SZATMÁRI FERENC[1]

Az elektronikus banki csatornák biztonsági kérdései és a fejlődési irányok

Security questions and developmental trends of electronic banking channels

Electronic banking is considered to be a relatively new and exciting field in the framework of the traditional banking world. In my article I describe the different areas of electronic banking and discuss all the solutions necessary to help bring about the secure utilization of each of these services. I devote a separate chapter to security questions, emphasising their special importance and the fact that a complex application of these security procedures is fundamental for the realization of successful electronic banking services.

Throughout the world the financial sphere has already recognized the opportunities provided by electronic banking. Today in the USA, 750-800 banks provide such a service. Similarly throughout Europe, the use of E-banking is spreading rapidly. According to an estimate given by Datamonitor, 1 million dollars per day was spent on installing electronic banking systems in 1999, and by 2004 this amount is expected to quadruple. In the future, banks will probably take full advantage of the opportunities offered by electronic banking, and following the logic of this new information channel, other adequate and secure products are likely to appear, especially in the world of mobile telephones.

1. Bevezetés

A bankvilág hagyományosnak mondható architektúrájában viszonylag új keletű és izgalmas, érdekes terület az elektronikus bankügyletek világa. A hazai bankrendszer most fejleszti ezen informatikai szolgáltatási területeit az EU normáknak is megfelelővé, illetve a világ élvonalához mérten is kompatibilis színvonalúvá. A bankvilágban tehát e terület forradalmi változás, fejlődés, intenzív fejlesztés alatt áll, amely tevékenység komoly szakmai kihívást is jelent.

Írásomban igyekszem bemutatni az *elektronikus bankügyletek* különböző területeit, milyen technikai eszközök szükségesek az egyes szolgáltatások igénybevételéhez, milyen számítógépes rendszerek kellenek ahhoz, hogy az ügyfelek használhassák az elektronikus banki szolgáltatásokat és kihasználhassák az ezekben rejlő lehetőségeket, megértve az alapvető működési módokat.

Külön részt szántam a *biztonsági kérdéseknek*, amelyek kiemelt jelentőséggel bírnak, s a különböző megvalósításoknál megkerülhetetlen ezen eljárások komplex alkalmazása.

A pénzügyi szféra világszerte felismerte az elektronikus banki szolgáltatások által kínált lehetőségeket. Az Egyesült Államokban napjainkban 750–800 bank nyújt ilyen szolgáltatást. Az International Data Corporation előrejelzése szerint

[1] BGF Pénzügyi és Számviteli Főiskolai Kar, Zalaegerszegi Intézet, Informatika Tanszék, főiskolai adjunktus.

2003-ban mintegy 32 millió háztartás fog interneten keresztül kezdeményezni banki tranzakciót. Európában ugyancsak gyorsan terjed az *e-banking*: 1999-ben a Datamonitor becslése szerint napi egymillió dollárt költöttek ilyen rendszerek telepítésére, s ez a szám 2004-re várhatóan megnégyszereződik.

A jövőben az *e-banking* kínálta lehetőségeket várhatóan teljesebb mértékben aknázzák majd ki, megjelennek az új csatorna logikájával adekvát termékek. Mivel ennek következtében szükségessé válik a bankok stratégiájának és szervezetének átalakítása, felértékelődik azon – tanácsadói, marketing- vagy rendszerintegrátori háttérrel rendelkező – vállalkozások fontossága, amelyek a pénzügyi szféra intézményeit segítik az „új gazdaság" követelményeihez való igazodásban.

A nemzetközi gazdaság szereplőihez hasonlóan a magyarországi pénzügyi szféra is felismerte az új technológiák és az *e-banking* által kínált lehetőségeket. A Telebanking 1997-es elterjedését követően 1998-ban a *remote banking*, 1999-ben az *internet bankig* bevezetése fémjelezte a banki szolgáltatások fejlődésének új irányát. A mintegy negyven honi bank csaknem fele rendelkezik valamilyen weboldallal, de csak a legnagyobb bankok kínálnak *internet bankinget*. A jövőben a közepes pénzintézetek várhatóan nagyobb súlyt helyeznek az ilyen szolgáltatások bevezetésére, azokat jól definiált piaci szegmensekbe való benyomuláshoz használva fel.

A tárgyalt értékesítési csatornákon túlmenően Magyarországon számottevő növekedési potenciál áll a *mobil banking* előtt, mivel igen magas a mobiltelefonnal rendelkezők aránya, és az ezeken a készülékeken keresztül intézett tranzakciókat sokan biztonságosabbnak ítélik, mint az *internet banking* folyamatait. A több bank által is kínált SMS-alapú szolgáltatások a *mobil banking* első fejlettségi szintjét képviselik. A jövőben fokozottabb interaktivitással járó termékek elterjedése várható, amelyek a WAP-technológiákon alapulnak majd.

Az elkövetkező három évben Magyarországon meghatározó trend lesz az elektronikus banki szolgáltatások gyors elterjedése. A hagyományos termékek mellett megjelennek az új, testre szabott és magas hozzáadott értéket képviselő szolgáltatások. Kritikus terület lesz a bankok életében a magas színvonalú ügyfélkapcsolat-kezelés, illetve rövidebb távon az új és a régi értékesítési csatornák integrált alkalmazása. Hosszabb távon az új típusú, hatékony és kényelmes elektronikus szolgáltatások széles körű térnyerése prognosztizálható, ami a hagyományos csatornák visszaszorulását vonja maga után.

2. Elektronikus bankügyletek definiálása és kategorizálása

A fogalmak, definíciók, csoportosítások terén ma még meglehetősen nagy a különbség az elektronikus bankügyletek területén, sok esetben szerző, fejlesztő, alkalmazó, vagy egy-egy elméleti iskola nyomja rá a bélyegét a meghatározásokra. Napjainkra azonban alapvetően már kikristályosodott az a fogalomkör, ami hűen írja le az *electronic banking* témakörét. Az egységes szakmai nyelv kialakulását segíti az is, hogy az elméletet tagadhatatlanul viszont-befolyásolja a gyakorlati megvalósítás folyamata.

Az *elektronikus bankügyletek* fogalomkörébe beletartozik mindazon bankszolgáltatás, melynek során a hitelintézet és az ügyfél között elektronikus úton jön létre a kommunikációs, illetve adatcserét is magában foglaló kommunikációs kapcsolat. A cserélt adatok szenzitív voltára tekintettel az elektronikus kapcsolat szükségszerűen mindenkor diszkrét, sőt külön is védett.

Az elektronikus kapcsolat lehet:

- *legális*: amikor az arra jogosult ügyfél és a bank között az előírt hivatalos módon jön létre a kapcsolat legális ügyintézés céljából;
- *illegális*: amikor az arra jogosulatlan személy (*hacker*) próbál – meg nem engedett módon – kapcsolatot teremteni, illegális tevékenység céljából.

Az *elektronikus bankügylet* kifejezést értelmezhetjük tágabb és szűkebb értelemben.

Tágabb értelemben az összes elektronikus kapcsolatteremtési módnak megfelelő bankügylet-féleséget az *elektronikus bankügylet* fogalomkörébe soroljuk, melyek az alábbiak lehetnek:

- *home banking*
- *office banking*
- *phone banking:*
  ⇒telefonbank
  ⇒*call center*
  ⇒faxbank
  ⇒mobilbank
- *internet banking*
- *egyéb*
  ⇒ügyfélkártya rendszerek: ATM, SST, POS terminál
  ⇒elektronikus készpénz: elektronikus pénztárca (*smart card*)
  ⇒internetes elektronikus pénz

A *home banking* az otthonok és a bankok, az *office banking* a hivatali irodák és a hitelintézetek közötti e-kapcsolat, általában bérelt telefonvonalon. A kapcsolat a bank és az ügyfél számítógépei között jön létre. A *phone banking* a két fél telefonos végberendezései, azok szoftverei, illetve az ügyfélszolgálat között jön létre. Az *internet banking (e-banking)* esetén a világháló segítségével jön létre az elektronikus kapcsolat (*e-banking*) az ügyfél és a bank számítógépei között. Az *egyéb* e-banking megoldásoknál az ügyfél kezelésébe, birtokába adott elektronikus eszköz (általában intelligens chip-kártya) és a bank számítógépe között jön létre kapcsolat.

Szűkebb értelemben az *elektronikus bankügylet* fogalmán az ügyfél és a bank közötti közvetlen számítógépes kapcsolatot értjük, amely természetesen valamely alkalmas kommunikációs közegen keresztül valósul meg (VSAT, mikrohullám, ISDN, ISDN bérelt, PSTN, PSTN bérelt).

3. Elektronikus bankügyletek biztonsága

Általános az egyetértés abban, hogy az elektronikus úton történő bankhasználat legalább olyan biztonságos, mint a hagyományos, sőt még biztonságosabb

is lehet. A hagyományoshoz képest azonban az elektronikus banki szolgáltatások igénybevétele során új veszélyek és hibaforrások keletkezhetnek, és ezeknek a hibáknak a kiküszöbölésére fel kell készülniük a bankoknak. A veszély jelentkezhet a *banki oldalon, ügyféloldalon* és a *kommunikációs csatornában*.

A szakemberek általános véleménye, hogy az egyéb okokon túlmenően az elektronikus banki szolgáltatások igénybevételének legnagyobb gátló tényezője a *kommunikációs csatornák iránti bizalom hiánya*.

A *bankbiztonság*, amely soha nem abszolút, hanem mindig csak relatív lehet, olyan kedvező állapot, amelynek megváltozása nem valószínű (nagyon csekély az eshetősége).

A biztonságnak két alapvető területe létezik, az egyik az *adatvédelem* (Data Protection, „DP"), amely a személyes, vagy személyre visszaazonosítható adatok kezelésével, védelmével foglalkozik az Adatvédelmi törvény előírásai szerint, a másik terület az *adatbiztonság* (Data Security, „DS"), amely az informatikai megközelítés szempontjából kiemelkedő jelentőségű.

3.1. Az adatbiztonság területei

Három fő területe létezik az adatbiztonságnak: *a rendelkezésre állás, a bizalmasság és a sértetlenség*.

A *rendelkezésre állás* azt jelenti, hogy az információs rendszer az arra jogosult számára megfelelő módon bármikor rendelkezésre álljon, még katasztrófa helyzet esetén is (Business Continuity Plan „BCP").

A *bizalmasság elve* szerint az erőforrásokhoz, adatokhoz csak az arra jogosultak, azon belül is jogosultsági fokuknak megfelelő mértékben férhessenek hozzá.

A *sértetlenség kritériuma* azt jelenti, hogy valamely információ, adat, az eredeti állapotnak megfelelő. A sértetlenség fogalomkörébe tartozik a hitelesség is, ami alatt az értendő, hogy az üzenet forrása a megjelölt és tartalma az eredeti.

A *humán védelmi módszerek* a bizalmasság védelmét szolgálják humánpolitikai, vezetési, oktatási és jogi eszközök alkalmazásával biztosítva a bank számára a kvalifikált, megbízható, tervezett életpályán mozgó, felelős munkatársakat, akik mindenkor „nem"-et mondanak a bankbiztonságot veszélyeztető esetleges „kísértéseknek".

A *fizikai védelem* módszerei mindhárom területre kiterjednek, a rendelkezésre állás, a bizalmasság és a sértetlenség védelmére. Főbb módszerei az objektum helyének kiválasztása, a belépés- és mozgásellenőrzés, a fizikai behatolásvédelem (PIR: passive infrared), vagyis az „intelligens épület" koncepciójának minél teljesebb megvalósítása.

A védelemszervezés e módja kitér továbbá az értéktárolás és az értékszállítás területeire is.

Informatikai szempontból a *logikai védelem* területe tartozik szorosan az elektronikus bankügyletek témaköréhez. Ezen eljárások a számítástechnikai rendszerek adatai és programjai rendelkezésre állásának, bizalmasságának és sértetlenségének védelmét biztosítják. Tudománya a *kriptológia*, amely magában foglalja a *rejtjelzés* és a *kriptoanalízis* (rejtjelfejtés) területeit. Módszerei az adatrejtjelzés, a kétfázisú hitelesítés és a tartalomhitelesítés.

3.2. Logikai védelmi módszerek

3.2.1. Adatrejtjelzés

Az adatrejtjelzés lényege, hogy arra alkalmas eljárással a nyílt szövegből a jogosulatlan számára értelmezhetetlen szöveget képzünk. Az eljárás lényege, hogy egy viszonylag állandó algoritmus, és egy gyakran változtatott kulcs segítségével a jelsorozatot teljesen átalakítjuk, s így továbbítjuk az üzenetet a hálózaton.

Az adatrejtjelzés két alapvető fajtája:

- a szimmetrikus kulcsú rejtjelzés;

  A hagyományos titkosítási módszerek mind az ún. szimmetrikus kulcsú kategóriába tartoznak. Ez azt jelenti, hogy a titkosító és a visszafejtő kulcs ugyanaz. Igen elterjedt eljárás például az 1977 óta alkalmazott DES (Data Encryption Standard). Ennél a korábban alkalmazott kulcs 56 bit hosszúságú volt, de ma már 75–80 bitben adják meg azt a kulcsméretet, amely már üzleti biztonságú titkosítást nyújt.

  A biztonság növelése érdekében alkalmazzák a TripleDES-t is, ahol háromszor kulcsolják át a szöveget, mindig különböző kulccsal. Ilyen módszereknél a legnagyobb gond a kulcs biztonságos cseréje a tranzakciók során. Ez titkos csatornát igényel, amely nehézkes és támadható.

- az aszimmetrikus kulcsú rejtjelzés.

  1977-ben új típusú algoritmusok is megjelentek, az ún. nyilvános kulcsú módszerek. Ezeknél a felhasználónak két kulcsa van. Az egyik a privát kulcs, amit csak ő ismer, a másik a nyilvános kulcs, amit szabadon terjeszthet. Az egyik kulccsal titkosított üzenet csak a másikkal fejthető vissza, s ez mindkét irányban igaz.

  Titkos üzenetet úgy küldenek a bankból, hogy az üzenetet a fogadó fél nyilvános kulcsával titkosítják, amit ettől kezdve csak a nyilvános kulcshoz tartozó privát kulccsal lehet visszafejteni, vagyis az üzenetet értelmezni. A saját privát kulcsunkkal is titkosíthatunk üzenetet, amit mindenki visszafejthet, aki a nyilvános kulcsunkkal rendelkezik (gyakorlatilag tehát bárki). Garantált viszont, hogy az üzenet feladója az, akinek a nyilvános kulcsával az üzenet visszafejthető – feltéve, hogy a privát kulcsát nem illetéktelen használta. A nyilvános kulcsú módszerek ilyen módon egyszerre alkalmasak titkosításra és autentikációra, azaz hitelességvizsgálatra is.

  A nyilvános kulcsú módszerek meglehetősen lassúak, ezért sok esetben szimmetrikus algoritmussal kombinálva használják őket. Ilyenkor a nyilvános kulcsú módszerrel csak a szimmetrikus kulcsot titkosítják, magának az üzenetnek a titkosítása pedig a szimmetrikus algoritmussal történik (Ez az eljárás egyébként csökkenti a biztonságot).

A mai titkosítási rendszerekben általában a vegyes kulcsú módszert alkalmazzák. Jelenleg a legnépszerűbb nyilvános kulcsú módszer az RSA, amelyhez jellemzően a DES, Triple-DES vagy IDEA szimmetrikus algoritmusokat párosítják.

Az adatrejtjelzés kiegészítő módszerei lehetnek a kulcsletéti rendszer, a titokmegosztás, az időbélyegzés és az osztott kulcsú rendszerek. Az osztott kulcsú rendszerek esetén a kulcsképzés részletekben történik, így az esetleges rosszhiszemű felderítés esélye sokkal kisebb.

3.2.2. Kétfázisú hitelesítés

A logikai védelem ezen módszerével a hálózatra való belépést, a hozzáférést védjük.

Az *I. fázis a LOGONID (ki vagy?)* kérdés megválaszolása, ahol kritérium a helyes username, továbbá a hardver-végpont azonosítása és csatlakozási jogosultságának megléte az azonosítás alapján.

A *II. fázis az azonosítás bizonyítása (mit tudsz?),* amely erősödő sorrendben jelenti a többször használatos jelszót, az egyszer használatos jelszót, valamint a biometriai jelszót, mely utóbbi az ember valamely fiziológiai paraméteréhez kötődik (ujjlenyomat, írisz, arckép, beszéd, járás, DNS-lánc). Ezek kombinációjából igazán biztonságos hitelesítés végezhető, mint amilyen pl. a BIOSCRYPT-eljárás, ahol az ujjlenyomat és valamilyen jelszó, vagy kód kombinációját alkalmazzuk.

3.2.3. Tartalomhitelesítés

A tartalomhitelesítés feladata:

- a tartalom eredetiségének ellenőrizhetővé tétele;
- a küldés ténye nem tagadható le;
- a fogadás ténye nem tagadható le.

Az eljárásnak különös jelentősége van a banki tranzakcióknál, de pl. az ingatlan-nyilvántartásban is. Módszere a digitális aláírás, amely lényegében a klasszikus iroda aláírás- és pecsét-funkcióját látja el. Eljárása során egy „hash" (zúzalék, vagy morzsa) algoritmussal, amely általában 168 bit hosszúságú, egy „eredeti" üzenetkivonatot képezünk a nyílt szövegből, amely abszolút módon jellemző az üzenetre, és csak arra az egyedi szövegre. A kivonatot titkosítva (pl. az RSA titkos kulccsal) kapjuk meg a digitális aláírást a küldő oldalon, amit csatolunk az üzenethez.

A fogadó oldalon a hash algoritmus és a küldő nyilvános kulcsának felhasználásával ellenőrizhetjük a kapott üzenet sértetlenségét, hitelességét.

3.3. Logikai védelmi módszerek alkalmazása

A gyakorlati alkalmazások területe az üzenetek feladójának hitelesítésében, az üzenetek sértetlenségének ellenőrzésében és a letagadhatatlanság (küldés, fogadás) biztosításában jelentkezik.

3.3.1. A küldő személyének hitelesítése

A hitelesség azt jelenti, hogy mind a bank, mind az ügyfél nyugodt lehet, az üzenet nem jöhet mástól, csak a partnertől. Ezt a különféle rejtjelzési eljárásokkal érik el. Ebben segít az RSA alkalmazására épülő nyilvános kulcsú infrastruktúra (Public Key Infrastucture, PKI). Magyarországon a tanúsítvány szolgáltatás nyújtásának működési, fizikai és informatikai biztonsági feltételeit a 2001. évi XXXV. tv. az elektronikus aláírásról szabályozza.

3.3.2. Az üzenet sértetlenségének ellenőrzése

A második követelmény a *sértetlenség* vizsgálata. Hasonlóan a tömörített adatállományhoz, amelyet sérülten nem lehet kicsomagolni, a kódolt üzenet is olvashatatlanná válik, ha sérül, ha megváltozik útközben. Módszere az elektronikus aláírás, amelynek fenti törvény 3 alaptípusát különbözteti meg.

3.3.3. Letagadhatatlanság biztosítása

Végül a letagadhatatlanság biztosítása teljes naplózással történik. Minden kiment és érkezett átutalást, kivonatot, intézkedést és a nyugtázást megváltoztathatatlan formában archivál mind a felhasználói modul, mind a banki fogadó szoftver. Ha vita van, minden üzenetváltás részleteiben visszakereshető, ellenőrizhető mind a küldő, mind pedig a fogadó oldal szerver és kliens gépein.

4. Biztonságos elektronikus banki szolgáltatások

Vizsgáljuk meg, hogy egy biztonságos bankügyletnek mik az elvi és gyakorlati kritériumai, utóbbiakat konkrét rendszerek megvalósítása kapcsán.

4.1. Biztonságos elvi rendszerek

Az elvi megközelítés szempontjából akkor mondhatunk egy üzenettovábbítást biztonságosnak, ha az megfelel a következő kritériumoknak:

- a küldő és a fogadó fél is rendelkezik saját tulajdonú tanúsítvánnyal, vagyis van saját titkos és nyilvános kulcsa;
- a tanúsítványokat (kulcsokat) mindketten arra jogosult (bankok esetében minősített) hitelesítés-szolgáltatótól szerezték be;
- a felek rendelkeznek a PKI alkalmazáshoz szükséges hardver, szoftver és tudásbázissal;
- korábbi együttműködési megállapodásuk keretében biztonságosan cseréltek algoritmust;
- az IR és az ÉR védelmében minden szükséges védelmi intézkedést megtettek;
- a tartalomhitelesítés érdekében digitális aláírást alkalmaznak;
- a hálózati adatátvitel biztonságának garantálása érdekében a kommunikációs közegben rejtjelzett adattovábbítást biztosítanak.

4.2. Biztonságos megvalósítások

Biztonságos banki hálózati megvalósításként a két klasszikus bankinformatikai rendszert, a *belföldi bankközi kapcsolatokat* megvalósító GIRO Rt. által üzemeltetett klíring rendszert, illetve a *nemzetközi bankközi kapcsolatokat* biztosító S.W.I.F.T. rendszert érdemes példaként megemlíteni.

4.3. Hazai banki alkalmazások

A bank leghatásosabb védelmét a postaláda elven működő elektronikus bankügylet szolgálja. Az ügyfél nem közvetlenül áll kapcsolatban a banki rendszerrel, tulajdonképpen strukturált fájlokat küld saját bankoldali elektronikus postaládájának.

A bankok egyre nagyobb gondot fordítanak az ügyfelek védelmi rendszerének biztosítására. A vállalkozások által végrehajtani kívánt tranzakciók csak több védelmi eszköz használatával valósulhatnak meg.

Két kulcsfontosságú területet kell a biztonság szempontjából kiemelni:

- *A banki számlavezető rendszer védelme a külső behatolókkal szemben.*
- Az adatok védelme, és biztonságos tranzakcionálása az ügyfél érdekében.

Ehhez a következő védelmi eszközök valamelyikét választják a bankok:

- Az ügyfélnek úgynevezett kulcslemezt vagy chipkártyát kell behelyezni a gépbe, és csak ezután lehet kapcsolatba lépni az elektronikus bankügyleti rendszerrel.
- A kulcslemezhez, illetve chipkártyához jelszó vagy kód is társul. A bank a rendszer installálásakor ad egy jelszót, amelyet azonban a felhasználónak az első kommunikációs kísérlet során meg kell változtatnia, ezáltal a banki ügyintéző sem tud róla.
- A felhasználókhoz a munkakörüknek megfelelő jogosultságok is rendelhetők: rögzítő, ellenőrző, kötegelő, küldő funkciók. Ez a munkafolyamatba épített biztonsági rendszernek is tekinthető.
- Az egyes felhasználóknak külön jelszavuk van, amit szintén nem ismer a bank.
- A bank és az ügyfél közötti kommunikáció során a banki rendszer folyamatosan visszaír a kulcslemezre, ill. kártyára. Ezt a visszaigazolást ellenőrzi a banki rendszer a kommunikáció újraindításakor.
- Az átutalások elektronikus aláírással jutnak el a bankba. Ehhez párosulhat még az ujjlenyomat-azonosító rendszer (*cyber mouse*: ujjlenyomat-olvasó egér).
- Az elektronikus utat kiegészítheti például egy cégszerűen aláírt telefaxváltás.
- Az ügyfél érdekét képviseli a megfelelő archiválási rendszer kiépítése.

Az *office banking* kifejlesztése során különös gondot fordítanak a bankok az adatvédelem és a hozzáférés-biztonság fokozására.

A tevékenység sok funkcióból összeállított rendszer. Az egyes funkciók egymástól jól elkülöníthető tevékenységekből állnak. Ezért ha a funkciók körének csak egy-egy részét tesszük hozzáférhetővé a banknál dolgozók számára, akkor ezzel a felelősségi köröket is meghatározzuk (pl. „rögzítők", „aláírók").

Ahhoz, hogy valaki dolgozhasson a rendszerben, felhasználói azonosítóra és jelszóra van szüksége. Minden egyes felhasználóhoz meg kell adni, hogy a funkciók mely részét érheti el.

A rendszer minden műveletről bejegyzéseket készít, amelyeket naplóállományban tárol el. A naplóállomány egy erre szolgáló lekérdező funkcióval megtekinthető, listázható. A napló-bejegyzés az esemény dátumát és idejét, a funkció nevét, a bejelentkező felhasználó azonosítóját, a tevékenység leírását tartalmazza a szükséges adatokkal kiegészítve.

Az adatok továbbítása telefonvonal felhasználásával történik. Az áramló adatok tömörítésen és rejtjelzésen esnek át. A rejtjelzés a titkos PIN kód és a kulcslemezen található információ felhasználásával történik. A PIN kódot a bank osztja ki és egy zárt PIN borítékban bocsátja az ügyfélterminál-tulajdonos rendelkezésére.

Alapvető elv, hogy egy rendszerelem csak abban az esetben fogad vissza egy másik rendszerelem által feldolgozott anyagot, ha az – a feldolgozást jelentő adatváltozáson túl – nem szenvedett módosulást. Többek között ezt a célt szolgálja az indított megbízások visszaigazolása és az ún. *egyeztetőpár-képzés*, valamint a visszaigazolás tételes egyeztetése az egyeztetőpárral. Itt jut szerephez az elektronikus aláírás is, amely az indított megbízások eredetiségét igazolja.

A helyi adatállományokról másolat készíthető egy megadott adathordozóra, pl. floppy lemezre – ez a *biztonsági mentés*.

Miután az állományokat tároló merevlemezek kapacitása véges, időnként szükség van arra, hogy a régi, feltételezhetően ritkán használatos adatbázisrészeket kimentsük egy adathordozóra. Ezt a műveletet nevezzük *archiválásnak*. Az archivált adatbázisrészek bármikor visszatölthetők egy munkaterületre.

Természetesen nem minden bank használja az összes fent leírt védelmi rendszert, de ezek közül 3-4 védelmi eljárás kiépítése feltétlen ajánlott.

5. Fejlődési irányok

A virtuális bankmodell felé történt elmozdulás eredményeként a fiókok száma csökkent a fejlett országok többségében, amely jelentős költségmegtakarítást jelent a bankok számára. Mint tudjuk, ebben a modellben a bankok különböző értékesítési csatornákat használnak (ATM-ek, *home-banking, direct banking* és *internet banking*), hogy megkönnyítsék az ügyfeleik számára a bankszolgáltatások elérhetőségét.

Az új technológia segítségével működő elektronikus bankszolgáltatások terjedése relatíve drágává teszik a bankfiókok működését. Egyes becslések szerint egy bankfiókban végrehajtott tranzakció 2 dollárjába kerül az ügyfélnek, az ATM-eknél ugyanez 60 centbe, az interneten keresztül 20 centbe. Mindezek után nem hangzik furcsán, ha kijelentjük, hogy az *internet banking* a telefonés *home banking* szolgáltatásokat megelőzve vezető elektronikus pénzügyi csatornává fog válni a közeljövőben.

5.1. Az elektronikus bankügyletek előretörése

A pénzügyi szféra világszerte felismerte az *internet banking* által kínált lehetőségeket. Az USA-ban napjainkban 750–800 bank nyújt ilyen szolgáltatást. Létezik az első olyan bank (Security First Network Bank) is, amely szolgáltatásait kizárólag az interneten keresztül nyújtja. Tehát a hagyományos bankok mellett megjelentek a kizárólag az *internet banking* szolgáltatásokra szakosodott, úgynevezett *internet only* vállalkozások. Ezek jellemzően alacsony költségszinten igen előnyös kondíciókat képesek kínálni ügyfeleiknek. A világháló

esetén a bank földrajzi elérése kevésbé fontos, sőt megadja a lehetőséget a felhasználóknak a legjobb termék megvásárlására.

A hazai pénzintézetek honlapjáról elérhető on-line bankműveletek magját a számlainformációk (egyenleg, korábbi tranzakciók) lekérdezése és átutalási megbízások indítása képezi. Tekintettel a lehetséges tranzakcióknak alapvetően a számlákhoz kapcsolódó – egyelőre szűk – körére, az internetes szolgáltatások alapfeltétele minden esetben az adott banknál történő számlavezetés. Önmagában az a tény, hogy a hagyományos számlaügyintézéstől eltérő – annál több kényelmet nyújtó, de az ügyfél részéről több önállóságot igénylő – szolgáltatásról van szó, nem von maga után többletköltséget. Természetesen az internethez való kapcsolódás technikai feltételeinek megteremtése (számítógép, modem és operációs rendszer) az ügyfelet terheli. A világhálón lebonyolított tranzakciók díja pedig hitelintézetenként eltérő, nullától a normál (bankfiókban bonyolított) tranzakció áráig terjedhet.

Az elkövetkezendő években Magyarországon meghatározó trend lesz az elektronikus banki szolgáltatások gyors elterjedése. A hagyományos termékek mellett megjelennek az új, testreszabott, és magas hozzáadott értéket képviselő szolgáltatások. Kritikus terület lesz a bankok életében a magas színvonalú ügyfélkapcsolat-kezelés, illetve rövidebb távon az új és régi értékesítési csatornák integrált alkalmazása. Hosszabb távon az új típusú, hatékony, és kényelmes szolgáltatások széles körű térnyerése prognosztizálható, amely a hagyományos csatornák visszaszorulását vonja maga után.

5.2. A WAP alapú mobiltelefonos szolgáltatások térhódítása

Megítélésem szerint ez a terület az, amely az elkövetkező években robbanásszerű fejlődésen megy keresztül. A megvalósuláshoz természetszerűen meg kell oldani azokat a technikai jellegű problémákat, amelyek jelenleg még akadályozzák az elektronikus banki szolgáltatások széles palettájú igénybevételét a mobiltelefonokon.

Melyek ezek a problémák?

- Az internet grafikus felülete nehezen, vagy egyáltalán nem jeleníthető meg a mobiltelefonokon, ehhez ki kell alakítani a vezeték nélküli adatátviteli szabványt (WAP), amely a wireless web kommunikáció alapja. Ez elsősorban adatátvitelre használható, a képi megjelenítések a webhez mérten korlátozottak.
- Magukat a mobiltelefon készülékeket is át kell alakítani, a jelenlegi kisméretű, fekete-fehér LCD-kijelzős készülékek alkalmatlanok az igazi grafikus, színes megjelenítésekre. A várható fejlődési irány a kinyitható kommunikátorok, illetve a Palm-Top-ok (marokszámítógépek) világa felé mutat, a kijelző méretét tekintve mindenképpen azokon természetesen túlhaladva, a színes plazma-képernyők irányába.

A WAP megvalósulása

Ami a világhálót olyan erőssé tette, az a fejlődés és a standardokhoz való gyors alkalmazkodás. A *Hypertext Markup Language* (HTML) standard révén bármely böngésző kapcsolódni tud bármely weboldalra. Hasonlóképpen a *wireless web* sem működhet standardprotokollok nélkül, s a *Wireless Applications Protocol* (WAP) ilyen szabvány. A WAPforum elnevezésű ipari standard csoport támogatásával (amelynek a HP is tagja) a WAP lehetőséget teremt a standard browserek és szerverek fejlesztésére, ami viszonzásképpen lehetővé teszi a wiereless-alkalmazások új generációjának használatát.

2003-ig előreláthatólag egymilliárd olyan mobiltelefon lesz használatban világszerte, amellyel hozzá lehet férni az internet alapú szolgáltatásokhoz. Európában ez már folyamatban van, mivel a mobiltelefon-birtokosok SMS-üzenetek millióit küldik és kapják naponta, s készülékeik segítségével lehetőségük van a tőzsdei árfolyamok, sporteredmények vagy más, akár banki információk (számlaegyenleg, számlatörténet, átutalás, tranzakciós napló) megismerésére is.

A mobil banki szolgáltatások a pénzintézeteknek is több számottevő előnyt nyújtanak:

- Az ügyfelek elégedettsége növekszik, a pénzintézetek új klienseket nyerhetnek meg, illetve erősíthetik a meglévők hűségét.
- Vonzó, könnyen használható csatorna.
- A mobiltelefonok már most is világszerte elterjedtebbek, mint a személyi számítógépek, és új feladatokra is használják őket.
- A biztonsággal kapcsolatos igények megoldásával a mobil banki szolgáltatások kiváltják a személyi számítógépeken és telefonon keresztül nyújtott banki szolgáltatások gyenge pontjait.
- A mobilfelhasználók vonzó ügyfelek, az átlagosnál tehetősebbek és fiatalabbak.
- Az ügyfeleknek mobilitást kínálnak, ott és akkor intézhetik tranzakcióikat, ahol és amikor akarják, teljesen biztonságos módon.
- Teljesen új bevételi forrást képviselnek.
- Potenciális költségkímélő megoldásról van szó, mivel az elektronikus csatornák költségei alacsonyabbak.

A biztonságos technológia

Az interneten történő ügyintézés gondolatát bizalmatlanság és kétség fogadta. Működni fog-e a technológia? Kiszivároghatnak-e bizalmas információk? Ma már tudjuk, hogy az új SSL rejtjelzési technológia biztonságos.

A HP/i-Cell WAPbank alkalmazása WTLS-t (*Wireless Transport Layer Security*) titkosítást használ, amely a kábel nélküli (wireless) információ továbbításához optimalizált. A WTLS-kódolás ugyanazon az elven alapul, mint az SSL (*Secure Socket Layer*), ami az interneten használatos. Az ügyfél PIN-kódja és azonosítója (*User ID*) is garantálja, hogy ne kerüljön sor jogosulatlan belépésre.

Véleményem szerint tehát a legnagyobb potenciális fejlődési lehetőség a mobiltelefonos banki szolgáltatások előtt áll. Nincs messze az idő, amikor minden

internet honlappal rendelkező banknak lesz WAP honlapja is, amin keresztül a mobiltelefonnal rendelkezők hatalmas tábora fogja elektronikus úton intézni bankügyeit.

Ehhez természetesen soha nem látott „csoda kis készülékeik" lesznek, mint pl. amilyet korábban éppen Magyarországon próbáltak ki a Westel közreműködésével. A világon elsőként ez az új készülék és technológia (MMS) színes fényképek továbbítására és megjelenítésére is alkalmas, a próbaüzemben akkor sikeresen vizsgázott, világméretű értékesítése azóta felfutott.

Nem kell tehát túl bátornak lenni ahhoz a jövendöléshez, hogy rövidesen az elektronikus bankügyletek terén a mobiltelefonos szolgáltatást igénybevevők száma nagyságrendekkel el fogja kerülni, az egyébként szintén gyorsan fejlődő más elektronikus csatornák használóinak számát.