A rendszer áttekintése, alkalmazási köre

A rendszer célja

A rendszer célja a napi szinten nagy mennyiségű (100-400 GB/nap aktív adat) archiválandó adatot termelő cégektől, szervezetektől az adatok begyűjtése, és biztonságos helyre juttatása, a megfelelő szolgáltatás és adatbiztonsági mutatók garantálása mellett.
A megvalósítás alapkoncepciói:

- Az adatok szállítását egy megfelelően biztosított és felszerelt kisteherautó végzi, a megfelelően képzett és biztosított személyzettel (a személyzetnek garantáltan nincs lehetősége az adatok manipulálására, kizárólag a folyamatot vezérelhetik).
- Amennyiben (kellő számú) felhasználó földrajzi elhelyezkedése lehetővé teszi, az adatmentést valamilyen dedikált adathálózattal biztosítjuk. A safety és security követelmények ebben az esetben is élnek, bár a safety tekintetében a mobilitást, és az ebből származó mechanikai behatásokat el lehet hanyagolni.

Megcélzott felhasználói kör

Olyan cégeket és szervezeteket céloztunk meg, akik

- Nagy mennyiségű adatot termelnek, de ezek biztonságos mentése (annak bekerülési költsége miatt) nem megoldott (esetleg csak több cég összefogásával építhető ki a megfelelő infrastruktúra).
- A cég több telephellyel rendelkezik, és az adatokat nem gazdaságos (és/vagy biztonságos) távközlési eszközökkel továbbítani.
- A katasztrófavédelmi távolság betartása problémákba ütközik.

Megcélzott felhasználási terület

A rendszer a Tivoli Storage Manager megoldásra épül, ezért képes minden olyan adatforrás kezelésére, amelyet a TSM kezelni képes. Ez meghatározza a felhsználási területeket is:

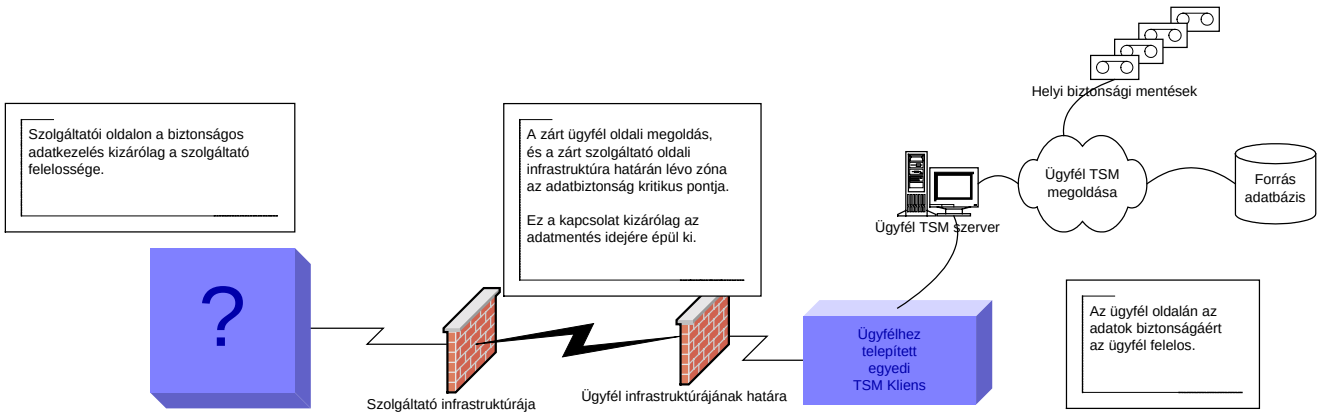
- Elektronikus levelezés
    - Lotus Notes
    - Microsoft Exchange
    - Jellemző aktív adatméret: 100-400 GB/nap
- Adatbázisok
    - IBM DB2
    - Oracle
    - MS-SQL Server
    - Jellemző aktív adatméret: 400-1000 GB/nap
- Egyéb, kis és középvállalati adatok
    - Fájlszerverek
    - WWW szerverek
    - Intranetes szerverek (LDAP, Active Directory …)
    - Jellemző aktív adatméret: 100-400 GB/nap
- Statisztikai adatbázisok
    - Pl. állami szerveknél

- Jellemző aktív adatméret: 500-3000 GB/nap

Természetesen a rendszert arra kell felkészíteni, hogy szükség esetén képes legyen fogadni akár az összes ügyfél teljes mentését is (ez legalább a teljes aktív adattömeg mérete).

Mobil adatmentő állomás biztonsági (security) kérdései

Az adatmentő megoldás áttekintő ábrázolását az alábbi ábra mutatja:



A megtervezendő komponenseket a kék téglatestek jelölik.
Mindkét rendszerkomponens kritikus adatbiztonsági (security) szempontból, a szolgáltatói oldalon szolgáltatásbiztonsági megfontolások is felmerülnek.
Az adatbiztonság szempontjából a szolgáltatói oldalon (eddig) az alábbi tervezési szempontok merültek fel:

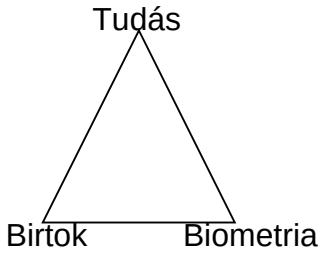
1. A kliensprogram nem férhet hozzá azokhoz az adatokhoz, amelyeket az ügyfél a szolgáltatónak nem kíván átadni.
2. A kliensprogram az ügyfél rendszerét kizárólag a mobil adatmentés ideje alatt érheti el.
3. A kliensprogram titkosítást végez.
4. A kliensprogram titkosítatlan adatokat nem tárol és nem továbbít.
5. Ebből adódóan a szolgáltató semmiféle adatot nem tárolhat az ügyfélnél (még adminisztrációs adatokat sem).

Az ügyféloldalt a szoláltatói oldallal egy *korlátozott sávszélességű, lehallgatható, de csak a mobil adatmentés idején kiépíthető* (pl. amúgy kikapcsolt) kommunikációs csatorna köti össze. Ezért:

6. A kommunikációs csatornán kizárólag *titkosított* adatok áramlása megengedett.
7. A kommunikáció a titkosítással együtt is kellően gyors kell legyen ahhoz, hogy a mentendő adatmennyiség áttöltési idejére egy, *szerződésben definiált korlát* minden körülmények között teljesüljön.
8. Az adatlopás megelőzésére a titkosítási protokollnak partnerhitelesítést is tartalmaznia kell.

A szolgáltató oldalán megvalósított komponensekre a következő *adatbiztonsággal kapcsolatos* követelmények adottak:

9. A szolgáltató nem képes az adatok visszafejtésére.
10. A szolgáltatónál nem tárolódhat titkosítatlan adat (még ideiglenesen sem).
11. Az adatok visszafejtését az ügyfél a szolgáltató hozzájárulása nélkül nem képes elvégezni.
12. Az ügyfél az adatokat visszaállításhoz (recovery) akkor is képes dekódolni, ha azokat nem az ábrán látható módon juttatják a rendszerbe (hanem pl. kazettán stb.) Ehhez a szolgáltató előtranszformációt végezhet.
13. A mobil állomás személyzete az adatokhoz sem titkosított, sem titkosítatlan formában nem juthat hozzá, az átvitelre került fájlok nevét és méretét sem ismerheti meg (természetesen a fogadó oldalon mindezt megismerhetik, a TSM rendszeren keresztül).
14. Az archiválandó adatok titkossága mellett célként jelöltük meg a tényleges állomás hozzáférésvédelmét is, itt az alapvető adatbiztonsági szabályoknak megfelelően kívánunk eljárni, azaz az autentikáció 3 pillére közül kettő megvalósítását tervezzük:



- Tudás/logikai alapú: a felhasznált operációs rendszer biztonsági lehetőségeinek kiaknázása.
- Birtok:
    i. Természetes védelem: az adatmentő állomás bemeneti perifériákkal nem rendelkezik, ennek megfelelően távoli eléréssel lehet csupán a működést befolyásolni. Ez dedikált hálózaton keresztül történik, valamint az elérést biztosító szerverprogram maga is logikailag védett.
    ii. Az adatmentő állomáson lévő szerver entitás valamilyen, az előzőektől független azonosítási procedúra sikeressége esetén indul el, ennek jellege tetszőleges (ajánlott a biometrikus vagy a birtok alapú).

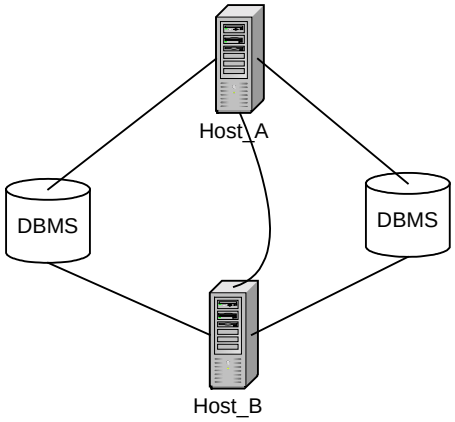
Ezen utóbbi intézkedésekre az esetleges illetéktelen birtokbavétel esetén van szükség, mivel enélkül többféle károkozási lehetőség is megnyílik:

- Az archiválási folyamat meghiúsítása
- Az ügyfél rendszerébe történő betörés az élő linken keresztül.

Összefoglalva: A fenti információk/eszközök hiányában az állomás legyen teljesen használhatatlan a támadó számára.

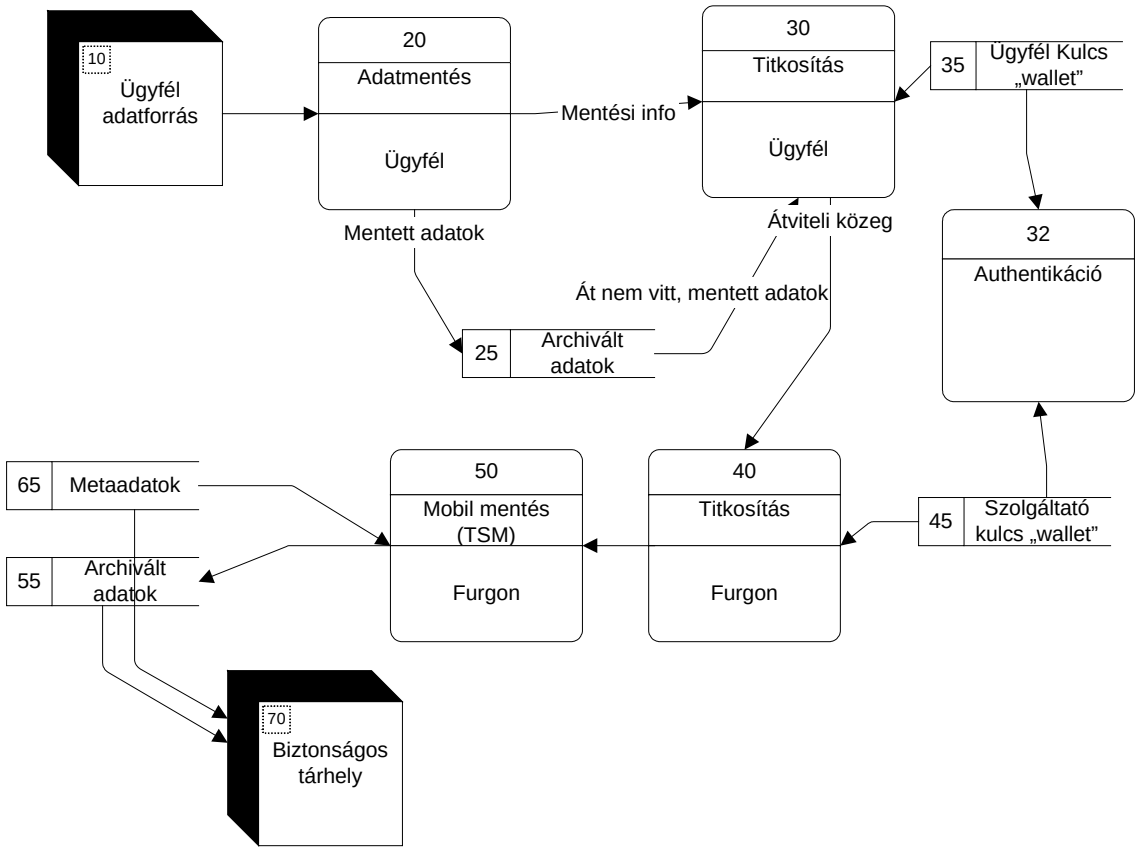
A mobil adatmentő állomással szemben támasztott szolgáltatásbiztonsági követelmények

1. Cél, hogy a mobil adatmentő állomás lehetőleg minden körülmények között képes legyen produkálni a tőle elvárt funkciókat, azaz bizonyos mértékű meghibásodás esetén is képes legyen véghezvinni a teljes adatmentési folyamatot. Szükséges tehát, hogy a teljes adatmentő rendszer rendelkezésreállási mutatói megfelelő szintet érjenek el a rendszer egyes komponenseinek hasonló mutatóitól függetlenül. Eddigi elképzeléseink szerint egy, az adatmentő állomáson belüli HA klaszterszervezés megfelelő lehet ezen cél eléréséhez.



2. Mind a megbízhatósági modellezés, mind az implementációs változások során figyelembe kell vennünk a gépjárművet, mint speciális hasznosítási környezetet, annak sajátosságaival együtt: pl. állandó rezgések, melyek károsíthatnak bizonyos alkatrésztípusokat. Cél ezen járulékos károk lehetőség szerinti elkerülése (rezgésre érzéketlen hardver választással), vagy ahol ez nem lehetséges, ott a meghibásodás valószínűségét kell csökkenteni.
3. Cél továbbá, hogy a már megírt, „kész” adathordozón lévő adathalmaz titkossága mellett a lehető legnagyobb mértékben annak integritása is biztosítva legyen – akár még a háttértárat alkotó adathordozó sérülése esetén is. Itt az előző félév során tanult hibakorrekciós módszereket alkalmaznánk a választott tárolóeszköz jellegétől függően (például RAID konfiguráció, paritásszegmensek stb.)

Formális leírás



Mobil Adatmentés
0. szintu DFD

Eddigi elképzelések:

- Gyors titkosító algoritmus kétszeri, két külön kulccsal (ügyfél és szolgáltató) történő alkalmazása a fenti ábrán „falakkal” jelölt helyeken.
- A fent megfogalmazott követelmények teljesülését *formális módszerekkel* kívánjuk bizonyítani.
- A partnerhitelesítéshez PKI használata
  - Szabványos,
  - Valószínűleg nem technológiai zsákutca.
- A kulcsmenedzsmentet a szerződő felek egymástól függetlenül valósítják meg.
- Az ügyfélhez való kapcsolódás várhatóan gyors ethernet kapcsolaton (pl. gigabit ethernet) keresztül megy végbe. Optimális esetben ez a csatorna megfelelő teljesítménytartalékkal rendelkezik a teljes mentés határidőn belül történő befejezéséhez.

Javasolt harvermegoldások

- LTU 3583, LTU 3581, LTU 3584 – 72 dat-drive fogadására képes, legfeljebb 2800 slottal szerelhető tömeges adattárolási eszköz. Egy magnó írási teljesítménye 10-20 MB/sec, ezt az eszköz multiplexálni képes.

Javasolt szoftvermegoldások

- A titkosítás RC6 vagy AES rendszerű lesz. (Esetleg választható, külön modulban.)
- TSM az adattárolás illetve archiválás megvalósítására.

Az AES és az RC6 összehasonlítása

Szempont	AES (128 bites blokk, 128 bites kulcs)	RC6 (128 bites blokk, 128 bites kulcs)
Titkosítási sebesség (Java JDK 200 MHz P2)	1100 Kbit/s	1590 Kbit/s
Legegyszerűbben alkalmazható törés	Kimerítő kulcskeresés.	Differenciális/Lineáris kriptanalízis (Külön tanulmányban).
Előnyei	Erős titkosítás, változtatható kulcs és blokkméret.	Nagyon egyszerű implementáció, kódoló=dekódoló. Változtatható kulcs és blokkméret.
Hátrányai	Dekódoló rész bonyolultabb, más adatokat használ.	Lineáris kriptoanalízissel törhető.