SZAKDOLGOZAT

Orosz Attila

Debrecen
2009

Debreceni Egyetem
Informatika Kar

Európai polgárkártyák funkcionalitása és alkalmazásai

Témavezető:
Prof. Dr. Pethő Attila

Beosztása:
egyetemi tanár, dékán, tanszékvezető

Készítette:
Orosz Attila

Szak megnevezés:
Mérnök informatikus

Debrecen
2009

Tartalomjegyzék

I. Bevezetés

Tanulmányaim és a magánéletem során egyaránt körvonalazódott a különböző kártyák használatának fontossága. Úgy érzem ezzel a témával foglalkozni emiatt több szempontból is hasznos lehet. Dolgozatomban arra keresek választ, hogy napjainkban az elektronikusan történő személyi azonosításra milyen technikai megoldások adják a legjobb választ.

A chippel ellátott kártya a különböző kártyafajták legkorszerűbb és legintelligensebb formája. A kártya egy aktív mikrokontrollert és jelentős mennyiségű memóriát tartalmaz, valamint hatékony kriptográfiai és hitelesítési algoritmusok bevezetésére nyújt lehetőséget. A chip kártya tehát sokkal nagyobb lehetőségeket ad a felhasználók és a szolgáltatást nyújtók számára arra vonatkozóan is, hogy az elsődleges feladatok mellett mindkét fél biztonsági igényeit kielégítse.

JAVA chip kártya: Az alkalmazások egyre növekvő száma és az új szolgáltatásokhoz való gyors alkalmazkodás a kártyák egyre sűrűbb cseréjét igényli. Ezen segít a letölthető JAVA alapú alkalmazásokat fogadni képes JAVA chip kártya, mely úgy tud alkalmazkodni újabb és újabb szolgáltatásokhoz, hogy magát a kártyát nem kell cserélni.

A mikrochipek által biztosított intelligencia mennyisége alapján három csoportba lehet sorolni a kártyákat:

- egyszerű memóriakártyák
- generikus kártyák
- programozható kártyák

A témával kapcsolatos eddigi ismereteim szerint az előzetes véleményem és feltevésem, hogy az elektronikus személyi azonosításra az intelligens kártyarendszerek a leginkább alkalmasak.

Ezért a dolgozatomat a következő nagyobb egységekre fogom bontani:

- Az első részben az intelligens kártyák műszaki jellemzőiről, lehetséges funkcióikról, alkalmazási területeikről írok.
- A második részben a kártyahasználat magyar vonatkozásait vizsgálom.

- A harmadik fejezetben néhány európai „jó gyakorlatról”, és bevezetés alatt lévő kísérleti programról is említést teszek, mert a téma újszerűsége miatt többéves jól működő bevált rendszerekről alig lehet még beszélni.

A dolgozatom középpontjába tehát a kártyatechnológiák vizsgálatát helyezem, hiszen, az intelligens kártyatechnológia egyre jelentősebb szerepet tölt be az informatikai piacon, a modern gazdaságban illetve a kiépülőben lévő információs társadalomban. Míg korábban elsősorban a bankrendszer igényeit szolgálta ki, mára már a felhasználás spektruma sokkal szélesebb. A fizikai és logikai hozzáférés-védelemtől kezdve, a tömegközlekedési rendszereken, a mobiltelefonokon át, az egészségügyi, oktatási és a nagy közigazgatási rendszerekig mindenhol találkozhatunk ezzel a technológiával. Az intelligens kártyák minden olyan rendszerben létjogosultsággal rendelkeznek, ahol a biztonság kulcsfontosságú. Mivel a mindennapi élet és munkavégzés terén a számítógépes hálózatok egyre nagyobb jelentőséggel bírnak, a hálózatok adatforgalmának biztonsága is egyre fontosabb, ezért ezen a területen is a chipkártyák szerepének erősödése várható.

Az Európai Unió - mivel az eEurope2005 akcióterv egyik kiemelt célja az intelligens kártyatechnológia elterjesztése - külön munkacsoportot hozott létre, eEurope Smartcard Charter néven, az intelligens kártyák unión belüli elterjesztésére. Ezen belül az egyes albizottságok olyan célterületeket vizsgálnak, mint az egészségügy, a közlekedés, a személyazonosítás, az elektronikus aláírás, a kompatibilitás, vagy a lehetséges felhasználói igények.

Az elkészült Magyar Információs Társadalom Stratégiának (MITS) is fontos része az intelligens kártyák alkalmazására vonatkozó részstratégia. ([4] MITS intelligens kártya …, 2003)

A MITS célkitűzései az intelligens kártyatechnológia nélkül nehezen valósíthatók meg, de annak elterjedése - az említett problémák miatt - akadályokba ütközik. A nemzetközi elemzések – főként kezdeti - rossz tapasztalatai (például FINnish Electronic Identity Card) és a hazai e-közigazgatási program nehézségei azt mutatják, hogy az erőltetett kártyakibocsátás nem vezethet az elvárt eredményre, helyette az előre megtervezett, több szintű, kereslet alapú kártyakibocsátás jelentheti a sikeres megoldást.

A MITS szerint az intelligens kártyarendszerek elterjedésében a kormánynak fontos szerep jut. Természetesen megjelenik kártyakibocsátóként is (pl. oktatási kártyacsalád), de legalább ennyire fontos szerepet kell vállalnia a saját kompetenciájába tartozó működtetési környezet megteremtésében. ([2] MITS, 2003)

II. Intelligens kártyák az informatikai piacon

1. Alkalmazási területek, történeti áttekintés

Az intelligens kártyatechnológia egyre jelentősebb szerepet tölt be az informatikai piacon, a modern gazdaságban illetve a kiépülőben lévő információs társadalomban. Míg korábban elsősorban a bankrendszer igényeit szolgálta ki, mára már a felhasználás spektruma sokkal szélesebb. A fizikai és logikai hozzáférés-védelemtől kezdve, a tömegközlekedési rendszereken, a mobiltelefonokon át, az egészségügyi, oktatási és a nagy közigazgatási rendszerekig mindenhol találkozhatunk ezzel a technológiával. Az intelligens kártyák minden olyan rendszerben létjogosultsággal rendelkeznek, ahol a biztonság kulcsfontosságú. Mivel a mindennapi élet és munkavégzés terén a számítógépes hálózatok egyre nagyobb jelentőséggel bírnak, a hálózatok adatforgalmának biztonsága is egyre fontosabb, ezért ezen a területen is a chipkártyák szerepének erősödése várható.

A mikroprocesszoros intelligens kártya, a gyakorlatban használt jelenlegi technikai körülmények között, a legfejlettebb elektronikus adathordozó megoldást valósítja meg. Az elnevezés széles termékskálát jelöl. Ide tartozik minden olyan bankkártya méretű műanyag kártya, amely beépített mikrochipet tartalmaz, de a mobiltelefonokban használatos SIM kártyák is ide sorolandók. Felhasználásuk és lehetséges alkalmazásuk nagyon sokrétű. Következzenek ezek néhány kiemelt terület köré csoportosítva. ([1] Dr. Ködmön József: Az intelligens kártyák … , 2003)

a) Azonosítás, hitelesítés

Az egyik legnagyobb kihívást személyek – különféle területeken történő – azonosítása jelenti. Jó eredményeket lehet elérni a személyi igazolvány, az útlevél, a gépjármű vezetői jogosítvány és más hasonló igazolványok használatában, ha azokat

megfelelő biztonságú chip-kártyák segítségével valósítjuk meg. Különösen fontos a hagyományos biztosítási és betegkártya kiváltása programozható intelligens kártyával. Eddig nagyon sok kísérlet volt, de a rendszerek általában nagyon sokba kerülnek nem működnek igazán hatékonyan.

A chipkártya alkalmas arra is, hogy fizikai beléptető rendszerekben belépő kártyaként üzemeljen, azaz ajtókra, kapukra szerelve egy-egy chip kártyát elfogadó beléptető terminált (olvasó terminált) kell telepíteni. A kártyát a terminálba helyezve nyithatjuk ki a megfelelő zárakat. A chipkártya programozhatósága miatt, egy ilyen rendszer nagyon rugalmas, sokfajta jogosultságot lehet definiálni az egyes belépési pontokhoz, így igen finoman szabályozható a hozzáférési jogosultság az egyes objektumokhoz. Ezekre a műveletekre szállodákban széles körben használnak mikrochipes kártyákat.

Az azonosító kártyákhoz kapcsolódó PIN, illetve jelszó használatát egyre inkább felváltja a biztonságosabbnak tekinthető biometriai azonosítás, amelyben nagy szerepe van az intelligens kártyák adattároló kapacitásának növekedése.

A fizikai objektumok azonosításának hatékony, új módszere a rádiófrekvenciás azonosítás (RFID), amely igen alacsony költséggel képes nagy mennyiségben objektumok megkülönböztetésére és azonosítására.

Az intelligens kártyák alkalmasak az elektronikus aláírás tárolására is, így hitelesítési megoldásokban is sokféle módon használhatók. A megfelelően kiválasztott chipkártyák nyilvános kulcsú titkosítási műveletek elvégzésére alkalmasak, így a felhasználók ennek segítségével írhatják alá elektronikusan elkészült dokumentumaikat.

A biztonságos elektronikus kereskedelemben is nagy szerepet kaphat a chipkártya, hiszen segítségével a kereskedelmi tranzakciók (rendelés, visszaigazolás, módosítás, fizetés, stb.) elektronikus aláírással hitelesíthetők.

A chipkártyával együtt alkalmazott elektronikus aláírás jól használható további más tranzakciók hitelesítéséhez. Például házibank tranzakciók, az orvos-beteg

találkozások alkalmával keletkezett adatok hitelesítése, vagy adóbevallások és egyéb fontos dokumentumok hitelesítése.

b) Kommunikáció

A korszerű mobiltelefónia elképzelhetetlen nagy biztonságú chipkártyák használata nélkül. A jelenleg használt GSM telefonok SIM kártyája természetesen intelligens kártya. Küszöbön áll a harmadik generációs mobiltelefon szabványnak megfelelő rendszerek bevezetése, ahol a legfejlettebb technológiájú chipkártyák kapnak meghatározó szerepet.

c) Fizetési eszköz

Szintén gyakori alkalmazás a készpénz használatát kiváltó „plasztikpénz”, a bankkártya. Jelenleg még főként mágnescsíkot tartalmazó bankkártyák vannak használatban, a nagy kártyarendszerekben (Visa, Master, stb.) már megkezdődött a chipet tartalmazó, nagyobb biztonságú bankkártyák bevezetése.

Az elektronikus pénztárca szintén intelligens kártyával működik, elsősorban kis összegű fizetések esetén használatos.

A chipkártyák képesek egy úgynevezett “gödör” alkalmazás segítségével pontokat is tárolni. Azaz egész számokat alapul véve pontokat írhatunk fel a kártyára és onnan a megfelelő kártyaolvasókkal pontokat tölthetünk le. A kártyánkra egy pénztárban vagy a megfelelő pontfelíró helyen pontokat tölthetünk fel, és utána a feltöltött kártyával fénymásolhatunk, vagy használhatjuk az ital automatáknál.

A chipkártya alkalmas arra is, hogy a vásárlásaik során a kereskedők hűségpontokkal jutalmazzák a vevőiket. Ekkor a kereskedő nem a vásárolt termék vagy szolgáltatás árából ad közvetlen százalékos kedvezményt, hanem a vevő a vásárlás értékével arányos pontokat kap a kártyájára, amit a következő vásárlások alkalmával elkölthet. Ez a loyalty rendszer.

Természetesen egy ilyen előre feltöltött kártya akár étkezési utalványként, könyvutalványként, speciális vásárlási utalványként is szerepet kaphat.

A chipkártyák szabad memória részén adatok tárolhatók. Az adatokat természetesen titkosítva, a kártyán tárolják, így offline módon - hálózati alkalmazás nélkül - lehet biztonságosan adatokat cserélni. Ennek a funkciónak gyakorlati jelentősége a különböző jegyek és bérletek vásárlásánál használható fel. Az intelligens kártyák használatával a jegyeket, bérleteket nem kell kinyomtatni, hanem a kártyán lehet tárolni. Ebben az esetben akár színház vagy mozijegyek, akár utazáshoz szükséges menetjegyek, bérletek tárolása is megoldható.

d) Szórakozás

A szórakoztató elektronika területén is egyre nagyobb teret nyernek a chipkártyás alkalmazások. Főként a kábeltelevíziós rendszerekben terjedt el, a hozzáférési jogosultságok szabályozásában. Magyarországon ezek a megoldások kevésbé terjedtek el.

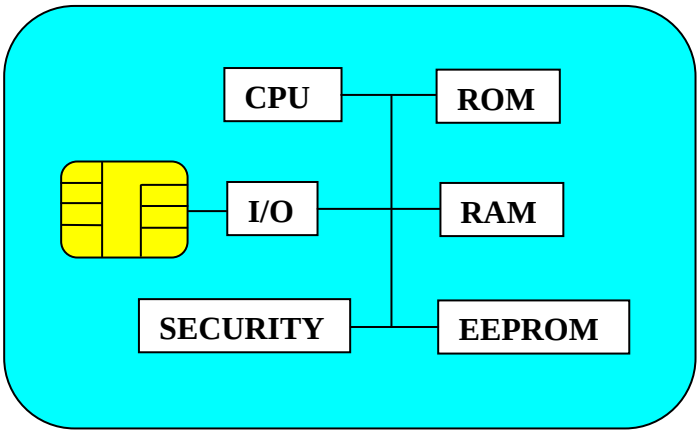
Ezen a területen jelentős gond a szerzői jogok megsértése, ezért a jövőben a CD és DVD lemezek használatát felválthatja az intelligens chipet tartalmazó multimédia kártya, amely lehetővé teszi a szerzői jogok hatékonyabb védelmét.

e) Számítógép használat

A számítógépek használatának jogosultsági ellenőrzésében is meghatározó szerepet kaphat a chipkártya. A felhasználó azonosítás biztonsága jelentős mértékben javítható, ha a jelszó megadásán túl egy chipkártya behelyezésével valósítjuk meg a „birtokol valamit és tud valamit” azonosítási elvet. A kártyán lévő adatok pedig meghatározzák a felhasználó jogosultságait a rendszerben.

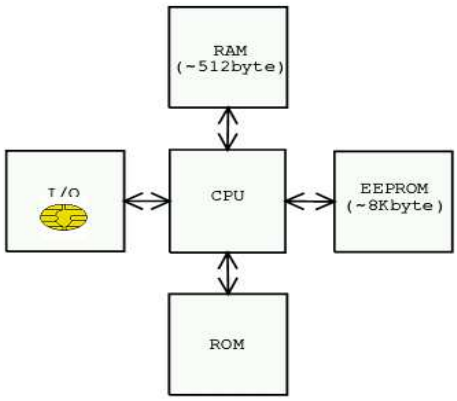
2. A kártya felépítése, működése

Az intelligens kártya (további elnevezései: chipkártya, mikroprocesszoros kártya, smartcard) egy olyan szabványos méretű plasztik lap, amely tulajdonképpen egy külső táplálású számítógép. Rendelkezik saját processzorral, RAM és ROM típusú memóriával, de háttértárolási lehetősége nincs. A külső táplálás pedig azt jelenti, hogy általában a kártyán nincs áramforrás, így az csak az író/olvasó berendezésbe helyezve képes működésre. A kártyán lévő chip programozható, egyszerre több funkciót is képes ellátni.



1. ábra. A kártya logikai felépítése

Ennek alapján a chipkártyát számítógépnek tekinthetjük. Valójában nem is egyszerű számítógépekről van szó, hanem különleges, biztonságos számítógépekről. A biztonság ezen kártyák fő erőssége. Ez kiderül blokkvázlatukból is (2. ábra). A fő különbség a Neumann-féle architektúrájú számítógépek és a chipkártyák között, hogy az utóbbi esetben az I/O perifériák nem kapcsolódnak közvetlenül a belső buszokra. ([13] CC Projekt, 2007)



2.ábra. Egy chipkártya belsejének blokkvázlata

Chipkártyák esetében a külvilág (I/O periféria) és az adattároló egység (EEPROM) között egy döntő logika helyezkedik el, amely a bemenetet megszűrheti, felülbírálhatja. Az ábrán látható egységek egyetlen chipben helyezkednek el, nincsenek közöttük buszok, amelyeket egy külső támadó esetleg lehallgathat. A chip pedig olyan mikroelektronikai technológiák segítségével készült, hogy minél nehezebb legyen belőle információkat a kártya felnyitása esetén kinyerni.

A kártyát kívülről egynek és oszthatatlannak szeretnénk tekinteni, amelyből információkat csakis a kontaktuson keresztül nyerhetünk ki. A kontaktusok jelentik a kártya egyetlen kapcsolatát a külvilággal. Ez fontos, hiszen a chipkártyák biztonságának egyik legjelentősebb pillére az, hogy csakis egy jól definiált és jól ellenőrzött interfésszel rendelkeznek a külvilág felé.

A chipkárya tehát abban különbözik egy egyszerű telefonkártyától, hogy míg a telefonkártya a gyártás után a továbbiakban már nem változtatható (memória kártyaként működik), addig a chipkártya a beépített mikroprocesszora segítségével programozható, a kibocsátás után is rendelkezik olyan területekkel, ahová további adatokat lehet írni, majd azokat feldolgozni és kiolvasni.

Vannak olyan chipkártyák is, amelyeket nem szükséges behelyezni az író/olvasó készülékbe, megfelelő távolságról képesek kis méretű antennájuk segítségével kommunikálni. Ezeket kontaktus nélküli chipkártyának nevezik.

A chipkártya input-output műveleteket csakis a mikrochip kontaktusain végezhet. Miközben ez a szűk interfész a kártya adatainak biztonságát szolgálja, megakadályozza a felhasználót azok közvetlen elérésében. A kártya nem képes közvetlenül kommunikálni még a saját felhasználójával sem, így ezt egy másik eszköz, az ún. terminál biztosítja.

A biztonságos adattárolás érdekében a kártyán tárolt adatokat a legtöbb esetben kriptográfiai módszerekkel titkosítják is, ezzel magasabb biztonsági követelményeket is ki tudnak elégíteni, szemben - a korábban bevezetett és mára eléggé elterjedt - mágneskártyákkal.

Az intelligens kártyák mindennapjaink részévé váltak. Megtalálhatóak minden GSM telefonban, törzsvásárlói kártya tulajdonosok millióinak pénztárcájában. Jelenleg már több mint 2.5 milliárd kártya van használatban világszerte. Kelet Európában is gyorsan fejlődik a kártyaipar, rengeteg új, izgalmas üzleti lehetőség kínálkozik számos szervezet számára. A jelenlegi trendek alapján az intelligens kártya projektek tömeges elterjedésének eljött az ideje Kelet Európában is.

Évről évre egyre több chipes intelligens kártyát bocsátanak ki a különféle ágazatokban. Az idei válság nemigen érinti az iparágat, hiszen az okos plasztiklapokkal költséget lehet megtakarítani, emellett növelik a biztonságot is.

3. A chipes kártyák csoportosítása

Ha azt mondjuk, „chipkártya” (smart card), akkor csupán azt mondtuk, hogy a kártyán mikrochip található. Arról nem szóltunk, hogy ez a mikrochip mekkora intelligenciát biztosít a kártya számára. E fejezetben a chipkártyák három csoportját, generációját, mutatjuk be, melyek nemcsak időben követik egymást, de a kártyában lévő intelligencia szempontjából is három egymást követő szinten helyezkednek el.

1) **A legegyszerűbb chipkártyák az ún. memóriakártyák.**

   Ez esetben a kártyán lévő IC lényegében egy memóriachip. A terminál közvetlenül hozzáfér a chip tartalmához: olvashatja, írhatja. Ezek a kártyák a logikai biztonság szempontjából nem jelentenek komoly áttörést a mágneskártyákhoz képest, az általuk nyújtott logikai biztonság egy floppy diskével egyenlő. Nem képesek számítások elvégzésére, elterjedten használják telefonkártyák kivitelezésénél.

2) **A generikus kártyák (vagy fájlrendszer-kártyák)**

   Jelentős előrelépést jelentett ezen eszközök megjelenése**.** Logikai és esetleg kriptográfiai módszerek segítségével védik a rajtuk tárolt adatokat. Az adatok fájlokba, azok pedig fájlrendszerekbe szerveződnek. A kártyán definiálhatunk felhasználókat, és azok jogosultságait. Megadhatjuk, mely felhasználóknak milyen módszerrel szükséges azonosítani magukat – PIN kód, kihívás és válasz, esetleg biometria -, illetve mely fájlokhoz, könyvtárakhoz milyen módon (írás, olvasás, inkrementálás, stb.) férhetnek hozzá. A legújabb generikus kártyák szimmetrikus és nyilvános kulcsú kriptográfiai módszerekkel is védhetik az adataikat. Ezen kártyák nevében a „generikus” szó arra utal, hogy a kártyagyártó általános eszközt ad el, amelynek funkciói testre szabhatóak, így az eszköz sokféle célra felhasználható. Nem szükséges tehát minden célra külön kártyát gyártani, a termelés legutolsó fázisa az ún. perszonalizálás (felhasználók, fájlrendszer, kulcsok, jogosultságok kártyára való

felvitele) a kártyakibocsátóhoz kerülhet, míg a gyártó általános célú kártyákat hozhat létre, így azokat – a nagy példányszám miatt – jelentősen olcsóbban állítja elő.

3) **A programozható kártyák képezik a chipkártyák harmadik generációját.**

Ezen eszközök a generikus kártyák minden tudása mellett, képesek felhasználói programok futtatására. Ez azt jelenti, hogy – akár a kártya élete során – letölthetünk rá újabb alkalmazásokat, s ezeket rajtuk futtathatjuk. Ez nemcsak azt eredményezi, hogy bármikor kiterjeszthetjük a kártya által nyújtott szolgáltatásokat, hanem azt is, hogy jóval nagyobb intelligenciával ruházhatjuk fel őket, mint a generikus kártyákat. Míg egy generikus kártya esetén csupán az adatok struktúráját, és azok hozzáférési lehetőségeit állíthatjuk be a perszonalizáció során, egy programozható kártya segítségével bármilyen védelmi mechanizmusok és műveletek implementálhatóak, határtalan teret nyitva ezzel a kártyakibocsátóknak.

Fontos kihangsúlyozni, hogy a generációk közötti határ korántsem éles. A memóriakártyák és a generikus kártyák egyaránt adattárolásra szolgálnak, csupán az utóbbi csoport kevésbé enged közvetlen hozzáférést az adatokhoz a külvilág számára.

A generikus kártyák és a programozható kártyák közti határ sem határozott. Egyes generikus kártyák jelentős kriptográfiai képességekkel rendelkeznek, és védelmi mechanizmusaik is roppant rafináltak lehetnek. A fő különbség – amely egyben jól definiált határvonalat is jelent – az, hogy amíg a generikus kártyák processzorán csakis az a kód futhat, amelyet gyártójuk engedélyezett, és rájuk telepített, a programozható kártyák felhasználó által írt kódot is végrehajthatnak.

4. Kártyák az üzleti világban

A világ intelligens biztonsági iparát képviselő Eurosmart szövetség legfrissebb előrejelzése szerint ebben az évben 4,4-4,6 milliárd új, a mikrokontrollert tartalmazó intelligens kártyát bocsátanak ki világszerte, ami akár 10 százalékos növekedés is lehet a 2008-ban forgalmazott chipes plasztiklapok számával összehasonlítva.

A nemzetközi chipkártya üzletág három vezető szereplője - a Gemplus, a Sun Microsystems és a Visa International - új, mindössze három dollár költséggel előállítható,

Open Platform alapú intelligens kártyát mutatott be 2008 júliusában. A GemXpresso Lite nevű intelligens kártya a több alkalmazást is támogató Java Card platformra épül. Az új plasztiklap különféle alkalmazáskombinációk hordozására képes. A törzsvásárlói, biztonságos Internet-hozzáférés és elektronikus pénztárca funkciók a Visa megszokott debit/credit fizetési alkalmazásaival párhuzamosan telepíthetők a kártyára. Az Open Platform egyik legnagyobb előnye a dinamikus letöltési képesség, amely révén a kártya funkcionalitása a kibocsátás után is rendkívül biztonságosan bővíthető új alkalmazásokkal, a szükségtelenné vált funkciók pedig könnyen eltávolíthatók a kártyáról.

Az Open Platform 2.0 és a Java Card 2.1 specifikációk előírásait teljes mértékben kielégítő GemXpresso Lite kártyát valamennyi, többfunkciós chipkártyák bevezetése iránt érdeklődő Visa partnerbank kínálhatja ügyfeleinek. Jelenleg ez a termék a piac legolcsóbb kártyája - előállítási költsége csupán fele a hasonló plasztiklapoknál megszokott átlagos összegnek.

A Visa kártyatársaság a Visa Smart Partner program keretében segítette a Gemplust az új termék kifejlesztésében. Ez a kezdeményezés a stratégiai tervezés, a termékfejlesztés, az árképzés, az értékesítés és a marketing terén nyújt támogatást a kártyapiac szállítóinak. A program a Visa szabványfejlesztési és márkaépítési törekvéseit, valamint pénzintézeti kapcsolatait kívánja összekapcsolni a nemzetközi szállítók erőfeszítéseivel. A résztvevők nyereségességi mutatóit javító kezdeményezés egyben a chipkártyákra való áttérést szorgalmazó Visa-stratégia megvalósítását is előmozdítja.

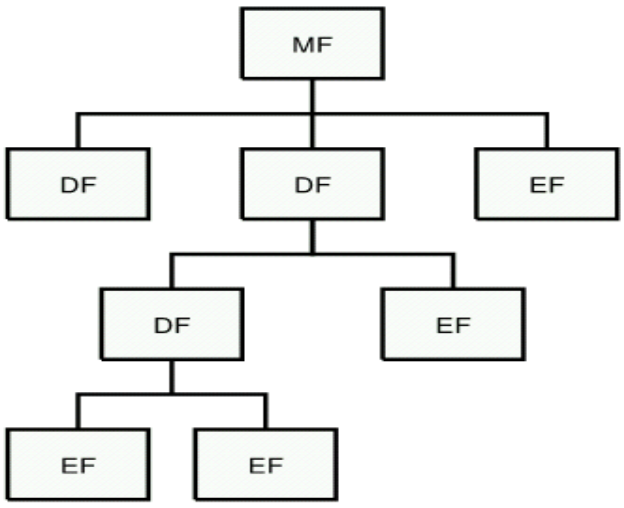
A Microsoft meglehetősen későn lépett be a smart card piacra, de kártyájuk hardware tekintetében napjaink egyik legerősebbje. Ugyanakkor a Microsoft – kijelentéseik szerint – az általuk készített intelligens kártyákat is csak Windows NT-s hálózatok kiegészítő alkatrészeinek tekinti. A kártyák feladata tehát első sorban a hálózati belépés (logon) illetve hálózati erőforrás-hozzáférés kezelésének támogatása, másrészt pedig – az Outlook részeként – elektronikus levelek titkosítása, hitelesítése.

A WinCardon egy 8 bites RISC AVR MCU processzor van, s rendelkezik emellett 32 kilobyte Flash Program Memory-val az applikációk számára, 32 kilobyte EEPROM-mal a tárolandó adatok és 1 kilobyte SRAM-mal a változók, dinamikus adatok, stack stb. számára, továbbá egy ATMEL kriptográfiai műveleteket támogató koprocesszorral.

A többfunkciós intelligens kártyák számos előnyt kínálnak a kártyapiac szereplőinek. Segítségükkel a bankok új, értéknövelt szolgáltatásokat vezethetnek be, amelyek révén növelhetik kártyáik forgalmát, új bevételi lehetőségekhez juthatnak, szorosabb kapcsolatot építhetnek ki ügyfeleikkel. Az intelligens kártyák hátterében álló fejlett chiptechnológia csökkenti a visszaélések gyakoriságát, és növeli a pénzintézetek működési hatékonyságát.

A piacvezető Gemplus vezeték nélküli és e-business alkalmazásokhoz szállít chipkártyaalapú megoldásokat. A tanácsadást, tervezést, szoftver- és hardverfejlesztést, valamint személyre szabott jellemzőket és teljes körű bevezetési szolgáltatásokat is kínáló cég átfogó, integrált és egyedi chipkártyaalapú rendszerek kiépítésében segíti ügyfeleit.

A vállalatcsoport ügyfélköre Gemplus mikroprocesszoros és memória-chipkártyákat, intelligens érintkezés nélküli kártyákat, elektronikus címkéket, különféle intelligens eszközöket és mágnescsíkos kártyákat használ az alkalmazások széles körének egyszerűsítésére és biztonságuk növelésére. A világhálós és mobilkereskedelemtől kezdve a pénzügyi tranzakciókon, törzsvásárlói programokon, szállításon, oktatáson és egészségügyön keresztül a személyazonosításig, előfizetéses rendszerű tévéprogramokig, valamint fizikai és logikai beléptetésig a Gemplus számos területen biztosít teljes körű intelligens megoldásokat, és növeli az emberek milliói által szerte a világon igénybe vett rendszerek biztonságát, kényelmét, illetve használatuk egyszerűségét.



3. ábra. Az ISO 7816-4 szabvány által definiált fájlrendszer

5. A kártya fájlrendszere, a legfontosabb szabványok

Az ISO 7816-4 szabvány definiálja az intelligens kártyákon használt fájlrendszert. A szabvány két fájltípust definiál: az egyik az ún. dedicated file (DF), amely a PC-s fájlrendszerekben a könyvtár fogalmának felel meg, a másik pedig az ún. elementary file (EF), amely adatokat tartalmazhat. Minden fájlt 2 bájt hosszú file identifier (FID) azonosít, ezen FID azonosítók az adott DF-en belül egyediek. A DF-ek az FID mellett névvel is rendelkezhetnek. Minden kártyán van egy kitüntetett DF, az ún. master file (MF), amely a PC-s fájlrendszerekben a gyökérkönyvtár fogalmának felel meg. Az MF FID-je kötött: 3F00.

Mindig van egy kiválasztott fájl, ez alapértelmezés szerint az MF. A Select File paranccsal más fájlokat (EF-et vagy DF-et) is kiválaszthatunk. Az írás/olvasás parancsok általában kiválasztott fájlokra vonatkoznak.

A napjainkban használatos technológiák lehetővé teszik, hogy egy kártyán több szolgáltatás is szerepeljen, több funkció is megvalósítható legyen (multifunkcionális kártyák).

A kormányzat által kialakítandó megfelelő működési környezet pedig lehetőséget biztosít arra, hogy az egyes kártyakibocsátók - a közös szabványok és szabályok keretein belül - más kártyakibocsátók szolgáltatásait is szerepeltethessék az általuk kiadott kártyákon illetve, hogy egy adott szervezet által kibocsátott kártyára később más szervezetek szolgáltatásai is felvihetők legyenek. Így a kibocsátó saját funkciói mellett más szervezetek funkcióit is egy kártyán lehet közösen működtetni (interoperabilitás).

Az Intelligens Kártya (Smart Card) kifejezés az e-ID White Paper és a CEN/CWA 15264 szellemében a fizikai kártyaformátum csak ott kötelező, ahol a kapcsolódó okmány funkció a kártya formátumot előírja, mely esetben a CEN/TS 15480-1 szabvány az irányadó. Intelligens kártya alatt tehát valamilyen intelligens – előre meghatározott funkcionalitás végrehajtására alkalmas – chip platformot (chipmodul, operációs rendszer, fájlrendszer, aláíró alkalmazás, vagy applet) értünk, ami többek között USB biztonsági eszközzel, vagy mobil SIM kártyával is kielégíthető.

Az intelligens kártyák múlti-funkcionalitása sokrétű felhasználást (azonosítás, értéktárolás, off-line adattárolás) biztosít, ezért elengedhetetlen az egységes kártyaszabványok elfogadása, honosítása. A legfontosabb szabványok az alábbiak:

- ISO 7810: a kártyák méretének és egyéb fizikai tulajdonságainak meghatározása,
- ISO 7811, 7812, 7813: mágnescsíkos kártya leírása,
- ISO 7816: chipkártya leírása,
- ISO 10356, 14443, 15593: kontaktus nélküli kártya leírása,
- EMV, SmartEMV: Euro pay, MasterCard és Visa bankkártya interoperabilitási szabvány.

A legfejlettebb megoldások egy intelligens kártyán képesek integrálni az alábbi öt lehetőség bármilyen kombinációját:

1) mágnescsík (klasszikus mágneskártya – nem intelligens),
2) kontaktusos chip (klasszikus intelligens chipkártya),
3) kontaktus nélküli chip antennával (13.56 MHz-es technológia),
4) kontaktus nélküli proximity chip antennával (125 kHz-es technológia),
5) Wiegand-csík (egyértelmű azonosítást segítő, biztonságot növelő technológia). Az intelligens kártyák programozására számos eszköz és módszer használatos, ezek közül a legelterjedtebb szabványos megoldások:

   - OpenCard Framework: a legnagyobb gyártók közös interfésze, amely Java technológián alapul, ezért a lehető legnagyobb portabilitást és interoperabilitást biztosítja az alkalmazások számára
   - PC/SC: az intelligens kártya és a számítógép Windows platformja között biztosít szabványos együttműködést
   - Az összetett, nagyméretű alkalmazások gyakran multifunkciós intelligens kártya használatával működnek. Lényegében két multiapplikációs operációs rendszerrel (MAOS) működő intelligenskártya-platform létezik: a Java Card és a MULTOS.

a) MULTOS inteligenskártya-platform

A MULTOS-t a brit NATWest Development Team fejlesztette ki. Ezt a biztonságos platformot eredetileg elektronikus pénztárcához szánták; nem véletlen, hogy a bankszektorban látta meg a napvilágot. Az összes platform közül ez tekinthető a legkiforrottabb megoldásnak. A szakma legmagasabb elismerését, az ITSEC E6 High minősítést is elnyerte, mivel egy MAOSCO nevű konzorcium ellenőrzi a kártya specifikációit. Ez a konzorcium a

biztonságot mindenek fölé helyezi, ragaszkodik ahhoz, hogy minden MULTOS implementáció elnyerje az ITSEC legmagasabb minősítését.

A MULTOS egy konkurens megoldás az intelligens kártya programozására. A rendszer egy saját operációs rendszert és programozási nyelvet (MEL) tartalmaz

A MULTOS-nak, mint szabványnak kitűnő az átjárhatósága. Tartalmaz operációs rendszert, virtuális gépet, valamint kártyamenedzsert. A fejlesztés Java, C vagy a gépi kódhoz hasonló MEL nyelveken történhet, amelyet a kifejlesztett fordítók bájtkódra fordítanak és az elektronikusan, CA által hitelesített alkalmazások installálhatók a kártyára. Kétségtelen, hogy ez a legdrágább kártya a piacon, de a legbiztonságosabb is.

Egy ilyen rendszerű intelligens kártya újdonsága a kártyára integrált komplett számítógép. A kártyán elhelyezett mikroprocesszorok mindenféle számítási és egyéb műveleteket végezhetnek a memóriájukban tárolt adatokkal és programokkal, vagyis alkalmazásokat futtathatunk rajtuk. Ebben a rendszerben több alkalmazást is fel lehet tölteni a kártyára, és azok egymástól függetlenül futhatnak. A biztonsági funkciók a feltöltött alkalmazásoktól teljesen elválasztva, azoktól függetlenül működnek.

b) Java Card inteligenskártya-platform

A Java Card alapja egy szilíciumlapkára felvitt, ROM-mal és EEPROM-mal felszerelt mikroprocesszor. A kártya a felhasználó által is programozható egy számítógéphez csatlakoztatott kártya író-olvasó segítségével. A felhasználó programozási ismereteit használva csökkentett képességű és kisebb memóriaigényű programokat (applet) írhat, amelyekkel a kártya lehetőségeit és a kártyán tárolt adatokat bővítheti, illetve kezelheti. ([1] Dr. Ködmön József: Az intelligens kártyák … , 2003)

Az intelligens kártyák használatához feltétlenül szükséges a megfelelő infrastruktúra kialakítása. Ennek a legfontosabb alkotóelemei a következők:

- intelligenskártya-kompetencia központ (a kártya, a kibocsátó, az alkalmazás és a szolgáltató hitelesítése, illetve regisztrálása),
- tranzakció hitelesítő központ.

Az intelligens kártyát használó alkalmazások biztonságát a fizikai, ügyviteli és algoritmusos védelem hármas egysége határozza meg Az informatikai alkalmazások és eszközök biztonságos fejlesztésére és biztonsági értékelésére létrehozott Common Criteria alapján kidolgoztak egy intelligenskártya védelmi profilt, amelynek hatóköre a kártyába ültetett chipre és a kártya operációs rendszerére terjed ki. A védelmi profil részletesen tárgyalja a veszélyforrásokat, az elérendő védelmi célokat és az azokat kielégítő követelményeket.

Kitüntetett szerepet kap az intelligens kártyák biztonságos működése terén a SAM (Security Access Modul), amely egy alkalmazás és a kártya közötti kommunikáció biztonságáért felelős. A felhasználó által működtetett alkalmazás valójában a SAM-ot utasítja, azzal kommunikál, majd pedig a SAM fordítja le az utasítást a kártya számára, miközben a kártyaprocesszor ellenőrzi a művelethez való jogosultságot is. Az alkalmazások működése során valójában két eszköz SAM-ja kommunikál egymással minden olyan esetben, amikor egy kártya és egy író/olvasó eszköz adat cserét hajt végre.

A kártya külső megjelenésében olyan biztonsági elemek megjelenítése szükséges, amelyek lehetővé teszik, hogy kellő bizonyossággal megítélhető legyen az adott kártya valódisága és bizonyos esetekben a kártyabirtokos személyazonossága is. A leggyakoribb, jellemző fizikai biztonsági elemek: a kártyatulajdonos fotója és aláírása, továbbá a hologram, a mikro-nyomtatás, a dombornyomás, a lézergravírozás és a kevéssé ismert Wiegand-csík.

A 3M új védőfóliát fejlesztett ki érintkezés nélküli intelligens kártyákhoz és elektronikus útlevelekhez. A papírtokra emlékeztető borító valójában vékony, rézbevonatú polimer. A fémréteg blokkolja a rádióhullámokat s ezzel megakadályozza a rosszindulatú hozzáférést a kártyachiphez. A bevonatra nyomtatni is lehet, így a kártya védőburkos felülete marketingcélokra is felhasználható.

Az ügyviteli védelem az informatikai rendszert üzemeltető szervezet ügymenetébe épített védelmi intézkedések, biztonsági szabályok, tevékenységi formák együttese, amelyet

jogszabályok, szabványok, ajánlások és az üzemeltető szervezet Informatikai Biztonsági Szabályzata ír le. Míg a fizikai védelem a rendszerbe való engedélyezett belépési pontokat jelöli ki, addig az ügyviteli védelem a belépési pontok igénybevételének elfogadható, elvárt formáit rögzíti. Az ügyviteli védelem mintegy összekapcsolja a fizikai és algoritmusos védelem eszközrendszerét, ezzel valósítva meg az informatikai biztonság teljességét.

A CEN/TS 15480 szabvány, amelyet a Magyar Szabványügyi Testület magyar szabványként is kihirdetett (European Citizen Card [ECC]), 2007 májusában történt elfogadásával megszületett az európai szinten a közös álláspont, ami lehetővé teszi az elektronikus azonosításra, hitelesítésre és aláírásra alkalmas ún. EID (Electronic Identity) kártyák kibocsátását. Ezek az eszközök egyrészt nemzetközi szinten is elfogadhatók, másrészt a szabvány keretein belül képesek alkalmazkodni a tagországok eltérő közigazgatási és adatvédelmi rendszeréhez. Lehetőség nyílt tehát arra, hogy a tagországok kormányai olyan elektronikus azonosító és aláíró eszközöket biztosíthassanak állampolgáraik részére, amik nemcsak az országhatárokon belül, hanem azon kívül is alkalmasak az állampolgár elektronikus azonosítására, illetve az okmányként kibocsátott kártyák esetén a vizuális azonosításra, valamint lehetővé teszik az elektronikus ügyintézést a független kártyaelfogadó infrastruktúrákon és információs rendszerekben.

A Közigazgatási Informatikai Bizottság 26. számú ajánlásaként adta ki 2008. július 15-én, a “A Magyarországon elektronikus azonosításra, hitelesítésre, aláírásra és elektronikus azonosítók hordozására alkalmas eszközök követelményei” című dokumentumot, amely egységes keretben, követelményjegyzékben fogja össze a Magyarországon az elektronikus azonosító (EID) kártyák kibocsátásához szükséges és meghatározó követelményeket. A Követelményrendszer – a Miniszterelnöki Hivatal Elektronikuskormányzati Központ megbízásából készült és az időközben elkészült [ECC] szabvány tükrében felváltja a korábban – 2005-ben – kiadott HUNEID specifikációt.

A dokumentum célja olyan egységes követelményrendszer megfogalmazása, amely egyértelművé teszi a Magyarországon biztonságos elektronikus azonosításra-hitelesítésre, aláírásra, valamint az egyéb azonosító adatok tárolására alkalmas intelligens kártyák kibocsátását és alkalmazását a közigazgatás egészére. Mindezekkel gyártófüggetlen, platformfüggetlen és alkalmazásfüggetlen módon kívánja elősegíteni az intelligens kártyák

elterjedését kibocsátótól függetlenül a magyar információs társadalmi törekvések megvalósításához.

Az intelligens kártyák használata nagyon fontos szerepet tölt be az információs társadalomban, azonban elterjedése a magas költség- és infrastruktúraigény miatt akadályozott. Ebben a helyzetben kimondottan fontos az állami szerep-vállalás.

III. Intelligens kártyák Magyarországon

1. A kormány szerepe feltételek megteremtésében

Az intelligens kártyák hazai alkalmazási lehetőségeivel kapcsolatos széleskörű szervezéssel a gyártók, az alkalmazás-szállítók, a felhasználók, valamint az állami szerepvállalók 1997-ben hívták létre az Intelligens Kártya Fórumot ([14] www.hscf.net), mely szakmai szervezetként a Neumann János Számítógép-tudományi Társaság keretein belül működik.

Az IKF rendszeres szakmai napokkal, szakértői tevékenységével valamint ajánlásaival a magyar kártyapiac szakmai közösségét hivatott megteremteni. Szolgáltatási tevékenysége nyilvános, azok a rendszeresen megjelenő hírlevelekben és az Interneten ismerhetők meg. A nyilvánosság, és a tájékoztatás kiterjed az Intelligens Kártya Fórum működésének, a szolgáltatások igénybevételének módjára, illetőleg a beszámolók tartalmára. ([7] www.ekk.gov.hu)

Hasonló szerepet tölt be a nemzetközi információszolgáltatás területén a Java Card Forum amely nagyon sokféle tematikus fórum működtetésével segíti a Java kártya felhasználók naprakész tájékozódását és fejlesztői munkáját.

A Magyar Köztársaság kormánya 2002. végén határozatot fogadott el a Magyar Információs Társadalom Stratégia (MITS) elkészítésére vonatkozóan.

Az Informatikai és Hírközlési Minisztérium az intelligens kártyák alkalmazását olyan nagy jelentőségű horizontális, sok ágazatot, alkalmazási kört érintő szakterületként értékelte, amelyre – a határozatnak megfelelően - külön részstratégiát dolgoztatott ki.

Az elkészült Magyar Információs Társadalom Stratégiának (MITS) is fontos része az intelligens kártyák alkalmazására vonatkozó részstratégia. A MITS az alábbi alapvető problémákat jelölte meg az intelligens kártyatechnológiák elterjedésével kapcsolatban:

- a kártyakibocsátás költségei jelentősek,
- jól üzemelő, viszonylag bonyolult háttér-infrastruktúrára van szükség,
- csak valós igényeket kielégítő, tökéletesen szervezett, következetesen kiépített kártyarendszerek működtethetők hatékonyan.

A MITS célkitűzései az intelligens kártyatechnológia nélkül nehezen valósíthatók meg, de annak elterjedése - az említett problémák miatt - akadályokba ütközik. A nemzetközi elemzések – főként kezdeti - rossz tapasztalatai (például FINnish Electronic Identity Card) és a hazai e-közigazgatási program nehézségei azt mutatják, hogy az erőltetett kártyakibocsátás nem vezethet az elvárt eredményre, helyette az előre megtervezett, több szintű, kereslet alapú kártyakibocsátás jelentheti a sikeres megoldást.

A MITS szerint az intelligens kártyarendszerek elterjedésében a kormánynak fontos szerep jut. Természetesen megjelenik kártyakibocsátóként is (pl. oktatási kártyacsalád), de legalább ennyire fontos szerepet kell vállalnia a saját kompetenciájába tartozó működtetési környezet megteremtésében:

- a szükséges keretrendszer, szabványok és jogszabályok kialakításában, és a szabályozási környezet kialakításában (különös tekintettel a multiapplikációs platformokra és az interoperabilitásra)
- részletes követelményspecifikáció (keretrendszer) kidolgozásában az elektronikus aláírás és az intelligens kártya használatához, az informatikai rendszerek (kiemelten az eKözigazgatás) biztonságának megteremtésében
- az e-személyazonosítás szabványosításában,
- a nyilvános kulcsú infrastruktúra és az elektronikus dokumentumkezelés általánossá tételében,
- a technológiai és biztonsági szabályok kidolgozásában és felügyeletében.
- források biztosításában
- az eKormányzat információs (szolgáltatási) rendszerének kifejlesztésében a kormányzati kártyakibocsátás rendszerének létrehozásában

- a nemzetközi kapcsolatrendszer kiépítésében

2007 áprilisában Szittner Károly tartott előadást „Úton a közigazgatási elektronikus közmű felé” az elektronikus azonosító rendszer továbbfejlesztésével kapcsolatban. Ebben beszámol az elmúlt időszak eredményeiről, de a következő ellentmondásokra is rávilágít:

- Törvényi szabályozás jelenleg csak dokumentumhitelesítést szolgáló elektronikus aláírásra létezik
- A közigazgatási eljárásokban az elektronikus aláírás használata csak formailag támogatott
- Hiányzik a közigazgatásban az elektronikus ügyintézés kultúrája
- Az elmúlt években jelentős ráfordítással szigetszerű rendszerek jöttek létre –nem alkotnak egységet
- A Központi Elektronikus Szolgáltató Rendszerben létrejött felhasználónév-jelszó páron alapuló azonosítás működik, de nem elég biztonságos mindenhez
- Párhuzamosan futó intelligenskártya kísérletek sorozatos kudarcokkal

A továbbhaladáshoz szükséges, hogy közművön keresztül történő elektronikus ügyintézés során (de egyéb feladatnál is) megfelelő biztonságot garantáló eszköz álljon rendelkezésre az állampolgár azonosításához, adatainak eléréséhez, a vele való kommunikációhoz, valamint ügyek intézéséhez. Továbbá egy olyan egységesen szabályozott állampolgári közmű rendszer kialakítása, ahol konzisztens módon valósul meg a szereplők hitelesítése, a rendszerben kezelt, tárolt dokumentumok bizalmassága, a végzett műveletek letagadhatatlansága

Az összehangolás előnyei között elsőként említi, hogy az államháztartásnak komoly megtakarítást jelentene, hiszen feleslegessé tenné:

- Az önálló TAJ kártyák kibocsátását: 10 millió db
- Az önálló „köztisztviselői kártyák” kibocsátását: kb. 20-50 ezer
- További speciális kártyák kibocsátását, pl. bírók részére, stb.
- Az önálló közlekedési kártyák kibocsátását stb.: legalább kétmillió darab
- Az újabb önálló kedvezményekre jogosító kártyák kibocsátását, pl. közgyógy kártya: több tízezer
- Az újabb diákigazolványok cseréjénél ezt is lehet alkalmazni: 1,2-1,5 millió db

A célok megvalósításához fejleszteni kell az azonosító eszközt, tehát intelligens kártyákat kell beszerezni, és a kibocsátásához, megszemélyesítéséhez, pl. okmányiroda szerű rendszereket kell létrehozni. ([15] http://ekmk.sztaki.hu)

Fontos továbbá a működéshez szükséges szabályozási környezet kialakítása:

- Az elektronikus személy- és szerepazonosítás, alapnyilvántartások szabályozására
- A közszolgáltatásokban alkalmazható szabványos azonosítási modell és kártyakoncepció kialakítására
- A szabványos felületek definiálására
- A műszaki ajánlások és dokumentáció elkészítésére.

Az Európai Unió - mivel az eEurope program egyik kiemelt célja az intelligens kártya-technológia elterjesztése - külön munkacsoportot hozott létre eEurope Smartcard Charter néven az intelligens kártyák unión belüli felhasználásának elősegítésére. Magyarországon az Információs Társadalom Koordinációs Tárcaközi Bizottság - az Elektronikus Közigazgatás Albizottságon belül - alakított ki egy Intelligens Kártya Munkacsoportot.

Ezek az egységes rendszert képező stratégiák kijelölik azokat az irányokat, amelyek az egyes ágazatokat a jelen helyzetből átvezetik az információs társadalomba, bemutatják, hogy az ágazatok szereplői számára milyen előnyöket kínál az információs társadalom.

Összességében elmondható, hogy az elektronikus kormányzati programok igénybevételét támogató megoldások között az egyik legfontosabb eszköz, a hiteles személyazonosítást lehetővé tevő és megbízható elektronikus aláírást létrehozó intelligens kártya. A Magyar Információs Társadalom Stratégia (MITS) célkitűzései az intelligens kártyatechnológia használata nélkül nem valósíthatóak meg. A kártyakibocsátás költségei viszont magasak, a kártyarendszerek csak jelentős háttér-infrastruktúra és valós igényeket kielégítő szolgáltatások kifejlesztése után működtethetők hatékonyan. Emiatt elterjedése, a felhasználások és a felhasználói csoportok bővülése nagyon lassú. Ebben a helyzetben alapvető jelentőségű egy megfelelő, minden részletre kiterjedő elektronikus kormányzati program következetes megvalósítása.

2. Az adatvédelem és biztonság elsődleges

2007 decemberében Dr. Péterfalvi Attila A személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. Törvényhez kapcsolódóan ajánlást fogalmazott meg az elektronikus ügyintézés során történő azonosítás adatvédelmi követelményeiről. Ebben a polgárkártya bevezetéséről, mint az elektronikus ügyintézés egy lehetséges koncepciójáról ír. Szerinte a hazai viszonyok között leginkább egy, a vonatkozó uniós jogszabályok, és a nemzetközi szabványok keretei között kialakítandó polgárkártya-koncepció képzelhető el. A polgárkártyának és a polgárkártya-koncepciót megvalósító más eszközöknek alkalmasnak kell lennie arra, hogy biztonságos aláírásokat hozzon létre, továbbá garantálja, hogy a kártyára telepített egyéb alkalmazások és funkciók az elektronikus ügyintézéshez nélkülözhetetlen személyes azonosítókat kezelő alkalmazástól biztonságosan elkülönítve legyenek használhatók.

Az azonosítót az adott állampolgárhoz kell hozzárendelni, a hozzárendelés módja a minősített tanúsítványok kiadásánál megkövetelt, központi adatbázisból támogatott, viszontazonosítás mellett megvalósított személyes regisztráció. A rendszer végrehajtó szervezete az okmányirodai hálózat lenne.

Az Alkotmánybíróság 15/1991. (IV. 13.) AB határozata alapján a természetes személy azonosítására több személyazonosító szolgál, ezek használatáról és használatának korlátairól törvény rendelkezik. A polgárkártya-koncepció megvalósítása keretében olyan egyedi azonosítók képzésére kerülhet sor, amely a polgárt a hagyományos személyazonosítási módoktól eltérően azonosítja.

Az elektronikus ügyintézés során gondoskodni kell arról, hogy a polgár egyes, egymástól független, a közigazgatás egyes ágazataiban kezdeményezett, majd lezárt ügyeinek dokumentumait – mint személyes adatokat – személyes adatai felhasználásával ne lehessen összekapcsolni. Az összekapcsolás folytán ugyanis a polgár „átlátszóvá” válna, személyes profilját lehetne meghatározni, amit a hatályos adatvédelmi rendelkezések is tiltanak.

E cél érdekében az egyes közigazgatási ágazatokban a polgár azonosítására egy ágazati azonosító szolgálhat, melynek képzésére a következő eljárás alkalmazható. A polgárkártya-koncepciót megvalósító eszközön a polgár személyes azonosítóihoz egy ún. váltószámot

rendelhet az arra felhatalmazott közigazgatási szerv. Ezt a váltószámot az iménti szerv vissza nem fordítható matematikai eljárással (pl. véletlenszám-generátorral) állítja elő, s egyrészt a polgár egyéb személyazonosítóihoz hasonlóan a polgárhoz rendeli másrészt a polgárkártyaként funkcionáló eszközön rögzíti, aminek hiteles voltát elektronikus aláírásával igazolja.

Amikor polgárkártyaként funkcionáló eszközzel a polgár valamelyik közigazgatási ágazatban ügyintézést kezdeményez, a polgárkártya-funkciót befogadó alkalmazás a polgár részére ágazati azonosítót képez. Az ágazati azonosító képzésének egyik adata a polgárkártyán rögzített váltószám, a másik az un. ágazati azonosító jel. E két adatra alkalmazott egyirányú (vissza nem fordítható) matematikai eljárás eredménye a polgárt az adott közigazgatási ágazatban egyértelműen és kizárólagosan azonosító ágazati azonosító.

Az ágazati személyazonosító képzése céljára a közigazgatási tevékenységi területeket úgy kell egymástól elhatárolni, hogy az összetartozó tevékenységi területek ugyanahhoz az ágazathoz tartozzanak, ugyanakkor az egymással össze nem egyeztethető adatkezelések ugyanahhoz a területhez ne tartozzanak. Az egymástól így elhatárolt területekhez pedig ágazati azonosító jelet kell rendelni. Tekintettel arra, hogy e területek száma nem túl sok (legfeljebb néhány tucat), az ágazati azonosító jel két karakter hosszúságú lehet.

A váltószámot kizárólag a polgárkártya rögzíti, s a polgár kizárólagos ellenőrzése alatt áll, Az ágazati azonosítókat pedig az érintett ágazati rendszer adatbázisa tartalmazza. Ezek összevonása és együttes tárolása nem megengedett.

Az elektronikus ügyintézés során az adatkezelés célja egyfelől az állampolgárok azonosítása, illetőleg a hatóság részéről a tranzakció megtörténtének bizonyítása. A célhoz kötöttség elvéből fakadóan a tranzakciókra vonatkozó adatok megőrzésének ideje nem lehet hosszabb, mint ami a hatóság feladatainak ellátásához szükséges, beleértve az archiválást is.

Lényeges követelmény, hogy az állampolgár az adatkezelés egész tartama alatt teljes körűen legyen tisztában a vele összefüggésben kezelt adatoknak sorsával.

Az adatbiztonsági követelmények érvényre jutása érdekében olyan garanciákat kell kidolgozni, melyek segítségével el lehet kerülni az adatok kompromittálódását.

A kizárólagos azonosító képzése véletlenszerű matematikai módszerrel történik, és az azonosító érvényességének tartama alatt a polgárt kizárólagosan azonosítja. Tekintettel arra, hogy a személyazonosító megváltoztatható, az osztott információs rendszerek és osztott hálózatok elvének megfelel.

Az egyes közigazgatási szervekkel való tranzakció kapcsán ágazati személyazonosítókat kell képezni, mégpedig a kizárólagos személyazonosítóval hasonló módon.

3. Példák többfunkciós alkalmazásokra

Az intelligens kártya technológia egyre jelentősebb szerepet tölt be az informatikai piacon. Míg korábban elsősorban a bankrendszer igényeit szolgálta ki, mára a felhasználás spektruma sokkal szélesebb. Az intelligens kártyák minden olyan rendszerben létjogosultságot szereztek, ahol a biztonság kulcsfontosságú. A számítógépes hálózatok a mindennapi életben egyre nagyobb jelentőségűek, az adatforgalmuk biztonsága is egyre fontosabb. A chipkártyák szerepe ezen a területen is egyre nő.

Magyarországon a leggyakrabban a benzinkutak törzsvásárlói kártyáinál, a budapesti belvárosi parkolásoknál bevezetett parkoló kártyán, az új felsőoktatásban bevezetett diákigazolvány esetében találkozhatunk intelligens chipekkel a kártyákon. A magyar kártyapiac tovább fejlődik. Egy nemzetközi benzinkút hálózat által kibocsátott törzsvásárlói kártyát más szolgáltatók, kereskedők is elfogadják, a diákigazolvány mellett az orvosok is speciális chipes bankkártyát kaptak az Orvosi Kamara közreműködésével, és elindult egy többszereplős törzsvásárlói program a SuperShop, ahol egy intelligens kártyán biztosított a pontgyűjtés és a pontbeváltás egy áruházlánc, egy bank, szupermarketek és egy benzinkút hálózat között.

4. ábra. A diákigazolvány Magyarországon

Az új diákigazolvány egy bankkártya méretű műanyaglap lett, amelyen a tulajdonos fényképe, aláírása és személyi adatai, az igazolvány egyedi azonosítója, az oktatási intézmény(ek) adatai, valamint a képzés típusára (nappali, esti, levelező, távoktatás) jellemző képecske, ún. piktogram szerepel. A kártyán az adatok lézergravírozásos eljárással kerültek feltüntetésre. A felsőoktatási igazolványokra még egy arany-színű elektronikus szerkezet, ún. chip is került. Ezzel a magyar felsőoktatási diákigazolvány lett a világon az első országosan használt hivatalos, "B" kategóriás biztonsági okmánynak minősülő mikroprocesszoros kártya.

5. ábra. Az igazolvány szerkezete.

Általános jellemzők:

- A diákigazolvány mérete: 85,6x54 mm
- Anyaga**:** PVC
- Grafika: vékony vonalakból álló biztonsági rajzolat, benne halványan "DIÁKIGA-ZOLVÁNY" feliratok látszanak reliefként.

1 Az elő- és hátoldalon szereplő léniák

2 "DIÁKIGAZOLVÁNY" szövegű mikroírások. (Nagyítóval válnak olvashatóvá.) A vonal-kód előtt szabad szemmel nem látható, UV fény hatására narancsszínnel világító "D" betű

3 látható, körvonalai mentén mikroírással, "DIÁKIGAZOLVÁNY" szöveggel. (A mintán ezt szabad szemmel is látható halvány szürke színnel nyomtattuk. Itt UV fényre nem reagál.)

4 Egyéb védelem: A fénykép fölött az Állami Nyomda Rt. hologramja látható 19x8 mm-es sarokkerekített téglalap alakban, benne negatív "D" betű.

5 Vonalkód: 10 számjegyű, benne ellenőrzőszám (CDV).

6 Piktogram: A sorszám mellett található a képzés típusát jelzi. Az Oktatási Minisztérium rendelete alapján a piktogramok megváltoztak! Jelenleg mindkét piktogram típus érvényben van! Korábbi piktogramok:


nappali tagozat


esti tagozat


levelező tagozat

A távoktatásban resztvevők diákigazolványán nincs piktogram, helyette az "UTAZÁSI KEDVEZMÉNYRE NEM JOGOSÍT!" felirat olvasható. Új piktogramok:


nappali tagozat


esti tagozat


levelező tagozat


távoktatás

A piktogram színe pasztell kék

7 Érvényesítő bélyeg: A hátoldalon az iskola által kiadott, az érvényesség időszakát jelző érvényesítő bélyeg kerül felragasztásra. Mérete: 20x 12,5 mm. A bélyeg világoskék biztonsági grafikát, mikroírást ("ÁLLAMINYRT" felirattal) valamint hologramot tartalmaz. A feliratok és a mikroírás sötétkék színűek, alatta szabad szemmel nem látható, UV fény hatására kék színnel világító körvonalas "D" betű látható. (A mintán ezt szabad szemmel is látható halvány szürke színnel jeleztük, itt UV fényre nem reagál.)

8 Chip: A felsőoktatási diákigazolványok chippel vannak ellátva. Ezzel a magyar felsőoktatási diákigazolvány lett a világon az első országosan használt hivatalos, "B" kategóriás biztonsági okmánynak minősülő mikroprocesszoros kártya. ([9] www.diakigazolvany.hu)

A távoli, de remélhetőleg elérhető cél egy olyan összetett oktatási kártyacsalád létrehozása, amely az oktatás valamennyi szereplőjének - beleértve a diákoktól kezdve a tanárokon, oktatókon át a technikai dolgozókig mindenkit - kedvezményeket és jogosultságokat nyújt. A diákigazolvány mellett papíralapú pedagógusigazolvány is létezik Magyarországon. Ezt a jövőben célszerű lenne multifunkciós plasztikkártyára cserélni, amely a személyazonosítás mellett az utazási kedvezmények igénybevételét, vagy akár a pedagógusok tankönyvtámogatásának felhasználását is lehetővé teszi. (A napjainkban használatos technológiák lehetővé teszik, hogy egy kártyán több szolgáltatás is szerepeljen, több funkció is megvalósítható legyen (multifunkcionális kártyák)). A felsőoktatásban dolgozó oktatók számára jelenleg nincs semmilyen kártya, noha egyre több intézményben diákigazolvánnyal léphetnek be a hallgatók egyes területekre. Ennek a problémának a megoldása is a közeli jövő célkitűzései között szerepel.

A szomszédos államokban élő magyarokról szóló 2001. évi LXII. törvény (közismertebb nevén a "státusztörvény") bevezetése óta a Kárpát-medencében, de Magyarország határain kívül élő honfitársaink számára is biztosított a Magyarországival közel azonos kedvezményeket nyújtó diák-, pedagógusigazolvány és oktatói kártya. Ezeket természetesen csak Magyarországon lehet felhasználni. Különösen reményteli a felsőoktatásban használt chipes diákigazolvány sorsa, amelynek elektronikus adathordozóját egyre több intézmény egyre szélesebb körben alkalmazza (Budapest, Szeged, Eger, Debrecen, Miskolc, Pécs, Győr).

Az e-tajkártya mellett készül az elektronikus személyi igazolvány bevezetésének koncepciója is, ennek lehetséges forgatókönyvét már el is készített az Igazságügyi és Rendészeti Minisztérium. Az elektronikus személyi igazolvány egy digitalizált anyakönyvi kivonat lenne, amelyekkel fokozatosan váltanák fel a mostani plasztikokat. Az elektronikus személyi igazolványok kiadására létrehozandó számítógépes rendszer pilótaprogramját 2010. július elsején hozzák működésbe. ([3] MITSESZ, 2003)

E-pénztárcával az e-piactéren

Magyarország legnagyobb online piactere, a Vatera április elején bevezette az Abaqoos elektronikus pénztárcát. Az új fizetési rendszernek köszönhetően gyorsabbá és biztonságosabbá válnak a tranzakciók.

Új, biztonságos interneten keresztül használható elektronikus fizetési megoldást vezetett be a Vatera online piactér. Az Abaqoos névre hallgató e-pénztárca biztosítja az anonimitást és az utalások pontos követhetőségét. A vásárló rajta keresztül virtuális letétbe helyezheti a felajánlott összeget, ezután az eladó postázza neki a kívánt terméket. A pénz és az áru cseréje ténylegesen csak akkor történik meg, ha az adásvétellel mind a vevő, mind az eladó maradéktalanul elégedett.

A megbízható eladók védelmét a jogosulatlan vevői reklamációkkal szemben a bankrendszerben is használt kockázatkezelési szabályok védik. Az eladó részére az is fontos elem, hogy a szolgáltatással bizalmat építhet a vásárlókban, ugyanakkor az adásvétel is felgyorsítható, hiszen az eladott áruk után az utalás akár azonnal is megérkezhet a számlájára.

Az új szolgáltatásra a Vatera-felhasználók ingyenesen regisztrálhatnak.

A virtuális pénztárcát elektronikus banki csatornákon keresztül lehet feltölteni. A vásárlás során nem szükséges semmilyen személyes adat, bankkártya vagy bankszámla információ megadása. Az Abaqoos-t jelenleg az OTPdirekt szerződéssel rendelkező felhasználók vehetik igénybe. A közeljövőben azonban további bankok csatlakozása várható.

IV. Európai Polgárkártyák

1. Az elektronikus személyazonosítás

Az Európai Unió információbiztonsági hivatala, az ENISA (European Network and Information Security Agency) új állásfoglalást jelentetett meg az elektronikus személyazonosító dokumentumokról (eID). Az ENISA közlése szerint Európában jelenleg 10 ilyen eszköz van használatban, és további 13 áll bevezetés előtt.

Ezekben közös, hogy személyes adatokat tartalmaznak, illetve ezek segítségével hozzáférést nyújtanak a legváltozatosabb szolgáltatásokhoz, nemzeti vagy európai szinten.

Az Unió által kialakítandó megfelelő működési környezet pedig lehetőséget biztosít arra, hogy az egyes kártyakibocsátók - a közös szabványok és szabályok keretein belül - más kártyakibocsátók szolgáltatásait is szerepeltethessék az általuk kiadott kártyákon illetve, hogy

egy adott szervezet által kibocsátott kártyára később más szervezetek szolgáltatásai is felvihetők legyenek. ([6] www.enisa.europa.eu)

A hivatal ugyanakkor felhívja a figyelmet, hogy noha adatvédelmi eljárásokat mindenhol fejlesztettek, teszteltek és bevezettek, ezek mindenhol nemzeti szinten történtek. Nincs egységes, koordinált európai stratégia, és ez gátja lehet a határokon átnyúló szolgáltatásoknak, az interoperabilitásnak. (A kibocsátó saját funkciói mellett más szervezetek funkcióit is egy kártyán lehet közösen működtetni (interoperabilitás)). A közzétett ajánlás összefoglalja a lehetséges veszélyeket és a továbblépés útjait is ezen a területen.

Definiálták, hogy az elektronikus azonosító kártya egy hitelesítő eszköz és személyes adatokat tartalmaz. Emiatt veszélyt jelent az állampolgárok magánéletére, mert a nem kívánt beavatkozások során lehetővé válik a személyes információk felfedése és az ezekkel való visszaélés. Alapvetően fontos felhívni a figyelmet a veszélyekre, mivel ezek fenyegetést jelentenek az alapvető állampolgári jogokra, amelyeket az Emberi Jogok Európai Egyezményének 8. paragrafusa tartalmaz, különösen azokban a szolgáltatási esetekben, ahol a kártya használata elkerülhetetlen.

Egy másik kormányzati szempont, hogy a magánéletre vonatkozó veszélyek elbátortalanítják az állampolgárokat a rendszer használatától, ezért az eID kártya bevezetésének elengedhetetlen feltétele a magánélet kellő védelme, különösen azokban az országokban, ahol az ID kártya már kötelező. Ez az oka annak, hogy az összes már meglévő és tervezett rendszer definiál valamilyen személyes azonosítót, mely megvédi a kártya tulajdonosát a személyes adatainak a nem kívánt feltárásától. A tanulmány összehasonlítja az Európában megvalósított kártya specifikációkat, és ezáltal megkönnyíti a legjobb gyakorlat megtalálását.

2. Ausztriában

Az e-kártya (ECARD), amely a betegek, az orvosok, a munkaadók és a társadalombiztosítási társaság számára is megkönnyíti a munkát.

Az e-card (továbbiakban magyarul: e-kártya) Ausztria nemzeti betegbiztosítási kártyája, melynek bevezetésére 2005-ben került sor, hogy a hozzá kötődő elektronikus adminisztratív

folyamatokkal együtt felváltsa a papíralapú kártyát. Mindezek mellett az e-kártya Európai Egészségbiztosítási Kártyaként is működik, és ún. állampolgári kártyaként is használható.

Az e-kártya rendszerét az SVC, az Ausztriai Társadalombiztosítási Intézetek Vezető Szövetsége 100%-os tulajdonában lévő leányvállalat dolgozta ki, továbbá ez felelős működtetéséért, karbantartásáért és további bővítéséért. Az e-kártya projektet az SVC rendszerintegráló szerepén belül valósította meg. Annak érdekében, hogy az e-kártya rendszere határidőre és hatékonyan kerüljön bevezetésre, a projektet számos részprojektre bontották, és ezeket külön-külön pályáztatták meg.

Az e-kártya kialakítása egy könnyű hozzáférhetőséggel jellemezhető online rendszerhez tartozó kulcskártyáénak felel meg, és így csak adminisztratív adatokat, titkosító kulcsokat és digitális azonosítókat tartalmaz.

Az első alkalmazás bevezetése óta (a papíralapú egészségbiztosítási igazolások lecserélése óta), számos új szolgáltatás elindítására került sor, így például orvosi jóváhagyás, preventív orvosi kivizsgálások, vagy éppen elektronikus fogyatékossági igazolások.

2005 vége óta az egészségügyi biztosításhoz használt csekkek a múlt emlékei közé tartoznak. Megérkezett az új egészségügyi kártya, vagy másképpen e-kártya, amely a betegek, az orvosok, a munkaadók és a társadalombiztosítási társaság számára is megkönnyíti a munkát. A beteg számára az e-kártya több mint egyszerűen az egészségügyi igazolvány helyettesítője: az egészségügyi rendszer kulcs-tényezője az állampolgár számára: a személyi (állampolgári) kártya pedig a kulcsot jelenti az e-kormányzat eléréséhez.

Ausztriában 2008 januárjától működik a chipes rendszer. Az országban egy gyors és hatékony rendszert sikerült kiépíteni, fél évvel a bevezetése után már majdnem minden osztrák állampolgár rendelkezik a kártyával. A plasztik chip személyi igazolványként is használható, de nem tartalmazza a személyesebb, kényesebb egészségügyi adatokat. Használható viszont elektronikus aláírásra, továbbá E111 biztosítási tanúsítványként is funkcionál.

Az e-kártya chipjeit a Philips és az Infineon szolgáltatja. Jelenleg 35 kilobájtos tárolókapacitással rendelkeznek, és elliptikus görbe alapú titkosítást használnak 192 bit

hosszú jelkulccsal. 2010-től új generációs kártyák bevezetésére kerül sor, ezek tárolókapacitása 52 kilobájt, a jelkulcs hossza pedig 256 bit lesz.

A központi rendszer egy konzultációs rendszerből és egy kártyarendszerből áll. A konzultációs rendszer kezeli a kommunikációt az orvosi egységgel a gyógyászati praxisokon belül. A kártyarendszer kezel minden tranzakciót az intelligenskártya-gyártás és a kártyaszolgáltatás ügyfelei között. A e-kártyák adminisztrációja a kártyarendszer komponensben történik. A konzíliumok, konzultációk aláírásának hitelesítését a jogosultsági rendszer generálja és biztosítja.

Az e-kártyához kapcsolódó állampolgári kártya-szolgáltatás Ausztria e-kormányzati stratégiájának része és hozzájárul a kormányzat szolgáltatásainak korszerűsítéséhez. Az e-kártya, az aláírási törvénynek és a kormányzati aláírási szabályzatnak megfelelően, háromféle „alvó” aláírási funkciót tartalmaz:

- Kormányzati aláírást (az e-kormányzati szolgáltatások eléréséhez)
- Normál aláírást (szabvány esetekre való alkalmazáshoz)
- Társadalombiztosítási aláírás (helyettesítendő az egészségbiztosítási igazolványt).

Az e-kártya jelenti a rendszer központi elemét, és ez a rendszeralapú szolgáltatások és adatok hozzáférési kulcsa. Ezt az teszi lehetővé, hogy a kártyatest megfelel az elektronikus aláírás hordozásához szükséges műszaki feltételeknek.

Az e-kártyán csak a kártyatulajdonos adminisztratív adatai tárolódnak, így például a neve, tudományos fokozata, biztosítási száma, a kártya azonosítószáma, valamint a nem és a felhasználói csoport azonosítója (nincs használatban).

Az osztrák e-kártya fő jellemzője, hogy kulcskártya elvén működik. Ennél fogva a smart kártya nem tartalmaz szoftverfunkciókat; csak azonosítási adatokat tartalmaz, melyek az alkalmazásokhoz kapcsolódó hozzáférési kulcsot jelentik. A társadalombiztosítás területén betöltött alapfunkciói mellett az e-kártya várhatóan az e-egészségügy (pl. a gyógyászati tranzakciók biztonságos kezelésének kulcskártyájaként), az e-kormányzás (pl. aláírási és titkosítási kártyaként), az e-kereskedelem és harmadik szolgáltatók e-alkalmazásának (egy fajta „infobox” koncepciót alkalmazva a titkosítási kulcsokra és engedélyezésekre) eszköze is lesz.

A kártyát személyi kártya funkció formában állították elő. Ausztria az első ország a világon, amely több területre érvényes személyi (állampolgári) kártyát ad ki. Minden állampolgár készít(tett)-het) e-kártyát a személyi igazolvány kártyájához és hozzájuthat az e-kormányzat szolgáltatásaihoz. A hivatalos elektronikus csatornákat az e-kártyával kényelmesen lehet kezelni otthonról is

Az osztrák egészségügyi információs hálózat, a GIN ADSL-technológiát alkalmaz, hogy összekösse az e-kártya adatközpontokat az egészségügyi szolgáltatókkal, egy központi ügyfélkapun, úgynevezett peering pointon keresztül. Biztonsági okokból a GIN zárt felhasználói csoport, ami azt jelenti, hogy csak az e-kártya rendszer partnereinek áll jogában az abban történő részvétel. A GIN egyetlen hozzáféréssel összeköttetést biztosít bármely felek között, sávszélessége 1 gigabitig skálázható, és hatékony tűzfalak védik. ([8] www.cisco.com)

Mivel teljes szélessávú kapacitásnak csupán egy része szükséges az e-kártya-szolgáltatások alkalmazásához, hozzáadott értéket jelentő szolgáltatásokat is lehet nyújtani ugyanazon hálózaton keresztül. Példa lehet erre a biztonságos internet, e-mail, a leletek továbbítása, VoIP- és ATM-szolgáltatások, távmunka, szoftver-távfelügyelet vagy éppen várótermi információs rendszer. A megfelelően biztonságos adattovábbítást minden egyes alkalmazás esetében prioritásvezérléssel a PPG végzi.

Az orvosi egység (MPU) egy felhasználói szoftvert tartalmaz, ennek segítségével kezelni lehet minden, az egészségügyi szolgáltató konzíliumához kapcsolódó eljárást, folyamatot. Az e-kártyák leolvasásához egy LAN chipkártya-leolvasó csatlakozik az MPU-hoz.

A pácienseknek mindig be kell mutatniuk e-kártyájukat, amikor orvoshoz mennek. Az e-kártya leolvasásakor az orvos a GIN-en keresztül ellenőrzi, hogy a beteg rendelkezik e biztosítással, és hogy mely egészségbiztosítási intézmény fog fizetni az egészségügyi ellátásért. Ez az adat nem tárolódik a kártyán, hanem online kérik le az e-kártya rendszerről.

Az “egészségbiztosítási igazolások cseréje” alkalmazás segít az adminisztrációs költségek csökkentésében, mégpedig oly módon, hogy egy évi körülbelül 42 millió papíralapú egészségbiztosítási igazolást helyettesít.

Az osztrák modellben az elektronikus úton benyújtott kérelmek esetén az illetékmentességet vezettek be ez olyan megoldás, amelyhez hasonló ösztönző megoldásokat

a projekt sikeressége érdekében érdemes bevezetni. A legtöbb külföldi példa ugyanis azt mutatja, hogy az elektronikus azonosítás nemcsak a digitális írástudás hiányosságai miatt nem halad olyan tempóban, mint az eredetileg tervezték, hanem azért is, mert az ösztönző - rendszerek hiányoznak. Az új megoldások esetén a költségeknek az állampolgárra terhelése vagy a bonyolult regisztrációs módok riasztóan hatnak.

A papírmunka csökkenése az orvosok tetszését is kiváltotta. A Bécsi Közgazdasági Egyetem 2008-ban végzett összehasonlító felmérése szerint az orvosok az e-kártyáknak köszönhetően negyedévente minimum öt munkaórányi adminisztrációtól mentesülnek. A számlázás nemcsak olcsóbb, hanem egyszerűbb is lett, mivel a rendszer integrált funkciójaként az orvosok azonnali visszaigazolást kapnak arról, ha egy adott kezelés ellenértéke kifizetésre kerül. Emellett a munkaadók is megszabadulnak az évi mintegy 42 millió papírkártyával járó pénzügyi és adminisztratív terhektől.

Országos szinten pedig az e-kártya a törvényi előírásoknak megfelelően elősegíti az orvosi szolgáltatások és költségek átláthatóvá tételét. Ebből adódik az a további előny is, hogy az osztrák egészségügyi szolgálat átfogóbb és pontosabb adatokkal rendelkezik majd a későbbi költségvetési tervek elkészítéséhez.

Ausztria egyik kisvárosában, Engerwitzdorfban állították fel az első internetes terminált, amely elektronikus személyi igazolvány (Bürgerkarte, magyarul polgárkártya) funkciókat is ellát. Engerwitzdorf lakói az elsők Ausztriában, akik a hét minden napján, huszonnégy órában használhatják a virtuális városházát. A terminál az osztrák polgárkártyával használható. Az elektronikus személyi igazolvány valójában nem egy kártya, hanem egy eszköz, amellyel különböző funkciók helyettesíthetők, mint a bankkártya, elektronikus kártya, munkavállalói kártya, valamint használható elektronikus aláírásra és személyazonosításra is. Bármikor, amikor megfelelő kártyaolvasó áll rendelkezésre, az állampolgárok azonosíthatják magukat a hatóságok felé, papír és akár személyes megjelenés nélkül. A terminál üzembe helyezése a helyi elektronikus kormányzat bevezetésének egyik fontos lépése, mellyel csökkenthetők az adminisztrációs költségek, emellett hatékonyabban és gyorsabban intézhetővé válnak a helyi önkormányzati feladatok.

2010-re az osztrák állampolgárok kézhez kaphatják a második generációs, új funkciókkal ellátott, elektronikus betegbiztosítási kártyájukat. Az elkövetkezendő két évben a lakosság

fele juthat hozzá a dokumentumhoz, melynek elterjedését az is segíti, hogy az eddigi kártya, melyet 2005-be bocsátottak ki, egyben európai betegbiztosítási okmányként is szolgál – öt év után elveszíti érvényességét. Az új funkciók közül az elektronikus receptfelírást (illetve ehhez kapcsolódóan a betegnek felírt gyógyszerek esetleges egymás kizáró hatásának vizsgálatát), vagy a védőoltás-tanúsítványt érdemes megemlíteni.

Minden orvosi rendelőben egy Cisco 800-as sorozatú ISR-útválasztó található, amely biztonságos és titkosított kapcsolatot ad az e-kártya hálózathoz, illetve teljesen elkülönített, nagy sebességű internetelérést és kapcsolatot biztosít más erőforrásokhoz. A Cisco technológiára épülő megoldás MPLS-technológiát alkalmazva számtalan logikai hálózatot (MPLS VPN) hoz létre egyetlen fizikai infrastruktúrán belül. Mindez fokozott biztonságot eredményez, amellyel garantálható, hogy az e-kártyás hálózat teljesen elkülönülten működik más alkalmazásokhoz használt hálózatoktól. Mivel négy különböző szolgáltató kínálja szolgáltatásait az e-kártya rendszeréhez, így az orvosok szabadon választhatják meg, hogy melyik szolgáltatót veszik igénybe a hálózatnak a rendelőből történő elérésére. Ezen hálózatok mindegyike teljesen elkülönülten működik. Különösen a fejlett országokra jellemző egyre öregedő népesség és a növekvő költségek miatt az élenjáró technológiák egyre inkább központi szerepet játszanak abban, hogy az egészségügyi szolgáltatások valamennyi jelentős elemét intelligens módon összekapcsolva javítsák az egészségügyi szolgáltatások és az adminisztráció hatékonyságát. Az e-kártyához tervezett, önmagában is biztonságos, megbízható és rugalmas infrastruktúra kiemelkedő példája annak, hogy a Cisco Systems miként hasznosítja a technológiát és a szakértelmet ahhoz, hogy az egészségügyi szolgáltatók és a központi kormányzat világszerte megvalósíthassa a hálózatba kapcsolt egészségügy rendszerét.

3. Spanyolországban

Két nagy felhasználó, szolgáltató van: az adóhivatal, adóbevallás céljára, valamint a társadalom-biztosítás (Securidad Social). 2004-ben pilot-kisérlet indult 100 ezer kártyával, amelyek PKI-val rendelkeznek, a hozzáférést PIN kód és biometriai ellenőrzés (ujjlenyomat) biztosítja.

A projekt költségeit 148.9 millió euróra becsülik. A kártyagyártó az FNMT, a spanyol pénzjegynyomda. A spanyol eID kibocsátója a National Spanish Police Departement

(Ministry of Interior), a 14 év feletti állampolgároknak kötelező, és azok 380 rendőrségen vehetik át 2006 első negyedév végétől. Várható darabszám 35 millió, 2007 végére kb. 5 millió eID kártyát vehetnek át.

Funkciók: hivatalos igazolvány, utiokmány, hozzáférő eszköz az e-szolgáltatásokhoz. Érvényesség 5-10 év kortól függően. Tartalom: személyi szám, név, születési adatok, nemzetiség. Alkalmas hitelesítésre PIN védett aláírásra. Biometrikus adatokat még nem tartalmaz. Tervezik a többfunkciós alkalmazását, de nem egészség/társadalombiztosítási célokra. Vannak tervek a technológiai továbbfejlesztésre (dual, vagy hybrid smart card (passport).

Azóta újabb milliókat pumpált a spanyol kormány a nemzeti elektronikus személyi igazolvány projektbe. Összesen 57 millió eurót, azaz több mint 17 milliárd forintot költöttek a megvalósításra, és ez nagyon segítette a terjedését.

6. ábra. Spanyol elektronikus személyi igazolvány

2008 márciusában a spanyol kormány úgy döntött, hogy kiterjeszti az elektronikus személyi igazolványra vonatkozó, 2007 júniusában megkezdett programot. A kormányzati szervek és az üzleti szféra együttműködésével megvalósuló projekt legfőbb célja, lehetőséget teremteni az állampolgárok számára, hogy az üzleti szféra, a közigazgatás és harmadik személyek felé on-line azonosítsák magukat és elektronikus aláírást használjanak.

A várakozások szerint ez a versenyre és az új szolgáltatások fejlesztésére és bővítésére is jó hatással lesz. Az elektronikus személyi igazolvány elterjesztése és alkalmazásai megfelelő használata érdekében az állampolgárok oktatására és támogatására kiegészítő program indul.

Emellett a kártyák használhatósága érdekében azoknak megfelelő szolgáltatások nyújtását kezdeményezi a spanyol kormány. ([11] www.technet.hu)

4. Franciaország

A Vitale elektronikus egészségügyi rendszer Franciaországban több mint 80.000.000 igénylő nyomtatványt dolgoz fel havonta, eddig 60 millió beteg és 1 millió orvosi kártya került kibocsátásra, valamint 60 ezer chipkártya-olvasót szereltek fel. A program évi 300 millió euró megtakarítást hozott az államháztartásnak. A betegek kényelmesnek és könnyen kezelhetőnek találják a rendszert.• Európa egyik legnagyobb volumenű, intelligens kártyát alkalmazó egészségügyi rendszere a francia – 1998-óta működő – SESAME-Vitale rendszer. Vitale egészség biztosítási kártyával és körülbelül 210 ezer orvos, illetve gyógyszerész használ munkája során szakmai kártyát (7. ábra). Az egészségbiztosítási kártya nem tartalmaz orvosi, egészségügyi adatot, csak a biztosítási jogviszony ellenőrzéséhez és a hitelesítés, aláírás funkció működéséhez szükséges adatokat tárolja, tehát kulcs kártya típusú rendszer. Minden ellátási eseményről egy elektronikus dokumentum készül, amelyre a beteg Vitale kártyája és az orvos szakmai kártyája segítségével hitelesítő elektronikus aláírás kerül.

A kártyaközpont az elektronikus dokumentumok alapján átlagosan 5 nap alatt végrehajtja az ellátási eseményhez tartozó pénzügyi tranzakciókat, amelyeket a korábbi, papíralapú rendszerben csak 2-3 hét alatt lehetett megvalósítani.

7. ábra, egy Vitale és egy szakmai kártya a duál író-olvasó eszközben

5. Németország

A németországi Schleswig-Holstein tartományban muködő pilot pojekt , a Gesundheitskarte nevű egészségkártyát (8. ábra) és orvosok, gyógyszerészek számára készült szakmai kártyákat (9.ábra) használja.

8. ábra. A német egészségkártya

Az egészségbiztosítás menedzselését a Vitale kártyához hasonlóan végzi, de – a biztosítási adatokon túl – orvosi, egészségügyi adatokat is tárol: sürgősségi adatok, anamnézisek, diagnózisok, elektronikus recept, beutalások, átirányítások és az elektronikus aláíráshoz szükséges PKI kulcsok. Ez a megoldás tehát – mint adatkártya – az elektronikus páciens rekord szinte teljes tárolását részesíti előnyben, a zsebben hordozható elektronikus kórlap elvét követve.

9.ábra. A német orvosi és gyógyszerész szakmai kártya

A német egészségügyi kártya bevezetése az eredetileg tervezett 2006 helyett 2007-ben zajlott. Az Egészségügyi Minisztérium közlése szerint minden egyes betegkártya a betegpénztáraknak kevesebb, mint 2 euróba került. Az egészségügyi kártya bevezetése összességében - ugyanúgy, mint eddig - mintegy 1,5 milliárd eurót tett ki. Az elektronikus betegkártya a betegpénztárak eddigi chip- kártyájának helyére lépett, és betegaktákat, röntgenképeket, ill. egyéb adatokat tartalmaz.

A berlini szövetségi kabinet 2008 júliusában döntött az elektronikus személyi igazolvány 2010-es bevezetéséről. A számos funkcióval rendelkező, bankkártya méretű okirat egy beépített chipen digitálisan tárolja a tulajdonos adatait. Az új kártyán tárolt elektronikus aláírás kiválthatja a jelenleg használatos PIN- kódokat és ezzel megkönnyítheti a banki tranzakciókat és az internetes vásárlásokat is. A korábbi elképzelésekkel ellentétben a tulajdonos ujjlenyomatát csak önkéntes alapon rögzítenék a kártyán.

A német belügyminisztérium 2009 nyarán nyilvánosságra hozta azoknak a vállalatoknak a listáját, amelyeket bevonnak az új elektronikus személyi igazolvány tesztelésébe. A szaktárcánál ügyeltek arra, hogy a tesztek életszerűek legyenek és a munkába éppen ezért nem csak nagyvállalatokat, hanem számos kisebb szolgáltatót is bevontak. A munka 2009 őszén elkezdődött. A tesztelés október elsején kezdődik és nem csak a dokumentumot, hanem az ahhoz kapcsolódó megrendelő-igénylő rendszert is vizsgálni fogják, hogy kiszűrhessék a hibákat.

Az új okmányt a tervek szerint 2010. november elsején vezetik be Németországban, hitelkártya méretű lesz és számos funkciót kínál majd. A személyes adatok mellett a chipen elhelyezhető a digitális aláírás és az igazolványnak köszönhetően könnyebbé válik majd az e-kereskedelmi, valamint az e-kormányzati szolgáltatások használata. Arról még nem döntöttek, hogy mennyibe fog kerülni a kártya, de hasonló azonosítót használó tagállamokban 10-42 euró (2,3-9,6 ezer forint) között változik ez az összeg. 2012-től további funkciókkal egészítenék ki a kártyát, például az állampolgárok munkavállalásával kapcsolatos adatait is ezen tárolnák.

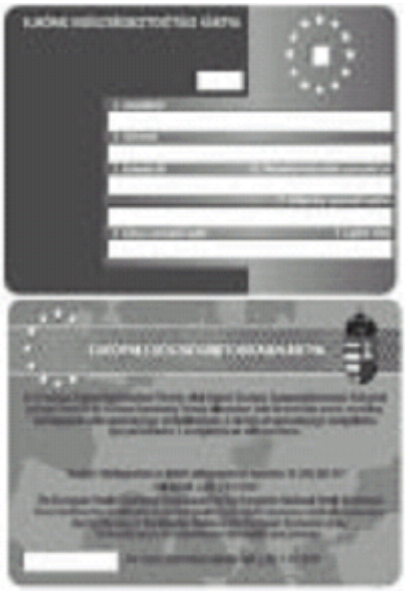
6. Belgium

Belgium 2007-ben többfunkciós elektronikus személyazonosító igazolványt vezetet be a gyermekek számára

Belgium pilot-programot kezdett a 12 éven aluli gyermekek új személyi igazolványokkal való ellátására. Belgiumban, szemben a magyar és a legtöbb uniós országgal a gyermekek születésükkor megkaphatják a személyazonosító igazolványt. Az új kártya a személyazonosító igazolványok klasszikus funkciói mellett arra is használható, hogy a gyerekek biztonságosan internetezhessenek, és hogy probléma esetén a szülők által megadott telefonszámokat hívjanak fel vele. A gyerekek a törvényes képviselők kérésére kapják meg a többfunkciós kártyát, ami három évig érvényes. A kártya gyors azonosítást tesz lehetővé Belgiumban, külföldön és az Interneten is. A hat éves kor fölöttiek számára kibocsátott kártyán egy pin kód is tárolásra kerül, amivel a gyerekek látogathatják a kizárólag számukra fenntartott chat-szobákat és internetes oldalakat. Minden igazolványt olyan chippel szerelnek fel, amivel a gyerekek bizonyos telefonszámokat, segélyvonalakat hívhatnak, ha bajba jutnak. A kártya használható lesz útlevél helyett (Litvánia kivételével) egész Európában, amennyiben a gyermek együtt utazik a szülővel. A kártyát a pilot-időszakban a hat és tizenkét év közötti gyerekek számára bocsátják ki Belgium egyes városaiban. Amennyiben a plasztiklap beváltja a hozzá fűzött reményeket, akkor a jelenlegi kártyarendszer teljes cseréjére kerül sor. A kártya nem tartalmaz biometrikus személyes adatokat.

7. Európai Unió

Az EU által bevezette az Európai Egészségbiztosítási Kártyát. Az Európai Unió – mivel az „eEurope 2005” akcióterv egyik kiemelt célja az intelligenskártya-technológia elterjesztése– külön munkacsoportot hozott létre eEurope SmartCard Charter néven az intelligens kártyák unión belüli hatékony felhasználásának elősegítésére. Az Európai Unió meghirdette egy elektronikus Európai Egészség biztosítási Kártya tervét, amelynek elektronikus változatban történő bevezetését 2008-tól kezdődően tervezték. A kártya első változata 2005. november 1-től hazánkban is bevezetésre került (4. ábra).



10. ábra. Az Európai Egészségbiztosítási Kártya magyar változata (2005. nov. 1.)

A feliratok szövege:

- Vezetéknév
- Utónevek
- Születési idő
- Társadalombiztosítási azonosító jel
- Intézmény azonosító száma
- Kártya azonosító szám
- Lejárat ideje

A kártya előlapján a nemzeti vagy regionális funkció jelenik meg, a hátoldalán pedig a szabványos Európai Egészségbiztosítási Kártya funkció.

Az Európai Bizottság által meghatározott szabvány nem terjed ki a Kártya másik oldalára. A Kártya másik oldalát és annak tartalmát a kibocsátó intézmény teljesen szabadon határozza meg. A másik oldal lehet nemzeti vagy regionális egészségügyi kártya (Németország, Olaszország, Csehország, Ausztria), de tartalmazhat közérdekű tájékoztatást is (Lengyelország, Egyesült Királyság).

Az Európai Egészségbiztosítási Kártyával Magyarországon a külföldi egészségbiztosítás terhére vehetők igénybe azok az egészségügyi szolgáltatások, amelyek a magyarországi átmeneti tartózkodás során orvosilag szükségessé válnak

Az európai egészségbiztosítási kártyát (European Health Insurance Card, EHIC) 2006. januárban vezették be az EU-s tagállamokban és négy EU-n kívüli országban (Izland, Lichtenstein, Norvégia, Svájc). Az EHIC a különböző E nyomtatványokat váltotta fel és elősegítette a papír nélküli kommunikációt a határon átívelő ellátás szereplői között (betegek, ellátók, társadalombiztosítási intézmények). Az indítvány sikeresnek bizonyult és 2006 végére több mint 150 millió európai állampolgár mondhatta magát a kártya tulajdonosának. Az európai egészségbiztosítási kártya valamennyi EU-s tagállamban azonos és a tulajdonos nevét, azonosító számát és születési adatait tartalmazza. Az EHIC újabb nemzedékét az elektronikus európai egészségbiztosítási kártya (eEHIC) képviseli. ([5] Király, Szege: Legjobb informatikai … , 2005)

A Magyarországon 2005 novemberétől kiadott plasztik európai egészségbiztosítási kártya - amely az uniós országokba utazó magyarok tb-jogviszonyát igazolja, még nem tartalmaz elektronikus adatokat, de az új, chipkártyaalapú okmányon feltüntetett adatok már olvashatók lesznek elektronikusan. A kártya bevezetése ugyanakkor hazánkban összekapcsolódik a taj-kártya elektronizálásával és a központi egészségügyi informatikai rendszer fejlesztésével is. Így az új, fényképpel ellátott kártya egyik oldalán az uniós, a másikon a nemzeti ellátásra jogosító adatok lesznek olvashatók. ([10] www.securifocus.com)

A chipkártya egyesíti majd a taj-kártya és az európai egészségbiztosítási kártya funkcióin túl a nyugdíjas-igazolványét, a közgyógy-igazolványét is, valamint egyben belépőt jelent a kormányzati portál ügyfélkapujához is. (Ott például a taj-szám megadásával bárki ellenőrizheti ellátási jogosultságát, és információt szerezhet "betegútjáról".) Az új okmány tehát kulcs lesz különböző adatbázisokhoz.

11. ábra Chippel ellátott Kártya

A hálózat kiépülésével az orvos megismerheti - a beteg hozzájárulásával - a páciens korábbi diagnózisait és kezeléseit, vénybeváltásait, függőben lévő vényeit, beutalóit, utazási költségeit, kórházi és szakrendeléseken kapott ellátásait. A kártya és a program segítségével az orvos - a papírt kiváltva - elektronikusan intézheti a vényeket és a beutalókat, az utazási utalványokkal és a vizitdíjakkal kapcsolatos adminisztrációt. A beteg kártyájának kiléptetése egyben rögzíti a betegforgalmi napló számát, a kezelés okát és a diagnózist. A kártya bevezetésével a szakrendelők és kórházak számára szintén leegyszerűsödik a betegek regisztrációja, a kórházak esetében pedig az elbocsátásuk is.

Az elektronikus személyazonosításra (eID) vonatkozó CEN/TS 15480 szabvány, amelyet a Magyar Szabványügyi testület magyar szabványként is kihirdetett (European Citizen Card, ECC), 2007 májusában történt elfogadásával megszületett az európai szinten közös álláspont, ami lehetővé teszi elektronikus azonosításra, hitelesítésre és aláírásra alkalmas ún. e-ID (electronic identity) kártyák kibocsátását. Ezek az eszközök egyrészt nemzetközi szinten is elfogadhatók, másrészt a szabvány keretein belül képesek alkalmazkodni a tagországok eltérő közigazgatási és adatvédelmi rendszeréhez. Lehetőség nyílt tehát arra, hogy a tagországok kormányai olyan elektronikus azonosító és aláíró eszközöket biztosíthassanak állampolgáraik részére, amelyek nemcsak az országhatárokon belül, hanem azon kívül is alkalmasak az állampolgár elektronikus azonosítására, illetve okmányként kibocsátott kártyák esetében a vizuális azonosításra, valamint lehetővé teszik az elektronikus ügyintézést a független kártyaelfogadó infrastruktúrákon és információs rendszereken.

A tervek szerint egy egységes, az EU 27 országára érvényes intelligens kártyát hoznak létre a lakóhely-változtatással és ideiglenes lakóhellyel, valamint a tartózkodás engedéllyel kapcsolatos teendők egyszerűsítésének és átláthatóvá tételének érdekében. A biometrikus azonosítókkal (arckép és két ujjlenyomat) is ellátott kártya 2010-ben kerülne bevezetésre, és

még az idén elfogadná az EU azt a szabályozást, amely megnyitja az utat az összes tagállamra egyformán érvényes alkalmazás előtt.

Az európai polgárkártya jellemzőiről a következőket lehet tudni:

Az új kártyán tárolt elektronikus aláírás kiválthatja a jelenleg használatos PIN- kódokat és ezzel megkönnyítheti a banki tranzakciókat és az internetes vásárlásokat is. A korábbi elképzelésekkel ellentétben a tulajdonos ujjlenyomatát csak önkéntes alapon rögzítenék a kártyán.

Az információk elérését egy prado nevű honlap is segíti. A PRADO olyan 22 nyelven elérhető, nyilvános internetes oldal, amely eredeti személyazonosító és úti okmányok, vízumok valamint bélyegzőlenyomatok biztonsági jellemzőire vonatkozóan tartalmaz információkat. A PRADO honlapon a felhasználók képeket és leírást találhatnak az Unió tagállamai, és egyes harmadik országok leggyakrabban használt okmányairól.

A PRADO célja, hogy naprakész információt szolgáltasson a nagy nyilvánosság, kormányzati és nem kormányzati szervek (pl.: postai szolgáltatók, bankok, munkáltatók, stb.) részére az okmányok biztonsági jellemzőivel kapcsolatban, ezzel előmozdítva a személyazonossággal való visszaélés elleni küzdelmet

Összegzés

Bárhol is történik a személyes adatok kezelése, azokhoz az adatalanyokon kívül mindenki más csak célhoz kötötten férhessen hozzá. Ezt a kártyák esetében megfelelő technikai intézkedésekkel kell garantálni, a nyilvántartások esetében ezzel szemben elsősorban szervezési és jogi garanciák szükségesek. Igaz ez a nemzetbiztonsági és bűnüldöző szervek adatigényére is. Az adatkezelés célja a közigazgatás és az állampolgár közötti biztonságos adatáramlás megteremtése, a megbízható azonosíthatóság és nem a bűnüldözés vagy nemzetbiztonság. A bűnüldözési és nemzetbiztonsági célú adatkezelés esetén jogi garanciaként a jogszabályok az adatokhoz való hozzáférést bírói engedélyhez kötik. Ugyancsak garanciális elem lehet az adatvédelmi biztosi és az ügyészi ellenőrzés.

Az önrendelkezési jogból következik, hogy az állampolgár számára lehetőséget kell biztosítani a személyes közreműködésre, ezzel biztosítva, hogy kontrollálni tudja adatai sorsát. Ebből következően például a kártyáján tárolt adatokhoz csak általa ismert jelszó használatával lehessen hozzáférni, illetve a polgár az adatai továbbításáról proaktív tájékoztatásban részesüljön.

Ezen alapelvből következik többek között a fizikai kártya elvesztése, ellopása, vagy más adatok illetéktelenek kezébe jutása esetére az adatok letilthatósága és lehetőség szerint értelmezhetetlenné tétele. Ebből következik az is, hogy az adatkezelési politika támogatandó, amelyben a személyes adatok a kártyát birtokló személy rendelkezése alatt állnak, szemben azzal, amelyben azok kikerülnek az rendelkezése alól.

Minden szakaszban vizsgálandó, miképpen kerülhető el a különböző célú adatkezelésekben tárolt, egy-egy személyre vonatkozó adatok jogellenes összekapcsolása, ezzel az egyes adatkezelési célok által szükségtelen személyiségprofil képzése. Az adatkezelések összekapcsolásán túl e cél érdekében kell előírni az adatok megfelelő időben történő törlését is. Miután az adatkezelés célja megvalósult, a célhoz kötöttség követelménye miatt az adatok további tárolására nincs törvényes lehetőség, az adatokat törölni kell. Az esetlegességek kiküszöbölése érdekében szabályokat kell alkotni az adatok megőrzésének rendjéről és idejéről, a selejtezéséről és a megsemmisítéséről is.

Olyan szervezési és technikai megoldásokat kell választani, amely az adatokat az egyes adatkezelések természetéhez mérten szükséges szinten megvédik a jogosulatlan hozzáféréstől, az indokolatlan sérülésektől, törlésektől. Az adatbiztonság szintjét állandóan tesztelni kell, hiszen annak nincs törvényben rögzíthető legmagasabb mértéke. Az adatkezelő annak színvonalát folyamatosan javítani köteles. Az adatfeldolgozó rendszerek komplexitása és folyamatos fejlődése, valamint a biztonságot veszélyeztető tényezők bővülése folyamatosan szélesíti az adatbiztonságra vonatkozó követelményeket.

E rövid áttekintés után megállapítható, hogy az eddigi kísérletek tapasztalatai, az eredmények és megfontolások alapján úgy tűnik, hogy az intelligens kártyarendszerek jelentik a megoldást az elektronikus azonosításra, különös tekintettel a biztonság, a személyes adatok védelme, az elektronikus aláírás lehetősége, a biometriai jellemzők alkalmazása szempontjából.

A nehézséget a folyamatos technikai fejlődés, a biztonsági követelmények szigorodása (privacy), az alkalmazási lehetőségek sokaságának harmonizálása (multifunkcionalitás), következésképpen a beruházási és működtetési költségek minimalizálása és megosztása, és mindezekkel együtt a nagymértékben összetett rendszerek biztonságos működtetése, a résztvevők fegyelmezett, pontos együttműködése jelentik. ([12] www.jegyzo.hu)

Ezek előrebocsátása után nézzük röviden, felsorolásszerűen, anélkül, hogy a részletekbe mennénk, hogy milyen kérdések merültek fel az intelligens kártyák azonosító rendszerekben történő felhasználása során:

- Az elektronikus azonosítás (eID) szabványosítás aktuális helyzete, különös tekintettel az interoperábilitásra.
- A kártya kapacitása, amely függvénye a multifunkciós lehetőségeknek.
- A lehetséges funkciók: azonosítás hitelesítés, elektronikus aláírás, idő-pecsét, biometrikus azonosítás, egészségbiztosítási kártya, szociális juttatások, jogosítvány, hozzáférés kormányzati, önkormányzati portálokhoz, információs kioszkokhoz, internethez, citizen card, elektronikus kereskedelem, adókártya, választói kártya, köztisztviselői kártya, student card, elektronikus pénztárca, parkolókártya, tömegközlekedési bérletkártya, stb.
- Melyek az egymást kizáró funkciók?

- Hány funkció legyen egy kártyán? Mely partnerek között lehet, illetve racionális a kooperáció?
- Érintkezős, érintkező nélküli, vagy hibrid kártya optimális adott esetben?
- Indokolt-e optikai tárolóréteg? (olasz eID kártya)
- A kártya alapanyaga, külső megjelenése, biztonsági jelek: hologram, digitális fénykép, bár-kód, rajzolatok, színezés.
- Kártyachip belső tartalma: adminisztratív adatok, lakcím csak a chipben (módosítható), hozzáférhető adatok, védett adatok.
- Kártya-chip biztonsági követelmények.
- Előkészítő tanulmányok.
- Jogi előfeltételek megteremtése.
- Beruházási, működési költségek becslése, költség/hatékonyság számítás.
- Közbeszerzési pályázat.
- Infrastruktúra kiépítése.
- Banki- és privát szféra bevonása.
- Fokozatos bevezetés, pilotok, kiértékelés ütemezés.
- Kockázati tényezők.

Az intelligens kártya technológia jelentősége tehát nő az informatikai szférában.. Míg korábban elsősorban a bankrendszer igényeit szolgálta ki, mára a felhasználás spektruma sokkal szélesebb. Az intelligens kártyák minden olyan rendszerben létjogosultságot szereztek, ahol a biztonság kulcsfontosságú. A számítógépes hálózatok a mindennapi életben egyre nagyobb jelentőségűek, az adatforgalmuk biztonsága is egyre fontosabb. A chipkártyák szerepe ezen a területen is folyamatosan nő..

IRODALOMJEGYZÉK

[1] Dr. Ködmön József: Az intelligens kártyák egészségügyi alkalmazási lehetőségei

[2] Magyar Információs Társadalom Stratégia (MITS), 2003 november

[3] Magyar Információs Társadalom Stratégia Egészség ügyi és szociális ágazat

[4] Magyar Információs Társadalom Stratégia intelligens kártya részstratégiája

[5] Király Gy., Szege Z.: Legjobb informatikai megoldások az Európai Unióban – INCO-HEALTH projekt, IME IV.évf. 7. szám, 2005.

[6] http://www.enisa.europa.eu/publications/position-papers

[7] http://www.ekk.gov.hu/hu/kib/ajanlasok

[8] www.cisco.com/web/HU/assets/docs/austriancard.pdf

[9] http://www.diakigazolvany.hu

[10] http://www.securifocus.com/portal.php?pagename=hir_obs_reszlet&&i=16577

[11] http://www.technet.hu/techtud/20090424/milliardokat_pumpalnak_az_elektronikus_szemelyibe

[12] http://www.jegyzo.hu/elektronikus-azonositas-intelligens-kartya-2006-6

[13] Intelligens Közösségi Kártya Projekt(CC Projekt) Megvalósíthatósági Tanulmány

[14] http://www.hscf.net/home/home.htm

[15] http://ekmk.sztaki.hu/index.php?option=com_content&task=view&id=79&Itemid=142