél felsoroltaktól, hogy az alábbi komponensek nem az iSave rendszer, hanem annak környezete részét képezik:

- elektronikus aláíró alkalmazás,
- aláíró eszköz (pl. BALE), olvasó egység, ezekhez szükséges meghajtó,
- megjelenítő alkalmazások.

2.2.2 Az iSave rendszer logikai hatóköre és határai

Az 5. ábra az iSave rendszer logikai hatókörét és határait tekinti át.



5. ábra: Az iSave rendszer logikai hatóköre és határai

2.2.3 Az iSave rendszer legfontosabb tulajdonságai

2.2.3.1 Az iSave_ugyfel kliens oldali szoftver legfontosabb tulajdonságai

1. Automatikus mentési lehetőség a szerver oldali Backup szerverre.
2. Rugalmasan kijelölhető mentendő adatok (könyvtárak, meghatározott kiterjesztésű állományok).
3. Adatbázis (pl. mySQL) mentési lehetősége.
4. Ugyanarra az állományra több különböző verzió mentési lehetősége.
5. Egyszerű kezelés a böngésző alapú felhasználói interfészen keresztül.
6. A mentésre kijelölt területen a változások automatikus észlelése (a mentésekre ennek megfelelően kerül sor).
7. A mentés során csak a változások kerülnek továbbításra (és nem mindig az egész állomány).
8. Hatékony tömörítés alkalmazása a mentésre továbbított adatokra (ZLIB algoritmus).
9. Erős titkosító algoritmus alkalmazása a mentésre továbbított adatokra (Blowfish algoritmus).
10. Részleges és teljes helyreállítás lehetősége a Backup szerverről.
11. Hatékony naplózás és napló áttekintési funkciók biztosítása.

2.2.3.2 Támogatott operációs rendszerek

- Windows Vista, Windows XP, Windows 2000,
- Windows 2000/2003 SBS/2003 Server
- Debian Linux 3.0
- Mandrake Linux 10.0 és felette
- RedHat Linux 8.x és felette
- SuSE Linux 9.x és felette
- Mac OS X 10.x
- FreeBSD 5.4 és felette

Megjegyzés: Az értékelés során a fentiek közül az alábbiak kerültek ellenőrzésre, tesztelésre:

- Szerver oldalon: Windows 2003 64 Bit R3 SP2
- Kliens oldalon: Windows Vista, Windows XP, Suse Linux 10.1

2.2.3.3 Támogatott böngészők

- Internet Explorer 5.5 és felette
- Firefox 1.0 és felette
- Netscape 7.0 és felette
- Opera 9.0 és felette
- Mozilla 1.5 és felette
- Safari 1.2.4 és felette.

Megjegyzés: Az értékelés során a fentiek közül az alábbiak kerültek ellenőrzésre, tesztelésre:

- Internet Explorer 6.0 (XP-n)
- Internet Explorer 7.0 (Vista-n)
- Firefox 3.0 (XP-n)
- Firefox 1.5 (Suse-n)

2.2.3.4 Rendszer követelmények az ügyfél oldalon

Minimális hardver elvárások:

- 64 MB RAM
- 50 MB szabad hely a merevlemezen

Minimális szoftver elvárások:

- egy támogatott operációs rendszer,
- egy támogatott böngésző program.

3. Az értékelés jellemzése

Az alábbiakban az értékelés során alkalmazott értékelési módszereket, technikákat és szabványokat dokumentáljuk.

3.1 Rendszer biztonsági értékelési módszertan

Az iSave rendszer értékelése során az e-Közigazgatási Keretrendszer keretén belül az informatikai rendszerek technológia szempontú biztonsági értékelésére kidolgozott módszertant tekintettük meghatározónak.

A módszertant az alábbi dokumentumok határozzák meg:

- Rendszerekre vonatkozó értékelési módszertan [1],
- Útmutató rendszer integrátorok számára [2],
- Útmutató rendszer értékelők számára [3].

Mindhárom fenti dokumentum az „e-Közigazgatási Keretrendszer Kialakítása” projekt keretében került kidolgozásra, elérhető az alábbi helyen: http://kovetelmenytar.complex.hu

3.2 Megfelelés értékelés módszertan

Az iSave rendszer az alábbi mértékadó dokumentumban megfogalmazott követelményeknek való megfelelőséget állít:

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

A fenti dokumentum 2 és 4 §-ában megfogalmazott funkcionális és biztonsági követelményeknek való megfelelőséget külön is vizsgálta az értékelés, melynek módszere a következő volt.

Az értékelés az egyes követelményekre külön-külön határozatot hoz, hogy az alábbiakból melyik vonatkozik az adott követelményre:

- az adott követelményt az iSave rendszer **teljesíti**,
- az adott követelményt az iSave rendszer **támogatja** (az informatikai vagy a nem informatikai környezetre megfogalmazott működtetési feltétel teljesülése esetén a követelményt az iSave rendszer teljesíti),
- az iSave rendszer a követelmény kielégítését az (IT és nem IT) **környezettől várja el**.

Az egyes követelményekre meghozott határozatok az alábbiak alapján születhetnek:

- Dokumentáció: a fejlesztők által készített írásos dokumentációk alapján,
- Tapasztalat: a rendszer használata során szerzett „felhasználói” tapasztalatokból leszűrt következtetések alapján,
- Teszt: az integrátorok és értékelők által végzett tesztelés eredményei alapján,
- Interjú: az integrátorokkal folytatott személyes konzultációk alapján,

A követelményekre meghozott határozatot rövid indoklás követi.

Az alkalmazott módszertan részeként, a különböző termékek későbbi összehasonlíthatósága érdekében a követelményekre hozott határozatokat egy táblázat foglalja össze.

Jelen megfelelés értékelési jelentés a második módszer szerint végrehajtott értékelési eredményeket tartalmazza. A rendszer biztonsági értékelési módszertan szerint külön (nem nyilvános) értékelési jelentés készült.

4. Az értékelés eredményei

A rendszer egészétől elvárt biztonsági funkcionalitást a [4] rendelet 2 és 4 §-a határozza meg, az alábbi módon:

2 §

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

(2) A megőrzésre kötelezett köteles biztosítani, hogy az őrzött elektronikus dokumentumok értelmezhetősége (olvashatósága) - a dokumentumok megjeleníthetőségét lehetővé tevő szoftver- és hardverkörnyezet biztosításával - a megőrzési kötelezettség időtartama alatt megmaradjon.

4. §

(1) Ha a megőrzésre szánt elektronikus dokumentumot az Eat. szerinti legalább fokozott biztonságú elektronikus aláírással látták el, a megőrzésre kötelezett a megőrzéssel az Eat.-ban meghatározott archiválási szolgáltatót is megbízhat (*a vizsgált esetben erre nem kerül sor*).
Ha a legalább fokozott biztonságú elektronikus aláírással ellátott dokumentum megőrzéséről a megőrzésre kötelezett nem az Eat.-ban meghatározott archiválási szolgáltató útján gondoskodik, akkor az e §-ban foglaltak szerint kell eljárnia a 2. § (1) bekezdés szerinti utólagos módosítás lehetőségének kizárása érdekében.

(2) Ha több elektronikus dokumentumon helyeztek el egyetlen, az Eat. szerinti legalább fokozott biztonságú elektronikus aláírást, akkor ezeket a dokumentumokat a megőrzés során együtt kell kezelni.

(3) A megőrzésre kötelezett köteles az elektronikus aláírás érvényességét ellenőrizni, majd - ha az elektronikus aláíráson még nincs elhelyezve - az Eat. szerinti minősített szolgáltató által kibocsátott időbélyegzőt elhelyeztetni az elektronikus dokumentum aláírásán.

(4) Ha a megőrzési kötelezettség időtartama hosszabb, mint az elektronikus aláírás elhelyezésétől számított 11 év, a megőrzésre kötelezett
- *a)* gondoskodik az elektronikus aláírás hosszú távú érvényesítéséhez szükséges információk (az érvényességi lánc) beszerzéséről és megőrzéséről;
- *b)* az Eat. szerinti minősített szolgáltató által kibocsátott időbélyegzőt helyeztet el az érvényességi láncon;
- *c)* a *b)* pontban meghatározott időbélyegzést megismétli akkor, ha a *b)* pont szerint korábban elhelyezett időbélyegző kriptográfiai algoritmusa az Eat. szabályai szerint már nem biztonságos.

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

SFR_1 (DigSign): A rendszer olyan módon őrizze meg az elektronikus dokumentumokat, amely kizárja az utólagos módosítás lehetőségét.

SFR_2 (TrustSave): 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_3 (AccessControl): A rendszer olyan módon őrizze meg az elektronikus dokumentumokat, amely megvédi az elektronikus dokumentumokat a jogosulatlan hozzáférés ellen.

SFR_4 (View): A rendszer őrizze meg az elektronikus dokumentumok értelmezhetőségét (olvashatóságát) a megőrzési kötelezettség időtartama alatt, az ezt lehetővé tevő szoftver- és hardverkörnyezet biztosításával.

SFR_5 (Audit): 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.

A DAR különböző alrendszerei a fenti biztonsági követelmények teljesítésében különböző szerepet játszanak, ahogyan azt az alábbi táblázat mutatja.

Követelmény	Határozat	Kiegészítő magyarázat
	az iSave alrendszer a követelmény kielégítését:	
SFR_1 (DigSign)	**a környezettől várja el (az aláíró programtól)**	**SFR_1 érvényre juttatásában az iSave alrendszer nem működik közre,** ezt az elektronikus aláíró alrendszernek kell teljesítenie.
SFR_2 (TrustSave)	**Teljesíti**	SFR_2 érvényre juttatását teljes mértékben az iSave alrendszer végzi.
SFR_3 (AccessControl)	**Teljesíti**	Az iSave alrendszer saját hatáskörében megvédi az elektronikus dokumentumokat a jogosulatlan hozzáférés ellen.
SFR_4 (View)	**a környezettől várja el (a dokumentum megjelenítő programtól)**	**SFR_4 érvényre juttatásában az iSave alrendszer nem működik közre,** ezt a dokumentum megjelenítő alrendszernek kell teljesítenie.
SFR_5 (Audit)	**Támogatja**	Az iSave alrendszer teljesíti a naplózással kapcsolatos elvárásokat a hatókörében kiváltott biztonsági eseményekre. Az elektronikus aláíró alrendszernek is teljesítenie kell ugyanezeket az elvárásokat a saját hatókörében kiváltott biztonsági eseményekre.

Az alábbiak tovább bontják azokat a követelményeket (SFR_2, SFR_3 és SFR_5), amelyek érvényre juttatásában az iSave rendszer is közreműködik, meghatározva és indokolva az egyes követelmények teljesülésére vonatkozó határozatokat.

Követelmény: SFR_2a:

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

Határozat: a fenti követelményt az iSave rendszer **teljesíti**.

A határozat alapja:

Dokumentáció	Tapasztalat	Teszt	Interjú
+	+	+	-

Indoklás:

Az elektronikus dokumentumok fogadása és letárolása alap szolgáltatása az iSave rendszernek.

Ezt a tulajdonságot részletesen leírják a különböző dokumentációk, köztük az alábbiak:

- rendszer biztonsági előirányzat,
- a rendszer-működés biztonsági koncepciója,
- iSave_ugyfel program - Help fájl.

A követelmény teljesülését az értékelők saját felhasználói tapasztalatai is megerősítik.

A követelmény teljesülését számos teszt ellenőrizte és igazolta, köztük az alábbiak:

- 1.1 /Mentési ütemező létrehozása, mentés egygépes kliens és szerver üzemmódban/,
- 2.1 /Mentési ütemező létrehozása, mentés különálló kliens, Backup szerver üzemmódban/,
- 3.1 /Mentési ütemező létrehozása, mentés különálló kliens, Backup szerver üzemmódban/,
- 3.3 /Mentési ütemező létrehozása, mentés különálló kliens, Backup szerver, Replikációs szerver üzemmódban/,
- 3.8 /Mentési adatbázisok ellenőrzése kliens és Backup szerver oldalon/,
- 3.10 /Mentési adatbázisok ellenőrzése kliens és Replikációs szerver oldalon/,
- 4.1 /Mentési ütemező létrehozása éles rendszerben/,
- 4.3 /Módosított adat mentése éles rendszerben/.

Összetett követelmény: SFR_2b:

> ***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:***
>
> - **SFR_2b_1** (a tárolt dokumentumok rendelkezésre állása),
> - **SFR_2b_2** (a tárolt meta-adatok rendelkezésre állása),
> - **SFR_2b_3** (a tárolt dokumentumok sértetlensége),
> - **SFR_2b_4** (a tárolt meta-adatok sértetlensége),
> - **SFR_2b_5** (a törlés lehetősége),
> - **SFR_2b_6** (a megőrzéssel kapcsolatos események naplózása).

Határozat: a fenti követelményt az iSave rendszer **teljesíti**.

Indoklás: Lásd az egyes részhatározatok (SFR_2b_1 - SFR_2b_6) alatt.

Követelmény: SFR_2b_1:

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

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

Határozat: a fenti követelményt az iSave rendszer **teljesíti**.

A határozat alapja:

Dokumentáció	Tapasztalat	Teszt	Interjú
+	+	+	+

Indoklás:

A szerver oldalon mentett elektronikus dokumentumok rendelkezésre állása (a pontos helyreállítás lehetőségének biztosítása) alap szolgáltatása az iSave rendszernek.

Az elektronikus dokumentumok biztos rendelkezésre állása az alábbi környezeti és műszaki biztonsági intézkedéseken alapul:

Környezeti biztonsági intézkedések:

1. A tárolást két fizikailag elkülönült szerver (Backup és Replikációs) végzi, melyek egy hosting szolgáltatás keretében egy védett adatközpont számítógép termében kaptak elhelyezést.

2. A szolgáltatást a Magyar Telekom Nyilvánosan Működő Részvénytársaság biztosítja, mely szerződésben (ÁSZF) vállalta az alábbiakat:

a) Géptermi kiépítés (álpadló és álmennyezet a kábelezésnek, érzékelőknek és légkondicionálóknak),

b) Garantált áramellátás (szünetmentes áramforrás, két független betáplálás, tartalék dízel generátorok, éves szinten **99,999%**-os minőségi célértékkel garantált elektromos áram rendelkezésre állás),

c) Állandó hőmérséklet (redundánsan kiépített és monitorozott klímaberendezések, éves szinten **99,999%**-os minőségi célértékkel garantált temperált hőmérséklet),

d) Tűzvédelem (független tűzvédelmi rendszer, tűzgátló ajtók, automatikus oltás gáz alapú oltórendszerrel, mely megvédi az eszközök állagát),

e) Elárasztás elleni védelem (vizesblokk nincs a közelben, szabályozott páratartalom, cseppvíz-érzékelők),

f) Túlfeszültség elleni védelem (villámhárító-rendszer, „C” típusú túlfeszültség-védelem),

g) A számítógépes hálózat ellenőrzése (központi monitoring rendszer, hibás működés esetén riasztás és naplózás),

h) Internet csatlakozás (éves szinten **99,5%**-os minőségi célértékkel garantált Internet kapcsolat rendelkezésre állás)

i) Cseregép szolgáltatás (a bérelt eszköz típusával azonos, vagy azzal kompatibilis eszköz raktáron tartása, a meghibásodás esetén szükségessé váló csere érdekében, merevlemez károsodás esetén funkcionálisan azonos cseregép biztosítása),

j) Védett hálózati elhelyezés (megadott IP protokoll portok korlátozása bizonyos IP címekről).

k) Egyedi felelősségbiztosítás (a szolgáltató évenként 5 milliárd forint fedezettel rendelkező felelősségbiztosítással bír az üzemeltetett eszközök esetleges megsemmisülése, értékcsökkenése esetére).

3. A védett környezet biztosítja, hogy a tárolt adatokat illetéktelenül nem lehet ellopni vagy megsemmisíteni (erről részletesebben lásd az SFR_3b követelményre vonatkozó határozat indoklását).

Műszaki biztonsági intézkedések:

1. A tárolás elsődleges adathordozója a Backup szerver, melyre minden klienstől a konfigurált mentési ütemezők szerint automatikusan kerülnek át a kijelölt elektronikus dokumentumok.

2. A tárolás fizikailag elkülönített tartalék adathordozója a Replikációs szerver, melyre minden Backup szerverre érkező adat azonnal átkerül (tükröződik).

3. A két szerver közötti (pont-pont közötti, nagy sebességű) adatátvitel fizikailag biztonságos, az SSL kapcsolat pedig garantálja az adatátvitel sértetlenségét is.

4. Mindkét szerver RAID-es technológiát alkalmaz a működtető szoftver és a mentett adatok tárolására. A RAID technológia lényege: több független merevlemez összekapcsolásával egy nagyobb méretű és megbízhatóságú logikai lemez létrehozása.

5 Mindkét szerveren **RAID 1**-es technológia biztosítja az operációs rendszer és a szoftver alkalmazás rendelkezésre állását. A RAID 1 eljárás alapja az adatok duplikált tárolása, azaz tükrözése. Az eltárolandó információ párhuzamosan két meghajtóra kerül felírásra, s e meghajtó párost a számítógép egy szimpla kapacitású logikai meghajtónak lát. Az eljárás igen jó hibavédelmet biztosít, bármely meghajtó meghibásodása esetén folytatódhat a működés.

6. Mindkét szerveren **RAID 6**-os technológia biztosítja a mentett elektronikus dokumentumok rendelkezésre állását. A ***RAID 2*** a sávokra bontás módszerét használja, emellett egyes meghajtókat hibajavító kód tárolására tartanak fenn. Ezen meghajtók egy-egy sávjában a különböző diszkeken azonos pozícióban elhelyezkedő sávokból képzett hibajavító kódot tárolnak. A módszer esetleges diszkhiba esetén képes annak detektálására, illetve kijavítására. A ***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. A ***RAID 4*** felépítése a RAID 3-mal megegyezik. 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. A ***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. A ***RAID 6*** a RAID 5 kibővítésének tekinthető, s ez jelenleg a legköltségesebb, egyúttal a legnagyobb rendelkezésre állást biztosító RAID-megoldás. A RAID 6 esetén 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.

7. Olyan fokú meghibásodás esetén, amelyet a RAID 6-os technológia sem képes helyreállítani, mindkét szerverről egy hibaüzenet generálódik a rendszer adminisztrátor felé.

8. A Backup szerver olyan fokú meghibásodása esetén, amelyet a RAID 6-os technológia sem képes helyreállítani, aktivizálható a Replikációs szerver, melyről a (kijavított) backup szerver teljes eredeti tartalma helyreállítható.

9. A Replikációs szerver olyan fokú meghibásodása esetén, amelyet a RAID 6-os technológia sem képes helyreállítani, a Backup szerverről a (kijavított) Replikációs szerver teljes eredeti tartalma helyreállítható.

A fenti környezeti biztonsági intézkedéseket részletesen leírja az alábbi dokumentum:

- Általános Szerződési Feltételek (a Magyar Telekom Nyilvánosan Működő Részvénytársaság és a szolgáltatást igénybe vevő iSave Informatika Kft.)

A fenti műszaki biztonsági intézkedéseket részletesen leírják az alábbi dokumentumok:

- rendszer biztonsági terv,
- a rendszer-működés biztonsági koncepciója.

A követelmény teljesülését az értékelők saját felhasználói tapasztalatai is megerősítik:

- a környezeti biztonsági intézkedések egy részét helyszíni látogatáson ellenőrizték, valamint elkérték és áttanulmányozták az automatikus monitorozó rendszer havi jelentéseit,
- a műszaki biztonsági intézkedéseket a gyakorlatban többszörösen kipróbálták.

A követelmény teljesülését számos teszt ellenőrizte és igazolta, köztük az alábbiak:

- 1.1 /Mentési ütemező létrehozása, mentés egygépes kliens és szerver üzemmódban/ (a,b),
- 1.2 / Fájl visszaállítása egygépes kliens-szerver üzemmódban / (d,e),
- 2.1 /Mentési ütemező létrehozása, mentés különálló kliens, Backup szerver üzemmódban/ (a,b),
- 3.1 /Mentési ütemező létrehozása, mentés különálló kliens, Backup szerver üzemmódban/ (a,b),
- 3.2 /Replikációs szerver telepítése és beállítása a Backup szerverben/ (c),
- 3.3 /Mentési ütemező létrehozása, mentés különálló kliens, Backup szerver, Replikációs szerver üzemmódban/ (a,b,c),
- 3.5 /Mentés visszaállítása kliens oldalon Backup szerverről/ (d,e),
- 3.6 /Mentés visszaállítása kliens oldalon Replikációs szerverről/ (f),
- 3.7 /Kliens újra telepítése és teljes mentés visszatöltése Replikációs szerverről kliensre/ (f),
- 3.8 /Mentési adatbázisok ellenőrzése kliens és Backup szerver oldalon/ (a,b,c),
- 3.10 /Mentési adatbázisok ellenőrzése kliens és Replikációs szerver oldalon/ (a,b,c),
- 3.11 /Backup szerver leállítása és újratelepítése/ (a,c,f),
- 3.12 /Replikációs szerver leállítása és újratelepítése/ (c,d),
- 3.14 /Kliens konfigurációs adatainak visszatöltése a Backup szerverről/ (d,e),
- 4.1 /Mentési ütemező létrehozása éles rendszerben/ (b,c),
- 4.3 /Módosított adat mentése éles rendszerben/ (b,c).
- 4.5 /Kliens adatainak visszaállítása éles rendszerben/ (d).

A követelmény teljesülését az értékelők és a szolgáltatást biztosító megbízó közötti szóbeli megbeszélések (interjúk, konzultációk) is megerősítik.

Követelmény: SFR_2b_2:

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

a) az archiválandó adatokhoz tartozó bizonyíték rekordok, leíró információk és rendszerinformációk adatbázisba írása,
b) az archiválandó adatokhoz tartozó bizonyíték rekordok, leíró információk és rendszerinformációk adatbázisból olvasása,
c) az adatbázis mentése,
d) az adatbázis helyreállítása mentésből.

Határozat: a fenti követelményt az iSave rendszer **teljesíti**.

A határozat alapja:

Dokumentáció	Tapasztalat	Teszt	Interjú
+	+	+	+

Indoklás:

A szerver oldalon mentett elektronikus dokumentumokhoz tartozó meta-adatok (bizonyíték rekordok, leíró információk és rendszerinformációk) rendelkezésre állása (a pontos helyreállítás lehetőségének biztosítása) alap szolgáltatása az iSave rendszernek.

Az elektronikus dokumentumokhoz tartozó meta-adatok biztos rendelkezésre állása az alábbi környezeti és műszaki biztonsági intézkedéseken alapul:

Környezeti biztonsági intézkedések:

A szerver oldalon mentett meta-adatokra pontosan ugyanazok a környezeti biztonsági intézkedések vonatkoznak, mint a mentett elektronikus dokumentumokra (lásd SFR_2b_1 követelményre hozott határozat indoklása).

Műszaki biztonsági intézkedések:

A szerver oldalon mentett meta-adatokra nagyon hasonló műszaki biztonsági intézkedések vonatkoznak, mint a mentett elektronikus dokumentumokra (lásd SFR_2b_1 követelményre hozott határozat indoklása). Az alábbiak az apróbb különbségeket határozzák meg.

1*. A tárolás elsődleges adathordozója a Backup szerver, melyre minden klienstől a konfigurált mentési ütemezők szerint automatikusan kerülnek át a kijelölt elektronikus dokumentumok, *s az ezekhez tartozó kiegészítő információk (meta-adatok, pl. mentési paraméterek, fájl és könyvtárnevek). A Backup szerverre kerülő meta-adatok adatbázisba kerülnek, melynek felhasználásával valósulhat meg az inkrementális (csak a változásokat továbbító) mentés, a mentett adatok kliens oldalról történő áttekintése, visszatöltése, esetleges törlése.*

A környezeti biztonsági intézkedéseket az alábbi dokumentum részletezi:
- Általános Szerződési Feltételek.

A műszaki biztonsági intézkedéseket az alábbi dokumentumok részletezik:
- rendszer biztonsági terv,
- a rendszer-működés biztonsági koncepciója.

A követelmény teljesülését az értékelők saját felhasználói tapasztalatai is megerősítik:

- helyszíni látogatás, havi jelentések áttanulmányozása,
- a műszaki biztonsági intézkedéseket a gyakorlatban többszörösen kipróbálták.

A követelmény teljesülését számos teszt ellenőrizte és igazolta, köztük az alábbiak:

- 1.1 /Mentési ütemező létrehozása, mentés egygépes kliens és szerver üzemmódban/ (a),
- 1.2 / Fájl visszaállítása egygépes kliens-szerver üzemmódban / (b),
- 2.1 /Mentési ütemező létrehozása, mentés különálló kliens, Backup szerver üzemmódban/ (a),
- 3.1 /Mentési ütemező létrehozása, mentés különálló kliens, Backup szerver üzemmódban/ (a),
- 3.2 /Replikációs szerver telepítése és beállítása a Backup szerverben/ (c),
- 3.3 /Mentési ütemező létrehozása, mentés különálló kliens, Backup szerver, Replikációs szerver üzemmódban/ (a,c),
- 3.5 /Mentés visszaállítása kliens oldalon Backup szerverről/ (b),
- 3.8 /Mentési adatbázisok ellenőrzése kliens és Backup szerver oldalon/ (a,c),
- 3.9 /Kliens oldali mentési paraméterek módosítása/ (a,c),
- 3.10 /Mentési adatbázisok ellenőrzése kliens és Replikációs szerver oldalon/ (a,c),
- 3.11 /Backup szerver leállítása és újratelepítése/ (a,d),
- 3.12 /Replikációs szerver leállítása és újratelepítése/ (b),
- 3.13 /Backup szerver konfigurációs adatainak visszatöltése a Replikációs szerverről/ (a,d),
- 3.14 /Kliens konfigurációs adatainak visszatöltése a Backup szerverről/ (b),
- 4.1 /Mentési ütemező létrehozása éles rendszerben/ (a),
- 4.2 /Mentési ütemező módosítása éles rendszerben/ (a),
- 4.4 /Kliens konfigurációjának visszaállítása éles rendszerben/ (d).

A követelmény teljesülését az értékelők és a szolgáltatást biztosító megbízó közötti szóbeli megbeszélések (interjúk, konzultációk) is megerősítik.

Követelmény: SFR_2b_3:

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

a) az elsődleges adathordozó olvashatóságának rendszeres időközönkénti ellenőrzése,
b) az elsődleges adathordozóról beolvasott archivált adatok sértetlenségének ellenőrzése,
c) szükség esetén az elsődleges adathordozó cseréje,
d) szükség esetén az elsődleges adathordozó tartalmának helyreállítása a másodlagos (tartalék) adathordozón tárolt információ segítségével,
e) a tartalék adathordozó olvashatóságának rendszeres időközönkénti ellenőrzése,
f) a tartalék adathordozóról beolvasott archivált adatok sértetlenségének ellenőrzése,
g) szükség esetén a másodlagos adathordozó cseréje,
h) szükség esetén a tartalék adathordozó tartalmának helyreállítása az elsődleges adathordozón tárolt információ megismételt duplikálásával.

Határozat: a fenti követelményt az iSave rendszer **teljesíti**.

A határozat alapja:

Dokumentáció	Tapasztalat	Teszt	Interjú
+	+	+	-

Indoklás:

Az elektronikus dokumentumok sértetlenségének biztosítása az alábbi műszaki és környezeti biztonsági intézkedéseken alapul:

Műszaki biztonsági intézkedések:

1. A mindkét szerveren alkalmazott **RAID 6**-os technológia biztosítja az elsődleges adathordozó (Backup szerver) és a tartalék adathordozó (Replikációs szerver) olvashatóságának folyamatos (lényegében minden írás és olvasás művelet során végrehajtott) ellenőrzését /a) és e)/.

2. A **RAID 6**-os technológia biztosítja, hogy a Backup szerver olvasása (a Replikációs szerverre töltés céljából) egyben az ott tárolt adatok sértetlenség ellenőrzését is elvégzi (ha a sorokra és oszlopokra kiszámolt paritások nem egyeznek, akkor a hibajavítási lehetőséget nem meghaladó sérüléseket kijavítja a rendszer). Az átvitel során aktivizált SSL pedig biztosítja a továbbított adatok sértetlenségét /b)/.

3. A RAID 6-os technológia, valamint a rendszer konfigurálása biztosítja, hogy mindkét szerver automatikus riasztást küld a rendszer adminisztrátornak, amennyiben a merevlemez olyan fokú meghibásodása következik be, amit a RAID már nem tud javítani /c) és g)/.

4. Az iSave rendszer alap funkcionalitása, hogy szükség esetén (a rendszergazda távolról megvalósítható beavatkozásának hatására) a Backup szerver tartalma helyreállítható a Replikációs szerver által tárolt információ segítségével /d)/.

5. Az iSave rendszer alap funkcionalitása, hogy szükség esetén (a rendszergazda távolról megvalósítható beavatkozásának hatására) a Replikációs szerver tartalma helyreállítható a Backup szerver által tárolt információ segítségével /h)/.

Környezeti biztonsági intézkedések:

1. A szolgáltatást a Magyar Telekom Nyilvánosan Működő Részvénytársaság biztosítja, mely szerződésben (ÁSZF) vállalta az alábbiakat:

a) Cseregép szolgáltatás: a bérelt eszköz típusával azonos, vagy azzal kompatibilis eszköz raktáron tartása, a meghibásodás esetén szükségessé váló csere érdekében, merevlemez károsodás esetén funkcionálisan azonos cseregép biztosítása / c) és g)/.

A környezeti biztonsági intézkedéseket az alábbi dokumentum részletezi:
- Általános Szerződési Feltételek.

A műszaki biztonsági intézkedéseket az alábbi dokumentumok részletezik:
- biztonsági architektúra leírás,
- rendszer biztonsági terv,
- a rendszer-működés biztonsági koncepciója.

A követelmény teljesülését az értékelők saját felhasználói tapasztalatai is megerősítik:
- a műszaki biztonsági intézkedéseket a gyakorlatban többszörösen kipróbálták.

A követelmény teljesülését az alábbi tesztek ellenőrizték és igazolták:
- 3.12 /Replikációs szerver leállítása és újratelepítése/ (b),
- 3.13 /Backup szerver konfigurációs adatainak visszatöltése a Replikációs szerverről/ (h).

Követelmény: SFR_2b_4:

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

a) adatbázis adminisztrálás,
b) adatbázis frissítés fogadás funkció aktivizálásának jogosultság ellenőrzése,
c) rendszer mentése,
d) rendszer helyreállítása.

Határozat: a fenti követelményt az iSave rendszer **teljesíti**.

A határozat alapja:

Dokumentáció	Tapasztalat	Teszt	Interjú
+	+	+	-

Indoklás:

Az elektronikus dokumentumok sértetlenségének biztosítása az alábbi műszaki biztonsági intézkedéseken (iSave_ugyfel funkciókon) alapul:

1. A szerver oldalon keletkező adatbázis lényegében a kliens oldalon létrehozott, módosított vagy törölt mentési ütemezők automatikusan létrejövő központosított tükörképe. Következésképpen a szerver oldali adminisztrálás ezen része a kliens oldalon történő adminisztrálásokon keresztül valósul meg /a)/.

2. A kliens oldalon létrehozott, módosított vagy törölt mentési ütemezők csak akkor jutnak át automatikusan a szerver oldalra (s válnak az ottani adatbázis részévé), ha a kliens felhasználó sikeresen hitelesíti magát. Ez a hitelesítés két lépésben történik:

- a telepítést követően a jogosult felhasználó beállíthatja a kliens oldalt hitelesítő jelszavát. Ennek a jelszónak a transzformált képe átjut a szerver oldalra, s mindkét oldalon letárolódik. Az éles működés során a kliens – szerver adatkommunikációban a szerver ennek alapján folyamatosan hitelesíti a kliens oldalt, de ez automatikusan történik, a felhasználónak nem kell ismételten megadni a jelszót. (A hitelesítés tulajdonképpen a kliens gép hitelességét ellenőrzi, méghozzá automatikusan).
- A web konzolról történő minden bejelentkezéskor a felhasználónak meg kell adnia saját (web konzol) jelszavát ahhoz, hogy a web konzolról aktivizálható iSave_ugyfel funkciókat aktivizálhassa. (Ez a hitelesítés a kliens felhasználót egyedileg hitelesíti, méghozzá minden web konzol indításkor).

A kettős hitelesítés eredményeként a központi adatbázis 1. alatt említett adminisztrálását (frissítését) csak egy hiteles kliens gép egy jogosult felhasználója képes végrehajtani /b)/.

3. A szerver oldali adatbázisok más módon is adminisztrálhatók. A Backup és Replikációs szerverhez hozzáférő rendszergazda a központi adatbázisokból kitörölhet egy mentési ütemezőt vagy egy felhasználót. A Backup szerveren végrehajtott törlés automatikusan átkerül a Replikációs szerverre. Fordítva ez nem igaz, tehát erre a funkcióra különösen vigyáznia kell a rendszergazdának. /a)/.

4. Az adatbázis frissítést (módosítást) csak a web konzolról a szerver felé magát sikeresen hitelesítő rendszeradminisztrátor hajthatja végre /b)/.

5. A rendszer mentése automatikusan megvalósul, abban az értelemben, hogy a Backup szerver aktuálisan módosuló tartalma azonnal automatikus továbbításra kerül a Replikációs

szerverre, ahol a forrás adatok tükörképe alakul ki folyamatosan (mentést biztosítva ezzel) /c)/.

6. A rendszeradminisztrátor sikeres hitelesítés után egyaránt képes a Backup szerver tartalmának helyreállítására (a Replikációs szerver tartalma alapján), valamint a Replikációs szerver tartalmának helyreállítására (a Backup szerver tartalma alapján) /d)/.

A fenti műszaki biztonsági intézkedéseket (iSave_ugyfel funkciókat) az alábbi dokumentumok részletezik:

- rendszer interfész specifikáció,
- rendszer biztonsági terv,
- a rendszer-működés biztonsági koncepciója.

A követelmény teljesülését az értékelők saját felhasználói tapasztalatai is megerősítik:

- a műszaki biztonsági intézkedéseket a gyakorlatban többszörösen kipróbálták.

A követelmény teljesülését az alábbi tesztek ellenőrizték és igazolták:

- 1.1 /Mentési ütemező létrehozása, mentés egygépes kliens és szerver üzemmódban/ (a),
- 2.1 /Mentési ütemező létrehozása, mentés különálló kliens, Backup szerver üzemmódban/ (a),
- 3.1 /Mentési ütemező létrehozása, mentés különálló kliens, Backup szerver üzemmódban/ (a),
- 3.2 /Replikációs szerver telepítése és beállítása a Backup szerverben/ (c),
- 3.3 /Mentési ütemező létrehozása, mentés különálló kliens, Backup szerver, Replikációs szerver üzemmódban/ (a,c),
- 3.8 /Mentési adatbázisok ellenőrzése kliens és Backup szerver oldalon/ (a,c),
- 3.9 /Kliens oldali mentési paraméterek módosítása/ (a,c),
- 3.10 /Mentési adatbázisok ellenőrzése kliens és Replikációs szerver oldalon/ (a,c),
- 3.11 /Backup szerver leállítása és újratelepítése/ (a,d),
- 3.12 /Replikációs szerver leállítása és újratelepítése/ (c),
- 3.13 /Backup szerver konfigurációs adatainak visszatöltése a Replikációs szerverről/ (a,d),
- 3.15 /Backup szerver egy felhasználójának egy mentési ütemezőjének törlése/ (a),
- 3.16 /Replikációs szerver egy felhasználójának egy mentési ütemezőjének törlése/ (a),
- 3.17 /Backup szerver egy felhasználójának törlése/ (a),
- 3.24 /Kliens oldali mentési kísérlet törölt szerver oldali autentikációs jelszó mellett/ (b),
- 4.1 /Mentési ütemező létrehozása éles rendszerben/ (a),
- 4.2 /Mentési ütemező módosítása éles rendszerben/ (a),

Követelmény: SFR_2b_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.

Határozat: a fenti követelményt az iSave rendszer **teljesíti**.

A határozat alapja:

Dokumentáció	Tapasztalat	Teszt	Interjú
+	+	+	-

Indoklás:

Az elektronikus dokumentumok törölhetőségét (a szolgáltatott mentési archívumból) az alábbi műszaki biztonsági intézkedések (iSave_ugyfel funkciók) teszik lehetővé.

1. Minden iSave ügyfél, megfelelő jogosultság ellenőrzést követően törölheti a saját maga által létrehozott mentési ütemezőt. Ennek következtében a Backup szerveren tárolt mentési ütemező másolat, illetve az ehhez tartozó elektronikus dokumentumok is automatikusan törlésre kerülnek.

Fontos megjegyzés a felhasználó által kiváltható törölhetőséghez: Minden tárolási szolgáltatásra vonatkozó alap elvárás, hogy a szolgáltatást igénybe vevő törölhessen a saját maga által archiválásra beküldött anyagokból, s így többek között fizetni se kelljen a továbbiakban a tárolásért. Ugyanakkor ez az elvárt funkció informatika biztonsági veszélyt is hordoz, a felhasználó nevében jogosulatlanul kiadott törlés lehetetlenné tenné a később szükségessé váló helyreállítást. A veszély ellenére a törlési lehetőség biztosítása kötelező, ugyanakkor erős hozzáférés-ellenőrzési biztonsági intézkedésekkel garantálni kell, hogy csak valóban a jogosult felhasználó töröltethesse saját dokumentumait, s erről hitelesen megőrzött naplóbejegyzések is keletkezzenek. A veszély kivédésére lásd az SFR_3 (AccessControl) és SFR_5 (Audit) követelményekre vonatkozó határozatokat és azok indoklását.

2. Az iSave rendszer rendszergazdája (aki távolról eléri a szervereket és aktivizálhatja annak adminisztratív funkcióit), megfelelő jogosultság ellenőrzést követően törölhet tetszőleges mentési ütemezőt, vagy akár egy ügyfelet is. Ennek következtében az adott szerveren tárolt mentési ütemező másolat, illetve az ehhez tartozó elektronikus dokumentumok is automatikusan törlésre kerülnek.

Fontos megjegyzés a rendszeradminisztrátor által kiváltható törölhetőséghez: Minden tárolási szolgáltatásra vonatkozó alap elvárás, hogy a szolgáltatást nyújtó is törölhessen a saját maga által fenntartott archívumból, s így többek között kizárhassa a nem fizető ügyfeleket a tárolásból. Ugyanakkor ez az elvárt funkció informatika biztonsági veszélyt is hordoz, a rendszeradminisztrátor nevében jogosulatlanul kiadott törlés lehetetlenné tenné a később szükségessé váló helyreállítást. A veszély ellenére a törlési lehetőség biztosítása kötelező, ugyanakkor erős hozzáférés-ellenőrzési biztonsági intézkedésekkel garantálni kell, hogy csak valóban a jogosult rendszeradminisztrátor töröltethessen a központi szerverekről, s erről hitelesen megőrzött naplóbejegyzések is keletkezzenek. A veszély kivédésére lásd az SFR_3 (AccessControl) és SFR_5 (Audit) követelményekre vonatkozó határozatokat és azok indoklását.

A fenti műszaki biztonsági intézkedéseket (iSave_ugyfel funkciókat) az alábbi dokumentum részletezi:

- rendszer interfész specifikáció,
- rendszer biztonsági terv,
- a rendszer-működés biztonsági koncepciója.

A követelmény teljesülését az értékelők saját felhasználói tapasztalatai is megerősítik:

- a műszaki biztonsági intézkedéseket a gyakorlatban többszörösen kipróbálták.

A követelmény teljesülését az alábbi tesztek ellenőrizték és igazolták:

- 3.15 /Backup szerver egy felhasználójának egy mentési ütemezőjének törlése/,
- 3.16 /Replikációs szerver egy felhasználójának egy mentési ütemezőjének törlése/,
- 3.17 /Backup szerver egy felhasználójának törlése/.

Követelmény: SFR_2b_6:

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

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

Határozat: a fenti követelményt az iSave rendszer **teljesíti**.

A határozat alapja:

Dokumentáció	Tapasztalat	Teszt	Interjú
+	+	+	-

Indoklás:

Az elektronikus dokumentumok megőrzésével kapcsolatos események naplózását az alábbi műszaki biztonsági intézkedések (iSave_ugyfel funkciók) biztosítják:

1. Kliens oldalon naplózásra kerülnek az alábbi események:
   - mentési ütemező létrehozása, módosítása és törlése,
   - mentések,
   - visszatöltések (restore),
   - helyreállítás (disastery recovery).

2. A web konzolról sikeresen bejelentkező kliens jelentést (report) nézhet meg az alábbiakról:
   - felhasznált tároló hely (összesítve),
   - összes mentés (mentési ütemezőnként),
   - összes visszatöltés (mentési ütemezőnként),
   - összes helyreállítás (összes ütemezőre együtt).

3. A web konzolról sikeresen bejelentkező kliens a teljes eseménynaplót áttekintheti, ebben szűrhet is az alábbiak szerint:
   - az esemény jellege (pl. backup, restore, authentication),
   - az esemény típusa (critical, major, minor, warning, information),
   - az esemény időpontja (from, to),
   - az esemény leírásában előforduló szövegrészlet.

4. A Backup szerveren naplózásra kerülnek az alább események:
- mentések (kliens felöl),
- visszatöltések (restore, kliens felé),
- mentések (Replikációs szerver felé),
- visszatöltések (restore, Replikációs szerver felöl),
- helyreállítások (disastery recovery, Replikációs szerver felöl),
- törlés (mentési ütemező, felhasználó),
- próba felhasználó véglegesítése,
- működési események.

5. A web konzolról sikeresen bejelentkező rendszergazda a Backup szerveren jelentést (report) nézhet meg az alábbiakról:
- felhasznált tároló hely (felhasználónként, összesítve),
- mentés, törlés, visszaállítás, helyreállítás, replikáció (felhasználónként, mentési ütemezőnként).

6. A web konzolról sikeresen bejelentkező rendszergazda a Backup szerveren teljes eseménynaplót áttekintheti, ebben szűrhet is az alábbiak szerint:
- felhasználó
- az esemény jellege (pl. backup, restore, authentication),
- az esemény típusa (critical, major, minor, warning, information),
- az esemény időpontja (from, to),
- az esemény leírásában előforduló szövegrészlet.

7. A Replikációs szerveren naplózásra kerülnek az alább események:
- visszatöltések (restore, Backup szerver felé),
- helyreállítások (disastery recovery, Backup szerver felé),
- törlés (felhasználó),
- működési események.

8. A web konzolról sikeresen bejelentkező rendszergazda a Replikációs szerveren jelentést (report) nézhet meg az alábbiakról:
- felhasznált tároló hely (felhasználónként, összesítve),
- mentés, törlés, visszaállítás, helyreállítás (felhasználónként, mentési ütemezőnként).

9. A web konzolról sikeresen bejelentkező rendszergazda a Replikációs szerveren a teljes eseménynaplót áttekintheti, ebben szűrhet is az alábbiak szerint:
- felhasználó
- az esemény jellege (pl. backup, restore, authentication),
- az esemény típusa (critical, major, minor, warning, information),
- az esemény időpontja (from, to),
- az esemény leírásában előforduló szövegrészlet.

10. Napló megosztási lehetőség: A rendszergazda aktivizálhatja a (shared events) funkciót, melynek hatására a Replikációs szerveren keletkező napló bejegyzések (events) mentésre kerülnek a Backup szerveren is. Ennek előnye, hogy így a rendszergazda a Backup szerveren áttekintheti mindkét szerver eseményeit.

11. Olyan fokú meghibásodás esetén, amelyet a RAID 6-os technológia sem képes helyreállítani, mindkét szerverről egy hibaüzenet generálódik a rendszer adminisztrátor felé.

12. Operációs rendszer szintjén is keletkeznek log fájlok, melyek hiba és információ bejegyzéseket tartalmaznak az iSave_ugyfel program működéséről.

13. Az iSave_ugyfel program nem teszi lehetővé a napló törlését (sem a kliens, sem a szerver oldalon). Konfigurálásként megadható, hogy az utolsó hány bejegyzés férjen el a naplóba (100, 1000 vagy 10 000).

A fenti műszaki biztonsági intézkedéseket (iSave_ugyfel funkciókat) az alábbi dokumentum részletezi:

- a rendszer-működés biztonsági koncepciója.

A követelmény teljesülését az értékelők saját felhasználói tapasztalatai is megerősítik:

- a műszaki biztonsági intézkedéseket a gyakorlatban többszörösen kipróbálták.

A követelmény teljesülését az alábbi tesztek ellenőrizték és igazolták:

- 3.2 /Replikációs szerver telepítése és beállítása a Backup szerverben/ (a),
- 3.3 /Mentési ütemező létrehozása, mentés különálló kliens, Backup szerver, Replikációs szerver üzemmódban/ (a),
- 3.16 /Replikációs szerver egy felhasználójának egy mentési ütemezőjének törlése/ (c),
- 3.17 /Backup szerver egy felhasználójának törlése/ (c).

Követelmény: SFR_2c:

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

Határozat: a fenti követelményt az iSave rendszer **teljesíti**.

A határozat alapja:

Dokumentáció	Tapasztalat	Teszt	Interjú
+	+	+	-

Indoklás:

Az elektronikus dokumentumok visszatölthetőségének biztosítása az alábbi műszaki biztonsági intézkedésen (iSave_ugyfel funkción) alapul:

1. A kliens oldalon a jogosult felhasználó (web konzolról való sikeres bejelentkezés után) aktivizálhatja a helyreállítási (disastery recovery) funkciót, amennyiben a kliens hitelesítve van a szerver felé. Ekkor a Backup szerver visszaküldi a mentési ütemező meta-adatait.

2. A kliens oldalon a jogosult felhasználó (web konzolról való sikeres bejelentkezés után) aktivizálhatja a restore funkciót (ezen belül több lépésben kiválaszthatja a visszatöltendő dokumentumokat), amennyiben helyesen megadja az adott mentési ütemezőben használt adat titkosító kulcsot. Ekkor a Backup szerver visszaküldi a kiválasztott dokumentumokat.

A fenti műszaki biztonsági intézkedéseket (iSave_ugyfel funkciókat) az alábbi dokumentumok részletezik:

- rendszer interfész specifikáció,
- a rendszer-működés biztonsági koncepciója.

A követelmény teljesülését az értékelők saját felhasználói tapasztalatai is megerősítik:

- a Backup szerverről a korábban mentett adataikat többször visszatöltötték.

A követelmény teljesülését az alábbi tesztek ellenőrizték és igazolták:
- 1.2 /Fájl visszaállítása egygépes kliens-szerver üzemmódban/,
- 3.5 /Mentés visszaállítása kliens oldalon Backup szerverről/,
- 3.6 /Mentés visszaállítása kliens oldalon Replikációs szerverről/,
- 3.7 /Kliens újra telepítése és teljes mentés visszatöltése Replikációs szerverről kliensre/,
- 3.14 /Kliens konfigurációs adatainak visszatöltése a Backup szerverről/,
- 4.5 /Kliens adatainak visszaállítása éles rendszerben/.

Követelmény: SFR_2d:

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.

Határozat: a fenti követelményt az iSave rendszer **teljesíti**.

A határozat alapja:

Dokumentáció	Tapasztalat	Teszt	Interjú
+	+	+	-

Indoklás:

Az elektronikus dokumentumok mentésre való továbbíthatósága az alábbi műszaki biztonsági intézkedéseken (iSave_ugyfel funkciókon) alapul:

1. A kliens szerverről automatikusan megtörténik a kijelölt állományok továbbítása a Backup szerverre, ahol biztonságosan letárolásra kerülnek.

2. A kliens oldali jogosult felhasználó (web konzolról való sikeres bejelentkezés után) képes létrehozni, módosítani és törölni azokat a mentési ütemezőket (mentési profilokat), melyekben a felhasználó kijelölheti a mentésre kerülő alkönyvtárakat és fájl típusokat, valamint meghatározhatja a mentés különböző paramétereit (pl. gyakoriság).

A fenti műszaki biztonsági intézkedéseket (iSave_ugyfel funkciókat) az alábbi dokumentum részletezi:
- rendszer biztonsági terv,
- a rendszer-működés biztonsági koncepciója.

A követelmény teljesülését az értékelők saját felhasználói tapasztalatai is megerősítik:
- a mentési funkciót a gyakorlatban többször kipróbálták.

A követelmény teljesülését az alábbi tesztek ellenőrizték és igazolták:
- 1.1 /Mentési ütemező létrehozása, mentés egygépes kliens és szerver üzemmódban/,
- 2.1 /Mentési ütemező létrehozása, mentés különálló kliens, Backup szerver üzemmódban/,
- 3.1 /Mentési ütemező létrehozása, mentés különálló kliens, Backup szerver üzemmódban/,
- 3.3 /Mentési ütemező létrehozása, mentés különálló kliens, Backup szerver, Replikációs szerver üzemmódban/,
- 3.8 /Mentési adatbázisok ellenőrzése kliens és Backup szerver oldalon/,
- 3.10 /Mentési adatbázisok ellenőrzése kliens és Replikációs szerver oldalon/,
- 4.1 /Mentési ütemező létrehozása éles rendszerben/,
- 4.3 /Módosított adat mentése éles rendszerben/.

Követelmény: SFR_2e:

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

Határozat: a fenti követelményt az iSave rendszer **teljesíti**.

A határozat alapja:

Dokumentáció	Tapasztalat	Teszt	Interjú
+	+	+	-

Indoklás:

Az elektronikus dokumentumok visszakérésének és helyreállításának biztosítása az alábbi műszaki biztonsági intézkedéseken (iSave_ugyfel funkciókon) alapul:

1. A kliens oldalon a jogosult felhasználó (web konzolról való sikeres bejelentkezés után) aktivizálhatja a helyreállítási (disastery recovery) funkciót, amennyiben a kliens hitelesítve van a szerver felé. Ekkor a Backup szerver visszaküldi a mentési ütemező meta-adatait.

2. A kliens oldalon a jogosult felhasználó (web konzolról való sikeres bejelentkezés után) aktivizálhatja a restore funkciót (ezen belül több lépésben kiválaszthatja a visszatöltendő dokumentumokat), amennyiben helyesen megadja az adott mentési ütemezőben használt adat titkosító kulcsot. Ekkor a Backup szerver visszaküldi a kiválasztott dokumentumokat.

A fenti műszaki biztonsági intézkedéseket (iSave_ugyfel funkciókat) az alábbi dokumentum részletezi:

- rendszer interfész specifikáció,
- a rendszer-működés biztonsági koncepciója.

A követelmény teljesülését az értékelők saját felhasználói tapasztalatai is megerősítik:

- a visszakérés (restore) és helyreállítás (disastery recovery) funkciókat a gyakorlatban többször kipróbálták.

A követelmény teljesülését az alábbi tesztek ellenőrizték és igazolták:

- 1.2 /Fájl visszaállítása egygépes kliens-szerver üzemmódban/,
- 3.5 /Mentés visszaállítása kliens oldalon Backup szerverről/,
- 3.6 /Mentés visszaállítása kliens oldalon Replikációs szerverről/,
- 3.7 /Kliens újra telepítése és teljes mentés visszatöltése Replikációs szerverről kliensre/,
- 3.14 /Kliens konfigurációs adatainak visszatöltése a Backup szerverről/,
- 4.5 /Kliens adatainak visszaállítása éles rendszerben/.

Követelmény: SFR_3a:

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

Határozat: a fenti követelményt az iSave rendszer **teljesíti**.

A határozat alapja:

Dokumentáció	Tapasztalat	Teszt	Interjú
+	-	+	+

Indoklás:

A szerver oldalon az elektronikus dokumentumok logikai hozzáférés elleni védelme az alábbi műszaki biztonsági intézkedéseken (iSave_ugyfel funkciókon) alapul:

1. A Backup szerverhez a kliens oldalról való logikai hozzáférés csak akkor lehetséges, ha a kliens oldali felhasználó sikeresen hitelesíti magát. Ez a hitelesítés két lépésben történik:
   - a telepítést követően a jogosult felhasználó beállíthatja a kliens oldal nevét és hitelesítő jelszavát. Ennek a jelszónak a transzformált képe átjut a szerver oldalra, s mindkét oldalon letárolódik. Az éles működés során a kliens – szerver adatkommunikációban a szerver ennek alapján folyamatosan hitelesíti a kliens oldalt, de ez automatikusan történik, a felhasználónak nem kell ismételten megadni a jelszót. (A hitelesítés tulajdonképpen a kliens gép hitelességét ellenőrzi, méghozzá automatikusan).
   - A web konzolról történő minden bejelentkezéskor a felhasználónak meg kell adnia saját (web konzol) jelszavát ahhoz, hogy a web konzolról aktivizálható iSave_ugyfel funkciókat aktivizálhassa. (Ez a hitelesítés a kliens felhasználót egyedileg hitelesíti, méghozzá minden program indításkor).

2. A Replikációs szerverhez kliens oldalról közvetlenül nem lehet hozzáférni.

3. A Backup és Replikációs szerverekhez a rendszergazda távolról, web konzoláról férhet hozzá. Ez a logikai hozzáférés csak akkor lehetséges, ha a rendszergazda sikeresen hitelesíti magát. Ez a hitelesítés két lépésben történik:
   - A megfelelő jelszó megadása szükséges ahhoz, hogy a VPN szerveren keresztül a rendszergazda elérje a szervereken futó web szerver alkalmazást (Apache).
   - A web konzolról történő minden bejelentkezéskor a rendszergazdának meg kell adnia saját (web konzol) jelszavát ahhoz, hogy a web konzolról aktivizálható adminisztratív funkciókat aktivizálhassa.

4. A szerver biztonsági tartomány hozzáférés-védelmét erősítő tűzfal kizárólag az alábbi portokon enged belépést:
   - a kliens-Backup szerver közötti adatkommunikáció által használt port,
   - a rendszeradminisztrátor web konzoljáról indított VPN (IPsec) kapcsolat működéséhez szükséges portok,
   - a megbízható időforrásból érkező pontos idő beengedéséhez szükséges port (de ezt is csak az időforrás IP címéről).

Minden más portot a tűzfal aktívan lezár.

A fenti műszaki biztonsági intézkedéseket az alábbi dokumentumok részletezik:
- rendszer biztonsági terv,

- a rendszer-működés biztonsági koncepciója.

A követelmény teljesülését az értékelők és a szolgáltatást biztosító megbízó közötti szóbeli megbeszélések (interjúk, konzultációk) is megerősítik.

A követelmény teljesülését az alábbi tesztek ellenőrizték és igazolták:
- 3.21 /Hibás kliens hitelesítés Backup szerver fele újra telepített kliens esetén/,
- 3.23 /Kliens oldali adat-visszaállítási kísérlet hibás jelszóval Backup szerverről/,
- 3.24 /Kliens oldali mentési kísérlet törölt szerver oldali hitelesítő jelszó mellett/.

Követelmény: SFR_3b:

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

Határozat: a fenti követelményt az iSave rendszer **teljesíti**.

A határozat alapja:

Dokumentáció	Tapasztalat	Teszt	Interjú
+	+	-	+

Indoklás:

A szerver oldalon letárolt elektronikus dokumentumok jogosulatlan fizikai hozzáférés elleni védelme az alábbi környezeti biztonsági intézkedéseken alapul:

1. Az elektronikus dokumentumokat tároló két szerver (Backup és Replikációs) egy hosting szolgáltatás keretében, egy védett adatközpont számítógép termében kapott elhelyezést.

2. A szolgáltatást a Magyar Telekom Nyilvánosan Működő Részvénytársaság biztosítja, mely szerződésben (ÁSZF) vállalta az alábbiakat:

a) Őrzés-védelem (24 órás, kettős őrszolgálat, mágneskártyás be- és kiléptető rendszer, belépés csak előzetes bejelentéssel és belső kísérővel),

b) Fizikai behatolás-védelem (be- és kiléptető rendszer naplózása, mozgásérzékelőkkel összekapcsolt, az őrszolgálatra bekötött riasztók, 24 órás, zárt láncos belső térfigyelő szolgálat),

c) Számítógépterem, munkaállomások megközelíthetősége (ügyfél a gépterembe csak írásos engedéllyel léphet be, a szerverek lezárt rack szekrényben vannak),

d) Operátori jelenlét (24 órás).

A fenti környezeti biztonsági intézkedéseket az alábbi dokumentum részletezi:
- Általános Szerződési Feltételek.

A követelmény teljesülését az értékelők és a szolgáltatást biztosító megbízó közötti szóbeli megbeszélések (interjúk, konzultációk) is megerősítik.

A követelmény teljesülésének egy részét a helyszíni látogatáson ellenőrizte (a biztonsági intézkedések tanulmányozása mintavétel mellett).

Követelmény: SFR_3c:

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

Határozat: a fenti követelményt az iSave rendszer **támogatja**, az informatikai és nem informatikai környezetre megfogalmazott 2. számú működtetési feltétel (Biztonságos operációs rendszer használata) teljesülése esetén a követelményt az iSave rendszer teljesíti.

A határozat alapja:

Dokumentáció	Tapasztalat	Teszt	Interjú
+	+	+	-

Indoklás:

A kliens oldalon a rendszerben tárolt elektronikus dokumentumok logikai hozzáférés elleni védelme az alábbi műszaki biztonsági intézkedéseken alapul:

1. A Backup szerveren tárolt elektronikus dokumentumokhoz a kliens oldalról történő illetéktelen logikai hozzáférés ellen az alábbiak védenek:
   - csak a hitelesített kliensgépről (a kliens oldalt hitelesítő jelszó transzformált képének automatikus átküldésével) lehet hozzáférni a Backup szerverhez,
   - csak hitelesített felhasználó (aki a web konzolon megadta nevét és jelszavát) tud hozzáférni a Backup szerverhez, és
   - csak az adott felhasználó által mentett adatokhoz férhet hozzá a már kétszeresen hitelesített felhasználó.

2. A kliens gépen tárolt elektronikus dokumentumokhoz a kliens oldalról történő illetéktelen logikai hozzáférés ellen az alábbiak védenek:
   - az iSave_ugyfel programon keresztül csak az a hitelesített felhasználó fér az elektronikus dokumentumokhoz, aki a web konzolon megadta nevét és jelszavát.

3. A kliens gépen tárolt elektronikus dokumentumokhoz elvileg más programokon keresztül is hozzá lehet férni. Az ez elleni védekezést az iSave rendszer a környezettől várja el, ahogyan ezt a 2. számú működtetési feltétel megfogalmazta.

A fenti műszaki biztonsági intézkedéseket az alábbi dokumentum részletezi:
- biztonsági architektúra leírás,
- rendszer interfész specifikáció,
- a rendszer-működés biztonsági koncepciója.

A követelmény teljesülését az értékelők saját felhasználói tapasztalatai is megerősítik:
- a logikai hozzáférés védelmi mechanizmusok működését a gyakorlatban többször megfigyelték.

A követelmény teljesülését az alábbi tesztek ellenőrizték és igazolták:
- 3.21 /Hibás kliens hitelesítés Backup szerver fele újra telepített kliens esetén/,
- 3.23 /Kliens oldali adat-visszaállítási kísérlet hibás jelszóval Backup szerverről/,
- 3.24 /Kliens oldali mentési kísérlet törölt szerver oldali hitelesítő jelszó mellett/.

Követelmény: SFR_3d:

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

Határozat: a fenti követelményt az iSave rendszer **a nem IT környezettől várja el.** (Lásd az 1. működtetési feltételt: A számítógép fizikai védelme)

A határozat alapja:

Dokumentáció	Tapasztalat	Teszt	Interjú
+	-	-	-

Indoklás:

Az elektronikus dokumentumok fizikai hozzáférését az iSave rendszeren kívüli eszközökkel (fizikai, személyi és eljárásrendi intézkedésekkel) kell biztosítani, ahogyan azt a rendszer biztonsági előirányzat alábbi feltétele (biztonsági célja) is megfogalmazta:

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).*

Követelmény: SFR_3e:

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.

Határozat: a fenti követelményt az iSave rendszer **támogatja**, az informatikai és nem informatikai környezetre megfogalmazott 4. működtetési feltétel /Az iSave_ugyfel Web Console program biztonságos telepítése és konfigurálása (első elindítás és a mentési ütemező beállítása)/ teljesülése esetén a követelményt az iSave rendszer teljesíti.

A határozat alapja:

Dokumentáció	Tapasztalat	Teszt	Interjú
+	+	+	-

Indoklás:

Az archiválandó elektronikus dokumentumok titkosításához használt kriptográfiai mechanizmusok az alábbiak:

1. Az iSave rendszer a kliens oldalon (a 4. működtetési feltétel teljesülése esetén) a Blowfish nevű nyilvános kriptográfiai algoritmussal titkosít minden mentésre továbbított dokumentumot. A Blowfish algoritmus ellenáll minden ismert kripto-analitikai támadási módszernek, a szakirodalomban nem ismert ellene hatékonyabb támadási módszer, mint az összes szóba jöhető titkosító kulcs szisztematikus, teljes kipróbálása (brute force).

2. Az iSave rendszer a lehető legegyszerűbb kulcselőállítási módszert alkalmazza (s ez a 4. számú működtetési feltétel teljesülése esetén megfelelően biztonságos is): változtatás nélkül elfogadja a felhasználó által megadott kulcsot (pontosabban kiegészítené azt egy rögzített karaktersorozattal, ha nem pont 16 hosszúságú kulcsot adna meg a felhasználó).

3. A titkosító kulcs (a 4. számú működtetési feltétel teljesülése esetén) pontosan az a 16 bájt lesz, amit a mentési ütemező létrehozásakor a felhasználó meghatároz. Ennek helyes megválasztása esetén (62 elemű jelkészletből véletlenszerűen választott 16 karakter) a támadónak több mint 2^{95} lehetőséget kellene kipróbálnia, ami a gyakorlatban nem megvalósítható.

4. A titkosító kulcsot nyílt formában nem tárolja, s nem továbbítja a rendszer.

5. A titkosító kulcsot védetten tárolja a kliens oldali iSave_ugyfel alkalmazás.

6. A titkosító kulcsot védetten továbbítja a kliens oldali iSave_ugyfel alkalmazás a Backup szervernek (az MD5-ös képe megy át, az is SSL védelem alatt: „The backup encryption keys will be transferred as MD5 values for verifying encryption key for continued backups and restores.”

7. A titkosító kulcsot a Backup szerver nem képes visszaállítani, az MD5-ös kép továbbításra kizárólag azért van szükség, hogy a szerver oldal ellenőrizhesse, megfelelő módon került-e titkosításra a kapott dokumentum.

A fenti műszaki biztonsági intézkedéseket az alábbi dokumentum részletezi:

- biztonsági architektúra leírás.

A követelmény teljesülését az értékelők saját vizsgálati tapasztalatai is megerősítik:

- újraprogramozással ellenőrizték és igazolták, hogy a gyakorlatban a dokumentált algoritmusok működnek.

A követelmény teljesülését az alábbi tesztek ellenőrizték és igazolták:

- 5.18 /Mentés titkosításának a verifikálása/.

Követelmény: SFR_5a:

> ***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.***

Határozat: a fenti követelményt az iSave rendszer **teljesíti**.

A határozat alapja:

Dokumentáció	Tapasztalat	Teszt	Interjú
+	+	+	-

Indoklás:

Az elvárt naplóesemények generálását az alábbi műszaki biztonsági intézkedések (iSave_ugyfel funkciók) biztosítják:

1. A Backup szerveren naplózásra kerülnek az alább események:
   - mentések (kliens felöl),
   - visszatöltések (restore, kliens felé),
   - mentések (Replikációs szerver felé),
   - visszatöltések (restore, Replikációs szerver felöl),
   - helyreállítások (disastery recovery, Replikációs szerver felöl),
   - törlés (mentési ütemező, felhasználó),
   - próba felhasználó véglegesítése,
   - működési események.

2. A web konzolról sikeresen bejelentkező rendszergazda a Backup szerveren jelentést (report) nézhet meg az alábbiakról:
   - felhasznált tároló hely (felhasználónként, összesítve),
   - mentés, törlés, visszaállítás, helyreállítás, replikáció (felhasználónként, mentési ütemezőnként).

3. A web konzolról sikeresen bejelentkező rendszergazda a Backup szerveren teljes eseménynaplót áttekintheti, ebben szűrhet is az alábbiak szerint:
   - felhasználó
   - az esemény jellege (pl. backup, restore, authentication),
   - az esemény típusa (critical, major, minor, warning, information),
   - az esemény időpontja (from, to),
   - az esemény leírásában előforduló szövegrészlet.

4. A Replikációs szerveren naplózásra kerülnek az alább események:
   - visszatöltések (restore, Backup szerver felé),
   - helyreállítások (disastery recovery, Backup szerver felé),
   - törlés (felhasználó),
   - működési események.

5. A web konzolról sikeresen bejelentkező rendszergazda a Replikációs szerveren jelentést (report) nézhet meg az alábbiakról:
- felhasznált tároló hely (felhasználónként, összesítve),
- mentés, törlés, visszaállítás, helyreállítás (felhasználónként, mentési ütemezőnként).

6. A web konzolról sikeresen bejelentkező rendszergazda a Replikációs szerveren a teljes eseménynaplót áttekintheti, ebben szűrhet is az alábbiak szerint:
- felhasználó
- az esemény jellege (pl. backup, restore, authentication),
- az esemény típusa (critical, major, minor, warning, information),
- az esemény időpontja (from, to),
- az esemény leírásában előforduló szövegrészlet.

7. Olyan fokú meghibásodás esetén, amelyet a RAID 6-os technológia sem képes helyreállítani, mindkét szerverről egy hibaüzenet generálódik a rendszer adminisztrátor felé.

8. Operációs rendszer szintjén is keletkeznek log fájlok, melyek hiba és információ bejegyzéseket tartalmaznak az iSave_ugyfel program működéséről.

9. Az iSave_ugyfel program nem teszi lehetővé a napló törlését (sem a kliens, sem a szerver oldalon). Konfigurálásként megadható, hogy az utolsó hány bejegyzés férjen el a naplóba (100, 1000 vagy 10 000).

A fenti műszaki biztonsági intézkedéseket az alábbi dokumentum részletezi:
- Help fájl,
- a rendszer-működés biztonsági koncepciója.

A követelmény teljesülését az értékelők saját felhasználói tapasztalatai is megerősítik:
- a szerver oldali naplózási funkciók működését a gyakorlatban többször megfigyelték.

A követelmény teljesülését az alábbi tesztek ellenőrizték és igazolták:
- 1.1 /Mentési ütemező létrehozása, mentés egygépes kliens és szerver üzemmódban/,
- 1.2 /Fájl visszaállítása egygépes kliens-szerver üzemmódban/,
- 2.1 /Mentési ütemező létrehozása, mentés különálló kliens, Backup szerver üzemmódban/,
- 2.2 /Backup szerver webes elérése másik számítógépről Microsoft Internet Explorerrel, HTTP felületen/,
- 2.3 /Backup szerver webes elérése másik számítógépről Firefox-szal HTTPS felületen/,
- 3.4 /Kliens, Backup szerver és Replikációs szerver naplóinak áttekintése/,
- 3.18 /Mentés és helyreállítás napló eseményeinek megtekintése/,
- 3.19 /Törlés napló eseményeinek megtekintése/.

Követelmény: SFR_5b:

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.

Határozat: a fenti követelményt az iSave rendszer **teljesíti**.

A határozat alapja:

Dokumentáció	Tapasztalat	Teszt	Interjú
+	+	+	-

Indoklás:

A naplóesemények megosztási lehetőségét az alábbi műszaki biztonsági intézkedés (iSave_ugyfel funkció) biztosítja:

1. Napló megosztási lehetőség: A rendszergazda aktivizálhatja a (shared events) funkciót, melynek hatására a Replikációs szerveren keletkező napló bejegyzések (events) mentésre kerülnek a Backup szerveren is. Ennek előnye, hogy így a rendszergazda a Backup szerveren áttekintheti mindkét szerver eseményeit.

A fenti műszaki biztonsági intézkedéseket az alábbi dokumentum részletezi:

- Help fájl,
- a rendszer-működés biztonsági koncepciója.

A követelmény teljesülését az értékelők saját felhasználói tapasztalatai is megerősítik:

- a szerverek közötti napló megosztás működését a gyakorlatban többször megfigyelték.

A követelmény teljesülését az alábbi tesztek ellenőrizték és igazolták:

- 3.4 /Kliens, Backup szerver és Replikációs szerver naplóinak áttekintése/,
- 3.20 /Megosztott napló események ellenőrzése Backup szerveren/.

Követelmény: SFR_5c:

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.

Határozat: a fenti követelményt az iSave rendszer **teljesíti**.

A határozat alapja:

Dokumentáció	Tapasztalat	Teszt	Interjú
+	+	+	-

Indoklás:

A kliens oldali biztonsági naplózás az alábbi műszaki biztonsági intézkedéseken (iSave_ugyfel funkciókon) alapul:

1. Kliens oldalon naplózásra kerülnek az alábbi események:
   - mentési ütemező létrehozása, módosítása és törlése,
   - mentések,
   - visszatöltések (restore),
   - helyreállítás (disastery recovery).

2. A web konzolról sikeresen bejelentkező kliens jelentést (report) nézhet meg az alábbiakról:
   - felhasznált tároló hely (összesítve),
   - összes mentés (mentési ütemezőnként),
   - összes visszatöltés (mentési ütemezőnként),
   - összes helyreállítás (összes ütemezőre együtt).

3. A web konzolról sikeresen bejelentkező kliens a teljes eseménynaplót áttekintheti, ebben szűrhet is az alábbiak szerint:
   - az esemény jellege (pl. backup, restore, authentication),
   - az esemény típusa (critical, major, minor, warning, information),
   - az esemény időpontja (from, to),
   - az esemény leírásában előforduló szövegrészlet.

4. Az iSave_ugyfel program nem teszi lehetővé a napló törlését a kliens oldalon (sem). Konfigurálásként megadható, hogy az utolsó hány bejegyzés férjen el a naplóba (100, 1000 vagy 10 000).

5. Operációs rendszer szintjén is keletkeznek log fájlok, melyek hiba és információ bejegyzéseket tartalmaznak az iSave_ugyfel program működéséről.

A fenti műszaki biztonsági intézkedéseket az alábbi dokumentum részletezi:
   - Help fájl,
   - a rendszer-működés biztonsági koncepciója.

A követelmény teljesülését az értékelők saját felhasználói tapasztalatai is megerősítik:
   - a kliens oldali naplózási funkciók működését a gyakorlatban többször megfigyelték.

A követelmény teljesülését az alábbi tesztek ellenőrizték és igazolták:
   - 1.1 /Mentési ütemező létrehozása, mentés egygépes kliens és szerver üzemmódban/,
   - 1.2 /Fájl visszaállítása egygépes kliens-szerver üzemmódban/,
   - 2.1 /Mentési ütemező létrehozása, mentés különálló kliens, Backup szerver üzemmódban/,
   - 3.4 /Kliens, Backup szerver és Replikációs szerver naplóinak áttekintése/,
   - 3.18 /Mentés és helyreállítás napló eseményeinek megtekintése/,
   - 3.19 /Törlés napló eseményeinek megtekintése/.
   - 4.6 /Napló állományok áttekintése éles rendszerben/.

5. Következtetések

5.1 Az értékelés összefoglaló eredménye

Az értékelés fő következtetése az alábbi:

Az iSave rendszer megfelel az 114/2007. (XII.29.) GKM rendelet a digitális archiválás szabályairól 2 § (1) bekezdésében megfogalmazott alábbi elvárásnak:

„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."

Az iSave rendszeren kívüli eszközökkel kell biztosítani az 114/2007. (XII.29.) GKM rendelet alábbi elvárásait:

- a 2 § (1) bekezdésből vett fenti (teljesülő) idézet kimaradó részét: „*kizárja az utólagos módosítás lehetőségét*, valamint",
- a 2 § (2) bekezdését: *„A megőrzésre kötelezett köteles biztosítani, hogy az őrzött elektronikus dokumentumok értelmezhetősége (olvashatósága) - a dokumentumok megjeleníthetőségét lehetővé tevő szoftver- és hardverkörnyezet biztosításával - a megőrzési kötelezettség időtartama alatt megmaradjon."*

Az értékelés másik következtetése az alábbi:

Az iSave rendszer megfelel az „Elektronikus aláírásra és online backup szolgáltatásra épülő digitális archiváló rendszer (DAR) - Rendszer biztonsági előirányzat" című dokumentumban megfogalmazott alábbi követelményeknek:

SFR_2: 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)

SFR_3: A rendszer olyan módon őrizze meg az elektronikus dokumentumokat, amely megvédi az elektronikus dokumentumokat a jogosulatlan hozzáférés ellen. (rövid név: AccessControl)

SFR_5: 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).

Az iSave rendszeren kívüli eszközökkel kell biztosítani a fent említett rendszer biztonsági előirányzat alábbi funkcionális biztonsági követelményeit:

SFR_1: A rendszer olyan módon őrizze meg az elektronikus dokumentumokat, amely kizárja az utólagos módosítás lehetőségét. (rövid név: DigSign)

SFR_4: A rendszer őrizze meg az elektronikus dokumentumok értelmezhetőségét (olvashatóságát) a megőrzési kötelezettség időtartama alatt, az ezt lehetővé tevő szoftver- és hardverkörnyezet biztosításával (rövid név: View)

5.2 Az értékelés eredményének értelmezése a 114/2007 alkalmazásában

Az 114/2007. (XII.29.) GKM rendelet alap elvárását a 2. § fogalmazza meg:

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

(2) A megőrzésre kötelezett köteles biztosítani, hogy az őrzött elektronikus dokumentumok értelmezhetősége (olvashatósága) - a dokumentumok megjeleníthetőségét lehetővé tevő szoftver- és hardverkörnyezet biztosításával - a megőrzési kötelezettség időtartama alatt megmaradjon.

A 3. § szerint a megőrzés az alábbi módokon végezhető:

a) az elektronikus aláírásról szóló 2001. évi XXXV. törvényben (a továbbiakban: Eat.) meghatározott legalább fokozott biztonságú elektronikus aláírással ellátott dokumentum 4. § szerinti megőrzésével,

b) az 5. §-ban meghatározott zárt rendszer alkalmazásával,

c) a 6. §-ban meghatározott esetben elektronikus adatcsere rendszer igénybevételével.

Az iSave szolgáltatás a 3. § a) bekezdését választóknak biztosít segítséget, az alábbi táblázat a megőrzésre kötelezett felelősségét vizsgálja a három választási lehetőség esetén:

114/2007. (XII.29.) GKM rendelet elvárása	a megőrzésre kötelezett nem az Eat.-ban meghatározott archiválási szolgáltató útján gondoskodik a megőrzésről		a megőrzésre kötelezett a megőrzéssel az Eat.-ban meghatározott archiválási szolgáltatót bíz meg
	nem veszi igénybe az iSave on-line backup szolgáltatást	igénybe veszi az iSave on-line backup szolgáltatást	
2. § (1) az e-dokumentumok utólagos módosítási lehetőségének a kizárása	**A megőrzésre kötelezettnek alá kell írnia a dokumentumokat**	**A megőrzésre kötelezettnek alá kell írnia a dokumentumokat**	**A megőrzésre kötelezettnek alá kell írnia a dokumentumokat**
2. § (1) Védelem az e-dokumentumok törlése, megsemmisítése, véletlen megsemmisülése és sérülése ellen	**A megőrzésre kötelezettnek kell biztosítania**	**A szolgáltató biztosítja**	**A szolgáltató biztosítja**
2. § (1) Védelem a jogosulatlan hozzáférés ellen	**A megőrzésre kötelezettnek kell biztosítania**	**A szolgáltató biztosítja**	**A szolgáltató biztosítja**
2. § (2) Az e-dokumentumok értelmezhetőségének (olvashatóságának) a fenntartása	**A megőrzésre kötelezettnek kell biztosítania**	**A szolgáltató biztosíthatja, amennyiben vállalja ezt a kiegészítő szolgáltatást**	**A szolgáltató biztosíthatja, amennyiben vállalja ezt a kiegészítő szolgáltatást**
4. § (2) A közösen aláírt e-dokumentumok együttes kezelése	**A megőrzésre kötelezettnek kell biztosítania (az aláíró programmal)**	**A megőrzésre kötelezettnek kell biztosítania (az aláíró programmal)**	**A megőrzésre kötelezettnek kell biztosítania**
4. § (3) időbélyegzés	**A megőrzésre kötelezettnek kell biztosítania (az aláíró program teljesíti)**	**A megőrzésre kötelezettnek kell biztosítania (az aláíró program teljesíti)**	**A szolgáltató biztosítja**
4. § (4) az elektronikus aláírás érvényességének hosszú távú fenntartása	**A megőrzésre kötelezettnek kell biztosítania**	**A megőrzésre kötelezettnek kell biztosítania**	**A szolgáltató biztosítja**

5.3 Feltételek

5.3.1 A biztonságos felhasználás feltételei a kliens oldalon

1. működtetési feltétel: A számítógép fizikai védelme

A kliens oldali számítógép környezetében elfogadható szintű fizikai védelemnek kell biztosítania azt, hogy a számítógéphez illetéktelen személyek fizikailag ne férjenek hozzá.

2. működtetési feltétel: Biztonságos operációs rendszer használata

Az értékelt konfigurációba az alábbi operációs rendszerek tartoznak (kliens oldalon):

- Windows Vista,
- Windows XP,
- SuSE Linux 10.1 és felette.

Az alkalmazott operációs rendszernek biztosítania kell az alábbiakat:

- Az iSave program fájljaihoz csak azok a személyek férhessenek (az operációs rendszer szintjén) hozzá, akik jogosultak az iSave_ugyfel program használatára is.
- más programokon keresztül csak az a felhasználó férjen hozzá az iSave program adat állományaihoz és az elektronikus dokumentumokhoz, aki az operációs rendszer felé sikeresen hitelesítette magát, s az operációs rendszer jogosultság-ellenőrző mechanizmusai az adott dokumentum elérését engedélyezi számára.

3. működtetési feltétel: Az iSave_ugyfel program biztonságos telepítése és konfigurálása

A biztonságos telepítés részletezésére lásd a kiegészítő útmutatót (5.3.2).

4. működtetési feltétel: Az iSave_ugyfel Web Console program biztonságos telepítése és konfigurálása (első elindítás és a mentési ütemező beállítása)

A biztonságos telepítés részletezésére lásd a kiegészítő útmutatót (5.3.2).

5. működtetési feltétel: A kliens oldal biztonságos üzemeltetése

Az 1. – 4. működési feltétel teljesülését hosszú távon biztosítani kell:

- folyamatosan biztosítani kell a fizikai védelmet,
- az operációs rendszert ne cseréljék le,
- ne rontsák el a iSave_ugyfel jó konfigurációját,
- ne hozzanak létre utólag nem megbízható mentési ütemezőket.

A hosszú távú biztonságos üzemeltetéssel kapcsolatban feltételezzük, hogy a kliens oldali felhasználók megbízhatók a tekintetben, hogy a számukra kijelölt feladatokat biztonsági szempontból korrekt módon hajtják végre (betartják az 1. – 5. működtetési feltételeket).

5.3.2 Kiegészítő útmutató a kliens oldali biztonságos telepítéshez és konfiguráláshoz

I. Operációs rendszer ellenőrzése

A rendszer telepítéséhez egy már működőképes operációs rendszer szükséges. A támogatott, egyben az értékelés által is ellenőrzött operációs rendszerek a következők:

1. Windows XP SP2, Windows Vista SP1,
2. SuSE Linux 10.1 és későbbi.

Amennyiben a megfelelő javító csomagok (XP-nél az SP2, Vista-nál az SP1) még nincsenek telepítve, az iSave_ugyfel telepítése előtt ezt pótolni kell.

Windows operációs rendszer esetén az iSave_ugyfel program biztonságosan használható több felhasználós környezetben is (lásd 1a telepítési pont).

SuSE Linux operációs rendszer esetén az iSave_ugyfel program biztonságosan csak egy felhasználós környezetben használható, vagy olyan több felhasználóval, akik azonos jogosultsággal érik el az összes dokumentumot az operációs rendszerben.

SuSE Linux operációs rendszer esetén további környezeti feltétel, hogy szoftver vagy hardver tűzfal legyen telepítve. (A Suse telepítő lemezén található szoftveres tűzfal.)

II. Az alapértelmezett böngésző ellenőrzése

Az iSave_ugyfel program telepítése előtt ellenőrizni kell az alapértelmezett böngészőt a gépen. Ez az alábbiak egyike lehet:

- Internet Explorer 6.0 (XP-n)
- Internet Explorer 7.0 (XP-n, Vista-n)
- Firefox 3.0 és felette (XP-n, Vista-n)
- Firefox 1.5 és felette (Suse-n).

Amennyiben az alapértelmezett böngésző nem a fentiek egyike, akkor át kell állítani az alábbi módon:

- XP-n: Internet Explorer 6.0 vagy felette, illetve Firefox 3.0 vagy felette
- Vista-n Internet Explorer 7.0, illetve Firefox 3.0 vagy felette
- Suse-n Firefox 1.5 vagy felette.

III. Hardver erőforrás ellenőrzése

Az iSave_ugyfel program hardver igénye minimális, az operációs rendszeren felül 50 MB merevlemezt igényel.

IV. Az iSave_ugyfel program telepítése

A telepítést az iSave Kft. munkatársa végezze, aki a kliens oldali szoftver hiteles, értékelt verzióját egy CD-n tárolt telepítőkészletről töltse fel.

A telepítés folyamata során bizonyos adatokat be kell állítani, ezeknek alapértelmezett értéket ajánl fel a telepítő készlet. A biztonságos üzemeltetés érdekében a következő beállításokat kell alkalmazni a telepítés során:

1a Windows operációs rendszer esetén: Az iSave_ugyfel programot Windows Szerviz vagy Windows Alkalmazás üzemmódban is lehet telepíteni. Több felhasználós környezetben a Windows Szerviz módban történő telepítés biztonsági kockázatok miatt nem megengedett. Ebben az esetben Windows Alkalmazás üzemmódban kell telepíteni a Kliens rendszert.

1b Suse linux operációs rendszer esetén: Az iSave_ugyfel programot csak úgy lehet telepíteni, hogy az rendszergazda jogosultsággal fusson.

2 Az iSave_ugyfel ID (alapértelmezésben a számítógép neve) szabadon választható, de egyedinek kell lenni a rendszerben. Ezzel a névvel azonosítja be a szerver a kliens felhasználót.

3 Az alapértelmezett felhasználói névvel és jelszóval történő telepítés kockázatokat rejt ezért nem megengedett. A telepítés során az alapértelmezett ’admin’ felhasználói nevet és ’admin’ jelszót le kell cserélni, valamint meg kell jegyezni, mert a web konzol indításához és a rendszer későbbi konfigurálásához ezt a (felhasználónév, jelszó) párt kell használni.

4 A szerver oldali beállítások miatt a kliens oldalon a kommunikációs portokat (Backup Server Port, UI Communication Port) az alapértelmezett értékeken kell hagyni, különben a szerver oldali szolgáltatás nem lesz elérhető. A web szerver portjai (Web Szerver Port, Web HTTPS Port) szabadon változtathatók, azok a szerverrel történő kommunikációt nem befolyásolják. A HTTPS protokoll engedélyezése ugyancsak szabadon választható.

5 A többi telepítési paraméter szabadon megválasztható, nem rejt biztonsági kockázatot.

6 A telepítés végeztével a iSave_ugyfel\conf\SGConfiguration.conf fájlban az <SSL Enabled =”0”> bejegyzést 1-re kell állítani, a többi paramétert változatlanul kell hagyni. Ezzel állítódik be a kliens-szerver adatkommunikáció SSL védelme a 32007-es porton.

7a Windows operációs rendszer esetén: A telepítés után közvetlenül, a Help fájl leírásának megfelelően engedélyezni kell a 32007-es portot TCP/IP kapcsolatban. Az Apache web szerver biztonsága érdekében pedig le kell tiltani a 6060 és 6061-es portok kívülről történő elérését. Amennyiben a működési környezetben hardver tűzfal is van, ott is engedélyezni kell a 32007-es portot.

7b Suse linux operációs rendszer esetén: Telepítés után az elérhető szoftveres vagy hardveres tűzfalon engedélyezni kell a 32007-es portot. Az Apache web szerver biztonsága érdekében pedig le kell tiltani a 6060 és 6061-es portok kívülről történő elérését.

V. A web konzol első elindítása

1. A web konzol (iSave_ugyfel Web Console program) első indításakor a bejelentkezés a telepítéskor lecserélt (felhasználónév, jelszó) pár megadásával történik.
2. Ezt követően a felhasználónak azonosítani kell magát a Backup szerver felé (storage.isave.hu). Ehhez a telepítéskor megadott iSave_ugyfel ID-t valamint a most kötelezően megadandó hitelesítő jelszót használja a rendszer. Ennek a jelszónak megfelelő bonyolultságúnak kell lenni. Ennek érdekében az alábbiakat kell követni:
   Backup server: ki kell választani az alábbi értéket: storage.isave.hu
   Password: pontosan 16 karaktert kell megadni az alábbi szabályokat betartva:
   - Papírra kell írni 16 véletlenszerűen kiválasztott 16 karaktert, az alábbiak társaságában: iSave_ugyfel ID (amit a telepítés 2. lépésében kellett megadni), „hitelesítő jelszó”,
   - a 16 karakter között legyen legalább 2 nagybetű, 2 kisbetű és 2 számjegy is,
   - a papírra leírt 16 karaktert be kell gépelni,
   - A jelszót tartalmazó papírt borítékba kell helyezni,
   - A borítékot le kell zárni, le kell pecsételni (hogy észrevehető legyen az esetleges jogosulatlan felbontása) és rá kell írni az alábbiakat: iSave_ugyfel hitelesítő jelszó
   - A borítékot védett helyen meg kell őrizni, mert egy esetleges újra telepítésnél ugyanezt az iSave_ugyfel ID-t és hitelesítő jelszót kell használni, hogy a mentések és a visszaállítások elérhetőek legyenek.
3. Ezután létre kell hozni a mentési ütemezőt. Ez 5 lépésben történik:

   1. lépésben meg kell adni a mentési ütemező nevét (tetszőleges lehet).

   2. lépésben ki kell választani a mentendő könyvtárakat és fájl típusokat (tetszőleges lehet).

   3. lépésben meg kell határozni a mentés helyét. Ennek keretében el kell fogadni valamennyi alap értelmezett értéket, kivéve azt, hogy a megtartott verziók száma 5 legyen (az 5 helyett tetszőleges értéke választható)

   4. lépés: a titkosító kulcs biztonságos meghatározása:
      Encryption Key Size: **128 bit** (a 64 –es alapértéket módosítani kell)
      Type Password: pontosan **16** karaktert kell megadni az alábbi szabályokat betartva:
      - véletlenszerűen kell a karaktereket választani,
      - a 16 karakter között legyen legalább 2 nagybetű, 2 kisbetű és 2 számjegy is,
      - a meghatározott jelszót fel kell írni egy papírra, a „Mentési ütemező neve” (Backup Schedule Name) mellé,

      Confirm Password: Az előbb leírt 16 karaktert ismételten meg kell adni (ezáltal a leírás helyessége is ellenőrzésre kerül),
      A jelszót tartalmazó papírt borítékba kell helyezni,
      A borítékot le kell zárni, le kell pecsételni (hogy észrevehető legyen az esetleges jogosulatlan felbontása) és rá kell írni az alábbiakat: iSave_ugyfel titkosító kulcs
      A borítékot védett helyen meg kell őrizni, mert egy későbbi esetleges dokumentum visszaállításnál ezt a titkosító kulcsot kéri a rendszer.

   5. lépésben meg kell határozni a mentés gyakoriságát (tetszőleges).

5.3.3 A biztonságos felhasználás feltételei a szerver oldalon

6. működtetési feltétel: Biztonságos operációs rendszer használata (teljesül)

Az értékelés megállapította, hogy megfelelő biztonságú, helyesen konfigurált operációs rendszer fut a szerver oldalon.

7. működtetési feltétel: Az iSave_ugyfel biztonságos telepítése és konfigurálása (teljesül)

Az értékelés megállapította, hogy az iSave_ugyfel program biztonságos módon került telepítésre és konfigurálásra a szerver oldalon.

8. működtetési feltétel: Az iSave_ugyfel Web Console program biztonságos telepítése és konfigurálása (teljesül)

Az értékelés megállapította, hogy az iSave_ugyfel Web Console program biztonságos módon került telepítésre és konfigurálásra a szerver oldalon.

9. működtetési feltétel: A szerverek fizikai védelme (teljesül)

Az értékelés megállapította, hogy a Backup és Replikációs szerverek megfelelő fizikai védelem alatt állnak a szerver oldalon.

10. működtetési feltétel: A szerver oldal biztonságos üzemeltetése

A 6. – 9. működési feltétel teljesülését hosszú távon is biztosítani kell.

A hosszú távú biztonságos üzemeltetéssel kapcsolatban feltételezzük, hogy a szerver oldalon a különböző szerepköröket betöltő adminisztrátorok (tűzfal, operációs rendszer, alkalmazás) ismerik feladataikat, s ezeket szakképzett módon, lehetőségeikkel nem visszaélve látják el.

6. Hivatkozások, rövidítések és szakkifejezések

6.1 Hivatkozások

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

[2] Útmutató rendszer integrátorok számára (az „e-Közigazgatási Keretrendszer Kialakítása” projekt keretében kidolgozott dokumentum, megtalálható az alábbi helyen: http://kovetelmenytar.complex.hu)

[3] Útmutató rendszer értékelők számára (az „e-Közigazgatási Keretrendszer Kialakítása” projekt keretében kidolgozott dokumentum, megtalálható az alábbi helyen: http://kovetelmenytar.complex.hu)

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

6.2 Rövidítések és szakkifejezések

Rövidítés	Angol	Magyar
BALE	---	Biztonságos aláírás létrehozó eszköz
BS	Backup server	Backup szerver
DAR	---	(Elektronikus aláírásra és online backup szolgáltatásra épülő) digitális archiváló rendszer
FW	Firewall	Tűzfal
IT	Information Technology	Információs technológia, informatika
OE	Object for the Environment	(Biztonsági) cél az üzemeltetési környezetre
OS	Operational System	Operációs rendszer
RAID	Redundant Array of Independent Disks	Redundáns független merevlemezes tömbök
RS	Replication server	Replikációs szerver
SSCD	Secure Signature Creation Device	Biztonságos aláírás létrehozó eszköz
STOE	System Target of Evaluation	Rendszer értékelés tárgya
VPN	Virtual Private Network	Virtuális magánhálózat

6.3 Szakkifejezések

Jelen megfelelés értékelési jelentés az alábbi fogalmakat az alábbi értelemben használja:

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

Elektronikus aláírás: Elektronikus dokumentumhoz azonosítás céljából logikailag hozzárendelt vagy azzal elválaszthatatlanul összekapcsolt elektronikus adat (2001. évi XXXV. törvény (Eat.) 2.§).

Elektronikus aláírás ellenőrzése: Az elektronikusan aláírt elektronikus dokumentum aláíráskori, illetve ellenőrzéskori tartalmának összevetése, továbbá az aláíró személyének azonosítása a dokumentumon szereplő, illetve a hitelesítés-szolgáltató által közzétett aláírás-ellenőrző adat, tanúsítvány visszavonási információk, valamint a tanúsítvány felhasználásával (2001. évi XXXV. törvény 2.§).

Elektronikus aláírás létrehozása: Elektronikus dokumentumhoz elektronikus aláírás logikai hozzárendelése vagy azzal elválaszthatatlan összekapcsolása.

Elektronikus dokumentum: Elektronikus eszköz útján értelmezhető adategyüttes (2001. évi XXXV. törvény).

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.

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.

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

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