Ajánlás elektronikus archiválási szolgáltatások nyújtásához felhasznált megbízható rendszerekre vonatkozó biztonsági követelményekre

Nemzeti Hírközlési Hatóság Hivatala

2008. június

Tartalomjegyzék

1 Bevezetés

Az elektronikus aláírás felhasználásával végzett elektronikus archiválási szolgáltatások megbízható működésének kialakítására és a megfelelőség ellenőrzésére két ajánlást jelentő követelményrendszer került kidolgozásra. Jelen dokumentum a megbízható rendszerek műszaki követelményeit tartalmazza, s összhangban áll a másik követelményrendszerrel [D1], mely az archiválási szolgáltatók működésére (eljárásrendjére, szabályzataira) vonatkozik. A két követelményrendszer teljesítésével lehetővé válik az elektronikus aláírásról szóló 2001. évi XXXV. törvény ([eat]) szerinti archiválási szolgáltatók megbízható működésének kialakítása és a megfelelőség ellenőrizhetősége.

A jelen követelményrendszer célközönsége az elektronikus aláírás felhasználásával megvalósított elektronikus archiválási szolgáltatások tervezői, megvalósítói és működtetői, valamint a szolgáltatások megfelelőségének vizsgálatát végző szakértők és a Nemzeti Hírközlési Hatóság (továbbiakban: Hatóság) munkatársai. Fel kell hívni a figyelmet arra, hogy bár a jelen követelményrendszer a kidolgozásakor hatályban lévő jogszabályokat figyelembe véve készült, azonban egy adott szolgáltatás megfelelőségének megítélésénél a mindenkor hatályos jogszabályi követelményeket, valamint a szolgáltatásra vonatkozó más kötelező előírásokat kell figyelembe venni. A jelen követelményrendszer kötelező erővel nem bír, célja csupán annyi, hogy az irányadó előírások teljesítéséhez segítséget nyújtson. Más, az előírásokat teljesítő megoldások természetesen szintén megfelelőnek minősülnek.

Jelenleg nincs olyan nemzetközileg általánosan elfogadott követelményrendszer, mely jelen dokumentum meghatározó forrása lehetne. Ugyanakkor számos nemzeti és nemzetközi projekt, valamint több szabványosítási tevékenység foglalkozik a kérdéskör különböző aspektusaival. Ezek egy része (rész)eredményekkel lezárult, más része különböző készültségi szinteken álló tervezetek formájában megismerhető. Jelen követelményrendszer egy részletes témafeldolgozáson alapul, mely hasznosította a nemzetközi tapasztalatokat, egyúttal figyelembe veszi a hazai jogszabályi környezetet is.

A követelményrendszer felépítése a következő:

A 2. fejezet áttekintést ad az archiválási szolgáltatók megbízható rendszereiről, (kötelező és választható) szolgáltatásairól, a szolgáltatás logikai felépítéséről, valamint a lehetséges biztonsági szintekről.

A 3. fejezet az archiválási szolgáltatás funkcionális modellezését adja meg, az [ISO1] nemzetközi szabvány által meghatározott nyílt archív információs rendszerekre vonatkozó általános referencia modellen alapulva, egyúttal figyelembe véve a hazai jogszabályi elvárásokból adódó speciális elvárásokat is, elsősorban az elektronikus aláírás kötelező felhasználásával és a törlés funkció kötelező megvalósításával kapcsolatban. A funkcionális modell csak szemléltetési célokat szolgál, a később meghatározott követelmények megértését segíti, s egy lehetséges megvalósítási irányt mutat be.

A 4. fejezet az archiválási szolgáltatók megbízható rendszereire vonatkozó biztonsági követelményeket határozza meg, külön alfejezetekben az általános (minden megbízható rendszerre vonatkozó), majd az egyes szolgáltatásokra vonatkozó elvárásokat.

Az 5. fejezet a megfelelőségi követelményeket foglalja össze.

Végül a 6. fejezet a hivatkozott forrásokat, a 7. fejezet pedig a követelményrendszerben használt rövidítések jelentését adja meg.

2 Áttekintés

2.1 Archiválási szolgáltatók megbízható rendszerei

Jelen követelményrendszer az elektronikus aláírásról szóló 2001. évi XXXV. törvény ([eat]) szerinti elektronikus archiválási szolgáltatás nyújtásához használt megbízható rendszerekre vonatkozik.

A követelményrendszer elsősorban az archiválási szolgáltatók megbízható rendszereinek tervezői, megvalósítói, működtetői és értékelői számára készült, de bárki más is alkalmazhatja, aki megbízható rendszerekkel foglalkozik, és eleget kíván tenni ezen dokumentum előírásainak. E dokumentum áttekintést ad egy különböző szolgáltatásokat nyújtó archiválási szolgáltató rendszeréről. A szolgáltatások némelyike kötelező, ezeket alapszolgáltatásoknak nevezik, míg más szolgáltatások szabadon választhatóak, ezek az úgynevezett kiegészítő szolgáltatások.

Egy megbízható rendszer (MR) számos alrendszert tartalmazhat, melyek mindegyike egyedi archiválási szolgáltatásokat nyújthat (az 1. ábrán ezeket MR_1, MR_2 és MR_n jelöli).

Minden archiválási szolgáltató megbízható rendszerének meg kell felelnie az alapszolgáltatásokra vonatkozó, jelen dokumentumban előírt minimális biztonsági elvárásoknak. Amennyiben egy archiválási szolgáltató az alapszolgáltatások mellett kiegészítő szolgáltatást is nyújt, akkor az általa működtetett megbízható rendszernek teljesítenie kell az adott kiegészítő szolgáltatásra vonatkozó, jelen dokumentumban meghatározott minimális biztonsági elvárásokat is.

Természetesen az archiválási szolgáltató olyan egyéb szolgáltatásokat is nyújthat, melyekre vonatkozóan jelen dokumentum nem tartalmaz előírásokat.

A 4.1 alfejezet néhány, az összes szolgáltatást érintő általános biztonsági követelményt rögzít. Ezek kötelezőek, és valamennyi szolgáltatásra vonatkoznak.

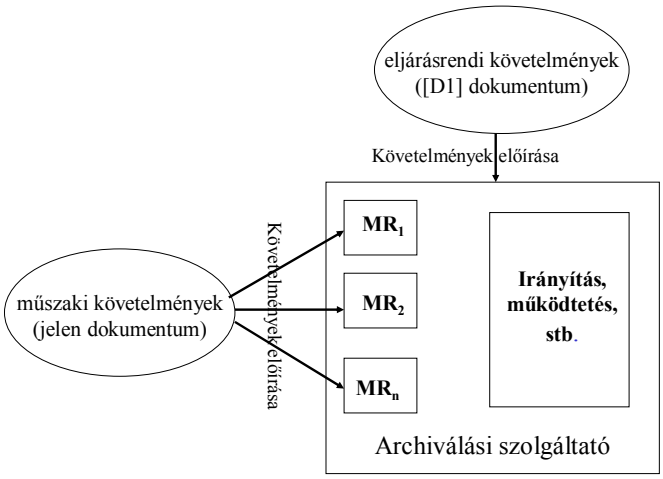
A 4.2 alfejezet a kötelező (alap) és a választható (kiegészítő) szolgáltatásokra vonatkozó biztonsági követelményeket határozza meg. Ezeket az alábbi csoportosításban vizsgálja:

- befogadással kapcsolatos funkciócsoport,
- megőrzéssel kapcsolatos funkciócsoport,
- kibocsátással kapcsolatos funkciócsoport.

A fentieket összefoglalva minden megbízható rendszernek meg kell felelnie a 4.1. alfejezet általános, valamint a 4.2. alfejezet alapszolgáltatásokra vonatkozó biztonsági követelményeinek. Ezen kívül az opcionálisan felvállalt szolgáltatásokra a 4.2. alfejezet megfelelő (kiegészítő jellegében külön jelzett) biztonsági követelményeit is teljesíteni kell.

Jelen dokumentum követelményeinek meghatározásakor az *Ajánlás eljárásrendi követelményekre elektronikus aláírás felhasználásával végzett elektronikus archiválási szolgáltatások szolgáltatói számára* című dokumentumot [D1] irányadónak tekintettük. Ennek alapján a [D1] dokumentum eljárásrendi követelményeinek teljesítéséhez a jelen dokumentumnak megfelelő megbízható rendszerek esetén az azokat használó archiválási szolgáltatóknak csak minimális konfigurálásról kell gondoskodniuk.

Az 1. ábra a két követelményrendszer közötti kapcsolatot szemléleti.



1. ábra: A műszaki és az eljárásrendi követelmények közötti összefüggés

2.2 Az archiválási szolgáltatók szolgáltatásai

2.2.1 Az archiválási szolgáltatás igénybevevői

Előfizető: Az a természetes vagy jogi személy, aki archiválási szerződést köt a szolgáltatóval és az archiválásra átadott adatok tulajdonosa.

Benyújtó (adatgazda): Az előfizető által meghatározott szerepkört betöltő természetes személy, aki:

- az archiválási szolgáltatónak adatot archiválásra benyújt,
- az általa benyújtott adat tekintetében
  - archiválási időt változtat,
  - teljes jogú hozzáférő,
  - további hozzáférő számára jogosultságot ad.

Hozzáférő: A benyújtó (adatgazda) rendelkezése szerint archivált adatot kikér, igazolást kér, feldolgoztat, értelmeztet vagy egyéb meghatározott tevékenységet végeztet.

2.2.2 A funkciók csoportosítása

Egy archiválási szolgáltatónak (s így megbízható rendszerének is) a következő funkciókat (funkciócsoportokat) kell biztosítania. Az egyes funkciók felsorolásánál feltüntetésre kerül, hogy azokat minden archiválási szolgáltató köteles-e biztosítani (*kötelező*), vagy az adott funkció biztosítása a szolgáltató vállalásától, illetve az előfizetővel kötött megállapodásától függ (*választható*) :

- Befogadással kapcsolatos funkciók (Befogadás funkciócsoport)
- Megőrzéssel kapcsolatos funkciók (Megőrzés funkciócsoport)
- Kibocsátással kapcsolatos funkciók (Kibocsátás funkciócsoport)

Befogadás funkciócsoport: Az archiválási szolgáltató által a benyújtók számára biztosított közvetlen funkciók a benyújtott információk befogadásával kapcsolatosan.

A befogadás funkciócsoport funkciói az alábbiak:

- A benyújtó azonosítása és jogosultságának ellenőrzése – *kötelező*
- Az archiválásra benyújtott információk fogadása – *kötelező*
- Az archiválásra benyújtott információk ellenőrzése – *kötelező*

- A megőrzési időtartam kezelése, befejezése – *kötelező*
- Az archiválással kapcsolatosan benyújtott információk visszaigazolása – *kötelező*
- A hozzáférési jogosultságok kezelése – *kötelező*

Megőrzés funkciócsoport: Az archiválási szolgáltató lényegi funkciói a befogadott információk folyamatos védelmére és megőrzésére.

A megőrzés funkciócsoport funkciói az alábbiak:

- Az archivált elektronikus adatok rendelkezésre állásának megőrzése – *kötelező*
- Az archivált elektronikus adatok sértetlenségének megőrzése – *kötelező*
- Az archivált elektronikus adatok bizalmasságának megőrzése – *kötelező*
- Az archivált elektronikus adatok titkosított formában történő megőrzése – *választható*
- Az archivált elektronikus adatok hitelességének és letagadhatatlanságának megőrzése – *kötelező*
- Az archivált elektronikus adatok értelmezhetőségének a fenntartása – *választható*
- Az archivált információk törlése az archiválásra vonatkozó szolgáltatási szerződés szerinti esetekben – *kötelező*

A megőrzési funkciók a benyújtók és a hozzáférők számára nem láthatók, ugyanakkor ezek alapozzák meg a számukra biztosított szolgáltatásokat.

Kibocsátás funkciócsoport: Az archiválási szolgáltató hozzáférők számára biztosított közvetlen funkciói az archivált adatokhoz való hozzáférés biztosítására és ennek ellenőrzésére.

A kibocsátás funkciócsoport funkciói az alábbiak:

- A hozzáférő azonosítása és jogosultságának ellenőrzése – *kötelező*
- Az archivált adat kiadása a jogosult hozzáférőnek (Adatkérés teljesítése) –*kötelező*
- Igazolások kiadása az archivált adatokra (Igazolás kérések teljesítése) – *kötelező*
- Az archivált adat és igazolás átadása más archiválási szolgáltatónak (A szolgáltatás befejezés előkészítése) – *kötelező*

2.2.3 Az archiválandó adatok csoportosítása

A benyújtó különböző tartalmú és formátumú adatot nyújthat be archiválásra, melyek érintik az igénybe vehető szolgáltatások körét. Az alábbi három csoport különböztethető meg:

- **Bitfolyam:** Az archiválási szolgáltató számára értelmezhetetlen bitsorozat. Bitfolyamra példák a titkosított, tömörített állományok, illetve az archiválási szolgáltató által (értelmezhetőség szempontjából) nem támogatott formátumú állományok.
- **Lenyomat:** Olyan speciális bitfolyam, amely az archiválási szabályzatban meghatározott hash függvény felhasználásával egy dokumentumból készült. Lenyomatra példa egy tetszőleges állományból SHA-512 hash függvénnyel készített 64 bájt.
- **Dokumentum:** Olyan speciális bitfolyam, amelynek a formátuma megfelel azon dokumentum formátumok egyikének, amelynek az értelmezhetőségét az archiválási szolgáltató (kiegészítő szolgáltatásként) felvállalhatja. Dokumentumra példák: rtf, txt, xml formátumú állományok.

Alkalmazási megjegyzés: Jelen dokumentumban, amennyiben a szövegkörnyezetből más nem következik, az adat szó alatt a bitfolyamot, lenyomatot és dokumentumot egyaránt értjük.

Az archiválandó adatoknak egy vagy több, fokozott biztonságú vagy minősített elektronikus aláírással kell ellátva lenniük.

2.2.4 Az archiválási szolgáltatások csoportosítása

Egy archiválási szolgáltatónak (s így megbízható rendszerének is) a következő (kötelező) **alapszolgáltatások**at kell biztosítania, az archiválás időtartama alatt:

- **Az archivált adat rendelkezésre állásának megőrzése (rendelkezésre állás):** Ez a szolgáltatás azt garantálja, hogy az archivált adatokat a szolgáltató (az archiválás időtartamának végéig) megőrzi, s az erre jogosult hozzáférők számára (folyamatosan) elérhetővé teszi.
- **Az archivált adat sértetlenségének megőrzése (sértetlenség):** Ez a szolgáltatás azt garantálja, hogy az archivált adatokat a szolgáltató oly módon őrzi meg, amely megakadályozza azok módosítását és jogosulatlan megsemmisítését.
- **Az archivált adat bizalmasságának megőrzése (bizalmasság):** Ez a szolgáltatás azt garantálja, hogy az archivált adatokat a szolgáltató oly módon őrzi meg, amely megakadályozza azok jogosulatlan megismerését az archiválás időtartama alatt.
- **Az archivált adat eredet hitelességének és tartalom letagadhatatlanságának a megőrzése (letagadhatatlanság):** Ez a szolgáltatás azt garantálja, hogy az – archivált adatot a benyújtás előtt elektronikus aláírással ellátó – aláíró utólag nem vitathatja, hogy az adat tőle származik.
- **Az archivált adat törlése (törlés):** A szolgáltató köteles biztosítani, hogy az archivált adatot az arra jogosult megfelelően hitelesített kérése alapján, továbbá az archiválás befejezésekor a rendszeréből visszaállíthatatlanul törli.
- **Igazolások kiadása:** Ez a szolgáltatás azt garantálja, hogy az archivált adatokkal kapcsolatos különböző tényekről a szolgáltató a hozzáférők számára hiteles igazolásokat képes kibocsátani.

Egy archiválási szolgáltató (s így megbízható rendszere is) a következő (választható) **kiegészítő szolgáltatások**at biztosíthatja, az archiválás időtartama alatt:

- **Az archivált adat értelmezhetőségének a fenntartása (értelmezhetőség):** Ez a szolgáltatás az archivált adat eredeti céljának folyamatos megvalósíthatóságát garantálja (pl. kép és szöveg esetén megjeleníthetőséget).
- **Az archivált adat titkosított formában való tárolása a szolgáltatónál (titkosítás):** A szolgáltató vállalhatja, hogy a hozzá részben vagy egészben nyílt formában (titkosítatlanul) benyújtott archivált adatokat a befogadás után titkosítja, és ilyen módon tárolja a bizalmasság fokozott biztosítása érdekében.

Egy archiválási szolgáltató (s így megbízható rendszere is) egyéb szolgáltatásokat is biztosíthat (pl. az archivált adatok egyedi megállapodás szerinti feldolgozását). Jelen dokumentum ezekre nézve nem fogalmaz meg kötelező elvárásokat, azon túl, hogy ezek az egyéb szolgáltatások nem akadályozhatják meg a kötelező követelmények teljesülését.

2.2.5 A különböző archiválandó adatokra biztosítható archiválási szolgáltatások

Egy archiválási szolgáltató szolgáltatási szabályzatában meghatározhatja, hogy milyen formátumú adatokat fogad be archiválásra (bitfolyamot és/vagy lenyomatot és/vagy dokumentumot), a dokumentum formátumok tételes meghatározásával.

Egy archiválási szolgáltatónak minden általa befogadott adatra kötelező biztosítania az alapszolgáltatásokat (rendelkezésre állás, sértetlenség, bizalmasság, letagadhatatlanság, törlés és igazolások kiadása).

Egy archiválási szolgáltató szolgáltatási szabályzatában minden általa befogadott adatra meghatározhatja, hogy milyen kiegészítő szolgáltatást vállal (értelmezhetőség, titkosítás)

Az alábbi táblázat a különböző formátumú archiválandó adatokra biztosítható kiegészítő szolgáltatásokat tekinti át.

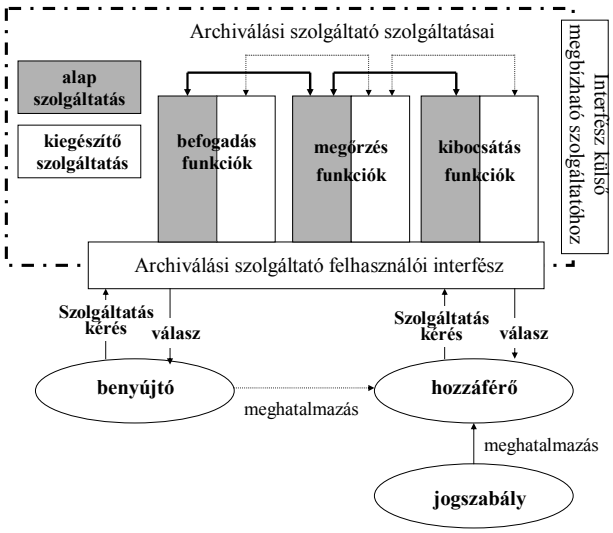
Az archiválandó adat formátuma	**Biztosítható kiegészítő archiválási szolgáltatások**	
	Szolgáltatás	**Biztosíthatóság**
Bitfolyam	Titkosítás	korlátozás nélkül
	Értelmezhetőség	nem biztosítható
Lenyomat	Titkosítás	nem értelmezhető
	értelmezhetőség	nem biztosítható
Dokumentum	Titkosítás	korlátozás nélkül
	értelmezhetőség	korlátozás nélkül

A táblázatból láthatók az alábbiak:

- titkosítás kiegészítő szolgáltatás lenyomat formátumra nem értelmezhető,
- az értelmezhetőség kiegészítő szolgáltatás csak olyan dokumentum formátumú benyújtott adatra biztosítható, mely a szolgáltatási szabályzatban meghatározott formátumoknak megfelel.

2.3 Általános felépítés

A 2. ábra egy archiválási szolgáltató logikai felépítését mutatja be, azt szemléltetve, hogy milyen úton biztosítja egy archiválásra benyújtott adat befogadását, megőrzését, illetve kibocsátását. Az ábrán kötelező és választható szolgáltatások egyaránt láthatók, egyúttal fel vannak tüntetve az archiválási szolgáltatónak a benyújtókkal, illetve a más érintettekkel (köztük bármilyen külső megbízható szolgáltatásokkal) való kapcsolódásai is.



2. ábra: Egy archiválási szolgáltató megbízható rendszerének logikai felépítése

A megbízható rendszer felhasználói interfésze garantált hozzáférést biztosít a benyújtó számára az alap és kiegészítő szolgáltatásokhoz, míg a benyújtó vagy egy jogszabály meghatalmazása alapján egyéb hozzáférők is igénybe vehetnek bizonyos szolgáltatásokat. A megbízható szolgáltatóhoz irányuló interfész pedig egyéb belső vagy külső szolgáltatások (pl. tanúsítvány állapot szolgáltatás vagy időbélyegzés szolgáltatás) felé nyújt hozzáférést.

Egy archiválási szolgáltató több megbízható alrendszert is igénybe vehet alap és (amennyiben van ilyen) kiegészítő szolgáltatásai megvalósításához.

2.4 Biztonsági szintek

Egy archiválási szolgáltató két különböző biztonsági szinten vállalhat szolgáltatásokat. A két szint: minősített és nem minősített szolgáltatások. A minősített szolgáltatást felvállaló archiválási szolgáltatókra esetenként szigorúbb biztonsági követelmények vonatkoznak. A követelmények leírásánál az alábbi jelölés alapján lehet a két biztonsági szintet megkülönböztetni:

[SR[1]1.1]
Olyan biztonsági követelmény, amely a minősített és a nem minősített szolgáltatásra egyaránt vonatkozik.

[SR1.2] – csak nem minősített szolgáltatásra
Olyan biztonsági követelmény, amely csak a nem minősített szolgáltatásra vonakozik.

[SR1.2] – csak minősített szolgáltatásra
Olyan biztonsági követelmény, amely csak a minősített szolgáltatásra vonatkozik.

Egy megbízható rendszernek vagy az „[SR1.2] – csak nem minősített szolgáltatásra", vagy az „[SR1.2] – csak minősített szolgáltatásra" követelményt kell teljesítenie, mindkettőt nem.

3 Az archiválási szolgáltatás funkcionális modellezése

Az alábbi funkcionális modell szemléltetési célokat szolgál. A később meghatározott kötelező követelmények megértését támogatja, s egy lehetséges megvalósítási irányt mutat.

Az alap és kiegészítő archiválási szolgáltatásokra vonatkozó követelmények meghatározása előtt szükséges meghatározni néhány alapfogalmat, valamint felvázolni egy olyan általános funkcionális modellt, mely a központosított és a szétosztott archiválási modellre egyaránt alkalmazható. (A központosított modellben az archiválási szolgáltató átveszi megőrzésre az archivált adatot, míg a szétosztott modellben csak lenyomatot nyújtanak be az archiválási szolgáltatónak megőrzésre.)

Az alábbiak az [ISO1] és [OAIS] által meghatározott nyílt archív információs rendszerekre vonatkozó referencia modellen alapulnak.

A 3. ábra egy archiválási szolgáltató környezetét mutatja.

3. ábra: Egy archiválási szolgáltató környezete

A **benyújtó** az a személy (vagy szerepkör), aki/amely a megőrzendő adatokat szolgáltatja az archiválási szolgáltató számára (aki benyújtásra jogosult).

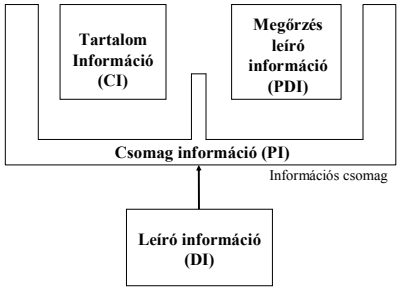
Az **irányítás (**szerepkör) határozza meg az archiválási szolgáltató általános szabályzatát.

[1] **SR**: **S**ecurity **R**equirement

A **hozzáférő** az a személy (vagy szerepkör), aki/amely az archiválási szolgáltatóval kapcsolatba kerül, hogy megtalálja és megszerezze az érdeklődésére számot tartó információt.

Minden benyújtó egyben hozzáférő is. Általában a hozzáférő a benyújtótól kapja, vagy jogszabálytól nyeri jogosultságát. Az archiválási szolgáltató szolgáltatási szabályzata meghatározhat egyéb eseteket (pl. ha egy szervezet nem reagál az archiválási szolgáltató megkeresésére, akkor az archivált adatokat az archiválási szolgáltató kiadhatja a szervezet tulajdonosainak).

Minden információ benyújtás (egy benyújtó által az archiválási szolgáltatónak) és minden információ kibocsátás (az archiválási szolgáltató által a hozzáférőnek) különálló átadásokként jelenik meg. Ezért hasznos az információs csomag fogalma, melyet a 4. ábra szemléltet.



4. ábra: Az információs csomag felépítése

Az **információs csomag** (Information Package, **IP**) egy képzeletbeli tároló, mely két különböző típusú információt tárol: tartalom információt és megőrzés leíró információt.

A **tartalom információ** (Content Information, **CI**) az eredetileg megőrzésre szánt (tipikusan még elektronikus aláírás nélküli) információ. Központosított modell esetén a CI a megőrzésre benyújtott bitfolyam vagy dokumentum. Szétosztott modell esetén CI hiányzik, pontosabban a benyújtónál marad.

A **megőrzés leíró információ** (Preservation Description Information, **PDI**) a tartalom információra (CI) vonatkozik, s a CI megőrzéséhez szükséges, biztosítva annak egyértelműségét, sértetlenségének és hitelességének megőrzését, valamint létrehozási környezetének megértését:

- A PDI egyik eleme a (szükség szerint megújított) **elektronikus aláírás**, mely a tartalom információ sértetlenségét, hitelességét és letagadhatatlanságát védi.
- A PDI egy másik eleme leírja a tartalom információ eredetét vagy forrását (a keletkezéstől kezdve), valamint történetét (beleértve a feldolgozás történetét is).
- A PDI harmadik típusú eleme azt írja le, hogy a tartalom információ hogyan viszonyul az információs csomagon kívüli egyéb információkhoz (pl. leírhatja, hogyan állították elő, vagy milyen kapcsolatban áll más elérhető információ tartalmakkal).
- A PDI negyedik típusú eleme egy vagy több azonosítót vagy azonosító rendszert tartalmaz, melyek egyértelműen azonosítják az információ tartalmat.

A **csomag információ** (Packaging Information, **PI**) az az információ, mely ténylegesen vagy logikailag összeköti, azonosítja és kapcsolatba hozza a CI-t és a PDI-t. (Ha pl. a CI és PDI egy CD-ROM egyes fájljainak tartalma, akkor a PI magában foglalhatja a CD-ROM ISO 9660 fájl struktúráját, valamint a lemezen tárolt fájlok név és könyvtár információit.)

A **leíró információ** (Description Information, **DI**) az az információ, melynek alapján meg lehet találni, hogy melyik csomag tartalmaz egy keresett CI-t. (Ez lehet egy egyszerű leíró cím, de lehet egy olyan attribútum halmaz is, melyre keresési lehetőség biztosított.)

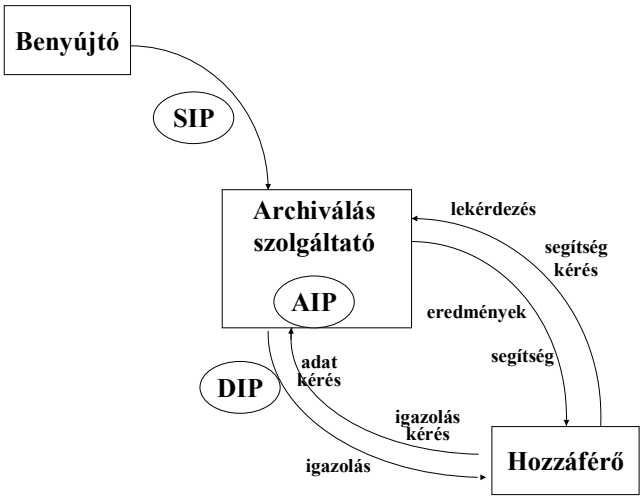
Szükséges még az archiválási szolgáltatók által tárolt, fogadott, illetve kibocsátott információs csomagok megkülönböztetése is (lásd 5. ábra).

A **benyújtott információs csomag** (Submission Information Package, **SIP**) az archiválási szolgáltatónak egy benyújtó által beküldött információs csomag. Formáját és tartalmát közvetlenül a benyújtó és az archiválási szolgáltató közötti szerződések, közvetve a szolgáltató archiválási szabályzata és általános szerződési feltételei határozzák meg.

Az archiválási szolgáltatóhoz benyújtott egy vagy több SIP átalakításából keletkezik a megőrzésre kerülő **archív információs csomag** (Archival Information Package, **AIP**). Az AIP az archiválási szolgáltató belső szabványa, idővel változhat is.

Egy adat kérésre adott válaszként az archiválási szolgáltató egy AIP egészét, vagy egy részét **kibocsátott információs csomag** (Dissemination Information Package, **DIP**) formájában adja át a hozzáférőnek. A DIP tartalmazhat több AIP-t is, egyúttal tartalmazhatja a teljes PDI-t, de ez hiányozhat is belőle. A PI valamilyen formájára szükség van, hogy a hozzáférő egyértelműen azonosíthassa azt az információt, melyet kért.

Az 5. ábra magas szintű áttekintést ad az archiválási szolgáltató, a benyújtó és a hozzáférő közötti külső adatáramlásokról.



5. ábra: Adatáramlások az archiválási szolgáltató és az igénybe vevők között

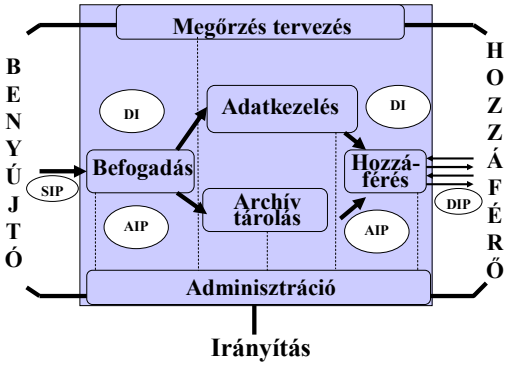
A **lekérdezés**ek az adatbázisban tárolt megőrzés leíró információkra (PDI) vonatkoznak, az erre adott válaszok (**eredmények**) alapján találhatja meg a hozzáférő azokat az archivált adatokat, melyeket lekérdezni kíván, vagy melyekről igazolásra van szüksége.

Az **adat kérés**ek az adathordozón tárolt archivált adatokra (tartalom információ, CI) vonatkoznak, tipikusan egy archivált adat letöltésére vagy megjelenítésére. A válasz: hozzáférés (letöltés vagy megjelenítés) engedélyezése a DIP-hez.

Az **igazolás kérés**ek egy része az adatbázisban tárolt elektronikus aláírások (melyek a PDI-k egy részét alkotják) érvényességére vonatkoznak, az ezekre adott **igazolás**ok létrehozásához általában nincs szükség az adathordozókhoz fordulni, az adatbázisban tárolt adatok alapján kiadhatók. Más igazolás kérések létrehozásához adathordozókhoz is kell fordulni.

A **segítség kérés**ek a különböző egyéb kérési/keresési lehetőségekre, vagy a korábban elküldött kérések állapotára vonatkozhatnak.

A funkcionális modell az archiválási szolgáltató rendszerét hat funkcionális egységre és az ezekkel kapcsolatos interfészekre osztja, ahogy azt a 6. ábra mutatja:



6. ábra: Funkcionális egységek

Befogadás: Ez a funkcionális egység fogadja a benyújtótól, vagy az adminisztrációs ellenőrzés alatt álló belső elemektől a benyújtott információs csomagokat (SIP), és felkészíti tartalmukat a tároláshoz és az archívum menedzseléséhez. A befogadás funkciói az alábbiakat tartalmazzák:

- SIP-ek fogadása (beleértve a már befogadott SIP-ek törlésére vonatkozó igények fogadását is),
- a SIP-ek ellenőrzése (ennek része az aláírás ellenőrzése),
- AIP létrehozása (ennek része az aláírást érvényesítő adatok összegyűjtése),
- A SIP-ek befogadásának visszaigazolása a benyújtónak,
- DI kinyerése az AIP-okból, s ezek archív adatbázisba foglalása,
- az archív tárolás és az adatkezelés frissítésének összhangba hozása.

Archív tárolás: Ez a funkcionális egység az AIP-ek tárolását, karbantartását és visszakeresését biztosítja. Az archív tárolás funkciók az alábbiakat tartalmazzák:

- AIP-ek fogadása (a befogadás funkcionális egységtől) és letárolása,
- a tárolási hierarchia kezelése,
- az archív állományt tároló adathordozók frissítése,
- a szokásos és a különleges hibaellenőrzések végrehajtása,
- katasztrófa helyreállítási képesség biztosítása,
- AIP-k biztosítása (a hozzáférés funkcionális egység számára) a kérések teljesítéséhez.

Adatkezelés: Ez a funkcionális egység az archív állományt azonosító és dokumentáló DI-k (leíró információ) és az archívum kezeléséhez használt adminisztrációs adatok telepítését, karbantartását és elérését biztosítja. Az adatkezelés funkciói az alábbiakat tartalmazzák:

- az archív adatbázis funkciók adminisztrálása,
- adatbázis frissítések végrehajtása, benne az elektronikus aláírások megújítása (a megőrzés tervezés funkcionális egység ajánlásai alapján, az adminisztráció funkcionális egység közvetítésével),
- az adatkezelés adataira irányuló lekérdezések és igazolás kérések végrehajtása, a végrehajtás kimenete (eredmények és igazolások) biztosítása a hozzáférés funkcionális egység számára.

Adminisztráció: Ez a funkcionális egység az archiválási rendszer általános működtetését biztosítja. Az adminisztráció funkciói az alábbiakat tartalmazzák:

- a benyújtóval kötendő (benyújtási-befogadási) szerződések kezelése,
- a benyújtott információs csomagok átvizsgálása az archiválási szabályoknak való megfelelés biztosítására,
- a rendszer hardver és szoftver elemeinek konfiguráció kezelése,

- rendszerfunkciók biztosítása az archiválás műveletek felügyeletére és javítására, valamint az archívum tartalmának leltározására, frissítésére (aláírás megújítások, új adathordozókra másolás), jelentések készítésére,
- archiválási szabványok és szabályzatok készítése és karbantartása,
- támogatás biztosítása a hozzáférők számára,
- a tárolt lekérdezések, adat kérések és igazolás kérések aktivizálása.

Megőrzés tervezés: Ez a funkcionális egység felügyeli az archiválási rendszer környezetét, valamint javaslatokat tesz annak érdekében, hogy az archiválási rendszer által tárolt információ hosszú távon érvényes és elérhető maradjon, még az alkalmazott kriptográfiai algoritmusok elévülése és az eredeti számítógépes környezet elavulása esetén is. A megőrzés tervezés funkciói az alábbiakat tartalmazzák:

- az archívum tartalmának értékelése és időszakos javaslatok az archivált információ frissítésére az aktuális archivált aláírások megújításával, vagy az archivált állomány új adathordozóra másolásával,
- javaslatok kidolgozása az archiválási szabványokhoz és szabályzatokhoz,
- a technológiai környezetben és a benyújtó/hozzáférő szolgáltatásra vonatkozó elvárásában bekövetkező változások figyelemmel kísérése,
- részletes frissítési tervek, szoftver prototípusok és tesztelési tervek készítése.

Hozzáférés: Ez a funkcionális egység támogatja a hozzáférőt az archiválási szolgáltató által tárolt információk létezésének, leírásának, elhelyezkedésének és elérhetőségének a meghatározásában, egyúttal lehetővé teszi, hogy a hozzáférő információkat kérjen és kapjon. A hozzáférés funkciói az alábbiakat tartalmazzák:

- a hozzáférővel való kommunikáció, a lekérdezések és a különböző (adat, igazolás, segítség) kérések fogadása,
- a védett információkhoz való hozzáférés korlátozása (a jogosultságok kezelése),
- a lekérdezések és a különböző (adat, igazolás, segítség) kérések végrehajtásának összhangba hozása a sikeres befejezés érdekében,
- válaszok létrehozása (eredmények, kibocsátott információs csomagok (DIP), igazolások és segítségek) és kibocsátása,
- a kibocsátott válaszok eljuttatása a hozzáférőkhöz.

4 Biztonsági követelmények

Ez a fejezet a kötelező eljárásokat és a velük kapcsolatos biztonsági követelményeket ismerteti, amelyek egy archiválási szolgáltató által nyújtott alap és kiegészítő szolgáltatásokra egyaránt érvényesek.

A megbízható rendszerek **általános** funkcióit és biztonsági követelményeit a 4.1. alfejezet ismerteti. Ezek egy archiválási szolgáltató minden szolgáltatására érvényesek.

A megbízható rendszerek **alap és kiegészítő szolgáltatás**ainak funkcióit és biztonsági követelményeit a 4.2. alfejezet határozza meg.

4.1 Általános biztonsági követelmények

Menedzselés [2]

MA1 Rendszer- és biztonságkezelés
Az archiválási szolgáltatónak a saját biztonságát is menedzselnie kell, hogy megbízható rendszereit üzemeltethesse.

[MA1.1]
A megbízható rendszereknek különböző jogokkal bíró munkaköröket kell biztosítaniuk.

[MA1.2] – csak minősített szolgáltatásra
Legalább a következő munkakörök (bizalmi szerepkörök) szükségesek a megbízható rendszerek menedzseléséhez:

biztonsági tisztviselő: az archiválási szolgáltatás biztonságáért általánosan felelős személy,

rendszeradminisztrátor: az informatikai rendszer telepítését, konfigurálását, karbantartását végző személy,

rendszerüzemeltető: az informatikai rendszer folyamatos üzemeltetését, mentését és helyreállítását végző személy,

független rendszervizsgáló: az archiválási szolgáltató naplózott, illetve archivált adatállományait (ide nem értve a szolgáltatás nyújtása keretében archiválásra átvett adatokat) vizsgáló, a szolgáltató által a szabályszerű működés érdekében megvalósított kontroll intézkedések betartásának ellenőrzéséért, a meglévő eljárások folyamatos vizsgálatáért és monitorozásáért felelős személy,

A fenti bizalmi szerepkörök mellett ajánlott a következő bizalmi szerepkör létrehozása:

archiválási tisztviselő: Archiválási tisztviselő: az archivált adatok kódolását és dekódolását, valamint az archivált elektronikus aláírások érvényességének folyamatos karbantartását és az archivált adatokkal kapcsolatos igazolások kiadását végző, illetve ezen tevékenységekért felelős személy,

[MA1.2] – csak nem minősített szolgáltatásra

A megbízható rendszer menedzseléséhez a szolgáltatónak elégséges számú, megfelelő képzettséggel, végzettséggel és gyakorlattal rendelkező személyzettel kell rendelkeznie. Bizonyos, a rendszer megbízható üzemelése szempontjából kritikus feladatköröket (bizalmi munkaköröket) indokolt megfelelő megbízhatóságú személyekre (bizalmi tisztségviselőkre) bízni. A bizalmi szerepkörök betöltőinek mentesnek kell lenniük minden olyan befolyástól, amely szerepkörük megfelelő ellátását veszélyeztethetné. A bizalmi szerepkörök kialakításánál arra kell figyelemmel lenni, hogy egy szerepkör betöltőjének kezében ne egyesülhessenek a rendszer megbízható működése szempontjából összeférhetetlen funkciók. A bizalmi szerepkörök lehetséges kialakítására példaként szolgálhat az alábbi felosztás:

biztonsági tisztviselő: az archiválási szolgáltatás biztonságáért általánosan felelős személy,

[2] [**MA**: **Ma**nagement]

rendszeradminisztrátor: az informatikai rendszer telepítését, konfigurálását, karbantartását végző személy,

rendszerüzemeltető: az informatikai rendszer folyamatos üzemeltetését, mentését és helyreállítását végző személy,

archiválási tisztviselő: Archiválási tisztviselő: az archivált adatok kódolását és dekódolását, valamint az archivált elektronikus aláírások érvényességének folyamatos karbantartását és az archivált adatokkal kapcsolatos igazolások kiadását végző, illetve ezen tevékenységekért felelős személy,

független rendszervizsgáló: az archiválási szolgáltató naplózott, illetve archivált adatállományait (ide nem értve a szolgáltatás nyújtása keretében archiválásra átvett adatokat) vizsgáló, a szolgáltató által a szabályszerű működés érdekében megvalósított kontroll intézkedések betartásának ellenőrzéséért, a meglévő eljárások folyamatos vizsgálatáért és monitorozásáért felelős személy,

[MA1.3]
A megbízható rendszereknek össze kell tudniuk kapcsolni a felhasználókat a fenti munkakörökkel.

Alkalmazási megjegyzés: Lényeges, hogy egyetlen felhasználó ne hajthassa végre a megbízható rendszerekre meghatározott összes funkciót. Ezért egy felhasználót nem ajánlott feljogosítani több munkakörre.

[MA1.4]
A megbízható rendszereknek biztosítaniuk kell, hogy:

- egy biztonsági tisztviselő munkakört betöltő felhasználó nem lehet független rendszervizsgáló,
- egy rendszeradminisztrátori munkakört betöltő felhasználó nem kaphat biztonsági tisztviselői vagy független rendszervizsgálói jogokat – **csak minősített szolgáltatásra**.

Alkalmazási megjegyzés: Amennyiben az archiválási szolgáltató egyben hitelesítés-szolgáltató is, akkor az [MA1.2]-ben említett munkaköröket betölthetik azok a munkatársak is, akik a hitelesítés-szolgáltatás kapcsán ugyanazt a munkakört töltik be.

Rendszerek és működésük[3]

SO1 Üzemeltetés menedzselése

[SO1.1]
Az üzemeltetés-menedzselési funkciók megfelelő biztonsága érdekében a megbízható rendszerek gyártói vagy az archiválási szolgáltató által olyan útmutatókat kell biztosítani, melyek lehetővé teszik a megbízható rendszerek vonatkozásában az alábbiakat:

1. helyes és biztonságos működtetés,
2. a rendszerhibák kockázatának minimalizálását biztosító telepítési mód,
3. vírusokkal és kártékony szoftverekkel szembeni védelem, a rendszerek és az általuk feldolgozott információk sértetlenségének fenntartása érdekében.

[3] [**SO**: **S**ystems and **O**perations]

Ezen követelmény kielégítése érdekében a megbízható rendszerek gyártóinak biztosítaniuk kell dokumentációt a következőkre:

- telepítés,
- adminisztrálás,
- felhasználás, kezelés.

SO2 A folyamatos szolgáltatás biztosítása

A szolgáltatások folyamatos biztosítása garantálja, hogy az archiválási szolgáltató szolgáltatásai a megbízható rendszerben bekövetkezett hiba esetén is elérhetők.

[SO2.1] - csak nem minősített szolgáltatásra

Az alábbi szolgáltatásokat biztosító megbízható rendszereknek ellen kell állniuk egy egyszeres hibának, és megszakítás nélkül folytatniuk kell a működést az alábbiakra:

- tárolási időtartam módosítása
- archivált adat törlése
- az archivált adatok közötti keresés (lekérdezés)
- az archivált adatok lekérése (adat kérés)
- az archivált adatokra vonatkozó különböző igazolások kiadása (igazolás kérés)
- a kérési lehetőségekre, illetve a korábban elküldött kérések állapotára vonatkozó információ kérés (segítség kérés)

A fenti szolgáltatásokra vállalt egyes rendelkezésre állásokat a szolgáltatási szabályzatban meg kell határozni.

[SO2.1] - csak minősített szolgáltatásra

Az alábbi szolgáltatásokat biztosító megbízható rendszereknek ellen kell állniuk egy egyszeres hibának, és megszakítás nélkül folytatniuk kell a működést az alábbiakra:

- tárolási időtartam módosítása
- archivált adat törlése
- az archivált adatok közötti keresés (lekérdezés)
- az archivált adatok lekérése (adat kérés)
- az archivált adatokra vonatkozó különböző igazolások kiadása (igazolás kérés)
- a kérési lehetőségekre, illetve a korábban elküldött kérések állapotára vonatkozó információ kérés (segítség kérés)

A fenti szolgáltatásokra legalább 99%-os rendelkezésre állást kell biztosítani éves átlagban, az eseti szolgáltatás kiesések időtartama nem haladhatja meg a három napot.

[SO2.2] – csak minősített szolgáltatásra

Katasztrófahelyzetben a megbízható rendszereknek olyan funkciókat kell biztosítaniuk, melyek az archiválási szolgáltatónak lehetővé teszik a működés folytatását, alternatív megbízható rendszerek használatával.

Alkalmazási megjegyzés: A rendelkezésre állásra vonatkozó követelmények nem alkalmazhatók katasztrófa helyzetben. Ilyen esetben a megbízható rendszereknek az elfogadható maximális szolgáltatás kiesésre vonatkozó követelményeknek kell megfelelniük.

[SO2.3] – csak minősített szolgáltatásra

Az elsődleges rendszerről az alternatív megbízható rendszerre való áttérés és az onnan történő visszaállás az elsődleges rendszerre nem okozhat elfogadhatatlan kockázatot a rendszerek megbízhatósági tulajdonságában.

Alkalmazási megjegyzés: A fenti követelmények nem jelentenek tartalék helyszínen biztosított teljes tartalék rendszer működtetési kötelezettséget. Az adathordozókon tárolt archivált adatok, valamint az adatbázisban tárolt metaadatok vonatkozásában azonban

megkövetelik a földrajzilag elkülönült tartalék helyszínen való tárolást. (Így egy katasztrófa esetén is biztosított az archivált adatok megőrzése.)

SO3 Időszinkronizáció

Alkalmazási megjegyzés: A befogadással és kibocsátással kapcsolatos szolgáltatások, valamint ezek menedzselése időfüggő, ezért szükséges, hogy biztosítva legyen a megbízható rendszerek megfelelő szinkronizálása egy szabványos időforráshoz.

[SO3.1] - csak nem minősített szolgáltatásra
A szolgáltatás nyújtásához felhasznált megbízható rendszerek gyártóinak állítást kell megfogalmazniuk az idő pontosságára, s arra, hogy ezt hogyan biztosítják.
Megbízható időforrást javasolt alkalmazni az idő pontosságának biztosítására.

[SO3.1] - csak minősített szolgáltatásra
A megbízható rendszerek minden időfüggő, archiválási szolgáltató szolgáltatáshoz használt óráját szinkronizálni kell a Co-ordinated Universal Time (UTC) egy másodperces időtartamán belül.
Két független UTC forrást javasolt alkalmazni az üzembiztos időforrás fenntartása érdekében.

Azonosítás és hitelesítés[4]

Alkalmazási megjegyzés: Az azonosítási és hitelesítési funkciók biztosítják, hogy csak jogosult személyek férhessenek a megbízható rendszerekhez, illetve csak ők használhassák ezeket.

Alkalmazási megjegyzés: Az azonosítás és hitelesítés biztosítható az alapot képező operációs rendszer által, vagy közvetlenül az egyes összetevőkön keresztül.

Alkalmazási megjegyzés: Az alábbi (azonosítási és hitelesítési) követelmények az archiválási szolgáltató valamennyi összetevőjére és valamennyi felhasználójára alkalmazandóak, az [MA1.2] alatt meghatározott bizalmi szerepeket betöltő személyeken kívül a benyújtókra és a hozzáférőkre is.

IA1 A felhasználó hitelesítése

[IA1.1]
A megbízható rendszereknek meg kell követelniük minden felhasználótól, hogy azonosítsák magukat, és sikeres azonosításnak kell megelőznie az adott felhasználó vagy a felhasználó munkaköre nevében történő bármely művelet végrehajtásának az engedélyezését.

[IA1.2]
A felhasználó kijelentkezése után kötelező az újrahitelesítés.

[IA1.3]
Amennyiben hitelesítő adatokat használnak, ezeknek egyedinek kell lenniük, és nem lehet többször kiadni ezeket.

Alkalmazási megjegyzés: Hitelesítési adatra példa a (felhasználói név, jelszó) páros.

[IA1.4]
Az archiválási szolgáltatás a felek megállapodása alapján oly módon is nyújtható, hogy az igénybe vevő (benyújtó vagy hozzáférő) nem bocsátja a szolgáltató rendelkezésére

[4] [**IA**: **I**dentification and **A**uthentication]

személyazonosító adatait. Ebben az esetben is szükséges az [IA1.1] - [IA1.3] követelmények kielégítése, de az azonosítás egy álnév alapján is történhet.

[IA1.5]
A visszaélés lehetőségének korlátozása szükséges automatikus kijelentkeztetés használatával, megadott inaktivitást követően, a tranzakció lezárásával vagy adott időn túl.

IA2 A hitelesítési hiba kezelése

[IA2.1]
A megbízható rendszereknek meg kell akadályozniuk a további hitelesítési kísérleteket, ha a sikertelen hitelesítési kísérletek száma elér vagy meghalad egy maximumként meghatározott értéket (hacsak nem rendszeradminisztrátori munkakörről van szó).

[IA2.2] - csak minősített szolgáltatásra
Ha a sikertelen hitelesítési kísérletek száma eléri vagy meghaladja a megengedett kísérletek maximális számát, és rendszeradminisztrátori munkakörről van szó, akkor megfelelő más csatornán értesítést (pl. riasztás, figyelmeztető üzenet) kell generálni.

Alkalmazási megjegyzés: Ez a követelmény nem alkalmazandó azokban az esetekben, amikor közvetlen token hitelesítési mechanizmusokat (pl. PIN-beolvasóval felszerelt intelligens kártyaolvasó) alkalmaznak.

IA3 A titkok ellenőrzése

[IA3.1]
A megbízható rendszereknek mechanizmust (vagy mechanizmusokat) kell biztosítaniuk annak ellenőrzésére, hogy a titkok (pl. jelszavak, PIN kódok) megfelelnek-e az egyes komponensekhez meghatározott követelményeknek. A kitalálás vagy a téves elfogadás próbálkozásonkénti valószínűségének mindig elhanyagolhatóan kicsinek kell lennie.

Alkalmazási megjegyzés: Példák ilyen mechanizmusra:
- annak ellenőrzése, hogy a jelszó legalább 6 karakter hosszú, s tartalmaz legalább egy-egy nagybetűt, kisbetűt és számot,
- annak ellenőrzése, hogy a jelszó hossza 7 és 9 között van, számjegyekből áll, de nem lehetnek benne szomszédos számpárok (1,2) (3,4), (9,8),
- annak ellenőrzése, hogy az új jelszó nem egyezik meg az utolsó öt lecserélttel.

Rendszer-hozzáférés ellenőrzés[5]

Alkalmazási megjegyzés: A rendszer-hozzáférés ellenőrzés funkciói azt felügyelik, hogy csak meghatalmazott személyek használhassák a megbízható rendszerek objektumait (tárolt adatokat, rendszerfunkciókat, stb.). Ez az archiválási szolgáltató valamennyi érzékeny objektumára alkalmazandó.

Alkalmazási megjegyzés: A rendszer-hozzáférés ellenőrzést biztosíthatja az alapot képező operációs rendszer, vagy közvetlenül maga az érintett komponens is.

[5] [**SA**: **S**ystem **A**ccess control]

Alkalmazási megjegyzés: A megbízható rendszerek különleges objektumaihoz való hozzáférési jogosultságot az adott objektum tulajdonosa határozza meg, a hozzáférést megkísérelő szubjektum azonosságán, valamint:

a) a szubjektumnak az adott objektumhoz biztosított hozzáférési jogosultsága, vagy
b) a szubjektum általános privilégiumai alapján.

SA1 Rendszer-hozzáférés ellenőrzés

[SA1.1]
A megbízható rendszereknek biztosítaniuk kell annak lehetőségét, hogy ellenőrizzék és korlátozzák az azonosított egyének hozzáférését azokhoz a rendszer-, illetve felhasználói objektumokhoz, melyeket birtokolnak, vagy melyekért felelősséggel tartoznak.

[SA1.2]
A megbízható rendszereknek hozzáférés védelmet kell biztosítaniuk az érzékeny maradvány információk számára.

Alkalmazási megjegyzés: Maradvány információ minden olyan információ, melyet a megbízható rendszer logikailag ugyan törölt vagy felszabadított, mégis megmaradt a rendszerben, s elvileg jogosulatlanul hozzáférhető maradt.

Kulcskezelés[6]

Alkalmazási megjegyzés: Egy megbízható rendszer kriptográfiai kulcsokat használhat a sértetlenség-, a bizalmasság- és a hitelesítés-funkciók biztosítására, saját alrendszereiben vagy alrendszerek között. A megbízható rendszerekben a kulcs jogosulatlan használata, felfedése, módosítása vagy helyettesítése a biztonság elvesztését eredményezné. Alapvető fontosságú, hogy a magán és/vagy titkos kulcsok egész életciklusuk során biztonságosan legyenek kezelve.

Alkalmazási megjegyzés: A megbízható rendszerek kulcsait különböző veszélyek fenyegetik, attól függően, hogy hol és hogyan kerülnek felhasználásra. Emiatt fontos, hogy a kulcsokat kockázati profiljuk szerint kategorizálják. Jelen követelményrendszer szerint a kulcsok az alábbi kategóriákba sorolhatók:

1. **Minősített aláíró kulcsok** - Az archivált elektronikus aláírások érvényességének folyamatos karbantartására használt **érvényesítő aláíró kulcsok (**amelyekkel az érvényességi láncokat írják alá), valamint a különböző **igazolásokat aláíró kulcsok.**
2. A különböző **visszaigazolásokat aláíró kulcsok,** valamint az archivált adatok titkosítása esetén a **titkosításhoz/dekódoláshoz szükséges kulcsok.**
3. **Infrastrukturális kulcsok -** a megbízható rendszerek által az alábbi folyamatokhoz használt kulcsok: kulcs-egyeztetés, alrendszer hitelesítés, napló aláírás, tárolt vagy továbbított adatok titkosítása. A rövid távú munkaszakasz kulcsokat nem tekintjük infrastrukturális kulcsoknak.
4. **Rendszervezérlési kulcsok** - személyek által a megbízható rendszer használatára vagy kezelésére használt kulcsok, melyek hitelesítési-, aláírási- vagy bizalmassági szolgáltatásokat biztosítanak a rendszerrel kölcsönhatásba kerülő személyek számára.

[6] [**KM**: **K**ey **M**anagement]

Alkalmazási megjegyzés: A különböző aláíró kulcsok jellegükből adódóan aszimmetrikusak. Az archivált adatok titkosításához/dekódolásához szükséges kulcsok, valamint az infrastrukturális és rendszervezérlési kulcsok egyaránt lehetnek szimmetrikusak vagy aszimmetrikusak.

Alkalmazási megjegyzés: A kulcskezeléssel kapcsolatban az alábbi fogalmakat az alábbi értelemben használjuk:

Kulcselőállítás: A kulcsok generálása, létrehozása.

Kulcselosztás: Az egyes kulcsok eljuttatása a szükséges szereplőkhöz.

Kulcshasználat: Az előállított kulcsok használatának ellenőrzése a kriptográfiai szolgáltatásokat biztosító kriptográfiai algoritmusokban.

Kulcscsere: A kulcscsere lehet:

1. tervezett - amikor egy kulcsot újonnan előállított kulccsal cserélnek fel, mivel az elérte használati idejének végét (ahogy azt a biztonsági szabályzat meghatározza),
2. nem-tervezett – amikor egy újonnan előállított kulccsal cserélnek le egy kulcsot, annak kompromittálódása esetén.

Kulcs megsemmisítése: Amikor egy kulcs kompromittálódik vagy eléri használati idejének végét, megsemmisítendő az esetleges újbóli felhasználás megakadályozása érdekében.

Kulcs tárolása, mentése és helyreállítása: A kulcs előállítását követően a kulcsok biztonságos környezetben tárolhatók, és a működési követelmények kielégítése érdekében másolat vagy mentés készülhet róluk. Szükség lehet ezen elmentett kulcsok helyreállítására, ha például a meglévő kulcs véletlenül megsemmisül.

Kulcs archiválása: Egy kulcs használati idejének végén archiválható, hogy esetleg később (nem meghatározott idő múlva) újra használatba vehető legyen. Ez különösen a digitális aláírás ellenőrzésére szolgáló nyilvános kulcsokra vonatkozik, de nem zárható ki más típusú kulcsok archiválása sem.

KM1 Kulcselőállítás

[KM1.1]
A minősített aláíró kulcsokat (érvényesítő aláíró és igazolásokat aláíró kulcsokat) biztonságos aláírás-létrehozó eszközben (BALE) kell előállítani és tárolni.

Alkalmazási megjegyzés: A minősített aláíró kulcsok előállítását végezheti egy hitelesítés-szolgáltató is, amelytől az archiválási szolgáltató beszerzi a BALE-ket. Ilyen esetekben a [KM1.1] és [KM1.3] követelmények nem vonatkoznak az archiválási szolgáltató megbízható rendszerére.

[KM1.2]
A visszaigazolásokat aláíró kulcsokat, az archivált adatok titkosításához/dekódoláshoz szükséges kulcsokat, valamint az infrastrukturális és rendszervezérlési kulcsokat hardver kriptográfiai eszközben kell előállítani.

Alkalmazási megjegyzés: A [KM1.2]-ben említett kulcsok előállítását végezheti egy hitelesítés-szolgáltató, melytől az archiválási szolgáltató beszerzi e kulcsokat. Ilyen esetekben a [KM1.2] és [KM1.3] követelmények nem vonatkoznak az archiválási szolgáltató megbízható rendszerére.

[KM1.3]
Minden kulcs előállításnak meg kell felelnie egy mértékadó dokumentumban meghatározott kriptográfiai követelményeknek.

Alkalmazási megjegyzés: Mértékadó dokumentumra példák a nemzetközi szabványok.

KM2 Kulcselosztás

[KM2.1]
A magán és titkos kulcsokat nem szabad nyílt formában elosztani.

Alkalmazási megjegyzés: Nem számít nyílt formában történő elosztásnak az a módszer, amikor nyílt formában, de hozzáférés védelemmel ellátott hardver kriptográfiai eszközben tárolva történik a kulcsok elosztása (átadása).

KM3 Kulcshasználat

[KM3.1]
Hozzáférés ellenőrzést kell alkalmazni minden olyan eszközhöz, melyet érvényesítő aláíró, igazolásokat aláíró, visszaigazolásokat aláíró, az archivált adatok titkosításához /dekódoláshoz szükséges, infrastrukturális, valamint rendszervezérlési kulcsokhoz használnak.

[KM3.2]
A [KM3.1] alatt említett kulcsok jogosult használata csak az adott kulcs működtetési életciklusán belül történhet (a biztonsági szabályzat által meghatározott módon).

[KM3.3]
Mielőtt a [KM3.1] alatt említett kulcsokat használnák, meg kell győződni arról, hogy az ezen kulcsokhoz kapcsolódó tanúsítványok érvényesek.

Alkalmazási megjegyzés: Ajánlott, hogy a különböző funkciókhoz különböző infrastrukturális kulcsok tartozzanak. Ez csökkenti egy kulcs kompromittálódásának kihatásait.

KM4 Kulcscsere

[KM4.1]
Az érvényesítő aláíró, igazolásokat aláíró, visszaigazolásokat aláíró, az archivált adatok titkosításához/dekódoláshoz szükséges, valamint az infrastrukturális és rendszervezérlési kulcsokat szabályos időközönként (pl. évente) cserélni kell.
Amennyiben a megbízható rendszerekben használt bármelyik algoritmust alkalmatlanná váltnak nyilvánítanak, vagy alkalmazása a rendelkezésre álló információk szerint már nem biztonságos (amit az NHH egy újabb, az elektronikus aláírásokkal kapcsolatos szolgáltatás nyújtás során alkalmazható biztonságos kriptográfiai algoritmusokat és paramétereiket meghatározó határozatában publikál), akkor haladéktalanul le kell cserélni az ezen algoritmuson alapuló kulcsokat.

[KM4.2]
A kulcscserét biztonságosan kell végrehajtani.

Alkalmazási megjegyzés: A kulcscserét on-line vagy out-of-band módon lehet végrehajtani. Az out-of-band mód az informatikai rendszeren kívüli megoldást (pl. különböző szervezési, ügyrendi intézkedések alkalmazását) jelenti.

KM5 Kulcs megsemmisítése

[KM5.1]
Amikor az érvényesítő aláíró, igazolásokat aláíró, visszaigazolásokat aláíró, valamint az archivált adatok titkosításához/dekódoláshoz szükséges kulcsok elérik élettartamuk végét, oly módon kell megsemmisíteni őket, hogy többé ne legyenek visszanyerhetők.

[KM5.2]
Amikor olyan rendszereket készülnek kivonni a szolgáltatásokból, melyeket titkos/magán kulcsok előállítására, használatára, vagy tárolására használtak, kulcsaikat meg kell semmisíteni.

[KM5.3]
A megbízható rendszereknek rendelkezniük kell azzal a képességgel, hogy visszaállíthatatlanul megsemmisítsék a bennük tárolt titkos/magán kulcsokat.

Alkalmazási megjegyzés: BALE alkalmazása esetén (melyek egy hitelesítés-szolgáltatótól vásárolt termékek) szervezeti intézkedésekkel (megsemmisítés, HSZ-nek visszaadás, stb.) is biztosítható, hogy a BALE eszközökben ne maradjon aktivizálható lejárt érvényességű magánkulcs.

[KM5.4]
A szoftveres kulcs megsemmisítésnek biztonságos törlési folyamatokat kell alkalmazniuk, melyek ténylegesen felülírják a kulcsokat.

Alkalmazási megjegyzés: Példák ilyen módszerekre: többszörös felülírás, mágneses tárolóeszköz többszöri átmágnesezése, a tárolóeszköz fizikai megsemmisítése.

KM6 Kulcs tárolása, mentése és helyreállítása

[KM6.1]
Minden magán/titkos kulcsot biztonságosan kell tárolni.

[KM6.2]
A minősített aláíró kulcsokat (érvényesítő aláíró és igazolás aláíró kulcsot) egy biztonságos aláírás-létrehozó eszközben (BALE) kell tárolni.

[KM6.3]
Amennyiben egy hardver kriptográfiai eszközben lévő bármilyen kulcs exportálására kerül sor, akkor az eszköznek meg kell védenie a kulcs bizalmasságát, mielőtt az eszközön kívül tárolásra kerülne. Bármely más érzékeny kulcsadat tárolása is tilos védetlen állapotban.

Alkalmazási megjegyzés: Amennyiben a magán/titkos kulcsot titkosítással védik, akkor ennek a titkosításnak meg kell felelnie egy mértékadó dokumentumban meghatározott követelményeknek.

[KM6.4]
A megbízható rendszereknek nem szabad olyan funkciókat tartalmazniuk, amelyek lehetővé teszik az érvényesítő aláíró, igazolásokat aláíró, visszaigazolásokat aláíró magánkulcsok mentését vagy letétbe helyezését.

[KM6.5]
A megbízható rendszereknek biztosítaniuk kell, hogy az infrastrukturális és rendszervezérlési kulcsok mentése és helyreállítása csak jogosult személy (pl. biztonsági tisztviselő) által hajtható végre.

[KM6.6] – csak az „archivált adat titkosított formában való tárolása a szolgáltatónál” kiegészítő szolgáltatás nyújtása esetén
A megbízható rendszereknek biztosítaniuk kell, hogy az archivált adatok dekódoláshoz szükséges magánkulcsok mentése és helyreállítása csak kettős személyi ellenőrzés mellett valósulhasson meg.

KM7 Kulcs archiválása

[KM7.1]
A megbízható rendszereknek nem szabad olyan funkciókat tartalmazniuk, amelyek lehetővé teszik az érvényesítő aláíró, igazolásokat aláíró és visszaigazolásokat aláíró magánkulcsok archiválását.

Naplózás[7]

Alkalmazási megjegyzés: Minden szolgáltatáshoz további naplózási követelmények tartoznak, melyeket az egyes szolgáltatásoknál külön-külön határozunk meg (lásd IN6, LA7 ésDS4 követelmények).

AA1 Napló adatok generálása

[AA1.1]
A következő események naplózása feltétlenül szükséges:
- a megbízható rendszerek környezetében bekövetkező, illetve a kulcsok kezelésével kapcsolatos jelentősebb események,
- a naplózási funkció elindítása és leállítása,
- a naplózási paraméterek megváltoztatása,
- a naplózás tárolási hibája miatt végzett tevékenységek.

A fentieken kívül javasolt a megbízható rendszerhez való minden hozzáférési kísérlet naplózása.

AA2 A napló adatok garantált rendelkezésre állása

[AA2.1]
A rendszernek karban kell tartania a naplózási adatokat és garantálnia kell ezen adatok számára a szükséges tárolóhelyet.

[AA2.2]
A naplóbejegyzéseket nem szabad törölni vagy felülírni.

AA3 Naplózási paraméterek

[AA3.1]
Minden naplóbeli rekordnak (beleértve a szolgáltatás specifikus naplózást is) tartalmaznia kell a következő paramétereket:
- az esemény dátuma és időpontja,
- az esemény típusa,
- a tevékenységért felelős egyén azonosítója,
- a naplózott esemény sikeressége vagy sikertelensége.

[7] [**AA**: **A**ccounting and **A**uditing]

AA4 A napló választható áttekintése

[AA4.1]
A megbízható rendszereknek gondoskodniuk kell a naplóbeli események közötti keresési lehetőségről az esemény időpontja, típusa és/vagy a felhasználó személye szerint.

[AA4.2]
A napló rekordokat ember számára értelmezhetően kell megjeleníteni.

AA5 Korlátozott naplómegtekintés

[AA5.1]
A megbízható rendszereknek a naplózási rekordok olvasását minden felhasználónak meg kell tiltaniuk, azon felhasználók kivételével, akik kifejezetten megkapták az olvasási jogosultságot (tipikusan a rendszervizsgáló munkakörbe tartozók).

[AA5.2]
Meg kell akadályozni a naplózási rekordok módosítását és törlését.

AA6 Riasztás generálása

[AA6.1]
A megbízható rendszereknek riasztást kell generálniuk a biztonság potenciális megsértésének észlelése esetén.

Alkalmazási megjegyzés: Riasztásra egy egyszerű példa a biztonsági tisztviselő értesítése e-mail-en, vagy riasztásokat generáló alkalmas figyelőprogramok alkalmazása.

AA7 A napló adatok sértetlenségének garantálása

[AA7.1] - csak nem minősített szolgáltatásra
A megbízható rendszereknek biztosítaniuk kell a napló adatok sértetlenségét.

[AA7.1] - csak minősített szolgáltatásra
A megbízható rendszereknek biztosítaniuk kell a napló adatok sértetlenségét.
Ennek elérése érdekében a megbízható rendszereknek digitális aláírást kell biztosítaniuk minden naplóbejegyzésre, amely vagy a napló egészére, vagy az aktuális bejegyzés és az előzők kriptográfiai eredményére vonatkozóan kerül kiszámításra.
A megbízható rendszereknek funkciót kell a napló adatok sértetlenségének ellenőrzésére.

AA8 A napló időbejegyzéseinek garantálása

[AA8.1]
Megbízható időforrást kell alkalmazni a naplózott esemény idejének jelzésére (ahogyan azt az SO3 követelmények előírják).

Archiválás[8]

Alkalmazási megjegyzés: Az alábbi követelmények az archiválási szolgáltató saját üzemmenetéből származó adataira vonatkoznak. Az archiválási szolgáltatásokra vonatkozó követelményeket a 4.2.2 alfejezet határozza meg.

[8] [**AR**: **Ar**chiving]

AR1 Archív adatok generálása

[AR1.1]
A megbízható rendszereknek képesnek kell lenniük archívum létrehozására.

[AR1.2]
Legalább az alábbiakat archiválni kell:
- minden naplóállomány.

[AR1.3]
Az archívum minden bejegyzésének tartalmaznia kell az esemény megtörténtének időpontját.

[AR1.4]
Az archívum nem tartalmazhat védetlen formában kritikus biztonsági paramétereket.

AR2 Szelektálható keresés

[AR2.1]
A rendszernek az archívumra vonatkozóan keresési lehetőséget kell biztosítania az események típusa szerint.

AR3 Az archivált adatok sértetlensége

[AR3.1]
Az archívum minden egyes bejegyzését védeni kell a módosítástól és a jogosulatlan törléstől.

Mentés és helyreállítás[9]

Alkalmazási megjegyzés: Az alábbi részben a mentés és helyreállítás csak azokra a rendszerre és szubjektumokra vonatkozó információkra és egyéb adatokra vonatkozik, melyek a rendszer hibát vagy katasztrófát követő helyreállításhoz szükségesek. Nem vonatkozik a kulcsok mentésére és helyreállítására, az ezekre vonatkozó követelmények külön kerültek meghatározásra (KM6).

BK1 Mentés generálása

[BK1.1]
A megbízható rendszereknek rendelkezniük kell mentési funkcióval.

[BK1.2]
A rendszer mentésében tárolt adatoknak elegendőnek kell lenniük a rendszer mentési időpontjában érvényes állapotának visszaállítására, az archivált adatokhoz tartozó adatbázist is beleértve.

[BK1.3]
Egy megfelelő jogokkal felruházott munkakört betöltő felhasználónak (a rendszerüzemeltetőnek vagy a biztonsági tisztviselőnek) szükség esetén képesnek kell lennie a mentési funkció meghívására.

Alkalmazási megjegyzés: A mentési funkció tipikusan automatikus folyamat.

[9] [**BK**: **B**ac**k**up and Recovery]

BK2 A mentési információ sértetlensége és bizalmassága

[BK2.1] - csak nem minősített szolgáltatásra
A mentést védeni kell a módosítás és a jogosulatlan törlés, valamint a hozzáférhetetlenné válás ellen.

[BK2.1] - csak minősített szolgáltatásra

A mentést digitális aláírások alkalmazásával védeni kell a módosítás ellen, valamint biztosítani kell, hogy a mentésben ne lehessen jogosulatlanul törölni, illetve ne lehessen a mentést hozzáférhetetlenné tenni.

[BK2.2]
A kritikus biztonsági paraméterek és más bizalmas információk csak titkosított formában tárolhatók. A titkosításnak meg kell felelnie egy mértékadó dokumentumban meghatározott kriptográfiai követelményeknek.

Alkalmazási megjegyzés: Mértékadó dokumentumra példák a nemzetközi szabványok.

[BK2.3]
Megfelelő eljárásokat kell kialakítani és alkalmazni annak biztosítására, hogy a mentett adatok a rendszer és a benne tárolt adatok mentéskori állapotát hitelesen rögzítsék.

BK3 Helyreállítás

[BK3.1]
A megbízható rendszereknek helyreállítási funkciót is biztosítaniuk kell, amely képes egy mentésből helyreállítani a rendszert.

[BK3.2]
Egy megfelelő jogokkal felruházott munkakört betöltő felhasználónak (a rendszerüzemeltetőnek vagy a biztonsági tisztviselőnek) szükség esetén képesnek kell lennie a helyreállítási funkció meghívására.

[BK3.3] - csak minősített szolgáltatásra
Megfelelő eljárásokat kell kialakítani és lefolytatni abból a célból, hogy a helyreállítást követően megállapítható legyen a helyreállított adatok hitelessége és ezt a későbbiekben bizonyítani lehessen.

Általános követelmények[10]

GE1 A szolgáltatások által létrehozott üzenetek védelme

[GE1.1]
Bármely szolgáltatás által létrehozott külső üzenetre biztosítani kell az alábbiakat:

- Az üzenet védve legyen az adott szolgáltatás infrastrukturális kulcsainak felhasználásával (pl. üzenet hitelesítési kódok használatával, digitális aláírással).
- Az üzenet tartalmazzon egy időpontot, amely azt jelöli, amikor a küldő létrehozta az üzenetet.
- Az üzenet biztosítson visszajátszáson alapuló támadás elleni védelmet (pl. egyszer használatos véletlen adatok felhasználásával).

Alkalmazási megjegyzés: Külső üzenet: olyan üzenet, amely elhagyja a megbízható rendszer határát.

[10] [**GE**: **Ge**neral]

GE2 Az archiválás szolgáltatást igénybe vevők regisztrációja

Alkalmazási megjegyzés: Benyújtásra vonatkozó kérelem: az archiválási szolgáltatások igénybevételének előfeltétele a benyújtó és hozzáférő szerepköröket betöltő igénybe vevők azonosítása, a kapcsolódó szolgáltatási szabályzat által meghatározott követelményeknek megfelelően.

Alkalmazási megjegyzés: A regisztrált igénybe vevők adatainak kezelése: a regisztráció szolgáltatás jellegéből adódóan az igénybe vevőkre (benyújtók és hozzáférők) vonatkozó adatokat kezel. Az ilyen adatokra többféle adatvédelmi követelmény is vonatkozhat.

[GE2.1]
Amennyiben ezt jogszabály nem tiltja, s a szolgáltatási szabályzat is lehetővé teszi, az archiválási szolgáltatás oly módon is nyújtható, hogy az igénybe vevő nem bocsátja a szolgáltató rendelkezésére személyazonosító adatait (pl álnevet használ).

[GE2.2]
Ha a regisztrált igénybe vevők adatai érzékeny információt is tartalmaznak az igénybe vevőkre vonatkozóan, akkor ezek védelmét biztosítani kell. A megbízható rendszereknek biztosítani kell ezt a védelmi funkcionalitást.

[GE2.3]
A regisztrált benyújtó rendelkezhet arról, hogy az általa archiválásra benyújtott adatokhoz ki férhet hozzá (hozzáférőként), milyen joggal, milyen azonosítással és milyen azonosítóval. A megbízható rendszereknek támogatnia kell ezt a jogosultság kezelési funkcionalitást.

[GE2.4]
A regisztrálás során rögzíteni kell a regisztrált igénybe vevővel való jövőbeli kapcsolattartáshoz szükséges információkat. A megbízható rendszereknek képesnek kell lenniük ezen információk használatára.

4.2 Biztonsági követelmények a megbízható rendszer szolgáltatásaira

4.2.1 A befogadással kapcsolatos funkciók követelményei

Befogadás[11]

IN1 Archiválásra benyújtott információk fogadása

[IN1.1]
A rendszernek fogadás funkciót (interfészt) kell biztosítania, amely képes a benyújtó által elektronikus archiválásra benyújtott információk (adat, adatra vonatkozó elektronikus aláírás, adatra vonatkozó kiegészítő információk), valamint korábban archiválásra benyújtott információk törlésére vonatkozó kérés (törlési kérés, adat azonosító) fogadására.

[IN1.2]
A fogadás funkció csak az IA1, IA2 és IA3 követelményeknek megfelelő sikeres azonosítás és hitelesítés után vehet át egy benyújtótól információkat.

[11] **In**gest

IN2 Archiválásra benyújtott információk ellenőrzése

[IN2.1]
A megbízható rendszernek ellenőrzés funkciót kell biztosítania, amely képes a benyújtó által szolgáltatott információk formai ellenőrzésére az alábbi szempontok szerint:

- a megőrzés leíró információ egyik elemeként a benyújtó meghatározta-e az esetlegesen igényelt kiegészítő szolgáltatások körét,
- az értelmezhetőség kiegészítő szolgáltatás igénylése esetén a benyújtott adat formátumának értelmezhetőségét támogatja-e az archiválási szolgáltató,
- a letagadhatatlanság szolgáltatás biztosítása érdekében a megőrzés leíró információ egyik elemeként a benyújtó szolgáltatott-e olyan elektronikus aláírást, melynek formátumát támogatja az archiválási szolgáltató,
- a megőrzés leíró információ egyik elemeként a benyújtó meghatározta-e az aláíráshoz alkalmazott lenyomatoló függvényt és az aláíró algoritmust,
- a megőrzés leíró információ egyik elemeként a benyújtó meghatározta-e az alkalmazandó archiválási rend azonosítóját.

Alkalmazási megjegyzés: [IN2.1] alapján a megbízható rendszer képes eldönteni, hogy bitfolyam, lenyomat vagy dokumentum formátumú adatot kapott-e archiválásra, az adathoz tartozik-e (fokozott biztonságú vagy minősített) elektronikus aláírás, illetve az elektronikus aláíráshoz milyen hash függvényt és aláíró algoritmust alkalmaztak.

Alkalmazási megjegyzés: Előfordulhat, hogy a benyújtott adat nem egy állomány, hanem egy „csomag”, vagyis több önálló dokumentum, melyek formátuma is eltérő lehet (pl. egy WORD dokumentum, egy PDF és egy EXCEL fájl). Ilyen esetben értelmezhetőségi szolgáltatást csak akkor ajánlott vállalni, ha minden dokumentum formátum elfogadható.

[IN2.2]
Az ellenőrzés funkciónak képesnek kell lennie a benyújtó által szolgáltatott, s az [IN2.1] szerinti formai ellenőrzésen túljutott adatra elektronikus aláírás kezdeti ellenőrzésére az alábbi szempontok szerint:

- az elektronikus aláírás ellenőrzésére szolgáló tanúsítványban megjelölt hitelesítési rendet, és a dokumentumon szereplő időbélyeg kibocsátásának alapjául szolgáló időbélyegzési rendet támogatja-e az archiválási szolgáltató,
- az elektronikus aláíráshoz használt aláíró és lenyomatképző algoritmusok a benyújtás időpontjában a Hatóság határozata szerinti, elfogadott kriptográfiai algoritmusok-e,
- az elektronikus aláírás kezdeti ellenőrzése sikeres-e.

A kezdeti ellenőrzés során, amennyiben létezik megbízható információ azon időpontról, amikor az elektronikus aláírás már létezett, akkor ezt kell az ellenőrzés alapjául tekinteni.

[IN2.3]
Az ellenőrzés funkciónak képesnek kell lennie a benyújtó által szolgáltatott, s az [IN2.2] szerinti kezdeti ellenőrzésen sikeresen túljutott elektronikus aláírás kiegészítésére, az elektronikus aláírás hosszú távú utólagos ellenőrizhetőségéhez szükséges érvényesítő adatok begyűjtésére.

[IN2.4]
Az ellenőrzés funkciónak képesnek kell lennie a benyújtó által szolgáltatott, s az [IN2.3] végrehajtásával begyűjtött érvényesítő adatokkal kiegészített elektronikus aláírás utólagos ellenőrzésére az alábbi szempontok szerint:

- az elektronikus aláírás hosszú távú, utólagos ellenőrizhetőségéhez szükséges valamennyi érvényesítő adat rendelkezésre áll-e,
- a teljes körű érvényesítő adatok alapján az elektronikus aláírás utólagos ellenőrzése sikeres-e.

Alkalmazási megjegyzés: Előfordulhat, hogy a benyújtott adatokhoz több elektronikus aláírás is tartozik. Letagadhatatlansági szolgáltatást csak akkor ajánlott vállalni, ha minden aláírás formai és tartalmi ellenőrzése sikeres.

[IN2.5]
A fogadás funkciónak az [IN2.4] szerinti utólagos ellenőrzés első sikeres végrehajtásakor az érvényesítő adatokkal kiegészített elektronikus aláírásra (azaz az aktuális érvényességi láncra) egy minősített szolgáltató által kibocsátott időbélyegzőt kell elhelyeznie.

[IN2.6] – csak az értelmezhetőség kiegészítő szolgáltatás igénylése esetén
A fogadás funkciónak az [IN2.1] szerinti formai ellenőrzés végrehajtásakor:

- jeleznie kell, ha az értelmezésre kerülő dokumentum olyan rejtett vagy aktív kódot tartalmaz, ami a dokumentum megjelenítésében változást okozhat,
- meg kell határoznia az értelmezhetőség biztosítására átadott dokumentum formátumát, s amennyiben a formátumot nem támogatja, el kell utasítani az értelmezhetőség vállalását.

IN3 A megőrzési időtartam kezelése, befejezése

[IN3.1]
A fogadás funkciónak képesnek kell lennie annak biztosítására, hogy egy (az IA1, IA2 és IA3 követelményeknek megfelelően) sikeresen azonosított és hitelesített benyújtó, az általa korábban benyújtott információkhoz tartozó egyedi azonosító (lásd [IN4.2]) megadása után módosíthassa az adott információk megőrzési időtartamát (befejezhesse, vagy a szolgáltatási szabályzatban meghatározott támogatott módosítási lehetőségek közül válasszon).

IN4 Archiválással kapcsolatosan benyújtott információk visszaigazolása

[IN4.1]
A fogadás funkciónak képesnek kell lennie visszajelezni a benyújtó felé az alábbiakat:

- az [IN2.1] szerinti formai ellenőrzés sikere/sikertelensége (formai befogadás)
- az [IN2.1] szerinti formai ellenőrzés által meghatározott formátum (bitfolyam / lenyomat / dokumentum)
- az [IN2.2] szerinti kezdeti ellenőrzés sikere/sikertelensége (siker esetén előzetes befogadás)
- az [IN2.3] szerinti érvényesítő adat begyűjtés és az [IN2.4] szerinti utólagos ellenőrzés sikere/sikertelensége, valamint ezek sikeressége esetén az [IN2.5] szerinti időbélyegző elhelyezés (végleges befogadás).

Alkalmazási megjegyzés: Az IN4.1 alatti végleges befogadás jelenti csak a benyújtott adatok archiválásra való átvételét. A végleges befogadás hiányában az archiválási szolgáltató különböző hibajelzések mellett visszautasítja a benyújtást.

[IN4.2]
A végleges befogadást visszaigazoló üzenetben az archiválási szolgáltatónak meg kell adnia legalább az alábbiakat:

- egy egyedi azonosítót, mellyel a benyújtó a jövőben az adott, véglegesen befogadott adatra hivatkozhat,
- a benyújtó azonosítóját,
- az archiválás időtartamát,
- az archiválási rend azonosítóját,
- az adatra vállalt kiegészítő szolgáltatást (ha van)
- annak egyértelmű jelzését, hogy a szolgáltatás az eat hatálya alatt álló elektronikus archiválás.

Alkalmazási megjegyzés: [IN4.2] alatt meghatározandó adatok némelyike implicit módon (pl. az archiválási rend azonosítóján keresztül) is megadható.

Alkalmazási megjegyzés: A visszaigazoló üzenetben a benyújtott adatra vonatkozó egyéb információ is megjelenhet (pl. méret, fájlnév).

[IN4.3]
A végleges befogadást visszaigazoló üzenetet a [GE1.1] általános követelmény kielégítésén túl, az archiválási szolgáltatónak fokozott biztonságú elektronikus aláírással és időbélyegzővel kell ellátnia.

[IN4.4]
A fogadás funkciónak képesnek kell lennie visszajelezni a benyújtó [IN3.1] szerinti, megőrzés befejezésre (törlésre) irányuló rendelkezése alapján az [LA6.1] szerinti törlés végrehajtását.

[IN4.5]
A törlést visszaigazoló üzenetben az archiválási szolgáltatónak meg kell adnia a törölt információ egyedi azonosítóját, a törlés időpontját, valamint a törlést kérő benyújtó azonosítóját is.

[IN4.6]
A törlést visszaigazoló üzenetet a [GE1.1] általános követelmény kielégítésén túl, az archiválási szolgáltatónak fokozott biztonságú elektronikus aláírással és időbélyegzővel kell ellátnia.

IN5 A hozzáférési jogosultságok kezelése

[IN5.1]
A fogadás funkciónak képesnek kell lennie annak biztosítására, hogy egy (az IA1, IA2 és IA3 követelményeknek megfelelően) sikeresen azonosított és hitelesített benyújtó az általa korábban benyújtott adathoz tartozó egyedi azonosító (lásd [IN4.2]) megadása után kezelhesse (a szolgáltatási szabályzatban meghatározott módon megadhassa, módosíthassa, illetve visszavonhassa) az archivált adathoz hozzáférők azonosítóját, kezdeti hitelesítő adatait és hozzáférési jogosultságait.

IN6 A befogadás funkciócsoport naplózása

[IN6.1]
A következő, befogadással kapcsolatos események naplózása feltétlenül szükséges:

- minden olyan esemény, amely az archiválásra benyújtott információk fogadásával kapcsolatos,

- minden olyan esemény, amely az archiválásra benyújtott információk ellenőrzésével kapcsolatos,
- minden olyan esemény, amely a megőrzési időtartam módosításával kapcsolatos,
- minden olyan esemény, amely az archiválásra benyújtott információk visszaigazolásával kapcsolatos,
- minden olyan esemény, amely a hozzáférők hozzáférési jogosultságainak módosításával kapcsolatos.

4.2.2 A megőrzéssel kapcsolatos funkciók követelményei

Hosszú távú megőrzés[12]

LA1 Az archivált elektronikus adatok rendelkezésre állásának megőrzése

[LA1.1]
A megbízható rendszernek az archivált adatok rendelkezésre állásának megőrzése érdekében az alábbi funkciókat kell biztosítania:

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

[LA1.2]
A megbízható rendszernek az archivált adatok rendelkezésre állásának megőrzése érdekében az alábbi funkciókat kell biztosítania:

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

LA2 Az archivált elektronikus adatok sértetlenségének megőrzése

[LA2.1]
A megbízható rendszernek az archivált adatok sértetlenségének megőrzése érdekében az alábbi funkciókat kell biztosítania:

- az elsődleges adathordozó olvashatóságának rendszeres időközönkénti ellenőrzése,
- az elsődleges adathordozóról beolvasott archivált adatok sértetlenségének ellenőrzése,
- szükség esetén az elsődleges adathordozó cseréje (frissítés, másolat készítés, újra csomagolás),
- szükség esetén az elsődleges adathordozó tartalmának helyreállítása a másodlagos adathordozón tárolt információ segítségével,
- a tartalék adathordozó olvashatóságának rendszeres időközönkénti ellenőrzése,
- a tartalék adathordozóról beolvasott archivált adatok sértetlenségének ellenőrzése,

[12] **L**ongterm **A**rchiving

- szükség esetén a másodlagos adathordozó cseréje (frissítés, másolat készítés, újra csomagolás),
- szükség esetén a tartalék adathordozó tartalmának helyreállítása az elsődleges adathordozón tárolt információ megismételt duplikálásával.

[LA2.2]
A megbízható rendszernek az archivált adatok sértetlenségének megőrzése érdekében az alábbi funkciókat kell biztosítania:

- adatbázis adminisztrálás,
- adatbázis frissítés fogadás funkció aktivizálásának jogosultság ellenőrzése (lásd [SA1.1] alatti követelmény),
- rendszer mentése (lásd BK1 alatti követelmény),
- rendszer helyreállítása (lásd BK3 alatti követelmény).

LA3 Az archivált elektronikus adatok bizalmasságának megőrzése

[LA3.1]
A megbízható rendszernek az archivált adatok bizalmassága megőrzése érdekében biztosítania kell, hogy az archivált adatokat feladatkörükön túlmenően még a bizalmi munkakört betöltő személyek sem ismerhetik meg külön felhatalmazás nélkül.

[LA3.2] – csak az „archivált adat titkosított formában való tárolásának biztosítása” kiegészítő szolgáltatás nyújtása esetén
A megbízható rendszernek megfelelő kriptográfiai mechanizmusokat kell alkalmaznia az archivált 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.

[LA3.3] – csak az „archivált adat titkosított formában való tárolásának biztosítása” kiegészítő szolgáltatás nyújtása esetén
Az [LA3.2] követelmény teljesítettnek tekinthető, ha a megbízható rendszer által alkalmazott titkosító algoritmusok, kulcsméretek, kulcselőállítási módszerek, kulcskezelési eljárások megbízhatóságát, s a megvalósítás helyességét szakértői vélemény vagy tanúsító szervezet által kiadott tanúsítvány igazolja.

LA4 Az archivált elektronikus adatok hitelességének és letagadhatatlanságának megőrzése

[LA4.1]
A megbízható rendszernek az archivált adatok hitelességének és letagadhatatlanságának megőrzése érdekében az alábbi (elektronikus aláírás megújítás) funkciót kell biztosítania:

- archivált adat érvényességi láncára minősített elektronikus aláírás és minősített szolgáltató által kibocsátott időbélyegző elhelyezése.

Alkalmazási megjegyzés: Ennek a funkciónak (elektronikus aláírás megújítás) a Hatóság határozata szerinti, vagy a szolgáltató saját döntésén alapuló aktivizálásával biztosítható, hogy még az érvényességi lánc érvényességét garantáló kriptográfiai algoritmusok meggyengülése előtt, egy új, megbízható (a Hatóság által elfogadott) kriptográfiai algoritmussal meg legyen hosszabbítva az érvényességi lánc (s ezen keresztül az eredeti elektronikus aláírás) érvényessége.

Alkalmazási megjegyzés: Az [LA4.1] szerinti elektronikus aláírás megújítás egyaránt megvalósítható adat-alapú ([ETSI1] és [ETSI2]) és adatbázis-alapú ([RFCd1], [RFCd2] és [RFCd3]) megközelítéssel. Adat-alapú megközelítés esetén a CAdES-A és a XAdES-A egyaránt alkalmazható, ezek közül (az együttműködés támogatása miatt) a XAdES-A az előnyben részesítendő.

[LA4.2]
Az [LA4.1] alatti elektronikus aláírás megújítás során az aláírás és az időbélyegző létrehozásánál figyelembe kell venni az archivált adat minden korábbi aláírását (az eredeti aláírást vagy aláírásokat, valamint a korábbi megújító aláírásokat) és valamennyi korábban elhelyezett időbélyegzőt is.

Alkalmazási megjegyzés: A korábbi aláírások figyelembe vétele azt jelenti, hogy az újonnan készülő aláírásba bele kell foglalni a megelőző aláírásokat, azaz ezeket is be kell számítani az új aláírás lenyomatába.

[LA4.3]
Ha az archivált adat több, különálló adatobjektumból áll, akkor az elektronikus aláírás megújításnak az összes objektumra egyszerre kell megtörténnie.

LA5 Az archivált elektronikus adatok értelmezhetőségének a fenntartása

[LA5.1] – csak az értelmezhetőség szolgáltatás vállalása esetén
A megbízható rendszernek képesnek kell lennie az alábbiak biztosítására:

- az archivált adat (jelen esetben archivált dokumentum) megjelenítése.

Alkalmazási megjegyzés: A fenti műszaki követelmény teljesíthetősége érdekében az archiválási szolgáltató a szolgáltatási szabályzatában meghatározott formátumokban benyújtott elektronikus adatok megjeleníthetőségének folyamatos fenntartása érdekében a benyújtóval kötött szerződésben, illetve az archiválási szabályzatban meghatározott megőrzési ideig köteles biztosítani az archivált dokumentumok értelmezhetőségét biztosító szoftver- és hardverkörnyezetet.

LA6 Az archivált információk törlése

[LA6.1]
A megbízható rendszernek képesnek kell lennie annak biztosítására, hogy az [IN3.1] szerint fogadott és sikeresen ellenőrzött, megőrzés befejezésre (törlésre) irányuló rendelkezés esetén az archivált adatot, s az ehhez tartozó érvényességi láncot visszaállíthatatlan módon törölje informatikai rendszeréből.

Alkalmazási megjegyzés: Abban az esetben, amikor az archivált adatok bizalmasságát az archiválási szolgáltató hozzáférés-védelmi mechanizmusokon keresztül biztosítja, az érvényességi lánc törlését az érintett adatok minden egyes példányának és bájtjának fizikai törlésével vagy véletlen adatokkal történő felülírásával lehet megvalósítani, a törlési kérés jogosultságának sikeres ellenőrzését követő 30 napon belül.

Alkalmazási megjegyzés: Abban az esetben, amikor az archivált adatok bizalmasságát az archiválási szolgáltató titkosítással is támogatja, az érvényességi lánc visszaállíthatatlan törlése átmenetileg megvalósítható az adott adathoz tartozó egyedi titkosító kulcs valamennyi példányának megsemmisítésével, melyet a törlési kérés jogosultságának sikeres ellenőrzését követő 30 napon belül kell végrehajtani. Ilyen esetben is szükség van a titkosított érvényességi lánc törlésére (az érintett adatok minden egyes példányának és bájtjának fizikai törlésével vagy véletlen adatokkal történő felülírásával), de ezt elegendő megvalósítani a törlési kérés jogosultságának sikeres ellenőrzését követő egy éven belül.

LA7 A megőrzés funkciócsoport naplózása

[LA7.1]
A következő megőrzéssel kapcsolatos események naplózása feltétlenül szükséges:

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

4.2.3 A kibocsátással kapcsolatos funkciók követelményei

Kibocsátás[13]

DS1 Adat kérések teljesítése

[DS1.1]
A megbízható rendszernek képesnek kell lennie annak biztosítására, hogy egy (az IA1, IA2 és IA3 követelményeknek megfelelően) sikeresen azonosított és hitelesített személy erre irányuló jogosult rendelkezése esetén az aktuális érvényességi láncról, benne az archiválásra átvett elektronikus adatról másolatot készítsen, s ezt a jogosultnak átadja, amennyiben erre az adatra vonatkozóan nincs befogadott törlési kérés (lásd [DS1.2]).

[DS1.2]
A megbízható rendszernek képesnek kell lennie annak biztosítására, hogy az [IN3.1] szerint fogadott és sikeresen ellenőrzött, megőrzés befejezésre (törlésre) irányuló rendelkezés esetén még a [DS1.1] alapján hitelesített személy jogosult kérését is visszautasítsa a törlési rendelkezéssel érintett érvényességi lánc és archivált adat vonatkozásában.

DS2 Igazolás kérések teljesítése

[DS2.1]
A megbízható rendszernek olyan funkciókat kell biztosítania, amelyek (amennyiben nincs erre vonatkozóan befogadott törlési kérés (lásd [DS2.8])) képesek elektronikus úton kiállított igazolások kiadására az alábbi tényekről:

- a megőrzésében lévő elektronikus adaton elhelyezett fokozott biztonságú vagy minősített elektronikus aláírás az igazolás időpontjában érvényes (a letagadhatatlanság igazolása),
- a megőrzésében lévő lenyomathoz kapcsolódó fokozott biztonságú vagy minősített elektronikus aláírás az igazolás időpontjában érvényes (a letagadhatatlanság korlátozott igazolása),
- a megőrzésében lévő, az érvényességi lánc részét képező elektronikus adat tartalma megegyezik a hozzáférő által bemutatott elektronikus adattal (a sértetlenség igazolása),
- a megőrzésében lévő, az érvényességi lánc részét képező lenyomat megegyezik a hozzáférő által bemutatott elektronikus adat lenyomatával (a sértetlenség korlátozott

[13] **Dis**semination

igazolása),
- a megőrzésében lévő, az érvényességi lánc részét képező elektronikus adaton, amelynek tartalma megegyezik a hozzáférő által bemutatott elektronikus adattal, meghatározott személy érvényes elektronikus aláírást helyezett el (az eredet hitelességének igazolása),
- az archivált adatok formátumától függően az alábbi típusú igazolások állíthatók ki:
  - Bitfolyam esetén: a letagadhatatlanság igazolása, az eredet hitelességének igazolása, a sértetlenség igazolása,
  - Lenyomat esetén: a letagadhatatlanság korlátozott igazolása, a sértetlenség korlátozott igazolása
  - Dokumentum esetén: a letagadhatatlanság igazolása, az eredet hitelességének igazolása, a sértetlenség igazolása,
- a lenyomat archiválása esetén értelmezhető igazolás típusok a hash függvény kriptográfiai meggyengülése esetén már nem adhatók ki.

Alkalmazási megjegyzés: A [DS2.1] által meghatározott eredet hitelesség igazolásban szereplő „meghatározott személyt” az archiválási szolgáltató is meghatározhatja, amennyiben a hozzáférő ezt kérésében nem határozta meg.

[DS2.2]
A megbízható rendszernek a [DS2.1] alatt meghatározott igazolások kiállíthatóságának eldöntése érdekében képesnek kell lennie az alábbiak bizonyítására:
- egy adott aláíró kulccsal és adott aláíró algoritmussal létrehozott aláírás érték már létezett az aláíró algoritmus biztonsági meggyengülése előtt,
- egy adott hash függvénnyel, adott adatokra számolt lenyomat érték már létezett a hash függvény biztonsági meggyengülése előtt.

[DS2.3]
A megbízható rendszernek képesnek kell lennie a [DS2.1] alatt meghatározott igazolások elkészítésére az igazolás kérésekor megadott alábbi információk alapján:
- a letagadhatatlanság igazolása esetén:
  - a kért igazolás típusa (letagadhatatlanság),
  - az archivált elektronikus adat (végleges befogadásakor meghatározott) egyedi azonosítója,
  - amennyiben az eredeti adathoz több elektronikus aláírás is tartozik, az igazolás kérés által érintett aláíró azonosítója,
- a sértetlenség igazolása esetén:
  - a kért igazolás típusa (sértetlenség),
  - az archivált elektronikus adat egyedi azonosítója,
  - az összehasonlításként bemutatott (beküldött) elektronikus adat,
- az eredet hitelességének igazolása esetén:
  - a kért igazolás típusa (eredet hitelesség),
  - az archivált elektronikus adat egyedi azonosítója,
  - az összehasonlításként bemutatott (beküldött) elektronikus adat,
  - az igazolás kérés által érintett aláíró azonosítója.

[DS2.4]
A megbízható rendszernek a [DS2.1] alatt meghatározott elektronikus úton kiállított igazolásokban el kell helyeznie legalább az alábbi információkat:
- a letagadhatatlanság igazolása esetén:
  - az igazolás típusa (letagadhatatlanság),

  - az archivált elektronikus adat egyedi azonosítója,
  - az archivált elektronikus adat lenyomata,
  - amennyiben az eredeti adathoz több elektronikus aláírás is tartozik, az igazolás által érintett aláíró azonosítója,
  - az igazolás eredménye (érvényes/érvénytelen),
  - az igazolás kiállításának időpontja,
- a sértetlenség igazolása esetén:
  - az igazolás típusa (sértetlenség),
  - az archivált elektronikus adat egyedi azonosítója,
  - az archivált elektronikus adat lenyomata,
  - az igazolás eredménye (érvényes/érvénytelen),
  - az igazolás kiállításának időpontja,
- az eredet hitelességének igazolása esetén:
  - az igazolás típusa (eredet hitelesség),
  - az archivált elektronikus adat egyedi azonosítója,
  - az archivált elektronikus adat lenyomata,
  - az igazolás által érintett aláíró azonosítója,
  - az igazolás eredménye (érvényes/érvénytelen),
  - az igazolás kiállításának időpontja.

[DS2.5]
Az elektronikus úton kiállított igazolásokat az archiválási szolgáltatónak minősített aláírással, valamint minősített szolgáltató által kibocsátott időbélyegzővel kell ellátnia. Ugyanakkor egy igazolás egyszerre több dokumentumra is vonatkozhat.

[DS2.6]
A [DS2.1] - [DS2.5] szerinti követelmények biztonsági szempontból teljesítettnek tekinthetők, amennyiben az elektronikus úton kiállított igazolások létrehozására (az igazolás alapját képező érvényességi lánc ellenőrzésére, valamint az igazolás aláírására) olyan elektronikus aláírási terméket (szoftvert) használ a megbízható rendszer, amely rendelkezik a Hatóság által nyilvántartásba vett, tanúsításra jogosult szervezetek által erre a célra kiadott igazolással.

[DS2.7]
A [DS2.1] - [DS2.5] szerinti követelmények együttműködési szempontból teljesítettnek tekinthetők, amennyiben az elektronikus úton kiállított igazolások létrehozására (az igazolás aláírásának formátuma szempontjából) olyan elektronikus aláírási terméket (szoftvert) használ a megbízható rendszer, amely rendelkezik a MELASZ-ready együttműködési képességre vonatkozó igazolással.

Alkalmazási megjegyzés: A [DS2.1] - [DS2.5] szerinti, elektronikus úton kiállított igazolások minősített elektronikus aláírásával a szolgáltató felelősséget vállal a benne foglaltakért. A [DS2.6] és [DS2.7] követelmények pedig azt biztosítják, hogy az igazolásokba a valóságnak megfelelő adatok kerülnek, s az igazolásokat széles körben értelmezni (ellenőrizni) tudják. Az igazolásoknak nem célja a hosszú távú érvényesség garantálása, a kiállítás időpontja utáni helyzetre nem lehet következtetni belőle. Szükség esetén újabb igazolások szerezhetők be.

[DS2.8]
A megbízható rendszernek képesnek kell lennie annak biztosítására, hogy az [IN3.1] szerint fogadott és sikeresen ellenőrzött, megőrzés befejezésre (törlésre) irányuló rendelkezés esetén még a [DS2.1] alapján hitelesített, elektronikus úton kiállított

igazolások kiadására irányuló kéréseket is visszautasítsa a törlési rendelkezéssel érintett érvényességi lánc és archivált adat vonatkozásában.

DS3 Szolgáltató-váltás előkészítése

[DS3.1]
A megbízható rendszernek olyan funkciókat kell biztosítania, amelyek képesek az általa archivált adatok átadására más archiválási szolgáltató részére, a következők biztosításával:

- az archiválási szolgáltatónak eredetileg benyújtott elektronikus adat,
- az archiválási szolgáltatónak eredetileg benyújtott, a fenti elektronikus adatra vonatkozó elektronikus aláírás(ok),
- az [DS2.1] alatt meghatározott elektronikus úton kiállított igazolás arról, hogy a fenti (eddig megőrzésében lévő) elektronikus adaton elhelyezett fokozott biztonságú vagy minősített elektronikus aláírás az igazolás időpontjában érvényes.

Alkalmazási megjegyzés: A fenti követelménynek való megfelelés lehetővé teszi, hogy egy másik archiválási szolgáltató anélkül tudja átvenni az archivált adatokat, hogy az érvényességi lánc építésben, (adat-alapú vagy adatbázis-alapú megközelítésű) elektronikus aláírás megújításban és egyéb megvalósítási részletekben (adatbázis felépítés és kezelés, adathordozón történő tárolás és ennek kezelése, stb.) teljes interoperabilitást biztosítson. Az igazolás (és ennek készítésének [DS2.6] alatti tanúsítása) garantálja, hogy az átvétel időpontjában az archivált adat sértetlen, s aláírása is érvényes. Ettől kezdve az új archiválási szolgáltatónak csak az átvett adatokra (eredeti adat, eredeti aláírás és az átadó archiválási szolgáltató aláírt igazolása) kell érvényességi láncot építenie, s ennek folyamatos érvényességéről kell csak gondoskodnia.

DS4 A kibocsátás funkciócsoport naplózása

[DS4.1]
A következő kibocsátással kapcsolatos események naplózása feltétlenül szükséges:

- minden olyan esemény, amely az adat kérések teljesítésével kapcsolatos,
- minden olyan esemény, amely az igazolás kérések teljesítésével kapcsolatos,
- minden olyan esemény, amely a szolgáltató-váltás előkészítésével kapcsolatos.

5 Megfelelőségi követelmények

Egy archiválási szolgáltatónak be kell mutatnia, hogy minden megbízható rendszere:

- megfelel a 4.1 alfejezetben meghatározott általános biztonsági követelményeknek;
- megfelel a 4.2 alfejezet alapszolgáltatásokra vonatkozó biztonsági követelményeinek;
- megfelel a 4.2 alfejezet azon kiegészítő szolgáltatásokra vonatkozó biztonsági követelményeinek, melyet az archiválási szolgáltató felvállal;
- esetleges egyéb szolgáltatásai nem veszélyeztetik az előző francia bekezdésekben meghatározott kötelezettségek teljesítését.

Alkalmazási megjegyzés: A megfelelőségi követelmények teljesíthetők például egy elektronikus aláírás szolgáltatási szakértő olyan szakértői véleményével, melyet alátámaszt a megbízható rendszer informatikai biztonságára vonatkozó, tanúsító szervezet által kiadott igazolás.

6 Hivatkozások

[D1] Ajánlás eljárásrendi követelményekre elektronikus aláírás felhasználásával végzett elektronikus archiválási szolgáltatások szolgáltatói számára

[ETSI1] ETSI TS 101733 CMS Advanced Electronic Signature (CAdES) v1.6.3, 2005-09

[ETSI2] ETSI TS 101903 XML Advanced Electronic Signature (XAdES) v1.2.2, 2004-04

[ISO1] ISO 14721:2003 Space data and information transfer systems – Open archival information systems – Reference model

[OAIS] Reference Model for an Open Archival Information System (OAIS)

[RFCd1] RFC 4810: Long-Term Archive Service Requirements (draft-ietf ltans-reqs-11.txt)

[RFCd2] RFC draft: Long-term Archive Protocol (LTAP) (draft-ietf-ltans-ltap-06.txt)

[RFCd3] RFC draft: Evidence Record Syntax (ERS) (draft-ietf-ltans-ers-16.txt)

7 Rövidítések

Általános rövidítések:

AIP	Archival Information Package	archív információs csomag
BALE		biztonságos aláírás-létrehozó eszköz
CEN	Comité Europeen de Normalization	Európai Szabványügyi Bizottság
CI	Content Information	tartalom információ
CWA	CEN Workshop Agreement	CEN munkacsoport megállapodás
DI	Description Information	leíró információ
DIP	Dissemination Information Package	kibocsátott információs csomag
IP	Information Package	információs csomag
ETSI	European Telecommunication Standards Institute	Telekommunikációs Szabványok Európai Intézete
HSZ		hitelesítés-szolgáltató
ISO	International Organization for Standardization	Nemzetközi Szabványügyi Szervezet
MELASZ		Magyar Elektronikus Aláírás Szövetség
MR		megbízható rendszer
PDI	Preservation Description Information	megőrzés leíró információ
PI	Packaging Information	csomag információ
RFC	Request for Comment	felhívás véleményezésre
SIP	Submission Information Package	benyújtott információs csomag
UTC	Co-ordinated Universal Time	koordinált egységes idő

A követelmények elnevezésében használt rövidítések:

MA	Management	menedzselés
KM	Key Management	kulcskezelés
AA	Accounting and Auditing	naplózás
AR	Archiving	archiválás
GE	General	általános
IN	Ingest	benyújtás
LA	Longterm Archiving	hosszú távú archiválás
DS	Dissemination	kibocsátás
IA	Identification and Authentication	azonosítás és hitelesítés
SO	Systems and Operations	rendszerek és működésük
SA	System Access control	rendszer-hozzáférés ellenőrzés
SR	System Requirements	biztonsági követelmények
BK	Backup and Recovery	mentés és helyreállítás