Az m-kormányzat biztonsági kérdései és lehetőségei

FAIGL, ZOLTÁN, IMRE SÁNDOR
BME Híradástechnikai Tanszék, imre@hit.hit.bme.hu
BUDAI BALÁZS
BKAE Közigazgatás-szervezési és Urbanisztikai Tanszék, E-government kutatócsoport
balazs.budai@e-government.hu

Kulcsszavak: adatvédelem, mobil tranzakciók, elektronikus aláírás, hitelesítés

A közigazgatás modernizálásának egyik kiemelkedő feladata az informatika bevonása, melynek fejlesztő hatásai megkérdőjelezhetetlenek, azonban ezekért az innovatív eredményekért nem áldozhatunk fel két alapvető dolgot, nevezetesen az adatbiztonságot és az adatvédelmet. A cikk áttekintést ad a mobil adminisztráció bevezetésének lehetőségeiről, technikai és törvényi szempontból is érzékelteti az ezzel járó kihívásokat. A lehetséges alkalmazási területek között részletesebben szerepel a mobil tranzakciók használata a közigazgatási ügyekben. Hangsúlyt kaptak azok a felhasználó-hitelesítési és elektronikus aláírás képzési sémák, amelyeket a mobil adminisztrációban alkalmazni lehet. Végül a szerzők nyitott tervezési kérdésekre, nevezetesen a megfelelő biztonságpolitikák és tanúsítványfajták kialakítására hívják fel a figyelmet.

Számos motiváló tényezője van a mobil kormányzat bevezetésének. Ma még hazánkban az 1957. évi Államigazgatási Eljárásról szóló törvény fogalmazza meg a közigazgatási eljárások formai követelményeit. Kidolgozás alatt áll a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól szóló törvény (KET) tervezete, ami lehetővé teszi majd az elektronikus út, így a mobil csatorna használatát is közigazgatási eljárásokban.

Az m-governement és m-commerce fejlődési folyamatában fontos motiváló tényezőként hatnak azok az EU-s direktívák és ajánlások, amelyek elektronikus ügyintézés lehetőségének bevezetését szorgalmazzák hatósági eljárásokban. Kiemelkedően fontos ezek között az elektronikus aláírás elfogadásáról és bevezetéséről szóló EU direktíva [1], valamint az eEurope akciótervek visszatérő eleme, a „Common List of Basic Public Services" (CLBPS) című dokumentum [2].

A cikk első részében bemutatjuk, miért és milyen feladatra célszerű mobiltelefont használni, a második részben összefoglaljuk, milyen esetekben indokolt a mobil csatorna alkalmazása a KET és CLBPS alapján a közigazgatásban és különböző hivatalos szerveknél. A harmadik részben leírjuk azokat a lehetséges módokat, ahogy a mobil csatorna beilleszkedhet egy ügymenetbe. A negyedik részben kitekintést adunk technológiai kérdéseken túlmutató rendszertervezési elvekre, amelyeket figyelembe kell venni, amikor elektronikus közigazgatási vagy más, széleskörűen elérhető, bizalmas jelleggel bíró elektronikus tranzakciókat vezetünk be.

1. A mobil technológia indokoltsága

A Nemzeti Hírközlési Hatóság 2004. májusi gyorsjelentése 8 145 298 aktív SIM kártyáról ad számot [3]. A legalacsonyabb kategóriájú készülékek is rendelkeznek SMS küldésen túl WAP képességgel. A technológia kellőképpen érett olyan újszerű szolgáltatások bevezetésére, ahol fontos a felek egyértelmű hitelesítése és a bizalmas kapcsolat megteremtése.

E szolgáltatások a WPKI (Wireless Public Key Infrastructure) technológián alapulnak, amely megfelel az internetes PKI infrastruktúrának, azzal a különbséggel, hogy a tanúsítványok formátumát és a tanúsítványszerzés menetét a kis sávszélességű, és a kis tárolási, számítási kapacitású mobil technikára adaptálták [19].

A mobiltelefon és hálózat két módon illeszkedhet be egy elektronikus üzleti modellbe:

– csatornát szolgáltat biztonságos partnerhitelesítéshez, felhasználó-azonosításhoz,
– megvalósíthatja a felhasználó-oldali digitális aláírást, az elektronikus aláírásról szóló törvénynek megfelelően.

Ez alatt a következőt értjük:

A felhasználó-azonosítás célja, hogy a rendszer ellenőrizni tudja egy adott személy jogosultságait, ez az első lépés egy bizalmas tranzakció lebonyolítása során. A digitális aláírás alatt a hosszú távon letagadhatatlan aláírást értjük. Számtalan esetben alkalmazhatunk elektronikus aláírást. A körülményektől függ, hogy mennyi idő múlva, mennyi ideig kell érvényesnek maradnia (szélsőséges példa erre a végrendelet), vagy milyen ügymenetben, milyen szereppel alkalmazzák (állampolgár, vállalatvezető, közjegyző, cégpecsét). Minden eset más és más követelményeket támaszt az aláírás hitelességét, letagadhatatlanságát, érvényességi idejét illetően.

A mobil elektronikus aláírásnak és felhasználó-azonosításnak széles felvevő piaca létezik, ezek közül az egyik az m-kormányzat, ahol a hatóságok kapcsolatba lépnek az állampolgárral. Ha GSM, vagy a közeljövőben elterjedő UMTS rendszeren keresztül végezzük az előfizetők azonosítását és a hozzáférés-engedélyezését, a rendszer kellőképpen biztonságosnak tekinthető. A biztonsági funkciót megtestesítő SIM kártyák kiosztása és felügyelete megfelelő keretek között zajlik. Az előfizetők személyes adatai – más néven identitás

információk [5] – a szükséges mértékben védettek. Következésképpen, a megbízható elektronikus tranzakciókhoz érdemes GSM/UMTS vagy más cellás rendszereket igénybe venni. A felhasználó-azonosításhoz és a digitális aláírás képzéséhez tipikusan kis sávszélességre van szükség, ezért elég a GSM adatátviteli sebessége.

A mobilszolgáltatók számára az új kihívást – amelyet a versenyképesség fenntartása, és a felhasználók kényelmesebb kiszolgálása diktál – a személyes adatok (identitás információk) és egyéb bizalmas információk elektronikus úton való közlése jelenti. Idegen mobil hálózatban a felhasználó azonosítása és hitelesítése úgynevezett identitás-roaminggal fog történni [7].

Számos nemzetközi szakmai szervezet alakult a 90-es évek végétől, amely a megbízható elektronikus tranzakciók kidolgozásán, az identitás információk biztonságos átvitelén dolgozik. Tagjaik általában mobilszolgáltatók, pénzügyi intézmények, kutató-, fejlesztő és szabványosítási szervezetek és fórumok. Tevékenységükről az *1. táblázatban* található összefoglalás.

2. Elektronikus ügymenetmozzanatok mobil csatornán keresztül

A mobil csatornán történő tranzakciókat sok területen fel lehet használni, banki szolgáltatások esetén beszélünk m-bankingról, adminisztratív jellegű feladatok végzésénél m-adminisztrációról, közigazgatásban zajló ügymenetek felváltásánál m-kormányzatról, és még sorolhatnánk. Ebben a fejezetben, a közigazgatásban bevezethető mobil szolgáltatásokat szemléltetjük.

Az első számú kérdés, hogy a közigazgatási eljárások mely mozzanatai válthatók ki mobiltelefonos tranzakció segítségével. A hazai jogszabályok és EU direktívák melyek használatát teszik lehetővé? M-kormányzat szintjén a közeljövőben bevezetendő „Közigazgatási hatósági eljárás és szolgáltatás általános szabályairól szóló törvény” (KET). Ez és a hozzá kapcsolódó kormányrendeletek határozzák meg a közigazgatási eljárások formai követelményeit – például milyen adatokat kell tartalmaznia egy kérelemnek – illetve garanciális szabályokat fogalmaz meg az ügymenetek sértetlenségére, bizalmasságára, és az állampolgár jogaira vonatkozóan. A KET műszaki szempontból kiindulópontot jelent az elektronikus ügymenetek biztonságpolitikájának kidolgozásához (lásd 4. fejezet).

A KET tervezete szerint a *2. táblázatban* felsorolt eljárási mozzanatokban lehetséges az elektronikus kapcsolattartás. A felsoroltak közül a mobil technológia alkalmazása elsősorban a kérelem, tájékoztatás, az értesítés, idézés és a felhívás területén lehetséges.

1. táblázat Megbízható mobil elektronikus tranzakciókat specifikáló szervezetek

Név	Alapítás	Tagok	Célja
Radicchio (T^2R) [8]	2002 március	GSMA, Liberty Alliance, ETSI	Globális identitás-menedzsment platform kidolgozása.
Liberty Alliance [9]	2001 szept.	VeriSign, Nokia, Sun, RSA, Vodafone, American Express, Novell	Identitás alapú webes szolgáltatások kialakítása, ún. *federated identity management* specifikálása.
GSMA [10]	1987	GSM szolgáltatók	Nemzetközi szintű kapcsolatok kiépítése pénzügyi szervezetek és GSM szolgáltatók között.
ETSI (M-COMM) [11]	2000 április	M-COMM Working Group	Elektronikus úton történő aláírást és fizetést végrehajtó rendszerek követelményeinek kidolgozása.
MPSA (SimPay) [12]	2003 március	Vodafone, T-Mobile, Orange, Telefónica Móviles	Globális micropayment rendszer kialakítása.
Mobey Forum [13]	2000 május	VISA, ABN-Amro Bank, Nokia, Deutsche Bank	Mobil fizetési rendszer kialakítása, m-payment, m-brokeraging, m-banking szolgáltatások.
MeT [14]	2000 április	NEC, Nokia, Panasonic, SonyEricsson	WAP-os szolgáltatások kialakítása, mobil tranzakciók kidolgozása.
PayCircle [15]	2002 február	HP, Siemens	M-payment szolgáltatás kialakítása.
Mobile Payment Forum (MPF) [17]	2001 november	American Express, JBC Co. Ltd., MasterCard International, Visa International	M-payment szolgáltatás kialakítása.
Open Mobile Alliance (OMA) [16]	2002 június	Vodafone, Ericsson, WAP Forum, IT vállalatok	Műszaki előírásokat fogalmaz meg a mobil kommunikáció területén használt alkalmazásokra és szolgáltatásokra vonatkozólag.

2. táblázat Az állampolgár és a hatóság kapcsolatfelvételével járó eljárási mozzanatok a közigazgatásban

a) kérelem, fellebbezési kérelem, újrafelvételi kérelem, méltányossági kérelem és a jogszabályban előírt mellékleteik benyújtása,
b) jogsegély iránti kérelem és annak teljesítése,
c) hiánypótlási felhívás és a hiánypótlás,
d) az eljárás irataiba való betekintés,
e) idézés,
f) igazolási kérelem előterjesztése,
g) ügyfél nyilatkozata, bejelentése, a hatósághoz intézett beadványa,
h) bizonyítékok ügyfél elé tárásának határnapját tartalmazó felhívás,
i) felügyeleti szerv eljárásához szükséges iratok felterjesztésére szóló felhívás,
j) az ügyfél tájékoztatására, értesítésére és felhívására vonatkozó egyéb hatósági közléseknek az ügyfél tudomására hozása,
k) a döntés közlése

A mobiltelefon minden olyan területen használható, ahol az adott szerv az elektronikus út használatát lehetővé teszi. Az eEurope akcióterv fontos dokumentuma – a „Common List of Basic Public Services (CLBPS)” – 20 ilyen elemet foglal össze: tizenkettőt az állampolgárnak és négyet az üzleti szférának szántak közül.

A *3. táblázatban* a kiemelt elemek egészben a többi eljárás csak részben tartalmazza a felhívás, kérelem, tájékoztatás, idézés vagy értesítés mozzanatot. Látható, hogy a közigazgatási eljárásoknál bevált, kormány-rendelkezésben megfogalmazott elektronikus ügymenet az üzleti szférában, vagy más hivatalos szerveknél is jól hasznosítható.

3. A mobil csatorna alkalmazási módozatai

Ebben a fejezetben bemutatjuk a mobil csatorna alkalmazási lehetőségeit az elektronikus eljárásokban. Az itt leírt tranzakciók csak ügymenetmozzanatok, általában az eljárás fennmaradó része Interneten keresztül, vagy hagyományos ügyintézéssel zajlik.

3.1. Felhasználó-hitelesítési módozatok

A felhasználó-hitelesítési lehetőségeket önkényesen, az azonosításhoz szükséges tényezők száma alapján csoportosítottuk.

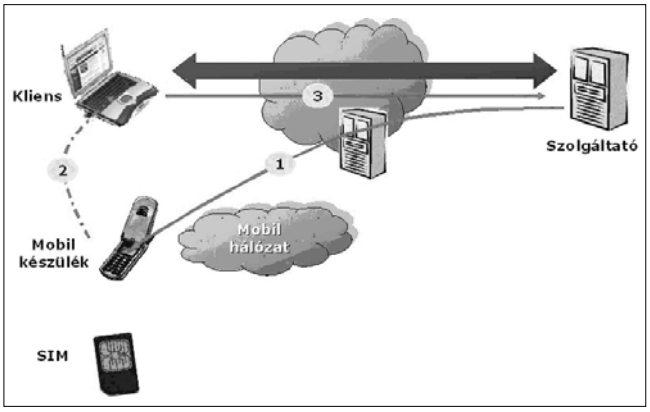
Személyes információ alapján történő hitelesítésnél

egyetlen tényező, a jelszó (például PIN kód) ismerete szükséges csak ahhoz, hogy a felhasználó azonosítsa magát. Statikus jelszavak használata köztudottan sebezhetővé teszi a felhasználó-azonosítást, mivel a jelszó nyilvánossá válásának valószínűsége folyamatosan növekszik az idő múlásával. Ebből fakadt az ötlet, hogy jobb lenne minden jelszót csak egyszer használni, majd használat után eldobni.

Az *egyszer használatos jelszavak (One-Time-Password, OTP)*, kiosztását és változását valamilyen módszerrel szinkronizálni kell a szolgáltató és a felhasználó között. Ha nem elég biztonságos az átviteli csatorna, nyilvánvaló, hogy a két oldal nem küldheti el egymásnak az új jelszót. Ilyen esetben chipkártyára, vagy más intelligens eszközre ültetett, megbízható számlálóval vagy időzítővel szokták megoldani a jelszavak változásának összehangolását.

A GSM, UMTS és más mobil hálózatok kellő biztonságot nyújtanak ahhoz, hogy egyszer használatos jelszót küldjünk a felhasználó mobil telefonjára. Az *1. ábrán* látható esetben a szolgáltató titkosítás nélkül küldi át a jelszót. A felhasználó elolvassa a kijelzőn, és begépeli a számítógépén a jelszót, hogy azonosítsa magát a szolgáltató portálján.

E megoldás biztonsága a mobil hálózat (GSM, UMTS) titkosításán és hitelesítésén alapszik. A statikus jelszavas módszereknél megbízhatóbban hitelesíti a felhasználót. A jelszó például SMS formájában érkezik az előzetesen regisztrált SIM kártyára. A mobil telefonszám egyértelműen azonosítja a SIM kártyát. A jelszó csak a SIM kártyát tartalmazó készülék képernyőjén olvasható, így illetéktelen kezekbe csak úgy kerülhet, ha a SIM kártyát, vagy a SIM-et tartalmazó készüléket elveszítik/eltulajdonítják, és a tulajdonos nem tiltatja azt le.



1. ábra Egyszer használatos jelszó (OTP) kiosztása nyíltan

Kis és közepes jelentőségű tranzakcióknál (például banki szolgáltatások) érdemes bevezetni e megoldást. Előnye, hogy minimális költséggel megvalósítható, a SIM kártya pedig nem igényel változtatást.

Kulcs és személyes információ alapján történő azonosításnál és hitelesítésnél

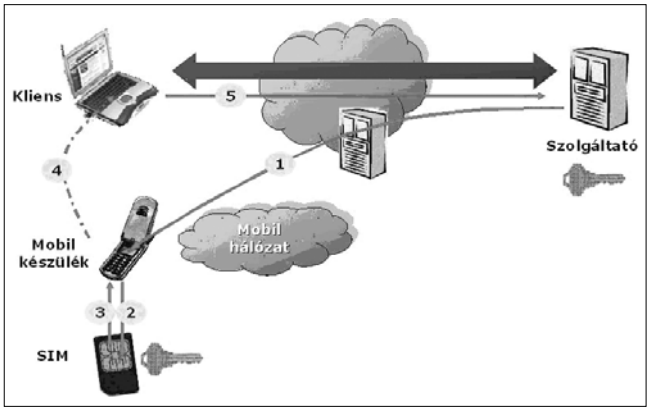
két tényező együttes megléte szükséges: birtokolni kell egy kulcsot (nem egyezik a GSM titkos kulcscsal), és ismerni kell egy PIN kódot (eltér a GSM PIN kódtól). A háttérben jelen van a mobil hálózat által nyújtott előfizető-hitelesítés és titkosítás a rádiós csatornán.

A *titkosított OTP kiosztás* mechanizmusa megegyezik az előző esettel, de megsokszorozza a felhasználó-hitelességének erejét azzal, hogy feltételezi, hogy a SIM kártyáján jelen van a titkos kulcs, amely hatását csak a megfelelő PIN kód ismeretében képes aktiválni a felhasználó. A szolgáltató oldalán tárolni kell a titkos kulcsot. Az egyszer használatos titkosított jelszó kiosztást a *2. ábra* szemlélteti (a következő oldalon).

A második lépés során a SIM kártya bekéri a PIN kódot a felhasználótól, és ha az megfelelő, akkor a harmadik lépésben megjeleníti a kijelzőn a jelszót. A PIN ismerete nélkül a jelszó nem válik olvashatóvá. A módszer biztonságát a PIN ismerete adja, jóval biztonságosabb nyílt OTP kiosztásnál. Ha a mobil készülék támadó kezébe kerül, nem tudja megszemélyesíteni a felhasználót, amíg nem ismeri a PIN kódot. A titkosított OTP kiosztáson alapuló felhasználó-hitelesítés már komolyabb elektronikus tranzakciók hozzáférés-engedélyezési részét is képezheti. A második lépésben sebezhető a módszer, ha a PIN

AZ ÁLLAMPOLGÁROK SZÁMÁRA NYÚJTOTT SZOLGÁLTATÁSOK	AZ ÜZLETI SZFÉRÁNAK NYÚJTOTT SZOLGÁLTATÁSOK
1. Jövedelemadó: adóbevallás megtétele, értesítés a kivetett adóról	13. Munkavállalók után befizetett hozzájárulások
2. Álláskeresés: munkaügyi hivatalok	**14. Társasági adó**
3. Társadalombiztosítási kifizetések (legalább három az alábbi négy lehetőség közül) - munkanélküliek járadékai - gyermekek után járó pótlékok - gyógyászati költségek - tanulói ösztöndíjak	**15. Általános forgalmi adó**
4. Személyi dokumentumok: útlevél, gépjárművezetői jogosítvány	**16. Új társaság bejegyzése**
5. Gépkocsik nyilvántartásba vétele: új, használt, importált autók	**17. Adatközlés a statisztikai hivatalnak**
6. Építési engedély kérelem	18. Vámnyilatkozat
7. A rendőrségnek tett bejelentések: pl. lopás esetében	19. Környezetvédelemmel összefüggő engedélyek
8. Közkönyvtárak: katalógusokhoz, keresési lehetőségekhez való hozzáférés	20. Közbeszerzés
9. Születési és házassági bizonyítványok: kérelmezésük és kiadásuk	
10. Felsőbb oktatásba történő jelentkezés (ide értve az egyetemeket is)	
11. Költözés bejelentése: lakcímváltozás	
12. Egészséggüggyel összefüggő szolgáltatások: pl. interaktív tanácskérési lehetőség a különböző kórházi szolgáltatások elérhetőségéről, kórházi bejelentkezések	

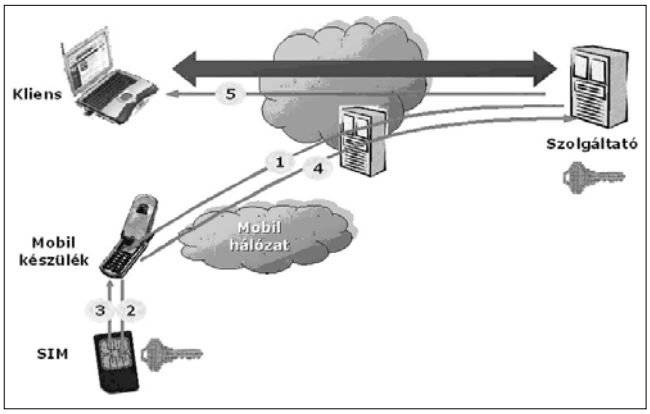
3. táblázat Common List of Basic Public Services (CLBPS)



2. ábra Egyszer használatos jelszó kiosztása titkosítva

kódot leolvassák, és a SIM kártyát (vagy a telefont) eltulajdonítják. A megoldás bevezetéséhez a SIM kártyát alkalmassá kell tenni a fenti műveletek elvégzéséhez (ki kell cserélni/át kell programozni). Az új SIM kártyára fel kell tölteni az azonosításra használt kulcsot és algoritmust. A kulcsok kezelése, érvényességük ellenőrzése extra komponenseket kíván a szerver oldalon is.

Kihívás-válasz mechanizmus alkalmazása esetében a szolgáltató egy kihívást generál, amelyre megfelelően kell válaszolnia a felhasználónak. Csak a megfelelő kulcs birtokában adhat jó választ a felhasználó. A válasz képzése történhet titkosítással, vagy bármilyen más kulcs alapú eljárással, például aláírás képzéssel. A *3. ábra* szemlélteti ezt a lehetőséget.

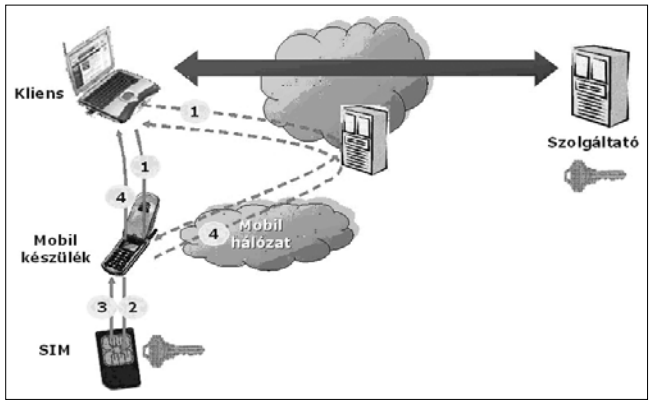


3. ábra Hitelesítés kihívás-válasz algoritmussal

Az eddig leírt felhasználó-hitelesítési lehetőségek közül ez a legbiztonságosabb. A hitelesítés erőssége persze függ a kulcshossztól, a kihívás-válasz algoritmus megválasztásától. Nagy biztonsági szintű, hosszútávon letagadhatatlan felhasználó-azonosítást eredményez, ha az üzeneteket megfelelően naplózzák és tárolják mind a hálózatban, mind a mobiltelefonon. A megoldás bevezetéséhez le kell cserélni/át kell programozni a SIM kártyákat és meg kell teremteni a kulcsok kezeléséhez szükséges infrastruktúrát.

Egycsatornás hitelesítés, kihívás-válasz alkalmazásával

Az előző esetekben a szolgáltató vette fel a kapcsolatot a felhasználó mobil készülékével és számítógépével is, ezáltal kétcsatornás megoldásról beszélhettünk. Elképzelhetőek olyan módszerek is, ahol a felhasználó számítógépe épít ki kapcsolatot a mobil készülékkel, mintegy smartkártya olvasóként használja. A szolgáltatónak ilyen esetekben csak a számítógéppel kell kapcsolatba lépnie, vagyis a felhasználó-hitelesítés egycsatornás [6] *(4. ábra)*.



4. ábra Egycsatornás, kihívás-válasz alapú hitelesítés

A kliens gépnek el kell érni a mobil telefont akár személyi hálózaton (PAN, pl. Bluetooth), akár Interneten és GSM/UMTS hálózaton keresztül. Ha az utóbbit használjuk, meg kell bíznunk a háttérben meghúzódó hálózat biztonságában. Bluetooth-on keresztüli elérés hátránya a kapcsolat felépítésének lassúsága, és nem kidolgozott biztonsági szolgáltatása.

A SIM kártyán tárolt rejtett kulcs megbízható hitelesítést nyújt a szolgáltató felé. Az egycsatornás hitelesítésnél viszont nagyobbak az elvárásaink a kliens oldalon, ezért az korlátozhatja a szolgáltatás mobilitását, skálázhatóságát, illetve veszélyeztetheti a felhasználó kulcsainak biztonságát.

A módszer előnye, hogy a felhasználó hitelesíthető bármilyen Interneten használt, régóta bevált protokollal (például SSL) úgy, hogy a felhasználó rejtett kulcsa a SIM kártyáján marad. Ez magas biztonsági foknak felel meg. A mobil csatorna kimaradásaira és késleltetésére a hagyományos hitelesítő protokollok azonban igen érzékenyek lehetnek, ezért az architektúra tervezése során körültekintően kell eljárni.

3.2. Aláírás mobil készülékkel

A következőkben a digitális aláírás-képzés lehetőségeit soroljuk fel. Az aláírás letagadhatatlanságát úgy lehet biztosítani, hogy semleges résztvevőket nevezünk ki, amelyek naplózzák az aláírás tranzakciók üzenetváltásait, és tárolják az aláírásokat.

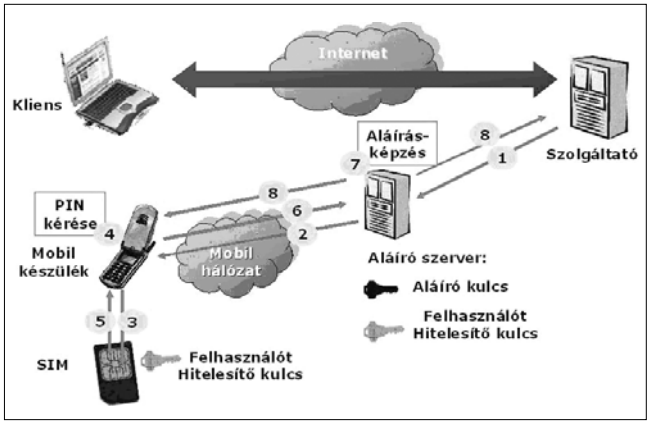
Szerver oldali aláírás, mobil készülék ad utasítást

A legegyszerűbben megvalósítható lehetőség az, ha aláíró szervert hozunk létre, amely tárolja a felhasználó aláíró kulcsát és az aláíró algoritmust. A mobiltelefon szerepe felhatalmazást adni az aláíró szervernek az aláírás létrehozására/végrehajtására. A felhasználó aláíró szerver általi hitelesítése elképzelhető bármelyik

előzőekben tárgyalt felhasználó-hitelesítési módozattal, és ettől függően különböző biztonsági szintű aláírások születhetnek. Fontos, hogy az eljárás során az aláíró szervert is hitelesítse a felhasználó. A módszer előnye, hogy nem kell az alacsony számítási kapacitással rendelkező SIM kártyának aláírnia, nem kell az aláíró kulcsot és algoritmust is tárolnia, és a szerveren hosszabb kulccsal biztonságosabb aláírás is képezhető. Emiatt bevezethetőségének nehézsége megegyezik a kulcs alapú felhasználó-azonosítással. Az aláírás hitelességének szűk keresztmetszete a felhasználó és az aláíró szerver közti kapcsolat biztonsági szintje.

A szolgáltató aláírást szeretne kérni a felhasználótól egy dokumentumra. Elküldi a dokumentumot az aláíró szervernek és esetleg a felhasználó mobil telefonjának. Ha csak az aláíró szerver kapta meg, akkor továbbküldi a dokumentumot – vagy annak egy kivonatát – a mobil telefonra, és kéri a felhasználót az aláírási szándékának megerősítésére. A felhasználó ezután hozzájárul az aláíráshoz egy PIN kód megadásával. A szerver oldali aláírás menetét az *5. ábra* mutatja.

Gyakorlatilag a dokumentum kézhez vétele az egyik legsebezhetőbb pontja a megoldásnak. Olyan módszert kell kidolgozni a dokumentumcserére, amely letagadhatatlan módon tükrözi a felhasználó szándékát. Ha a megerősítés megérkezett, a szerver elkészíti a felhasználó aláírását és visszaküldi mind a szolgáltatónak, mind a felhasználónak, akik azt tárolják.



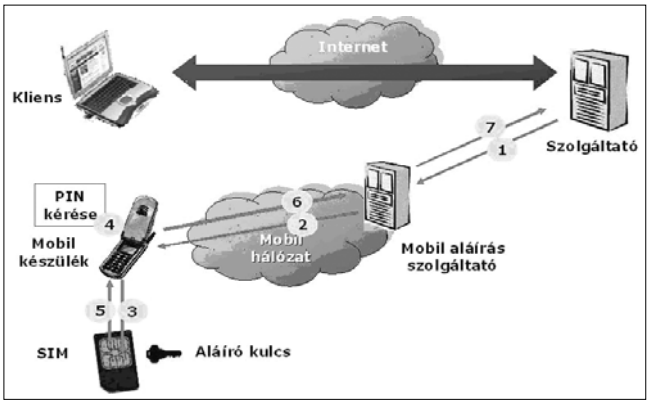
5. ábra Szerver oldali aláírás

A megoldás hátránya, hogy kiemelt hitelességet igénylő aláírás készítésére a megoldás alkalmatlan. A módszer nem felel meg az elektronikus aláírási törvényben leírtaknak, biztonsága a kulcs alapú azonosításnál is maximum közepesnek mondható.

Mobil oldali aláírás (ETSI M-COMM)

Magasabb fokú biztonság a felhasználó kezében lévő chipkártyával, vagyis felhasználó oldali aláírással érhető el. Az ETSI M-COMM Workgroup erre előírásokat dolgozott ki, meghatározta a rendszer komponensek követelményeit és definiált néhány interfészt [4].

Ebben az esetben a szolgáltatók egy speciális hozzáférési szervernek, a mobil aláírás szolgáltatónak (Mobile Signature Server) küldik az aláírandó dokumentumot. A mobil aláírás szolgáltató továbbküldi ezt a mobil csatornán a felhasználó mobil telefonjára. A telefonban lévő chipkártya létrehozza az aláírást. Ehhez a SIM kártyának tartalmaznia kell az aláíró kulcsot és algoritmust. A mobil készülék visszaküldi az aláírást a mobil aláírás szolgáltatónak, aki továbbküldi a szolgáltatónak *(6. ábra)*.



6. ábra Mobil aláírás folyamat

A megoldás biztonságát itt is nagyban befolyásolja a mobil csatornán választott technológiai megoldás biztonsága (WAP, SMS). Bevezetéséhez ebben az esetben le kell cserélni a SIM kártyát, és implementálni kell a mobil aláírás szolgáltatást (mobil aláírás szolgáltató és kapcsolódó funkciói).

Az M-COMM szabványok részletesen leírják a résztvevők feladatait, meghatározzák, hogy milyen interfésszel kell rendelkeznie mobil aláírás szolgáltatónak a szolgáltató felé. A mobil aláírás szolgáltató és a mobil készülék közötti interfészeket viszont nem definiálja. Elképzelhető adatkapcsolt vagy csomagkapcsolt (GPRS), WAP vagy SMS átviteli technológiai megoldás.

Egycsatornás mobil oldali aláírás

A felhasználó-azonosítási módszerekhez hasonlóan, az aláírási folyamat is megvalósítható egycsatornás módszerrel *(4. ábra)*. A szolgáltató elküldi a kliensnek az aláírandó dokumentumot, a kliens gép továbbítja ezt – vagy egy kivonatát – a mobil készülékre. A SIM kártya létrehozza az aláírást, és visszaküldi a kliens gépnek. Ezután a kliens visszaküldi az aláírást a szervernek. A SIM kártyának kell tárolnia az aláíró kulcsot és algoritmust. Nagy biztonságú megoldást jelent, de feltételezi, hogy a felhasználó számítógépe kapcsolatba tud lépni a mobil telefonnal. Bevezethetősége nehézkes, mivel a mobil készülék és a kliens gép közötti kapcsolatnak speciális követelményeket kell kielégítenie (például mindkettő támogassa a Bluetooth technológiát, vagy a felhasználó rendelkezzen adatkábellel).

4. Szempontok a rendszertervezéshez

Az előzőek alapján meg van minden lehetőség arra, hogy olyan eljárások kerüljenek kidolgozásra, amelyek részben vagy egészben tartalmaznak elektronikus ele-

meket, és ezen belül részben vagy teljes egészében a mobil csatornán zajlik. A KET tartalmazza, hogy senki nem kényszeríthető elektronikus ügyintézési út használatára, illetve az eljárás alatt az állampolgár szabadon válthat az elektronikus és hagyományos ügyintézési út között.

Adottak jól működő, szabványosított technológiák és olyan specifikációk, amelyek meghatározzák az elektronikus ügyintézés biztonsági követelményeit. Azonban, hogy minőségileg is megfelelő, sikeres szolgáltatásokat teremtsünk, fontos, hogy a műszaki követelményeknél és a technikai interfészeknél a jelen törvényeket tükröző biztonsági politika kerüljön érvényre. Például meg kell határozni, hogy adott körülmények között milyen adatokat tartalmazzon egy tanúsítvány, mire kell felhívni az állampolgár figyelmét, hogy ne sérülhessenek a jogai, milyen elágazások legyenek az ügyintézésben, így a megvalósító szoftverben.

Vegyük példaként a mobiltelefonnal végzett elektronikus aláírást. Az aláírási politika meghatározza, hogy adott ügymenetben milyen szereplők aláírását várjuk, mire szóljon az aláírásuk, hosszú- vagy rövid távú letagadhatatlanságot nyújtson stb. [18]. Az aláírás többféle szereppel bírhat: felhasználó azonosítása, névvel való ellátás, szervezet pecsétje, delegált személy aláírása, szerződés legális vonzatainak vállalása, tanú, közjegyzői aláírás stb. Fontos, hogy az aláírás megtételénél eleget tegyünk az adott eljárásra érvényes rendelkezéseknek, és az Elektronikus aláírási törvény által megkövetelt biztonsági szintnek.

A biztonsági politikának minél inkább automatizáltan kell működnie, de úgy, hogy a felhasználó egyértelműen kinyilváníthassa szándékát. Az emberi tényező okozhatja a legtöbb hibát, félreértést a mobil aláírórendszer használata során. Fontos, hogy amikor részletekig menően kigondolják a biztonsági politikát, azt is vizsgálják, hogy mi az, ami automatizálható, és mi az, amihez kérni kell az aláíró személy megerősítését. A felhasználó semmiképpen ne mondhassa azt utólag, hogy nem állt rendelkezésére egy szándékát tükröző opció, vagy hogy félrenyomott egy menüpontot.

A biztonságpolitika létrehozása tehát nemcsak mérnöki feladat, hanem egy igen hosszadalmas munka, amelyben mérnököknek és jogászoknak kell együtt dolgozniuk. Az ETSI M-COMM szabványok megfelelő iránymutatást adnak a mobil aláírás tranzakciók és felhasználó-hitelesítés technikai megteremtéséhez, azonban ez még korántsem elég egy használható rendszer megvalósításához.

5. Összegzés

A cikkben bemutattuk, hogy miként használható a mobil csatorna, és hogy ez milyen biztonsági jellemzőket von maga után. Láthattuk, hogy van helye a mobil technológiának egyes közigazgatási és hivatalos eljárások bizonyos mozzanatainak felváltásában, azonban bármilyen rendszert is szeretnénk kialakítani, előtte körültekintően számba kell venni és harmonizálni az esedékes törvényeket, rendeleteket, hogy jogi szempontból is megfelelő biztonságpolitika érvényesüljön. A technológiai feltételek adottak.

A cikk alapját képezi az IKTA 00046/2003 számú pályázat („Elektronikus aláírás mobil telefonnal”) keretében készült tanulmány, illetve az IBM Magyarország Kft. által az Informatikai és Hírközlési Minisztérium részére „Részletes követelményspecifikáció kidolgozása elektronikus aláírás és intelligens kártya használatához a közigazgatás informatikai biztonságának érdekében” című közbeszerzés keretében átadott vonatkozó dokumentumok, melyeket az E-Group Magyarország Rt. készített jelen cikk szerzőinek közreműködésével.

Irodalom

[1] “Directive 1999/93/EC of the European Parliament and of the Council of 13 Decembre on Community framework for electronic signatures”, Official Journal L 013, 19/01/2000, pp.12–20.
[2] “Common List of Basic Public Services”, www.innovazione.gov.it/eng/intervento/e_europe/010501_basicpublicservices_eng.pdf
[3] „Digitális Mobil Gyorsjelentés, 2004. május”, NHH, www.nhh.hu/menu3/m3_2/mobil/2004/majus.pdf
[4] ETSI TR 102 203: “Mobile Commerce (M-COMM); Mobile Signatures; Business and Functional Requirements”.
[5] Liberty Alliance Project: “Introduction to the Liberty Alliance Identity Architecture Revision 1.0”, 03/2003
[6] S. Lannerstrom: ”White Paper Mobile Authentication”, MPM 02:0041, SmartTrust, August 2002
[7] Radicchio Best Practice Working Group: “A universally recognized and accepted identity scheme that leverages the mobile infrastructure.” Working Document, 26th September 2002
[8] Radicchio – http://www.radicchio.org
[9] Liberty Alliance – http://www.projectliberty.org
[10] GSM Association – http://www.gsmworld.com
[11] ETSI – http://www.etsi.org/m-comm/summary.asp
[12] SimPay – http://www.simpay.com
[13] Mobey Forum – http://www.mobeyforum.org/
[14] MeT Ltd. – http://www.mobiletransaction.org
[15] PayCircle – http://www.paycircle.org
[16] Open Mobile Alliance – http://www.openmobilealliance.com
[17] Mobile Payment Forum – http://www.mobilepaymentforum.com/
[18] ETSI TR 102 045: “Electronic Signatures and Infrastructures (ESI); Signature policy for extended business model”, V1.1.1 (2003-03)
[19] WAP Forum: ”Wireless Application Protocol, Public Key Infrastructure Definition”, WAP-217-WPKI, Version 24-Apr-2001
[20] WAP Forum: “Wireless Application Protocol, WAP Certificate and CRL Profiles Specification”, WAP-211-WAPCert, 22-May-2001