Pleva Péter

Anonim digitális pénz mobilkörnyezetben

Debrecen
2008

Debreceni Egyetem
Informatika Kar

Anonim digitális pénz mobilkörnyezetben

Témavezető:
Dr. Pethő Attila
egyetemi tanár

Készítette:
Pleva Péter
programtervező matematikus

Debrecen
2008

Ezúton szeretnék köszönetet mondani mindazon a személyeknek, akik hozzájárultak diplomamunkám elkészítéséhez:

Témavezetőmnek, Dr. Pethő Attilának, aki szaktudásával, tanácsaival és véleményével segített a dolgozat témájának kiválasztásában, a szakirodalom felkutatásában és a diplomamunka végleges formába öntésében.

Nem utolsó sorban szeretném megköszönni szüleimnek azt a türelemet, bátorítást és anyagi áldozatvállalást, mellyel lehetővé tették egyetemi tanulmányaim elvégzését.

Tartalomjegyzék

Ábrák jegyzéke

1. Bevezetés

Ahogy a hagyományos üzleti élet, úgy az e-business területeinek is van egy közös mozgatórugója: az e-fizetés. Az elektronikus kereskedelem valamint a mobileszközök ilyetén méretű elterjedésével egyre nyilvánvalóbb az igény a mobilkommunikáció egy új szolgáltatása iránt, ez nem más, mint az *m-vásárlás*. Ezen víziót számos a témához kapcsolódó tanulmány ([3]-[5]) ill. piackutatási eredmény[1] erősíti meg. Így az *m-kereskedelem* – várhatóan – rohamléptékű térhódításával a mobileszközzel történő vásárlás a közeljövőben a legfelkapottabb mobilszolgáltatássá válhat. Az iránta mutatott növekvő igény könnyen magyarázható: a vásárló szempontjából a mobiltechnológia kényelmet, gyorsaságot és személyreszabhatóságot nyújt. A kereskedő szemszögéből nézve az m-kereskedelem lehetővé teszi a piac bővítését és a költségei csökkentését. A mobilszolgáltató számára lehetőség nyújt az ügyfeleitől érkező bevételeinek növelésére. A pénzügyi szolgáltató (általában bank) pedig a mobileszközökre személyes ügyfélterminálként számíthat.

A legkézenfekvőbb az lenne, ha m-vásárlási szándékunkat a mobilkészüléken tárolt ún. *digitális pénz* segítségével, a készpénzes ügyintézés előnyeit megtartva tudnánk véghezvinni. Habár az első, 1983-as publikáció [1] óta számos tudományos cikk valamint tanulmány látott napvilágot a témában, a bennük ([6], [7], [8], [9] etc.) bemutatott e-fizetési protokollok vagy nem valósítanak meg *anonim fizetést* és *átruházhatóságot*, vagy alkalmatlanok mobil implementációra. Ezen felül egy részük, mint például [14], [15] speciális hardverigénnyel is rendelkezik (intelligens kártya[2], POS készülék[3], etc.).

Jelen dolgozat elsődleges célja egy olyan, mobilkörnyezetben is jól alkalmazható digitális pénz protokoll ajánlása, mely – analóg módon a hagyományos, készpénzzel történő tranzakciókkal – egyrészt lehetőséget nyújt a vásárló személyének elfedésére, és így akár *anonim számla* igénylésére, másrészt biztosítja a fizetőeszköz átruházhatóságát. Mindezek realizálása során a protokoll olyan közismert kriptográfiai technikákat, technológiákat alkalmaz, mint a digitális aláírás, aszimmetrikus titkosítás, nyilvános kulcsú infrastruktúra,

[1] „[...] Az m-fizetés szignifikáns hatást fog gyakorolni a bank és kereskedelem világára az elkövetkezendő öt évben. [...]" *(M-Payments 2007-2012: Commerce and banking in the mobile world, Visiongain Research Comp., 2007)*

[2] Olyan – memóriával ill. processzorral rendelkező – hordozható chipkártya, mely kriptográfiai algoritmusok végrehajtására valamint kulcsok tárolására szolgál.

[3] A Point-of-Sale készülék egy olyan hardvereszköz, melynek megléte – a vásárlás helyén és idejében – szükséges előfeltétele a tranzakció sikeres lebonyolításának (lásd bankkártya).

digitális ujjlenyomat, anonim válaszcsatornák. Habár az alapvető támadási lehetőségek, úgy mint a *tokenhamisítás* ill. *ismételt felhasználás* (vásárlás, átruházás) kizárása érdekében a rendszer tartalmaz biztonsági mechanizmusokat, ugyanakkor – a komplexitás csökkentése és a lényegi működés kiemelése céljából – nem küszöböl ki néhány egyéb, a szakirodalmak által gyakran tárgyalt biztonsági problémát (lásd . fejezet).

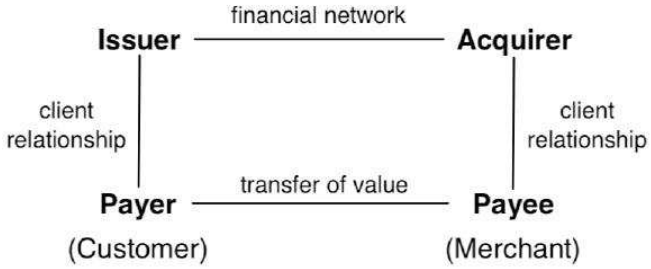
A dolgozat további része a következőképpen tagolódik: a 2. fejezetben a napjainkban alkalmazott e-fizetési mechanizmusokkal ill. azok tulajdonságaival ismerkedhetünk meg, majd a 3. fejezet a mobilfizetésekkel szemben támasztott elvárásokat tárgyalja, végül a 4. rész egy lehetséges m-fizetési digitális pénz protokollt mutat be.

2. E-fizetés a gyakorlatban

Elektronikus kereskedelem, vagy röviden csak e-kereskedelem alatt definíció szerint ([16]) tetszőleges pénzügyi tranzakciót érthetünk, beleértve magának az információnak elektronikus úton történő továbbítását is. Ezeket az információcsomagokat közösen *elektronikus tokenek*nek nevezzük.

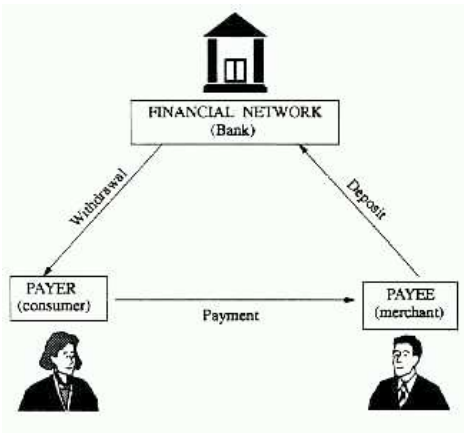
Az e-kereskedelem egyik közismert formája, az e-fizetés nem más, mint tranzakciók egy olyan sorozata, melynek eredménye egy harmadik fél által hitelesített elektronikus token felhasználásával végbement vásárlás. Habár a mobil eszközzel támogatott ún. m-fizetési megoldások is ide sorolhatók, azokat a 3. fejezetben külön tárgyaljuk. Általános esetben (lásd 1. ábra) az e-fizetési protokollok négy szereplőjét különböztetik meg a rendszernek:

- *ügyfél*: A digitális fizetőeszközt igénylő és azt az elektronikus kereskedelemi forgalomban fizetésre felhasználó entitás.
- *kedvezményezett*: Az e-kereskedelem szolgáltatói oldalán megjelenő, elektronikus fizetőeszközt ellenértékként elfogadó fél, vagy alternatív esetben egy az ügyféltől különböző szintén fogyasztói entitás.
- *pénzügyi hálózat*: A fizetőeszközt elektronikus úton előállító és azt az ügyfél részére kibocsátó szolgáltató vagy ilyen szolgáltatók egy halmaza.
- *"harmadik", bizalmi fél (TTP)*: A szereplők hitelességét biztosító entitás.



1. ábra. Egy általános, négyszereplős e-fizetési protokoll modellje

A leggyakoribb esetet szem előtt tartva az irodalmak az ügyfelet, kedvezményezettet, pénzügyi hálózatot ill. bizalmi felet informálisan rendre *vásárló*, *kereskedő*, *bank* ill. *hitelesítésszolgáltatóként* szokták emlegetni. Az általános modell a pénzügyi hálózat és a bizalmi fél összevonásával, a 2. ábrán látható módon egyszerűsíthető.



2. ábra. Egy leegyszerűsített, háromszereplős e-fizetési séma

A továbbiakban ez utóbbi modellt fogjuk kiindulásnak tekinteni, a formális ill. informális terminológiát pedig egymás szinonímájaként használjuk majd.

2.1. E-fizetési megoldások

Az elektronikus fizetési rendszerek megjelenési formája a mindennapokban meglehetősen sokszínű, ott vannak mindjárt a hitelkártyák, a bankkártyák vagy az elektronikus csekkek. Ahogy az összes digitális fizetési megoldás, úgy ezek is rendelkeznek három kritikus biztonsági szolgáltatással:[4]

[4] A második ill. harmadik szolgáltatást közösen hitelességként hivatkozhatjuk.

1. *bizalmas adatkezelés*

   Az üzenetek bizalmas kezelését végző (vagy másként adatvédelmet biztosító) szolgáltatás az érzékeny adatok elérését csak az arra jogosultak számára teszi lehetővé. Így megakadályozza, hogy lehallgatás útján az információ jogosulatlan személyek vagy folyamatok számára hozzáférhetővé váljon, és azt később rosszhiszeműen használják fel.

2. *authentikáció* (üzenetintegritás és partnerazonosítás)

   A továbbított információ integritásával, vagy *adatsértetlenséggel* kapcsolatos szolgáltatások az adatok jogosulatlan vagy véletlen megváltoztatásának kérdését kezelik. Ilyen lehet például az adatbeszúrás, adattörlés vagy adatmódosítás. A küldött üzenet sértetlenségének biztosítása érdekében a rendszernek alkalmasnak kell lennie az efféle jogosulatlan manipulációk azonosítására. Általuk a címzett meggyőződhet arról, hogy a fogadott adatokban idő közben nem történt változás.

   A *partnerazonosítást* garantáló szolgáltatásoknak köszönhetően a kommunikáló felek – egy időben a kommunikációs csatorna kiépülésével – minden kétséget kizáróan megbizonyosodhatnak egymás személyazonosságáról. Ez által a partnerek biztosak lehetnek abban, hogy a küldött ill. fogadott információk a kívánt helyre ill. helyről érkeznek.

   Authentikáció biztosításához a legkényelmesebb megoldást az ún. *nyilvános kulcsú infrastruktúrák* alkalmazása nyújtja (lásd 2.9. fejezetben).

3. *letagadhatatlanság*

   A letagadhatatlansággal kapcsolatos szolgáltatások meggátolják egy már végbement tranzakció későbbi letagadásának lehetőségét. Ezáltal a címzett megbizonyosodhat arról, hogy a feladó ily módon nem követhet el csalást, vagy legalábbis az ilyen visszaélésekből neki nem származhat kára.

A kártyás ill. csekkes megoldásokon kívül még jónéhány fizetési lehetőség áll a rendelkezésünkre elektronikus vásárlás esetén, ezek nagy hányada makro- és ún. *mikrotranzakciók*[5] esetén egyaránt használható (lásd [13]). Ahhoz, hogy megismerkedjünk ezen

[5]Leginkább webes tartalmak vásárlásához kötődő fogalom, ahol a felmerülő költségek viszonylag alacsonyak. Ilyen lehet például egy fizetős online magazin különálló cikkének letöltése.

rendszerek használata során felmerülő biztonsági problémákkal ill. a velük szemben támasztott elvárásokkal, tekintsük az online bankkártyás protokollt, és vegyük szemügyre néhány tulajdonságát.

(p_1) gyenge általános biztonságosság

Először is a számítógépes rendszerek nyitottságából ill. a kártyás authentikáció primitivitásából fakadóan a kártyaadatokhoz illetéktelenek is könnyedén hozzáférhetnek.

(p_2) szűk alkalmazhatóság

Bankkártyával történő fizetésre csak az arra jogosult, nagyobb online szolgáltatóknál van lehetőség.

(p_3) "magas" hozzáadott költség

Annak ellenére, hogy ez a fizetési mód általában relatíve kis pótlólagos költséggel jár, mikrotranzakciók esetén ez a költség összességében jelentős is lehet.

(p_4) anonimitás és *nyomonkövethetetlenség* hiánya

Végül a bank által kiállított nyugta további bizalmas információkat hordoz, melyek segítségével a kiállító meg tudja állapítani a vásárlás tárgyát, időpontját, összegét valamint az elfogadó és a vásárló személyét. Szigorú értelemben véve akkor mondunk anonimnak egy fizetési protokollt, ha tranzakció közben titokban marad az ügyfelek kiléte. Ám létezik olyan definíció, mely szerint az anonimitásról csak nyomonkövethetetlen protokolloknál beszélhetünk. Azaz a banknak soha (kivéve csalás esetén) nem szabad tudnia összekapcsolni az elköltött pénzt az azt elköltő ügyféllel. Mi a későbbiekben, ha mást nem mondunk, ez utóbbi definíciót fogjuk anonimitásként értelmezni.

Tekintve azt, hogy az elektronikus fizetési rendszerek különböző mértékben birkóznak meg a fent említett problémákkal (lásd 3. ábra), ez egyfajta csoportosításra ad lehetőséget:

(1) Bankkártya alapú rendszerek

A bankkártyaszám illetéktelen kezekbe való jutását elkerülve a normál kártyás tranzakció biztonsága növelhető. Az egyik első internetes fizetési szolgáltatást, melynek segítségével a kártyaszám helyett virtuális PIN-nel lehetett vásárolni a First Virtual vezette be 1994-ben. Habár ezzel egyidőben több online fizetési megoldás született,

bizonyos szempontból mégis egyedi volt: ez volt az egyetlen, mely nem használt titkosítást. A rendszer filozófiája szerint vannak olyan információk, melyek továbbíthatók interneten keresztül, és vannak, amik nem. Ez utóbbi kategóriába sorolja a kártyaszámot is. A protokoll működése:

(a) Az ügyfél regisztrál a First Virtual-nál, melynek eredményeként emailben megkapja számlájához tartozó személyes PIN-kódját. Ezután telefonon keresztül a cég rendelkezésére bocsátja kártyaadtait.

(b) Vásárlási szándék esetén az ügyfél a kapott PIN-kódot elküldi a kereskedőnek, aki opcionálisan leellenőrzi azt, majd fizetési tranzakciót kezdeményez a First Virtual-nál.

(c) A vásárló részére egy megerősítő email kerül kiküldésre.

(d) A rendszer értesíti a kereskedőt a vásárló visszajelzésének megfelelően.

(e) Pozitív válasz esetén, egy normál online banki tranzakciót követően megjelenik a pénz a kereskedő számláján. Természetesen ezzel párhuzamosan ugyanez az összeg levonásra kerül a vásárló számlájáról.

PROTOKOLL TÍPUSA	p_1	p_2	p_3	p_4
kártya alapú	✓	×	✓	×
csekk alapú	✓	✓	✓	×
készpénz alapú	✓	✓	✓	✓

3. ábra. Különböző e-fizetési rendszerek és tulajdonságaik

Mivel magát a kártyaszámot nem küldtük át a nyilvános hálózaton, így a rendszer eleget tesz az általános biztonságosság kritériumának, nem nyújt megoldást azonban a többi hiányosság kiküszöbölésére. A First Virtual által megvalósított szisztéma továbbfejlesztésének tekinthetők, az ún. *digitális P2P*[6] *fizetési protokollok*. A legelterjedtebb ilyen P2P rendszer a PayPal. A PayPal egy olyan internetes számlaszolgáltatás, ahová az ügyfelek hagyományos kártyás tranzakció útján tölthetik fel pénzüket, majd utalhatják át fizetés esetén a megvásárolni kívánt termék

[6]person-to-person: Olyan kommunikációs protokoll, mely a partnerek között közvetlen kapcsolatot biztosít, így nem igényli egy harmadik, közvetítő fél közrejátszását.

vagy szolgáltatás ellenértékeként. A vásárlókhoz hasonlóan az eladók is nyithatnak számlát, így a vevő fizetéskor ide utalhatja át a vételárat, melyet az eladó később átvezethet hagyományos folyószámlájára. A PayPal előnye, hogy a rendszeren belül szinte azonnal megtörténik a pénzmozgás. Így az eladó gyorsabban megkapja bevételét, következésképpen hamarabb juttathatja el az árut vagy szolgáltatást a vevő részére. Sőt a rendszer a különböző devizanemek közti átváltást is képes automatikusan elvégezni. Mindezen előnyök mellett az általános biztonságosság kritériuma változatlanul teljesül, hiszen egyrészt a vásárlónak elegendő feltöltésenként egyszer megadnia bankkártyájának adatait (nem kell minden vásárlásnál elküldenie azokat), másrészt a napjainkban elterjedt többi bankkártya alapú e-fizetési protokollhoz hasonlóan a PayPal is SSL[7]-csatornát használ a kommunikáció kiszolgálására, mely tovább fokozza a rendszer biztonságosságát. Ráadásul az alacsony pluszköltségeknek köszönhetően lehetőséget nyújt mikrotranzakciók lebonyolítására is. Ezek után nem meglepő, hogy a megszokott online kártyás tranzakció mellett a digitális P2P fizetés az egyik legfelkapottabb e-fizetési mód.

(2) Csekk alapú rendszerek

Elviekben a tranzakció módját tekintve a csekk közelebb áll a készpénzhez, mint a bankkártyához, hiszen bárki bárkinek adhatja. Ennek eredményeképpen született is jópár csekk alapú e-fizetési megoldás (CyberCash, NetCheck, etc.). A protokoll első lépéseként az ügyfél regisztrál egy tetszőleges banknál. Vásárláskor a kívánt termék kiválasztása után egy előzetesen bank által hitelesített digitális csekket állít ki a kereskedő "nevére", melyet elküld a kedvezményezettnek. A címzett ezt ellenőrzés céljából továbbküldi a banknak, mely pozitív válasz esetén jóváírja az összeget a kedvezményezett számláján. Ez a rendszer már tetszőleges szolgáltatónál elérhetővé tehető, sőt a némileg kisebb kezelési költség miatt elvileg mikrotranzakciók esetén is használható, azonban ez sem nyújt megoldást az anonimitás problémájára.

(3) Készpénz alapú rendszerek

A készpénz alapú rendszerek, vagy másképpen *digitális pénz protokollok* működése hasonló a csekk alapú megoldásokéhoz: a vásárló előzetesen számlát nyit egy digitá-

[7]Secure Socket Layer: A felhasználó kliensszámítógépe és egy távoli szerver közötti kommunikációs csatorna titkosítását végző protokoll.

lis pénz kiadásásra jogosult banknál, majd benyújtja elektronikus készpénz igényét az intézmény felé. A bank ezután a számláról levont pénzösszeg fejében elküldi ügyfelének hitelesített digitális fizetőeszközét, amit a vásárló fizetéskor elküld a kereskedőnek. Átvétel után a kereskedő elküldi a pénzt a banknak, mely a hitelesség ellenőrzés után a kedvezményezett számláján jóváírja a megfelelő összeget, vagy alternatív esetben digitális pénzt állít ki részére. Ez a protokoll a bankkártyás vásárlásnál megismert hiányosságok mindegyikét (p_1, p_2, p_3, p_4) kiküszöböli.

Habár az ebben a fejezetben bemutatott csoportosítás az egyik leggyakrabban alkalmazott kategorizálása az e-vásárlási protokolloknak, vizsgálhatjuk őket természetesen más aspektusból is, így például:

- *vásárolt termék típusa*: kézzel fogható eszköz, digitális termék vagy jog
- *terhelés és jóváírás módja*: bi-/multilaterális vagy közvetítő általi
- *földrajzi tagoltság*: belföldi vagy határon átnyúló
- *devizanemek száma*: egy- vagy többvalutás
- *tényleges fizetés ideje*: előre, közvetlenül vagy utólag fizetett
- *fizetés helye*: valós(F2F[8]) vagy virtuális
- *fizetés gyakorisága*: alkalmankénti(megtekintés után) vagy egyszeri(termékegységenként)
- *fizetés módja*: online vagy offline
- *számlainformáció elhelyezkedése*: szerver- vagy kliensoldali
- *tranzakciós partnerek viszonya*: B2B[9], B2C[10] vagy C2C[11] típusú

[8]face-to-face: A partnerek között szemtől szembeni kommunikációt igénylő protokoll.
[9]business-to-business: Az üzleti szektor képviselői közti e-ügyletek összessége.
[10]business-to-consumer: A vállalatok és a fogyasztók között megvalósuló e-kereskedelem.
[11]consumer-to-consumer: A végfelhasználók közötti elektronikus kereskedelem.

2.2. Digitális pénz protokoll

Egy 2000-ből származó európai uniós direktíva[12] szerint a digitális pénz nem más, mint egy a kibocsátó által igény alapján, egy nála nem kisebb értékű pénzösszeg átvételekor kiállított, a kibocsátótól különböző elfogadók által fizetőeszközként elfogadott, elektronikus eszközön tárolt monetáris érték.
Ahogy az az angol terminológiából (e-cash vagy digital cash) is következik, a digitális pénz a hagyományos, papír alapú pénzt hivatott helyettesíteni elektronikus környezetben, megtartva annak olyan előnyös tulajdonságait, mint:

- könnyű hordozhatóság
- egyszerű felismerhetőség (azonnali elfogadás vagy visszautasítás)
- átruházhatóság (ügyfelek között)
- anonimitás (és nyomonkövethetetlenség)
- felosztható ság (a pénz kisebb címletekre történő felosztása)

A fenti felsorolásból kiemelendő az anonimitás tulajdonsága, megvalósításának szükségessége ugyanis erősen megosztja a témában érdekelt feleket. Míg a digitális pénz protokollok fejlesztői számára elsődleges ezen előnyös jellemző megtartása, addig a napjaink financiális politikáját meghatározó vélemények aggályosnak tartják az anonimitás gazdaságjogi következményeit. Habár a pénzmosás ill. pénzhamisítás veszélye tetszőleges e-fizetési rendszer esetén fennáll, anonim protokolloknál ezek a rizikófaktorok hatványozottan vannak jelen. A pénzhamisítással (lásd 2.8. fejezet) ellentétben a pénzmosás és a digitális pénz gazdaságra gyakorolt hatása nem képezi a dolgozat tárgyát, ezen témákkal részletesen [10] foglalkozik.

A papír alapú készpénz fentebb felsorolt előnyei mellett természetesen minden digitális pénz protokoll eleget tesz olyan kritériumoknak, mint a bizalmas adatkezelés, authentikáció, letagadhatatlanság, nagyfokú általános biztonság és alacsony hozzáadott költség.

A digitális pénzt alkalmazó e-fizetési megoldások három alapvető rendszertevékénységet különítenek el:

[12] Az Európai Parlament és az Európai Tanács által 2000. szeptember 18-án elfogadott irányelv (2000/46/EC).

(1) *pénzfelvétel*, amikor az ügyfél a bank segítségével számlájáról pénzt helyez át digitális pénzt tároló eszközére

(2) *fizetés*, amikor az ügyfél digitális pénzét átadja a kereskedőnek

(3) *pénzbeváltás*, amikor a kereskedő digitális pénztárcájából pénzt helyez át folyószámlájára a bank közreműködésével

Nyilvánvaló, hogy a felsorolt tevékenységek sorrendje egy-egy konkrét tranzakción belül kötött.

Habár az első teljesen anonim és nyomonkövethetetlen protokoll már 1988-ban megszületett (David Chaum et al., [2]), az első ideális rendszer csak az 1991-es Crypto'91 konferencián került bemutatásra Tatsuaki Okamoto és Kazuo Ohta "Univerzális elektronikus pénz" című előadásán ([12]). Az általuk ideálisnak definiált rendszerrel szemben a következő követelményeket támasztották:

(1) *függetlenség*

A rendszer biztonsága nem függhet semmilyen fizikai feltételtől, ily módon a pénz akár számítógépes hálózaton keresztül is továbbítható.

(2) *biztonságosság*

A másolás (újrafelhasználás) ill. hamisítás lehetőségét ki kell zárni.

(3) *titkosság* (nyomonkövethetetlenség)

A felhasználó személyét el kell fedni, azaz a vásárló és a vásárlás közti kapcsolatot mindenki számára nyomonkövethetetlenné kell tenni.

(4) *offline fizetés*

Ha egy vásárló digitális pénzzel fizet a kereskedőnél, az eladó és a vevő közti protokollnak offline módon, harmadik fél közreműködése nélkül kell végbemennie. Ezzel szemben léteznek online rendszerek is, melyek esetén fizetéskor a kereskedőnek egy központi szolgáltatóhoz kell kapcsolódnia.

(5) *átruházhatóság*

Biztosítani kell a pénz ügyfelek közti átruházhatóságát.

(6) *feloszthatóság*

Egyetlen C értékű digitális pénz több részre osztható kell, hogy legyen úgy, hogy az

előállt, egyenként C-nél kisebb értéket képviselő darabok összértéke egyenlő legyen C-vel.

Vegyük észre, hogy online mód esetén a fizetés és a beváltás lépései nem feltétlenül különülnek el egymástól.

2.2.1. Pénzhamisítás

Ahogy minden pénzhez kötődő fizetési rendszernél, úgy digitális környezetben is történhetnek visszaélések a pénzügyi hálózat vagy a fizetési mechanizmus kijátszásával. Hasonlóan a valódi készpénzhez itt is két módja van a csalásnak[13]:

- *tokenhamisítás*: valósnak látszó pénz előállítása a bank megkerülésével
- *ismételt felhasználás*: ugyanannak a tokennek többszöri felhasználása

A hamisításhoz kapcsolódó visszaélésekkel szemben többféle védelmi mechanizmust alkalmazhatunk, melyekről részletesen a 2.8 fejezetben esik majd szó.

2.3. Digitális aláírás

Digitális pénz protokollok számára authentikációt legegyszerűbben digitális aláírás segítségével biztosíthatunk. Egy ilyen "elektronikus kézjegy" nem más, mint a hagyományos aláírás digitális analógja, azaz hasonlóan a kézzel írt változathoz egy dokumentum hitelességét hivatott biztosítani. Ezt elektronikus környzetben aszimmetrikus, vagy másképpen *nyilvános kulcsú kriptográfiát* alkalmazva érhetjük el. Aszimmetrikus kriptorendszerekben, melyek alapjait még az 1970-es évek közepén Whitfield Diffie és Martin Hellman munkássága teremtette meg, minden felhasználó rendelkezik egy titkos(privát) valamint egy nyilvános(publikus) kulccsal. Míg a titkos kulcs csak az azt generáló felhasználó (tulajdonos) számára elérhető, és üzenetek titkosítására ill. digitális aláírások előállítására szolgál, addig a kulcspár publikus részét bárki megtekintheti, és üzenetek dekódolására ill. digitális aláírások ellenőrzésére használjuk. A titkos kulcs egyik legfontosabb tulajdonsága, hogy – habár generálása vele együtt történik – nyilvános párjának ismerete nélkül

[13] A már említett letagadás is egy lehetséges módja a csalásnak, azonban az nem tartozik a pénzhamisítás kategóriájába.

az nem meghatározható, azaz a két kulcs egymásból nem számítható. A nyilvános kulcsú titkosítás működése egy olyan lakattal szemléltethető (lásd 4. ábra), amelynek két kulcslyuka van, egy-egy beleillő kulccsal. Ha a két kulcs közül az egyikkel zárjuk a lakatot, akkor az kizárólag annak párjával nyitható ki, azaz még a bezárást végző kulccsal sem.

4. ábra. Aszimmetrikus titkosítás
(Forrás: Netlock Kft.)

Titkosított üzenet küldéséhez a feladó levelét egy "ládába" helyezi, a láda lakatját pedig a címzett nyilvános kulcsával lezárja. Az így lezárt láda – azaz a titkos üzenet – csak a záró kulcs párjával, azaz a címzett titkos kulcsával nyitható. Ily módon egymást nem ismerő személyek között is létrejöhet biztonságos kommunikáció.

Digitális aláírás készítésekor a kulcsok használata fordított: aláírandó üzenetünket – saját – titkos kulcsunkat használva helyezzük a ládába, melyet a címzett (vagy bárki, aki hozzáfér) nyilvános kulcsunk segítségével kinyit, megbizonyosodva így arról, hogy az üzenetet olyasvalaki írta alá, aki rendelkezik a titkosított dokumentumot dekódoló publikus kulcs privát párjával. Ahhoz azonban, hogy egy hitelesített üzenetről meg tudjuk mondani, ki írta alá, nem elég rendelkeznünk az azt dekódolni képes nyilvános kulccsal, tudnunk kell azt is, hogy az adott publikus kulcs mely felhasználóhoz tartozik. Ez az ún. *kulcsmenedzselési probléma*, melynek megoldásához egyrészt valamilyen *authentikációs infrastruktúrára* (lásd 2.9. fejezet), másrészt megfelelő szintű lokális és hálózati biztonságra van szükség a nyilvános kulcsok védelme érdekében.

Az elektronikus aláírással szemben támasztott általános elvárások:

- egyetlen személy tudja csak létrehozni a rá jellemző aláírást úgy, hogy az ne legyen hamisítható vagy létrehozása után később letagadható
- legyen egyszerűen létrehozható és ellenőrizhető

- az aláírás olyan módon kapcsolódjon az eredeti dokumentumhoz, hogy az az aláírást követően már ne legyen észrevétlenül módosítható

A két leggyakrabban alkalmazott algoritmus a faktorizáció problémáján alapuló RSA[14] ill. a diszkrét logaritmus problémájára épülő DSA [15] protokoll.

Standard aláíró protokoll

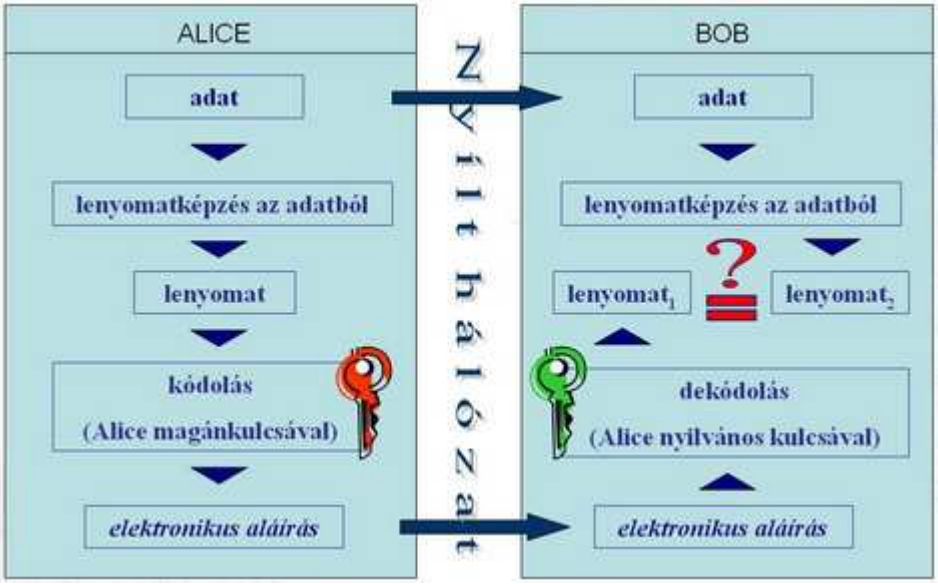
A gyakorlatban a digitális aláírása folyamata két lépésből áll: aláírás generálása, aláírás ellenőrzése. Az első fázisban elő kell állítanunk aláírásra szánt dokumentumunk *digitális ujjlenyomatát*. Ehhez számos biztonságos hash algoritmus[16] áll a rendelkezésünkre, így használhatunk például MD5-öt, RIPEMD-t vagy éppen SHA algoritmust. Közös jellemzője ezen függvényeknek az egyirányúság, azaz az általuk generált "lenyomat" vissza nem fejthető. Az adott hash algoritmus alkalmazása után a tényleges aláírás fázisa következik, amikor is az előállt lenyomatot privát kulcsunkat alkalmazva titkosítjuk. Üzenetváltáskor ezt az aláírt lenyomatot (vagy csak egyszerűen aláírást) juttatjuk el az eredeti dokumentum kíséretében a címzettnek. Végül az üzenet hitelességének ellenőrzése céljából a fogadó fél a megadott titkosító eljárás ill. nyilvános kulcs segítségével dekódolja az aláírást, majd ennek eredményét összehasonlítja a dokumentumon alkalmazott hash-algoritmus által generált értékkel. Ha a két érték megegyezik, a címzett biztos lehet abban, hogy a kapott dokumentumot az adott nyilvános kulcs titkos párjával írták alá. Azonban a kulcsmenedzselési probléma folytán továbbra is nyitott marad annak kérdése, hogy ez a publikus kulcs valóban a feladó személyéhez kötődik-e. A digitális aláírás folyamatát az 5. ábra szemlélteti.

A digitális aláírás egy speciális fajtája az ún. *egyszer használatos elektronikus aláírás*, mely – a hagyományos aláíró protokolltól eltérően – egyetlen üzenet egyszeri aláírására szolgál. Ez azt jelenti, hogy minden egyes aláírási folyamat megkezdése előtt új nyilvános kulcsot kell generálnunk. Az ellenőrzés elvégzéséhez szükséges nyilvános információkat ebben az esetben *érvényesítő paramétereknek* nevezzük. Egyszer használtos aláírások alkalmazása elsősorban intelligens kártyáknál előnyös, ahol a kis számítási teljesítmény

[14] Rivest-Shamir-Adleman protokoll: napjainkban a legelterjedtebb nyilvános kulcsú titkosító és aláíró protokoll.

[15] Digital Signature Algorithm: az Egyesült Államok Nemzetbiztonsági Hivatala által, kizárólag digitális aláírás előállítására kifejlesztett algoritmus.

[16] A kriptográfiában hash algoritmus alatt olyan transzformációt értünk, mely bemenetként tetszőleges méretű üzenetet fogad, kimenetként pedig egy fix hosszúságú karakterláncot állít elő.



5. ábra. A digitális aláírás folyamata
(Forrás: Netlock Kft.)

miatt kisebb, következésképpen kevésbé biztonságos kulcsokat használnak.

A vak aláírás protokollja

Az előzőekben bemutatott mechanizmusoktól eltérően vak aláírás esetén a küldő és az aláíró fél (közjegyző) személye különbözik. Emellett egy másik lényeges különbség az is, hogy a hitelesítő számára nem ismert az általa alárásra váró dokumentum konkrét tartalma. A protokoll váza a következő: az Ügyfél egy véletlenszám (*vaksági faktor*) segítségével felismerhetetlenné teszi az aláírásra szánt dokumentumot, majd az így előállt karakterláncot elküldi a Közjegyzőnek. A fogadó fél – annak tartalma ismerete nélkül – egyszerűen aláírja azt és visszaküldi a feladónak. Az Ügyfél eltávolítja a vaksági faktort, ezzel megkapja az eredeti dokumentum Közjegyző által hitelesített változatát.

2.4. A legegyszerűbb digitális pénz protokoll sémák

Elsőként két olyan e-fizetési séma kerül bemutatásra, melyek a standard protokollkövetelményeken felül nem tartalmaznak semmilyen hozzáadott ("kényelmi") funkciót. A bemutatott protokollokban – hasonlóan a később tárgyaltakhoz – a vevőt, eladót ill. bankot informálisan rendre Alice, Bob ill. Bank néven hivatkozzuk.

Protokoll$_1$(online)

Felvétel

(1) Alice jelzi a Bank felé digitális készpénzigényét.

(2) A Bank kiállítja a pénzt, majd aláírja.

(3) A Bank levonja Alice számlájáról a kért összeget és az ügyfél rendelkezésére bocsátja a fizetőeszközt.

Fizetés-Beváltás

(1) Alice átadja a pénzt Bobnak.

(2) Bob a *Bank* felé továbbítja a fizetőeszközt.

(3) A Bank ellenőrzi a pénzen aláírását.

(4) A Bank adatbázisában utána néz, hogy nem használták-e már a tokent.

(5) Megerősítésképpen a Bank kikeresi a pénzhez tartozó rekordot a pénzfelvételek listájában. (opcionális)

(6) A Bank beszúr egy újabb sort a felhasznált pénzek adatbázisába.

(7) A Bank jóváírja Bob számláján a megfelelő összeget, majd értesíti őt.

(8) Bob átadja a kért terméket Alicenak.

Megjegyzendő, hogy bank alatt a pénzügyi hálózat tetszőleges elemét érthetjük, mely pénzt bocsát ki ill. von ki a forgalomból. Ezáltal a beváltás fázisában a Bank szó épp úgy takarhat egyetlen, konkrét pénzügyi szolgáltatót, mint azoknak egy halmazát. Utóbbi esetben előfordulhat, hogy Alice és Bob különböző bankoknál rendelkeznek számlával, ami némiképp megbonyolítja a működést, hiszen a bankok között plusz információcserét igényel.

Protokoll$_2$(offline)

Felvétel

(1) Alice jelzi a Bank felé digitális készpénzigényét.

(2) A Bank kiállítja a pénzt, majd aláírja.

(3) A Bank levonja Alice számlájáról a kért összeget és az ügyfél rendelkezésére bocsátja a fizetőeszközt.

Fizetés

(1) Alice átadja a pénzt Bobnak.

(2) Bob leellenőrzi a Bank aláírását. (opcionális)

(3) Bob átadja a kért terméket Alicenak.

Beváltás

(1) Bob a Bank felé továbbítja a fizetőeszközt.

(2) A Bank ellenőrzi a pénzen aláírását.

(3) A Bank adatbázisában utána néz, hogy nem használták-e már a tokent.

(4) Megerősítésképpen a Bank kikeresi a pénzhez tartozó rekordot a pénzfelvételek listájában. (opcionális)

(5) A Bank beszúr egy újabb sort a felhasznált pénzek adatbázisába.

(6) A Bank jóváírja Bob számláján a megfelelő összeget.

2.5. Nyomonkövethetetlen digitális pénz protokoll sémák

A következőkben az imént bemutatott algoritmusokat igyekszünk úgy módosítani, hogy azok eleget tegyenek a nyomonkövethetetlenség feltételének. Ehhez nyújt segítséget a már ismertetett vak aláírás protokollja. Az ügyfél által előállított pénzt a bank vakon fogja aláírni, melyet az igénylő a vaksági faktor eltávolítása után tud majd hiteles fizetőeszközként használni. Ezáltal beváltáskor a PROTOKOLL$_1$ (5)-ös ill. PROTOKOLL$_2$ (4)-es pontja által megfogalmazott opcionális ellenőrzésre nincs többé lehetőség.

PROTOKOLL$_3$(online)

Felvétel

(1) Alice előállítja digitális készpénzét, majd egy véletlenszám segítségével olvashatatlanná teszi.

(2) Az így előállt token elküldésével Alice jelzi a Bank felé digitális készpénzigényét.

(3) A Bank vakon aláírja a tokent.

(4) A Bank elküldi az aláírt tokent és levonja Alice számlájáról a kért összeget.

(5) Alice a vaksági faktort eltávolításával olvashatóvá teszi pénzét.

Fizetés-Beváltás

(1) Alice átadja a pénzt Bobnak.

(2) Bob a Bank felé továbbítja a fizetőeszközt.

(3) A Bank ellenőrzi a pénzen láírását.

(4) A Bank adatbázisában utána néz, hogy nem használták-e már a tokent.

(5) A Bank beszúr egy újabb sort a felhasznált pénzek adatbázisába.

(6) A Bank jóváírja Bob számláján a megfelelő összeget, majd értesíti őt.

(7) Bob átadja a kért terméket Alicenak.

PROTOKOLL$_4$(offline)

Felvétel

(1) Alice előállítja digitális készpénzét, majd egy véletlenszám segítségével olvashatatlanná teszi.

(2) Az így előállt token elküldésével Alice jelzi a Bank felé digitális készpénzigényét.

(3) A Bank vakon aláírja a tokent.

(4) A Bank elküldi az aláírt tokent és levonja Alice számlájáról a kért összeget.

(5) Alice a vaksági faktor eltávolításával olvashatóvá teszi pénzét.

Fizetés

(1) Alice átadja a pénzt Bobnak.

(2) Bob leellenőrzi a Bank aláírását. (opcionális)

(3) Bob átadja a kért terméket Alicenak.

Beváltás

(1) Bob a Bank felé továbbítja a fizetőeszközt.

(2) A Bank ellenőrzi a pénzen aláírását.

(3) A Bank adatbázisában utána néz, hogy nem használták-e már a tokent.

(4) A Bank beszúr egy újabb sort a felhasznált pénzek adatbázisába.

(5) A Bank jóváírja Bob számláján a megfelelő összeget.

Vegyük észre, hogy a Bank a pénzfelvétel (3)-as lépésében nem tudhatja, hogy az általa aláírt pénz címlete megegyezik-e az Ügyfél által kért összeggel, így az Ügyfél könnyedén csalhatna. Ezt kizárandó két lehetőségünk van:

(1) Rögzítjük a pénzfelvétel lehetséges címleteit, és minden egyes összeghez külön titkos kulcsot rendelünk. Így a Bank a (3)-as lépésben mindig az aktuális igénynek

megfelelő kulccsal ír alá. Ez a módszer nem zárja ki a csalást, de – online és offline módban egyaránt – leleplezi a csalót még a tranzakció lezárás előtt (az aláírás ellenőrzésekor).

(2) Alice digitális készpénz igényének jelzése előtt az (1)-es pontban ne egy, hanem rögtön m darab pénzt állítson elő ugyanazokkal a paraméterekkel. Majd a (2)-es pontnak megfelelően továbbítsa az összeset a Bank felé. A Bank véletlenszerűen válasszon ki $m-1$ darab tokent, és kérje meg Alice-t, hogy tegye olvashatóvá őket. A címletek ellenőrzése után a Bank írja alá az egyetlen még olvashatatlan tokent, és ezt küldje vissza Alice-nak. Ez esetben Alice-nak van esélye a csalásra anélkül, hogy lelepleződne, ám ennek valószínűsége mindössze $1 : m$. Így kellően magas m ill. kellően szigorú büntetés megválasztásával a csalás esélye minimalizálható.

2.6. Anonim digitális pénz protokoll sémák

A vásárló és a kereskedő szempontját tekintve az ideális az lenne, ha – teljesen anonim módon – a fizetés során mindkét fél kiléte titokban maradna. Ez azonban kizárná annak lehetőségét, hogy az ügyfél a kereskedő által hitelesített(aláírt) számlát kapjon a vásárlásról. Így kénytelenek vagyunk pusztán a vásárló anonimitására fókuszálni. Online esetben nincs további teendőnk, hiszen $\textsc{Protokoll}_3$ változtatás nélkül eleget tesz az anonimitás feltételeinek. Ellenben egy anonim offline protokoll megvalósítása nem várt problémákat vet fel: ha a kereskedő egy már beváltott tokent küld el a banknak, akkor azt a bank rögtön észreveszi, azonban éppen az anonimitás miatt nem fogják tudni, hogy ki próbált ily módon csalni. A protokollnak ennek ellenére biztosítania kellene a csaló leleplezését úgy, hogy a szabályokat betartó ügyfelek anonimitása ne sérüljön. A megoldás olyan azonosító információ beépítése a tokenbe, melynek darabjait a pénz előállításakor az ügyfél generálja olyan módon, hogy a darabok egyenként ne fedjék fel személyét, azonban bármelyik kettő elegendő legyen azonosításához. A kriptográfiában ezt az eljárást *titokmegosztásnak* nevezik. A pénzfelvétel fázisában a bank az információ tartalmának ismerete nélkül ellenőrzi annak meglétét és azt, hogy ténylegesen az ügyfélhez köthető-e. Fizetéskor egy ún. *Challenge/Response protokoll*[17] szerint ennek az infromációnak egy darabját kell felfednie az

[17] A magyar irodalmakban még "kihívás/válasz" eljárásként is ismert.

ügyfélnek úgy, hogy a kereskedőtől kapott véletlenszámra, azaz a kihívásra válaszként a véletlen(nonce) által meghatározott információszeletet küldi vissza a feladónak. Mivel a felfedéshez szükséges ismeretekkel csak a pénz előállítója rendelkezik, így azt felhasználni is csak a tulajdonos tudja. Beváltáskor a pénzzel együtt az azonosító információ is eljut a bankhoz. Ha a tulajdonos egyszer használta fel pénzét, a bank képtelen őt azonosítani (egyetlen rendelkezésre álló információdarab lévén). Ismételt fizetés esetén viszont a két tokenen nagy valószínűséggel két különböző információdarab lesz olvasható, melyek együttesen fel fogják fedni a csaló kilétét. A tettes minden bizonnyal a pénz előállítója lesz, hiszen fizetni – így csalni is – csak ő képes vele.

Protokoll$_5$(offline)

Felvétel

(1) Alice az őt azonosító információk beépítésével előállítja digitális készpénzét.

(2) Egy véletlenszám segítségével Alice olvashatatlanná teszi pénzét.

(3) Az így előállt token elküldésével Alice jelzi a Bank felé digitális készpénzigényét.

(4) A Bank ellenőrzi az azonosító információ meglétét.

(5) A Bank vakon aláírja a tokent.

(6) A Bank elküldi az aláírt tokent és levonja Alice számlájáról a kért összeget.

(7) Alice a vaksági faktort eltávolításával olvashatóvá teszi pénzét.

Fizetés

(1) Alice átadja a pénzt Bobnak.

(2) Bob leellenőrzi a Bank aláírását.

(3) Bob elküld Alice-nak egy véletlenszámot (kihívás).

(4) Alice visszaküldi az azonosító információ egy meghatározott szeletét. (válasz)

(5) Bob ellenőrzi a kapott választ.

(6) Bob átadja a kért terméket Alicenak.

Beváltás

(1) Bob a Bank felé továbbítja a fizetőeszközt (a véletlenszámmal és az arra kapott válasszal együtt).

(2) A Bank ellenőrzi a pénzen aláírását.

(3) A Bank adatbázisában utána néz, hogy nem használták-e már a tokent.

(4) A Bank beszúr egy újabb sort a felhasznált pénzek adatbázisába (tárolva a véletlenszámot és az arra kapott választ is).

(5) A Bank jóváírja Bob számláján a megfelelő összeget.

Figyeljük meg, hogy az anonimitás miatt – az előző offline sémákkal szemben – fizetéskor Bob nem hagyhatja ki a Bank aláírásának ellenőrzését, azaz a (2)-es lépést. Hiszen csak így lehet biztos abban, hogy nem éri őt kár, tudniillik vagy megkapja valódi digitális pénzét vagy megismeri a csalni szándékozó Alice identitását.

2.6.1. Az azonosító információ beépítése

Ahogy arra már az előző protokoll is rávilágított, az azonosító információ elhelyezése és kezelése kulcsfontosságú szerepet tölt be anonim e-fizetési sémák esetén. Most nézzük meg, milyen módszerek jöhetnek szóba az azonosító információ beépítésére, és így az ismételt fizetés kiszűrésére.

Vágás és kiválasztás (Cut and Choose)

Alice a pénz előállításával egyidőben legenerál k darab (ahol k kellően nagy ahhoz, hogy egy 2^{-k} valószínűségű esemény gyakorlatilag soha ne következhessen be) rendezett számpárt úgy, hogy tetszőlegesen kiválasztva közülük egyet, az felfedje Alice identitását, de az össze nem tartozó darabok használhatatlanok legyenek. A számpárok pénzen történő elhelyezése után Alice a – már ismert módon olvashatatlanná tett – fizetőeszközt elküldi a Banknak. A Bank vakon leellenőrzi a k darab számpár meglétét valamint azt, hogy az egyes számpárok rendelkeznek-e a szükséges tulajdonsággal.

Amikor Alice fizetni szeretne Bobnak, Bob kihívásként egy k hosszúságú random bitsorozatot küld Alicenak. Az egyes biteknek megfelelően Alice felfedi a számpárok valamelyik tagját. Ha például a `0110...` sorozatot kapja, akkor az első pár első, a második pár második, a harmadik pár második, a negyedik számpár első (és így tovább) tagját kell felfednie.

Amennyiben Alice ismételten fizetni akar a pénzzel, másodszor is kap egy kihívást. Mivel minden egyes kihívás egy véletlen bitsorozat elküldését jelenti, az új karakterlánc minimum egy pozícióban meg fog egyezni a régivel. Így Alice kénytelen felfedni legalább

egy számpár eddig nem ismert felét. Amikor a Bank újból megkapja a pénzt rajta az újonnan olvashatóvá tett azonosító információ részekkel, veszi az előző beváltáskor felfedett darabokat, és az első összeillő pár alapján megfejti Alice személyazonosságát.

Habár a vágás és kiválasztás módszere a lehető legegyszerűbb megoldása a problémának, az egyes tokenekhez hozzáadott $2k$ darab relatíve nagy szám miatt sajnos a legkevésbé sem mondható hatékonynak.

Nullaismeretű bizonyítás (Zero-Knowledge Proof)

Nullaismeretű bizonyítás alatt tetszőleges aszimmetrikus kriptográfiai protokollt érthetünk, melynek segítségével a konkrét (titkos) adatok felfedése nélkül tudjuk bizonyítani, hogy a szóban forgó információ a birtokunkban van. Természetesen az sem megengedhető, hogy a bizonyítás által egy esetlegesen rossz szándékú partner számára megkönnyítsük a bizalmas információ kitalálását. Ez a módszer szintén alkalmazható azonosító információ beépítésekor. Ekkor a pénzgenerálás fázisában Alice a tokennel együtt létrehoz egy aszimmetrikus kulcspárt is, ahol a titkos kulcs az ő identitását takarja. A Bank ellenőrzéskor a kapott nyilvános kulcs segítségével bizonyosodik meg arról, hogy a kulcs Alice-nél lévő titkos párja valóban az előállító személyazonosságát fedi-e. Fizetéskor Alice a pénzzel együtt a hozzá tartozó nyilvános kulcsot is átadja Bobnak, majd egy nullaismeretű bizonyítással igazolja, hogy rendelkezik a kulcspár privát felével. Amennyiben ismételt fizetéskor Alice – válaszként egy újabb kihivásra – egy újabb bizonyítást küld, úgy az új és a régi válasz együttesen, a titkos kulcson keresztül fel fogja fedni a Bank számára a csaló identitását.

2.7. Átruházhatóság megvalósítása

Ahogy már arról szó esett, egy ideális e-fizetési rendszerben biztosítanunk kell digitális pénzünk ügyfelek közti átruházhatóságát. A pénzátadásnak ezt a módját az különbözteti meg a fizetéstől, hogy míg utóbbit mindenképpen a pénz beváltása követi, addig átruházás esetén az új tulajdonos három lehetőség közül is választhat:

- felhasználja pénzét fizetési kötelezettségei rendezésére,
- beváltja a tokent, így jóváiratva az összeget számláján,
- továbbadja a fizetőeszközt (újbóli átruházázás).

Egy digitális pénz protokoll akkor teljesíti az átruházhatóság követelményét, ha a rendszerben tokenenként legalább egy átruházás megengedett. A pénz továbbadásának ez a módja offline rendszereknél lenne igazán előnyös, hiszen ez nagyban lecsökkentené az ügyfél és a bank közti interakciók számát (amennyiben maga az átruházás nem igényli a bank beavatkozását). Annak, hogy a szakirodalmak kevés figyelmet fordítanak ezen előnyös tulajdonság megvalósítására, az egyik legfőbb oka a pénz méretének korlátossága. Az ismételt felhasználás – fizetés vagy átruházás – kiszűrése ugyanis a pénz méretének folyamatos növekedését vonja maga után, hiszen a csaló kézrekerítéséhez rögzítenünk kell a tulajdonos azonosító információit. Mivel ez a méretnövekedés offline esetben elkerülhetetlen (lásd [18]), nem engedhetjük a pénz tetszőleges sokszori továbbadását, azaz a tokenméret maximumának megfelelően korlátoznunk kell a tokenek átruházásának a számát.

Az átruházással kapcsolatban felmerül egy másik probléma is: a beváltás pillanatáig a bank rendelkezésére álló egyetlen információ a pénzt felvevő személy identitása. Az összes többi – köztes – tranzakció csak a beváltás után, a pénz mindenkori tulajdonosainak bevonásával rekonstruálható. Ez ugyanaz a probléma, amit – tranzakciós rekordok híján – a hagyományos készpénz vet fel a pénzmosással ill. adócsalással kapcsolatban (lásd [10]). Ráadásul minden egyes továbbadás késlelteti az újrafelhasznált pénz detektálását, hiszen az csak akkor lehetséges, ha ugyanazon token mindkét kópiája végül a beváltás fázisához ér. Ekkor már viszont lehet, hogy túl késő lesz a bűnös előkerítésére. A hamis pénz élettartamának növekedésével ráadásul az azt elfogadó károsultak száma is nő. Így offline rendszereknél ez a kései detektálás nem elegendő a probléma megoldásához, további, fizikai biztonsági védelemre van szükség (lásd 2.8.1. alfejezet).

2.8. Biztonsági kérdések

Először nézzük, miként és milyen beépített eszközökkel védekezhetünk a már tárgyalt visszaélésekkel szemben: az egyik és inkább preferált módszer a *megelőzés*, a másik a csaló utólagos *leleplezése*. Míg ideális esetben elegendő lenne bíznunk a tárolóeszköz valamint a kommunikációs csatorna biztonságosságában, addig publikus hálózati viszonyok esetén a pénzhamisítás ellen további biztonságot fokozó technikák alkalmazása szükséges:

- tokenhamísítás

A csalás ezen fajtájával szemben a már említett authentikáció (ügyfélazonosítás és üzenetintegritás) biztosítása nyújthat védelmet.

- ismételt felhasználás

  Az újrafelhasználást megakadályozandó – a korábban bemutatott protokollsémákhoz hasonlóan – egy *banki adatbázist* kell létrehoznunk, ahol a már felhasznált fizetőeszközöket tároljuk. Ezen felül egy esetleges fizetésenkénti maximális összeghatár bevezetése tovább fokozhatja a rendszer biztonságosságát, hiszen így korlátozni tudjuk a kereskedő veszteségét visszélés esetén. Ez persze nem akadályozza meg a csalót abban, hogy egy viszonylag alacsony értékkel bíró tokent különböző helyeken tetszőlegesen sokszor felhasználjon.

Online rendszereknél a fentiek elégséges feltételei a megelőzésnek, offline esetben viszont vagy a csalás utólagos detektálásra vagy valamilyen fizikai védelmet biztosító eszközre hagyatkozunk. Míg előbbi passzív módon, leleplezés útján, addig utóbbi megelőzéssel próbál gátat szabni a visszaéléseknek.

2.8.1. Ismételt felhasználás elleni offline védelem

Az újrafelhasználással szembeni védekezés legprimitívebb formájának, vagyis a csaló utólagos leleplezésének módszereiről már esett szó, tekintsük most tehát, milyen lehetőségeink vannak a megelőzés terén. A fizikai védelemről lévén szó, kézenfekvő megoldásnak tűnhetnek az ún. "befolyásolásbiztos" kártyák, melyeket alkalmazva a tokeneket első felhasználásuk után letilthatnánk, de akár törölhetnénk is. Sajnos a valóságban száz százalékig befolyásolhatatlan eszközök nem léteznek, így a befolyásolásnak leginkább ellenálló intelligens kártyákra kell szorítkoznunk.

Intelligens kártyák alkalmazása

Az intelligens kártyák egyik legfőbb tulajdonsága, hogy tartalmuk fizikai kialakításuknak köszönhetően nem, pontosabban csak nagyon nehezen módosítható. Ezáltal az esetek legnagyobb hányadában megakadályozható a csalás, egy átlagember ugyanis nem rendelkezik a kártya befolyásolásához szükséges eszközökkel. Természetesen még intelligens kártyák használata mellett sem maradhat el a szoftveres kriptográfiai védelem, mivel rendszerünknek akkor is védettnek kell lennie a pénzhamisítással szemben, ha a kártya a

tartalmát valamilyen úton mégiscsak módosítani tudták. Az intelligens kártyák továbbá megnehezítik a bűnözők abbéli szándékát, hogy a kártyatulajdonos bizalmas adataihoz hozzáférjenek.

Pénztárca obszerverek

Az intelligens kártyák alkalmazásának egyetlen hátulütője, hogy a felhasználónak – lévén, nincs mód a kártyán áthaladó információk monitorozására – teljes mértékben meg kell bíznia az alkalmazott eszköz biztonságosságában. Így elképzelhető, hogy a tulajdonos tudta nélkül bizalmas információk hagyják el a készüléket. Chaum és Pedersen [19]-ben felvetette egy az intelligens kártyákhoz hasonlóan biztonságos chip olyan külső modulba (például mobiltelefonba) történő beágyazásának ötletét, melyet a felhasználók egyszerűen felügyelhetnek. Ez által a kártya nyújtotta előnyöket úgy lehet kihasználni, hogy nem kell feltétlenül megbíznunk annak hibátlan működésében. A külső ill. belső modult együttesen elektronikus pénztárcának, magát a beépített chipet pedig obszervernek nevezik. Az obszervert érintő minden kimenő és bejövő információ áthalad a külső modulon, így biztosítva a monitorozás lehetőségét. A külső modul szintén támaszkodik az általa beágyazott chipre, hiszen annak közreműködése nélkül nem képes tranzakciók végrehajtására. Ez az, ami lehetővé teszi a pénz többszöri felhasználásának megakadályozását. Chaumot és Pedersent követően Brands valamint Ferguson is az obszerveres megoldást ajánlotta saját digitális pénz protokolljának védelmére. Mivel a kettő közül Ferguson módszere egy kevésbé hatékony megoldás, tekintsük inkább Brands sémáját. Az obszerver nélküli alaprendszerben Brands a titkos kulcsok tokenbe való beágyazását javasolja. Fizetéskor az ügyfél ezt a privát kulcsot használva képes válaszolni a kedvezményezett kihívására, aki a válasz ellenőrzése után dönt a token elfogadásáról vagy annak visszutasításáról. Ezzel szemben az obszerveres változatban a titok az ügyfél és az obszerver között megosztva kerül tárolásra. Ez az összetett titok, vagyis az egyes titokszeletek moduláris összege szükséges egy kihívás megválaszolásához. Így fizetéskor érvényes válasz küldéséhez a vásárlónak és az obszervernek együtt kell működnie, mégpedig olyan módon, hogy se a vásárlónak se az obszervernek ne kelljen felfedni saját titkát a másik előtt.

Mivel az obszerver képes az ügyfél által végrehajtott összes tranzakció rögzítésére, így alkalmazása kézenfekvő lehet nyomonkövetéskor. Ez persze azt feltételezi, hogy a bank,

vagy bárki, aki a nyomonkövetést végzi valahogyan hozzáférjen magához az obszerverhez, és analizálni tudja annak tartalmát.

2.8.2. Lehetséges hibaforrások

Bármely kriptorendszernél, így e-fizetési protokollok esetén is fennáll a rendszerhiba lehetősége. Ez digitális pénzt alkalmazó rendszerekben nagy mértékben megnövelheti a pénzhamisítás lehetőségét. A hibák mögött számos biztonságot befolyásoló tényező állhat. Az egyik és legsúlyosabb problémát az jelentheti, ha maga a kriptográfia protokoll vagy a mögötte álló matematikai háttérapparátus nem nyújtja a kívánt biztonságot[18]. Ez lehetővé tenné ugyanis, hogy valaki valósnak látszó pénzt állítson elő anélkül, hogy ismerné az illetékes bank titkos kulcsát. Sőt hasonló módszerrel az illető akár érvényes privát kulcsot is generálhat a bank adatbázisának feltörése nélkül. Ez azt jelenti, hogy bárki, akinek tudomása van a rendszernek erről a gyengepontjáról, létrehozhat olyan tokent, melyet semmi nem különböztet meg a legitim bank által kiadottaktól.

Egy másik súlyos probléma a protokollsémát megvalósító konkrét implementációnak a hibáiból eredhet. Vegyük például azt az esetet, amikor az alkalmazott véletlenszámgenerátor működése nem megfelelő. Ekkor ugyanis elképzelhető, hogy valaki meg tudja mondani, mi lesz a következő, generátor által előállított random érték. Ezt a tudást – rosszhiszeműen – felhasználva az illető új titkos kulcsot generálhat, ami az előző rendszerhibához hasonlóan visszaélésekhez vezethet.

Tegyük fel, hogy mind protokollsémánk mind pedig az azt megvalósító implementáció helyesen, a tőle elvárt biztonságot szolgáltatva működik. Ebben az esetben még mindig fennáll a rendszer fizikai veszélyeztetettsége. Fizikai rendszerhibáról beszélhetünk például akkor, ha egy hacker, tolvaj vagy akár egy rossz szándékú banki alkalmazott hozzáférést szerez az ügyfelek titkos kulcsának nyilvántartásához, majd a számlatulajdonosok identitása alatt pénzt állíttat elő a bankkal. Ezzel a módszerrel azonban nem csak az ügyfeleket tudják megkárosítani, hiszen a banki privát kulcs megszerzésével – a bank nevében – is képesek lehetnek jogosulatlan pénz kiállítására. A fizikai beavatkozás egy következő szintje lehet magának a banki szoftvernek a befolyásolása, mely által mesterséges biztonsági rések

[18] A dolgozatban ismertetett protokollok esetén (ma még) nem tudunk ilyenről.

képezhetők.

Az említett biztonsági problémák a fizetési rendszeren túl az authentikációs infrastruktúra kapcsán is felmerülnek. Ahogy az e-kereskedelem tetszőleges formája, úgy az e-fizetés is nagy mértékben függ az ügyfelek authentikációs mechanizmusokba vetett bizalmától. Ha például egy támadó képes meghamisítani az infrastruktúra hitelesítésszolgáltatójának digitális aláírását, akkor az elbizonytalanítaná a feleket abban a meggyőződésükben, hogy az alkalmazott azonosítási technika kellően megbízható. Így a hitelesítésszolgáltató biztonsági mechanizmusainak megtervezésekor ugyanolyan körültekintően kell eljárnunk, mint a bank esetében.

2.8.3. A rendszerhibák következményei

Rendszerhiba bekövetkeztekor a legsúlyosabb következménye az anonimitás tulajdonságának van, ez gátolja meg ugyanis a bankot abban, hogy össze tudja rendelni az ügyfelek által felvett és a kereskedők által már beváltott pénzeket. Így lehetetlenné teszi a valódi és hamis pénzek megkülönböztetését rendszerhiba esetén. Mivel még maga a bank sem ismeri fel az általa kibocsátott tokeneket, elképzelhető, hogy a pénzhamisításra egészen addig nem derül fény, még észre nem veszik, hogy a beváltott pénzek összeértéke meghaladja a kiadottakét. Sajnos ekkorra már a bank veszteségei elég súlyos méreteket ölthetnek. Sőt amennyiben a bank rájön, hogy titkos kulcsa illetéktelen kezekbe került, még mindig nem fogja tudni kiszűrni a hamis pénzeket. Az egyetlen megoldás az, ha lecseréli a tokenek generálásához használt kulcspárt, majd érvényteleníti a régi kulccsal aláírt fizetőeszközöket. Ekkor a még fel nem használt tokeneket beválthatja, de a már elköltött pénzek valódisága nem dönthető el az ügyfél közreműködése nélkül. Ennek egyrészt a nyomonkövethetetlenség, másrészt az anonimitás az oka, míg előbbi csak a bankot akadályozza meg az vásárló azonosításában, addig utóbbi a kereskedő számára is lehetetlenné teszi azt. Az okozott kár minimalizálása érdekében célszerű bizonyos időközönként (vagy egy meghatározott kiadott token darabszámot elérve) lecserélni a bank nyilvános ill. titkos kulcsát. Ezáltal persze némileg sérülni fog a vásárlók anonimitása, hiszen így nem kívánt módon leszűkítjük egy adott pénzbeváltáshoz tartozó pénzfelvétel lehetséges halmazát (és vice versa).

2.9. Nyilvános kulcsú infrastruktúra alkalmazása

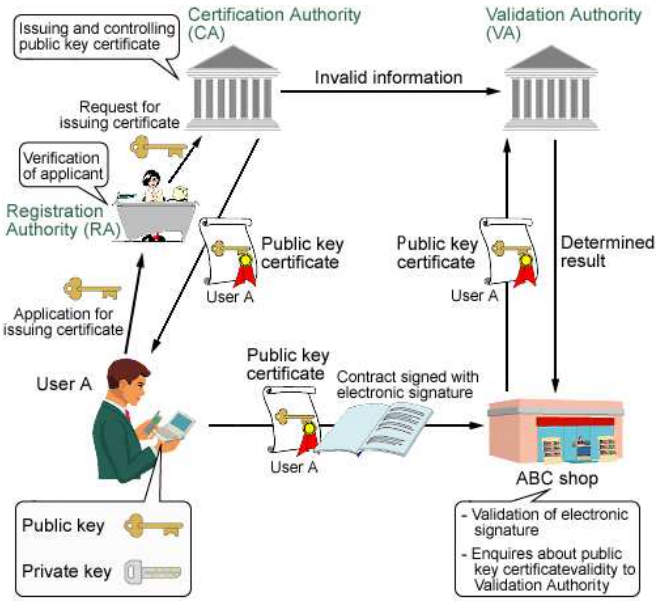
Ahogy az már említésre került, a nyilvános vagy más szóval publikus kulcsú infrastruktúrák szorosan kapcsolódnak az aszimmetrikus kriptográfiát alkalmazó rendszerek authentikációs szolgáltatásaihoz (üzenetintegritás és partnerazonosítás). Egy aszimmetrikus kriptorendszerben authentikáció megvalósításához biztosítanunk kell, hogy az egyes szereplők nyilvános kulcsát hitelt érdemlő módon ismerhessék meg a vele kommunikálni szándékozó partnerek. Habár a szereplők személyes találkozásakor elviekben megoldható lenne a nyilvános kulcsok kicserélése, ez az üzleti életben, ahol a piaci szereplők nem feltétlenül ismerik egymást, nehezen kivitelezhető. Arra azonban van mód, hogy a nyilvános kulcsokat elektronikus formában küldjék el egymásnak, vagy egy adatbázisból letöltsék azokat. Ekkor viszont számolnunk kell annak veszélyével, hogy nyílt kommunikációs csatornát alkalmazva a kulcsot rosszhiszeműen módosítják. A kulcs manipulációja elleni védekezés egyik leghatékonyabb formája az, ha az adott személy azonosítóinformációit (név, cím, etc.) és nyilvános kulcsát egy mindenki által megbízhatónak tartott harmadik fél elektronikus dokumentumban rögzíti, majd saját titkos kulcsát felhasználva aláírja azt. Ez a digitális aláírás zárja ki annak lehetőségét, hogy valaki észrevétlenül módosíthassa a dokumentumban rögzített adatokat. Az ilyen módon és tartalommal előállított dokumentumot *tanúsítványnak*, még az azt kiadó bizalmi felet *tanúsítványkiadónak* (CA), vagy egzaktabb módon hitelesítésszolgáltatónak nevezzük. Ahhoz, hogy egy CA tanúsítányokat adhasson ki, előbb meg kell bizonyosodnia a tanúsítványban rögzíteni kívánt azonosító információk hitelességéről. Ennek ellenőrzését valamint a felhasználók regisztrációját a tanúsítványkiadó egy általa is megbízhatónak tartott TTP-re, a *regisztrációs szervezetre* (RA) bízza. A létrehozott tanúsítványokat a CA egy, a nyilvánosság számára elérhető *tanúsítványtárban* tárolja, melyen keresztül a felhasználók hozzáférhetnek egy adott tanúsítvány státuszához. Komplexebb PKI hálózatokban előfordul, hogy a tanúsítványtárhoz való hozzáférést korlátozzák, és a tanúsítványok státuszának lekérdezését csak egy újabb TTP-n, a validációs szervezeten (VA) keresztül teszik lehetővé. Ekkor a felhasználó az authentikáció során elküldi a kérdéses tanúsítványt a VA-nak, mely válaszként megadja annak érvényességét. A CA-k tevékenysége azonban nem korlátozódik a tanúsítványok kiadására. Tegyük fel, hogy egy felhasználó elveszíti titkos kulcsát vagy az bármilyen más

módon illetéktelen kezekbe kerül, azaz kompromittálódik. Ekkor a titkos kulcsot jogosulatlanul birtokló személy a valódi tulajdonos identitása mögé bújva, hiteles módon készíthet digitális aláírást. Ezt rosszhiszeműen felhasználva az illető akár hivatalos ügyekben is eljárhat az eredeti tulajdonos nevében. Az ilyesféle visszaéléseket megelőzendő kézenfekvőnek tűnik a tanúsítvány használatának azonnali letiltása vagy visszavonása. Ezt a hitelesítésszolgáltatók ún. *visszavonási listák* (CRL) kezelésével oldják meg. A CRL nem más, mint egy a CA által digitálisan aláírt lista az érvényüket vesztett tanúsítványokról és azok visszavonásának időpontjáról. A listára kerülés lehetséges okai a következők:

- lejár a tanúsítvány érvényességi ideje
- a tanúsítványt birtokló felhasználó titkos kulcsa kompromittálódik
- a tanúsítványt kiállító CA titkos kulcsa kompromittálódik
- a regisztrált felhasználó töröltetni kívánja magát akár az RA, akár a CA nyilvántartásából

A nyilvános kulcsú infrastruktúrát alkalmazó protokollok partnerazonosítás során előbb az aláíráson keresztül megvizsgálják magának a tanúsítványnak a hitelességét, majd megbizonyosodnak arról, hogy az nem szerepel a tanúsítványkiadó CRL-jén. Hiteles aláírás elfogadásához elegendő az is, ha egy CRL-en lévő tanúsítvány visszavonási időpontja későbbre datálódik a digitális aláírás keletkezésének időpontjánál. A visszavonást megelőzően aláírt dokumentumok azonban a továbbiakban is hitelesek maradnak. Ebből is látható mekkora jelentőséggel bír a tanúsítványvisszavonás ill. digitális aláírás időpontjának pontos és hiteles rögzítése. A hangsúly ebben az esetben is a hitelességen van. Vegyük pédául azt az esetet, amikor az aláírás időpontját egyszerűen az aláírást végző személy írja bele a dokumentumba. Ekkor nyilvánvalóan fennáll a veszély, hogy akár jóhiszeműen, akár rossz szándékból az illető által helytelen időpont kerül rögzítésre. Ennek számos oka lehet: előfordulhat, hogy egyszerűen csak rosszul jár az órája, de az is lehet, hogy a csaló így próbálja meg visszadátumozni az aláírást arra az időpontra, amikor még érvényes volt az azóta már visszavont tanúsítvány. A megoldást természetesen egy újabb TTP alkalmazása nyújtja: az *időbélyeg-szolgáltatóé* (TSA). Egy protokoll szereplőinek a TSA-ra úgy kell tekintenie mint egyetlen hiteles időforrásra a rendszerben. Egy TSA által kiadott

hiteles *időbélyeg* nem más, mint egy az időbélyeg-szolgáltató órája szerinti pontos időt tartalmazó, annak digitális aláírásával hitelesített dokumentum. Egy TSA működésének megbízhatósága feltételezi, hogy soha nem kerül kibocsátásra időbélyegző olyan időpontról, ami még nem múlt el. Az időbélyeg-szolgáltató tehát lehetővé teszi, hogy egy felhasználó dokumentumába időbélyeget helyezve, majd azt aláírva, a későbbiekben bizonyítani tudja, hogy ő a szóban forgó dokumentumot ez után az időpont után írta alá. Azt, hogy egy dokumentum egy adott időpont előtt létezett, csak úgy lehet garantálni, ha a már aláírt dokumentumot maga a TSA is aláírja az időbélyeg elhelyezését követően.
A tanúsítványkiadás ill. validálás menetét illusztrálja a 6. ábra.



6. ábra. Tanúsítványok kezelése PKI-ban

Látható, hogy a fentiekben vázolt, nyilvános kulcsú titkosításon alapuló rendszer működéséhez komoly háttérinfrastruktúra szükséges. Ezen háttérinfrastruktúra elemeit összefoglaló néven nyilvános kulcsú infrastruktúrának (PKI) nevezzük. Egy PKI általában az alábbi alkotóelemekből épül fel:

- nyilvános-titkos kulcspárok,
- tanúsítványok,
- tanúsítványkiadó,
- regisztrációs szervezet,

- validációs szervezet,
- időbélyeg-szolgáltató,
- kulcsok létrehozásához és tárolásához valamint digitális aláírások létrehozásához és ellenőrzéséhez szükséges szoftver- és hardvereszközök,
- a kommunikációhoz szükséges hálózati elemek,
- tanúsítványtár,
- biztonsági előírások és a jogi szabályozás.

3. Az m-fizetés

Az m-fizetés (vagy mobilfizetés) az elektronikus fizetésnek az a formája, amikor a tranzakciós folyamat kezdeményezése, authorizációja és véglegesítése egyaránt valamilyen mobileszköz támogatásával történik; mobileszköz alatt értve itt (lásd [20]) a noteszgépet, PDA-t, mobiltelefont és minden olyan mobilkommunikációs eszközt, mely alkalmas lehet fizetés lebonyolítására. A mobilfizetés megvalósulásával és széles körű elterjedésével új, eddig ismeretlen távlatok nyílnak meg a kereskedelem számára: igény szerinti zene- és videóletöltések, helyfüggő mobilszolgáltatások[19], utazás és szórakozás ad hoc megszervezése. Ezekkel az új kényelmi szolgáltatásokkal az m-fizetés jól illeszkedik a készpénzes, bankkártyás ill. csekk alapú ügyintézés palettájába. Sőt alternatív megoldás lehet például számlák befizetése vagy banki átutalások esetén is.

Ahhoz, hogy egy m-fizetési rendszer elfogadott fizetési móddá váljon a piacon, rendelkezie kell bizonyos jellemzőkkel (lásd [20]):

(1) *egyszerűség és használhatóság*

Egy m-fizetési alkalmazásnak egyrészt már az első használatkor (vagy egy viszonylag rövid tanulási időszakot követően) felhasználóbarátnak kell lennie, másrészt biztosítania kell az ügyfél számára a személyreszabhatóságot.

[19] Mobileszköz nyújtotta helymeghatározásra épülő tartalomszolgáltatások.

(2) *univerzalitás*

Egy m-fizetési rendszernek támogatnia kell C2C, B2C és B2B típusú tranzakciók lebonyolítását belföldi, regionális és globális környezetben egyaránt. Emellett használhatónak kell lennie mind mikro-, mind pedig makrofizetések esetén.

(3) *interoperabilitás*

A fejlesztésnek szabványokon alapulva, nyílt technológiákat használva kell zajlania, lehetővé téve ezzel, hogy egy újonnan implementált rendszer közreműködjön a már meglévőkkel.

(4) *bizalom, titkosság és biztonság*

A felhasználónak elsősorban meg kell tudni bíznia az m-fizetési rendszer üzemeltetőjében, hogy az nem él vissza kártyaadataival, ahogy a felhasználó kilétének is titokban kell maradnia a nyilvánosság előtt a tranzakcióinformációk rözítése után. Azaz a készpénzes fizetéshez hasonló anonimitást kell biztosítania. Végül a rendszernek "bolondbiztosnak", valamint a hackerekkel és terroristákkal szemben ellenállónak kell lennie.

(5) *költséghatékonyság*

Az m-fizetés nyújtotta kényelem árának nem szabad meghaladnia azt a szintet, hogy az már ne tudja felvenni a versenyt a már létező fizetési mechanizmusokkal.

(6) *gyorsaság*

A fizetés lebonyolításához szükséges időnek mind az ügyfél, mind pedig a kereskedő számára elfogadhatónak kell lennie.

(7) *nyitottság*

A minél szélesebb körű elfogadáshoz biztosítanunk kell az alkalmazás globális elérhetőségét.

3.1. M-fizetési megoldások

Az e-fizetési rendszerekhez hasonlóan az m-fizetési megoldások is számos szempont szerint csoportosíthatók. A dolgozat áttekinthetőségét szem előtt tartva vizsgálatunk ezúttal is a megoldás alapjául szolgáló tényleges fizetési mechanizmusokig terjed. A fizetés alapját

tekintve három különböző m-fizetési modell létezik[20]:

- Bankszámla alapú rendszerek

  Az egyaránt sokmilliós ügyfélbázissal rendelkező bankszféra ill. mobilkommunikációs piac összefogásával olyan m-fizetési megoldások hozhatók létre, melyek az érintett üzletágak számára extra profitot teremthetnek. Egy ilyen m-fizetési rendszerben – mint például a PayBox – az ügyfél telefonszámát összekapcsolják annak bankszámlájával olyan módon, hogy mobilfizetés esetén a felmerülő költségek közvetlenül a vásárló számláját terhelik. Természetesen ekkor a kereskedőnek szintén rendelkeznie kell saját folyószámlával, melyen – a pénzmozgás átvezetését követően – megjelenik az áru vagy szolgáltatás ellenértéke. A folyamat maga a bankkártya alapú e-fizetési módszereknél ismertetett módon megy végbe.

- Bankkártya alapú rendszerek

  A bankkártya alapú mobilmegoldások annyiban különböznek az m-fizetési rendszerek előzőekben ismertetett modelljétől, hogy ez esetben a telefonszámhoz nem az ügyfél számlaszámát, hanem annak bankkártya-azonosítóját rendelik hozzá. Használatának egyetlen korlátozó tényezője a kártyás fizetési mód elterjedtségének szintje lehet. Ilyen – bankkártyához kötött – megoldás a MobiPay.

- Mobilszámla alapú rendszerek

  Ebben az esetben a felmerülő költségek közvetlenül az ügyfél mobilszolgátató által vezetett számláján jelennek meg, melyeket a vasárló – feltölthető egyenleg esetén – azonnal vagy előfizetői szolgáltatás mellett a számla befizetésével egyidőben (utólag) kiegyenlít. Ezen az elven működik a Németországban elérhető infin-Micropayment.

3.2. Nyilvános kulcsú infrastruktúra mobilkörnyezetben

A vezetéknélküli PKI, vagy WPKI (Wireless PKI) olyan nyilvános kulcsú infrastruktúrát takar, ahol a felhasználók mobileszközük segítségével vesznek részt az authentikációs folyamatokban. Ehhez mobiltelefonok esetén egy olyan befolyásolásbiztos modulra van

[20] Andriew S. Lim, 2007

szükség, mely egyrészt lehetővé teszi a felhasználó titkos kulcsainak valamint tanúsítványainak tárolását, másrészt képes aszimmetrikus eljárások (leginkább RSA) hatékony végrehajtására. Ezek az elvárások gyakorlatilag megegyeznek az intelligens kártyákkal szemben támaszott kritériumokkal. Ezek után természetesnek tűnhet ennek az ún. WIM (Wireless Indentity Module) egységnek közvetlenül a SIM-kártyába történő beépítése. A WIM funkcióinak ellátásához azonban a mai standard SIM-kártyák számítási ill. tárolási kapacitása egyaránt kevés, az új authentikációs modul működtetéséhez 32 (esetleg 16) bites processzorra, plusz memóriára valamint véletlenszám-generátorra van szükség. Ez a chipkártyák egy újabb generációjának, a WSIM-eknek a kifejlesztését feltételezi. Emellett a technológiai kihívás mellett azonban meg kell oldani az üzembehelyezés (a kezdeti aszimmetrikus kulcspár ill. tanúsítvány elhelyezése) kérdését is. Tudniillik, a SIM-kártyákat forgalmazó mobilszolgáltatónak nyilvános kulcsú infrastruktúrát[21] kellene kiépítenie, majd üzemeltetnie a szükséges kulcspárok ill. tanúsítványok előállításához, azaz a WIM inicializálásához. A problémára – [14] alapján – megoldást jelenthet, egy a pénzintézetektől és mobilszolgáltatóktól független, államilag adminisztrált nemzeti PKI bevezetése. Sőt ez által a különböző PKI rendszerek együttes alkalmazásából fakadó interoperabilitási kérdés is megválaszolható. A megoldás hatékonyságát jól szemlélteti a [14]-ben bemutatott, Finn Nemzeti Nyilvános Kulcsú Infrastruktúrára épülő m-fizetési rendszer.

A WIM implementálásának egy másik lehetősége – a WSIM mellett – a ma még egyetlen chippel rendelkező telefonok újabb kártyahellyel való bővítése (dual-slot)[22], mely a SIM-kártyától függetlenül lehetővé tenné intelligens kártyák használatát WIM-modulként. A módszer egyetlen hátránya, hogy ekkor a felhasználónak le kell cserélnie régi telefonját egy új, kétchipes változatra. Viszont így nem merül fel sem az üzembehelyezés sem az interoperabilitás problémája, hiszen a pénzügyi szolgáltató a mobiltársaságtól függetlenül inicializálhatja az intelligens kártyát.

3.3. Anonim kommunikációs csatornák

A 2.5 ill. 2.6 fejezetekben bemutatott anonimitást szolgáló technikák olyan kommunikációs csatorna használatát feltételezik, mely szintén támogatja a vásárló személyének elfe-

[21] A gyakorlatban elegendő lenne egy pusztán RA-ból és CA-ból álló egyszerűsített PKI működtetése.
[22] Ezzel ekvivalens a külső kártyaolvasó egységet alkalmazó ún. dual-chip megoldás.

dését. Ilyen (titkosított) anonim kommunikációt biztosítanak publikus halózatok számára az ún. *mixnetek*. A mixnetek olyan szerver-kliens architektúrájú hálózatok, melyekben a kommunikáló felek (kliensek) anonimitását a küldött üzenetek permutálásával érik el. Ez a permutálás az ún. mixing szerverek feladata, melyek a hálózatban feladott üzeneteket pufferelik, majd – elérve a szükséges darabszámot – véletlen sorrendben továbbítják őket. Ezen mixnetek utódjának a [21]-ben bemutatott *újrafelhasználható anonim válaszcsatornák* (RARC) tekinthetők. Működésükben nagyban hasonlítanak elődjükre, azonban míg a mixnetek pusztán egyszeri, egyirányú névtelen kommunikációt tettek lehetővé, addig az anonim válaszcsatornák párbeszédszerűen, oda-vissza irányban biztosítják a felek anonimitását.

Egy anonim válaszcsatornán küldött üzenet rendelkezik a következő tulajdonságokkal:

- *megválaszolható*

  A címzett képes anonim módon érkezett üzenetére névtelenül válaszolni, melyre szintén anonim módon kaphat viszontválaszt.

- csatornája *újrafelhasználható*

  Ugyanaz a csatorna különböző címzettekkel történő kommunikáció esetén is használható.

- *átruházható*

  Egy anonim üzenet átruházásával a válaszadás képessége is továbbadódik.

- *kompatiblis*

  Az eredeti és válaszüzentek nem különböztethetők meg egymástól a permutációs fázis lezárulásával.

A RARC védelmet nyújt a forgalomfigyeléses támadás időintervallum és üzenetszámlálós módszere ellen egyaránt. Biztonságos működésének egyetlen feltétele a felhasználók különböző partnerekkel történő folyamatos kommunikációja.

A protokoll egyes fázisainak leírásánál az alábbi jelölési konvenciókat fogjuk alkalmazni:

$\|\|$	a konkatenáció művelete
SK_s, PK_s	a szerverek által közösen generált titkos ill. nyilvános kulcs
E_x, D_x	egy tetszőleges x kulcsot használó titkosító ill. dekódoló függvény
S_x, V_x	egy tetszőleges x kulcsot alkalmazó aláíró ill. aláírásellenőrző algoritmus
T_A, PK_A	Alice azonosítója ill. publikus kulcsa
T_B, PK_B	Bob azonosítója ill. publikus kulcsa

Üzenetküldés

Amennyiben Alice névtelen, titkosított üzenetet szeretne küldeni Bob számára egy anonim újrafelhasználható csatornán keresztül, úgy a következő vektort kell előállítania:

$$m_1 = [E_{PK_s}(T_A||PK_A); E_{PK_s}(M); E_{PK_s}(T_B||PK_B)]$$

Ahol M jelöli Alice titkosítatlan üzenetét. Az üzenet elküldéséhez Alice-nak nullaismeretű bizonyítással igazolnia kell $T_A||PK_A$ és $T_B||PK_B$ ismeretét.

Permutáció

A megfelelő vektorszám elérése után, a szerver sorra veszi a vektorokat (köztük m_1-et). A többi szerverrel közösen aláírja $E_{PK_s}(T_A||PK_A)$-t, dekódolja $E_{PK_s}(T_B||PK_B)$, Bob nyilvános kulcsával újratitkosítja $E_{PK_s}(M)$-t, majd az így előálló

$$m_1' = [E_{PK_s}(T_A||PK_A); E_{PK_B}(M); S_{SK_s}(E_{PK_s}(T_B||PK_B))]$$

hármast, a már szintén feldolgozott vektorokkal együtt véletlen sorrendben továbbítja a címzettek felé.

Válasz küldése

Amennyiben Bob válaszolni szeretne Alice üzenetére szintén anonim módon, úgy nem kell egyebet tennie, mint előállítania a következő vektort:

$$m_2 = [E_{PK_s}(T_B||PK_B); E_{PK_s}(N); E_{PK_s}(T_A||PK_A); S_{SK_s}(E_{PK_s}(T_B||PK_B))]$$

Ahol N jelöli Bob titkosítatlan válaszüzenetét. Az üzenet elküldéséhez Bob-nak nullaismeretű bizonyítással igazolnia kell $T_B||PK_B$ ismeretét. A permutációs fázisban az aláírás ellenőrzésével a vektor negyedik komponensét a szerver elhagyja, minek után az m_2 alakú válaszokat semmi nem fogja megkülönböztetni az m_1 alakú üzenetektől.

Architektúrájuknak köszönhetően az anonim válaszcsatornák adaptálása kézenfekvőnek tűnhet a mobilkommunikációban. A RARC forgalmát irányító mixing szerverek funkcionalitása ugyanis könnyen beépíthető lenne az SMS-szolgáltatásban alkalmazott üzenetközpont szervereibe.

4. Egy anonim, átruházható m-fizetési protokoll

Az alábbiakban egy olyan anonim, átruházható m-fizetési megoldás kerül bemutatásra, mely az eddig implementált rendszerektől eltérően (lásd 3.1. fejezet) digitális pénzt alkalmaz a fizetés lebonyolítására. A cél egy olyan kvázi ideális digitális pénz protokoll megvalósítása volt, mely extra hardvereszközök bevezetése nélkül szolgáltatja az m-fizetés által nyújtott kényelmet. Ahogy arra Huang és Chen is rámutatott m-fizetésről szóló cikkükben (lásd [22]): a 3G-s technológiák és a mobilkommunikáció mai fejlettségi szintje mellett az online fizetés megvalósítása nem vet fel problémákat sem hatékonysági, sem kényelmi szempontból. Ezen megfontolásból, továbbá tekintettel az offline mód által generált aránytalanul nagy számú biztonsági problémára (lásd 2.7. és 2.8. fejezet) az ajánlott protokoll – a napjainkban leggyakrabban alkalmazott e-fizetési rendszerekhez hasonlóan – online fizetést valósít meg. Az anonimitás biztosításához anonim válaszcsatornák rendelkezésre állását feltételezzük.

Protokoll$_6$(online)

Felvétel

(1) Alice egy PIN-kód valamint a címlet megadásával jelzi a Bank felé digitális készpénzigényét.

(2) A Bank kiállítja az összegről szóló digitális pénzt, majd aláírja azt.

(3) A Bank levonja Alice számlájáról a kért összeget, adatbázisában elhelyezi a pénzazonosítót a hozzárendelt PIN-kóddal, majd az ügyfél rendelkezésére bocsátja a

fizetőeszközt.

Fizetés/Átruházás

(1) Alice egy anonim csatornán keresztül felveszi a kapcsolatot Bobbal, és megegyeznek az átadni kívánt pénzösszegben.

(2) Alice a szükséges adatok megadásával jelzi digitális számlaigényét. (opcionális)

(3) Alice a PIN-kód, a kedvezményezett (Bob) azonosítója valamint a fizetés összegének kíséretében elküldi a Banknak a fizetőeszközt.

(4) A Bank ellenőrzi a pénzen aláírását.

(5) A PIN-kód alapján a Bank adatbázisában ellenőrzi Alice jogosultságát.

(6) A Bank megkéri Bobot, hogy hagyja jóvá az átruházandó pénz összegét, és küldje el a pénz későbbi használatához szükséges PIN-kódot.

(7) Bob a PIN-kód elküldésével jóváhagyja a tranzakció összegét.

(8) A Bank felülírja a pénzhez tartozó PIN-kódot adatbázisában, majd elküldi Bobnak fizetőeszközét.

(9) Bob elküldi Alicenak a tranzakciót igazoló digitális számlát. (opcionális)

(10) Fizetés esetén Bob átadja a kért terméket Alicenak.

Beváltás

(1) Bob a PIN-kód kíséretében elküldi beváltandó pénzét a Banknak.

(2) A Bank ellenőrzi a pénzen aláírását.

(3) A PIN-kód alapján a Bank adatbázisában ellenőrzi Bob jogosultságát.

(4) A Bank a pénz azonosítójához egy speciális PIN-kódot rendel, mely azt jelzi, hogy a pénz beváltották.

(5) A Bank jóváírja Bob számláján a megfelelő összeget.

4.1. A protokoll tulajdonságai

Nézzük, hogy az imént definiált protokoll, miként kívánja megvalósítani az e-fizetési rendszerek általános biztonsági szolgáltatásait:

(1) *bizalmas adatkezelés*

A szereplők kommunikációja során minden üzenet titkosított formában kerül a publikus hálózatba legyen szó akár anonim, akár nevesített csatornáról.

(2) *authentikáció*

Az authentikáció biztosításához egy már kiépült, államilag adminisztrált nyilvános kulcsú infrastruktúra meglétét feltételezzük.

(3) *letagadhatatlanság*

A TTP-ként működő bank garantálja azt, hogy a felek ne tudják később letagadni cselekedetüket.

A következőkben vegyük sorra az ideális rendszerre vonatkozó feltételeket.

(1) *függetlenség*

Lévén, hogy az ügyfél mobiltelefonján kívül nincs szükség egyéb hardvereszköz jelenlétére fizetéskor, protokollunk teljesíti a függetlenség kritériumát.

(2) *biztonságosság*

A újrafelhasználás ill. pénzhamisítás ellen egyaránt az aktuális tulajdonos által szolgáltatott PIN-kód nyújt védelmet, mely által a bank minden esetben megbizonyosodhat a pénzt felhasználni kívánó személy fizetési jogosultságáról.

(3) *titkosság* (nyomonkövethetetlenség)

A nyomonkövethetetlenséget az anonim válaszcsatornák használata mellett az online működés biztosítja.

(4) *offline fizetés*

A már említett okból protokollunk nem ad lehetőséget fizetés offline lebonyolítására.

(5) *átruházhatóság*

A pénz ügyfelek közti átruházhatóságát az online mód és a PIN-kód alkalmazása együttesen garantálja. Vegyük észre, hogy az offline rendszerekkel szemben, protokollunk tetszőleges számú átruházást tesz lehetővé.

(6) *feloszthatóság*

A pénz feloszthatóságának biztosítása szintén könnyen beépíthető a protokollba: ha az átruházás (3)-as pontjában átadott pénz címlete nagyobb a megvásárolni kívánt

termék értékénél, akkor a Bank a címlet módosítása után visszaküldi a fizetőeszközt Alice-nak, majd Bob részére új tokent állít elő a termék árának megfelelő címlettel.

4.2. A protokoll működése

A következőkben egy tipikus felvétel-vásárlás-beváltás folyamatot fogunk végigkövetni. A protokoll működésének részletes leírása során az alábbi jelölési konvenciókat alkalmazzuk:

$\|\|$	a konkatenáció művelete
$-$	az aritmetikai kivonás művelete
$CUST$	ügyfél (Alice)
$BENE$	kedvezményezett (Bob)
$MERCH$	kereskedő (Bill)
$BANK$	bank (Bank)
ID_X	egy tetszőleges X entitás azonosítója
PIN_X	egy tetszőleges X entitás tetszőleges PIN-kódja
SK_X	egy tetszőleges X entitás titkos kulcsa
PK_X	egy tetszőleges X entitás nyilvános kulcs
$CERT_X$	egy tetszőleges X entitás tanúsítványa
$\{m\}_k$	egy tetszőleges k kulccsal titkosított m üzenet
MSG	egy tetszőleges üzenet
SIG_{X_Y}	egy tetszőleges X entitás által valamely Y entitás számára előállított digitális aláírás
$ORDER$	egy rendelés részletei (termékazonosító, mennyiség, etc.)
$PRICE$	egy rendelés végösszege
$NOTE$	egy digitális pénz címlete
$ACCNO_X$	egy tetszőleges X entitás számlaszáma
$NONCE_X$	egy tetszőleges X entitás által generálst véletlenszám
$CASH_X$	egy tetszőleges X címlettel rendelkező digitális pénz

Felvétel

A bank és az ügyfél között a következő üzenetváltások mennek végbe pénzfelvétele esetén:

(1) $CUST \rightarrow BANK$

$MSG = ACCNO_{CUST}||CERT_{CUST}||PIN_{CUST}||NOTE$

A Bank $ACCNO_{CUST}$ és $CERT_{CUST}$ segítségével végzi el az authentikációt, majd levonja az ügyfél számlájáról a megfelelő összeget ($NOTE$).

(2) $BANK \rightarrow CUST$

$MSG = CASH_{NOTE}$

$CASH_{NOTE} = \{NOTE||NONCE_{BANK}\}_{SK_{BANK}}$

Ahol $NONCE_{BANK}$ az előállított digitális pénz azonosítója.

Fizetés

A bank, az ügyfél és a kereskedő között az alábbi üzenetváltások zajlanak le fizetés alatt:

(1) $CUST \rightarrow MERCH$

$MSG = PROD||DATA_{CUST}$

Ahol $DATA_{CUST}$ a vásárló számla kiállításához szükséges adatait jelöli.

(2) $CUST \rightarrow BANK$

$MSG = PIN_{CUST}||ID_{MERCH}||PRICE||CASH_{NOTE}$

(3) $BANK \rightarrow MERCH$

$MSG = PRICE$

(4) $MERCH \rightarrow BANK$

$MSG = PIN_{MERCH}$

(5) $BANK \rightarrow MERCH$

$MSG = CASH_{PRICE}$

$CASH_{PRICE} = \{PRICE||NONCE_{BANK}\}_{SK_{BANK}}$

(6) $MERCH \rightarrow CUST$

$MSG = BILL_{CUST}$

Ahol $BILL_{CUST}$ a vásárló számlázási adatai ($DATA_{CUST}$) alapján kiállított számla.

(7) $BANK \rightarrow CUST$ *(opcionális)*

$MSG = CASH_{NOTE-PRICE}$

$$CASH_{NOTE-PRICE} = \{NOTE - PRICE || NONCE_{BANK}\}_{SK_{BANK}}$$

Beváltás

A bank és a kereskedő között egyetlen üzenetváltás szükségeltetik a pénz beváltáshoz:

(1) $MERCH \rightarrow BANK$

$MSG = ACCNO_{MERCH} || CERT_{MERCH} || PIN_{CUST} || CASH_{PRICE}$

A Bank $ACCNO_{MERCH}$, $CERT_{MERCH}$ és PIN_{CUST} segítségével elvégzi az authentikációt, majd jóváírja a kereskedő számláján a megfelelő összeget ($PRICE$).

5. Összefoglalás

A dolgozat első részében az elektronikus fizetési rendszerek működésébe nyerhettünk betekintést, majd részletesen megvizsgáltuk azoknak egy speciális típusával, az ún. digitális pénz protokollokkal szemben támasztott elvárásokat, és ezen rendszerek tulajdonságait. Végül egy olyan m-fizetési digitális pénz protokollal ismerkedhettünk meg, mely a mobilfizetési megoldások kényelmét ötvözi a készpénzes ügyintézés alábbi előnyeivel:

- anonim vásárlás és számlaigénylés
- univerzális alkalmazhatóság
- anonim átruházhatóság
- minimális hozzáadott költség

Az ajánlott rendszer az offline fizetési mód kivételével teljesíti az ideális digitális pénz protokollokra vonatkozó kritériumokat.

Hivatkozások

[1] D. Chaum,

Blind Signature for Untraceable Payments,

Advances in Cryptology, Crypto'82, Plenum Press, pp. 199-203, 1983

[2] D. Chaum, A. Fiat, N. Naor,

Untraceable Electronic Cash,

Advances in Cryptology, Crypto'88, Springer-Verlag, vol. 403, pp. 319-327, 1990

[3] K. Taga, J. Karlsson,

Global M-Payment Report 2004. Making M-Payment a Reality,

The Strategy Consultancy Arthur D. Little, Vienna, July 2004

[4] A. Herzberg,

Payments and banking with mobile personal devices,

Commun. ACM 46 (5) pp. 53-58, 2003

[5] N. Mallat, M. Rossi, V. K. Tuunainen,

Mobile banking services,

Commun. ACM 47 (5) pp. 42-46, 2004

[6] R. Abbadasari, R. Mukkamala, V. Valli Kumari,

MobiCoin: Digital Cash for M-Commerce,

ICDCIT 2004 pp. 441-451, 2004

[7] C. Popescu,

An Anonymous Mobile Payment System based on a Group Blind Signature Scheme

Proc. of the 13th IST Mobile and Wireless Communication Summit pp. 196-200, 2004

[8] S. J. Aboud, M. A. AL-Fayoumi,

Anonymous and Non-Repudiation E-Payment Protocol

American Journal of Applied Sciences vol. 4 pp. 538-542, 2007

[9] R. Song, L. Korba,
How to Make E-cash with Non-Repudiation and Anonymity,
Info. Technology: Coding and Computing ITCC 2004, pp. 167-172, 2004

[10] Tanaka T.,
Possible Economic Consequences of Digital Cash,
Center for Global Communications, International University of Japan, Tokyo, 1997

[11] J. Ondrus, F. Bodart,
Electronic Payment Systems,
Faculty of Business and Economics, University of Lausanne, 17/5/2004

[12] Okamoto T., Ohta K.,
Universal Electronic Cash,
Advances in Cryptology, Crypto'91, Springer-Verlag, pp. 324-337, 1992

[13] J-M. Sahut, M. Galuszewska,
Why does SSL dominate the e-payment market?,
Journal of Internet Banking and Commerce vol. 9, 2004

[14] M. Hassinen, K. Hyppönen, E. Trichina,
Utilizing national public-key infrastructure in mobile payment systems,
Electronic Commerce Research and Applications, In Press, 2007
(doi:10.1016/j.elerap.2007.03.006)

[15] H. Tewari, D. O'Mahony, M. Peirce,
Reusable Off-Line Electronic Cash Using Secret Splitting,
Computer Science Department, Trinity College, Dublin,
Technical Report TCD-CS-1998-27, 1998

[16] L. Law, S. Sabett, J. Solinas,
How to make a mint: The cryptography of anonymous electronic cash,
National Security Office of Info. Security Research and Technology,
18/06/1996

[17] D. R. Kuhn, V. C. Hu, W. T. Polk, S-J. Chang,
Introduction to public key technology and the federal PKI infrastructure,
National Institute of Standards and Technology, February 2001

[18] D. Chaum, T. Pedersen,
Transferred Cash Grows in Size,
Advances in Cryptology, Eurocrypt'92, Springer-Verlag, pp. 390-407, 1993

[19] D. Chaum, T. Pedersen,
Wallet Databases with Observers,
Advances in Cryptology, Crypto'92, Springer-Verlag, pp. 89-105., 1993

[20] S. Karnouskos, F. Fokus,
Mobile Payment: a journey through existing procedures & standardization initiatives,
IEEE Communications Surveys and Tutorials, vol. 6, pp. 44-66, 2004

[21] P. Golle, M. Jakobsson,
Reusable anonymous return channels,
Proceedings of WPES'03, Washington DC, USA, October 2003

[22] Z. Huang, K. Chen, *Electronic Payment in Mobile Environment*,
Proceedings of DEXA'02, 2002

A. Mozaikszavak és rövidítések

Mozaikszó	Feloldás	Magyarázat
API	Application Programming Interface	alkalmazásprogramozási felület
B2B	Business-to-Business	vállalatok közti
B2C	Business-to-Consumer	vállalatok és fogyasztók közti
C2C	Consumer-to-Consumer	fogyasztók közti
CA	Certification Authority	hitelesítésszolgáltató
CRL	Certificate Revocation List	tanúsítványvisszavonási lista
DSA	Digital Signature Algorithm	digitális aláíró algoritmus
F2F	Face-to-Face	szemtől szembeni
GPRS	General Packet Radio Service	általános rádióhullámos csomagkapcsolt adatszolgáltatás
GSM	Groupe Spécial Mobile vagy	egységes mobiltávközlési rendszer
MD5	Message-Digest Algorithm 5	egyirányú hashfüggvény
NFC	Near Field Communication	kis hatótávú rádiófrekvenciás adtátviteli technológia
P2P	Peer-to-Peer	közvetlen partneri kapcsolat
PDA	Personal Digital Assistant	tenyér méretű számítógép
PIN	Personal Identification Number	személyes azonosítószám
PKI	Public Key Infrastructure	nyilvános kulcsú infrastruktúra
POS	Point-of-Sale	vásárlás helyéhez kötött

(folyt.)

Mozaikszó	Feloldás	Magyarázat
RA	Registration Authority	regisztrációs szervezet
RIPEMD	RACE Integrity Primitives Evaluation Message Digest	egyirányú hashfüggvény
RARC	Reusable Anonymous	újrafelhasználható anonim
RSA	Rivest-Shamir-Adleman	aszimmetrikus protokoll
	Return Channels	válaszcsatornák
SHA	Secure Hash Algorithm	egyirányú hashfüggvény
SIM	Subscriber Identity Module	előfizetői azonosító modul
SMS	Short Message Service	rövidüzenet-szolgáltatás
SSL	Secure Sockets Layer	titkos kommunikációt biztosító réteg
TSA	Time Stamping Authority	időbélyeg-szolgáltató
TTP	Trusted Third Party	abszolút megbízható harmadik fél
USSD	Unstructured Supplementary Service Data	strukturálatlan kiegészítő adatszolgáltatás
VA	Validation Authority	validációs szervezet
WAP	Wireless Application Protocol	vezeték nélküli adatátviteli szabvány
WIM	Wireless Identity Module	vezetéknélküli azonosító modul
WPKI	Wireless PKI	vezetéknélküli PKI