1. Tartalomjegyzék

2. Bevezetés

Ma egy különös világban élünk, az általunk használt gépek, járművek technikai színvonala a XXI.-ik századot képviseli, míg utcáik burkolatának minőségét és az utak szélességét még mindig a XIX.-ik század, és az akkor elfogadott rendezési tervek határozzák meg. A magyar tömegközlekedési viszonyokra, és legfőképp Budapest tömegközlekedésére is ezek a tényezők vannak a legnagyobb hatással. Útjaink túlterheltek, zsúfoltak, keskenyek, már nem képesek átereszteni azt a mennyiségű járművet, amely rajtuk közlekedik. Ez a probléma a tömegközlekedésben is megjelenik, a buszok, a villamosok és az összes tömegközlekedési eszköz csúcsidőben szinte elviselhetetlenül zsúfolt, ezt az érzést csak fokozza, hogy az egyéni közlekedés rohamosan szaporodó résztvevőitől nem tartható a tömegközlekedési eszközök menetrendje. Európai viszonylatban mégis kiemelkedően magas a magyar közlekedésben a tömegközlekedés aránya az egyéni közlekedéssel szemben, (ez gazdasági okokra vezethető vissza), amit meg kell őrizni, sőt még inkább vissza kellene szorítani az egyéni közlekedést. Ennek érdekében fel kell használni a technika által megteremtett lehetőségeket, beleértve ebbe a legmodernebb félvezető-, és chip technológiát is. A szervezés, a pénzügyi elszámolás, és a hálózattervezés területén is vannak még jelentős hiányosságok, a Budapesti Közlekedési Szövetség (BKSz) létrehozása Budapesten és környékén a térségben működő tömegközlekedési társaságok (BKV Rt, MÁV Rt, Volánbusz Rt) szolgáltatásainak koordinálásával, szövetségi viteldíjrendszer bevezetésével a tömegközlekedés igénybevételének könnyebbítésére és a szolgáltatás vonzóbbá tételére jönne létre. A BKSZ bevezetésének egyik legfontosabb, az utasok által közvetlenül érzékelhető vetülete az új, szövetségi viteldíj- és jegykezelési rendszer, amely a szövetségi szolgáltatások legfőbb használati szabályait és kereteit jelenti, ugyanis ennek révén történik a szolgáltatások "eladása" ill. azoknak az utasok általi "vétele". Ezért a viteldíjrendszer és technikai eszközrendszere, amely magába foglalja a viteldíjrendszer szabályait, a díjhordozókat (jegyeket, bérleteket), az árusító és ke-

zelő berendezéseket, az utasok és a szolgáltató vállalatok szempontjából is kiemelt jelentőségű, amelynek főbb ismérvei és követelményei a következők:

- terjedjen ki a szövetségi szolgáltatások teljes körére, valamennyi résztvevő üzemeltető társaság szolgáltatásaira,
- legyen áttekinthető és az utasok által könnyen használható,
- legyen tekintettel a különböző használói csoportokra (pl. rendszeres, időszakos és eseti használók),
- tegye lehetővé megfelelő viteldíjválaszték és kedvezmények nyújtását a különböző használói csoportok számára (pl. tanulók, nyugdíjasok, ingyenesek stb.),
- tegye lehetővé az igénybevett teljesítmények arányában történő díjszabást és díjlerovást,
- legyen lehetőség az érvényesség területi és időbeli differenciálására,
- az utazási dokumentumot jelentő viteldíjhordozók választéka (jegyek, bérletek fajtái) igazodjanak a használat gyakoriságához,
- a különböző utas-csoportok minél kevesebb viteldíjhordozó (jegy- és bérlet-) típussal legyenek kezelhetők,
- a jegykezelési rendszer tegye gyorsan és biztonságosan lehetővé a díjlerovást ill. az érvényesség megállapítását és igazodjon a különböző használói csoportok adottságaihoz,
- a helyileg és időbelileg elváló jegyeladás és a szolgáltatás igénybevétele, oly módon legyen összekapcsolható, hogy a bevételek a szolgáltatókhoz helyesen hozzárendelhetők legyenek,
- a jegyhez/bérlethez területileg és időbelileg, valamint műszakilag megfelelő módon lehessen hozzájutni,
- a jegy- és bérleteladásból befolyó pénzeket biztonságosan lehessen kezelni,
- a viteldíjak viszonylag egyszerűen változtathatók legyenek,

- az utasok utazási dokumentumai az érvényesség ill. az igénybevett szolgáltatásnak megfelelő díjlerovás tekintetében legyenek egyértelműen ellenőrizhetők,
- a jegyeladási és jegykezelési rendszer tegye lehetővé az utazások regisztrálását és szolgáltasson a megfelelő utas-, teljesítményi és bevételi statisztikai adatokat.

Ezen szempontok és a lehetőségek figyelembevételével alakítandó ki az új szövetségi viteldíjrendszer. A szempontok egymástól nem függetlenek (pl. a viteldíj-hordozók fajtája meghatározza a jegykezelést, a jegykezelő készülékek műszaki színvonala meghatározza az alkalmazható díjszabást stb.), vagyis a viteldíjrendszer részelemei ill. a vele kapcsolatos szempontok nem kombinálhatók tetszőlegesen. A leginkább meghatározó tényező a jegyeladó, jegykezelő műszaki megoldás miléntje, amely erősen eszköz-, ill. pénzfüggő, és döntően meghatározza az utazásokkal, a teljesítmény-bevételekkel és azok felosztásával kapcsolatos vezetési információkat. Ebből a szempontból két fő megoldási lehetőség kínálkozik:

- az egyszerűbb mechanikus jegykezelést és (papíralapú) jegyrendszert használó megoldások (ilyen rendszerek működnek Münchenben, Frankfurtban, Hamburgban, Bécsben)
- elektronizált, mágneses alapú jegyeket, chipkártyákat alkalmazó rendszerek, amelyek a kiépítés színvonalától függően árban is igen eltérőek lehetnek (a teljesen elektronizált rendszer Európában még ritka, részleges mágnes-, ill. chipkártyás megoldások találhatók pl. Londonban, Brüsszelben, Párizsban, Göteborgban, vagy pl. Hongkongban, de újabban a volt keleti tömb egyes nagyvárosaiban is léteznek részleges megoldások (pl. Moszkva, Szentpétervár, Bukarest).

Az egyszerűbb, papírjegyet és mechanikus jegykezelést alkalmazó, viszonylag olcsó rendszer legfőbb hiányossága, hogy nem teszi lehetővé a jegy/bérletvásárlás (díjfizetés) és a szolgáltatások igénybevétele közötti megfeleltetést, vagyis nem nyújt kellő információkat a bevételek szolgáltatók közti felosztásához. Ezt csak megfelelő időszakonként

végrehajtott utas felmérések teszik lehetővé. Jelen diplomaterv a jegyeladás és jegykezelés korszerű elektronikus változatának rendszertervét vázolja fel, elsősorban arra törekedve, hogy a legfontosabb kérdésekre (mely utas csoport tagja, melyik területen, melyik szolgáltatást, milyen mértékben, milyen jeggyel/bérlettel vette igénybe) megbízható válaszokat találjon, ill. adatokat szolgáltasson. A rendszer megvalósítása, az utasok magasabb szintű kezelésén felül, a bevételeknek a szolgáltató társaságok közötti igazságos felosztását is szolgálja, ami - több más szempont mellett - az egyik legfontosabb indok az elektronikus díjbeszedési és ellenőrzési rendszer mellett. A diplomaterv nem foglalkozik a lehetséges viteldíjszintekkel és a kedvezmények mértékével, ugyanis a rendszer műszaki képességeinek kialakítása az elsődleges szempont. Azonban ahhoz, hogy érdemben megválaszolhatóak legyenek az előbbi kérdések, tanulmányoznunk kell a már bevezetett, működő rendszereket. Meg kell vizsgálnunk azok műszaki megoldásait, előnyeit és hátrányait is egyaránt. Ilyen rendszerek bemutatását láthatjuk a 4. és 5. fejezetben, míg a 3. fejezet a chipkártyák műszaki lehetőségeinek széles skáláját ismerteti.

3. Chipkártyák műszaki paraméterei

3.1. Bevezetés

Ebben a fejezetben a chipkártyákról próbálok egy átfogó képet nyújtani, azok különböző fajtáinak, a rájuk vonatkozó szabványoknak, előírásoknak, normáknak a bemutatásán, egyes típusok összehasonlításán, valamint a két legelterjedtebb titkosítási eljáráson keresztül.

3.2. Alapfogalmak és meghatározások

Asymmetric cryptography (Aszimmetrikus titkosítás): Olyan titkosítási technika, amelyben két különböző kulcsot (egy saját és egy nyilvános) használnak az adatok kódoláshoz és visszafejtéséhez. A saját kulcs csak a felhasználó számára, míg a nyilvános kulcs mindenki számára elérhető.

Authentication (Autentikáció): Egy metódus, melyet az üzenetek eredetiségének ellenőrzésére, vagy az adott rendszerhez való kapcsolódás jogosultságának megítélésére, valamint az üzenetek adatátvitel során történő változásának, módosításának megítélésére használnak

Availability (Hozzáférhetőség, elérhetőség): Szolgáltatások és információk azon képessége, hogy a felhasználók kérés esetén beléphessenek az adatbázisba, illetve igénybe vegyék az adott szolgáltatást.

Certification authority (Hozzáférés igazolás): Egy egyedi meghatalmazás egy nyilvános kulcs hozzáférését igazolja.

Chip card (Chipkártya): Egy kártya, mely egy vagy több chipet vagy integrált áramkört tartalmaz azonosítási feladatokra, adattároláshoz vagy különleges számítási eljárásokhoz személyi azonosító kódot (PIN) használ, képes a személyes adatok, valamint érték hiteles, ellenőrzött tárolására.

Ciphertext: Az adatok kódolt formája.

Clearing house (Klíring ház, elszámoló központ): Egy központi hely, vagy központi feldolgozó mechanizmus, mely pénzügyi egyeztetést végez fizetési megbízások vagy más pénzügyi kötelezettségek alapján. Lehetőséget van a részletekben történő elszámolásra a ház szabályai és eljárásai értelmében. Néhány esetben a klíringház elfogadhat kiemelkedő értékű megbízásokat, melyek teljesítéséért a vezetőség tartozik felelősséggel.

Clearing system (Klíring rendszer): Egy eljárás, amivel pénzügyi elszámolás valósul meg, adatok és/vagy dokumentumok cseréjével az ide vonatkozó tőke vagy más biztonsági szállítást igénylő pénzügyi mozgás nélkül, egy helyen.

Closed network (Zárt hálózat): Telekommunikációs hálózat azzal a szándékkal, hogy a fizetési rendszer és a belépés korlátozott legyen

Contact cards (Érintéses kártyák): Olyan kártya, amely fizikai kontaktust igényel az elektromos kapcsolat megvalósításához a kártya és a kártyaolvasó vagy terminál között.

Contactless cards (Érintés nélküli kártyák): Olyan kártya, amely nem igényel fizikai kontaktust a kártya és az olvasó közötti kapcsolat megteremtéséhez.

Credit card (hitelkártya): Egy kártya típus, mely birtokosának folyamatos hitelt garantál. Lehetővé teszi a birtokos számára vásárlást és készpénz felvételt előre meghatározott keret erejéig.

Credit card company (Hitelkártya társaság): Egy társaság, amely saját névjeggyel ellátott hitelkártyát bocsát ki.

Cryptographic algoritthm (Kriptográfiai algoritmus): Egy matematikai függvény, amely egy kulcs kombinációt használ bizalmas adatok autentikációjához.

Cryptography (Kriptográfia): Minden olyan matematikai elv és algoritmus, mely adatok hitelességének biztosítására szolgál.

Derived key: egy kriptográfiai kulcs, amely kombinációit egy aritmetikai függvény használ a mesterkulccsal a CSN előállításához.

DES Data Encryption Standard: Egy szimmetrikus titkosítási algoritmus, amit leginkább a pénzügyi szférában alkalmaznak.

Digital signature (Digitális aláírás): olyan adatsor, melyet egy kriptográfiai eljárás állított elő és alkalmas agy üzenet sértetlenségének, valamint küldőjének azonosítására.

EEPROM Electronically Erasable Programabla Read-only Memory: Olyan integrált áramkör, mely képes adatot tárolni, valamint elektronikusan törölhető és újraírható.

Electronic money (Elektronikus pénz): Pénzbeli érték, valuta egység elektronikus formában tárolva a fogyasztó birtokában lévő elektronikus eszközön. Ezt az elektronikus értéket a fogyasztó elköltheti, tárolhatja, és bármikor vásárolhat vele. Az a különbség a hagyományos elektronikus pénzügyi tranzakciókkal szemben, hogy .a kredit és debit kártyákon nem tároltak értéket, csak azonosították a tulajdonost, és minden kártya tranzakciót online banki tranzakció kísért. Két különböző típusa van az elektronikus értéktároló eszközöknek: előre fizetett kártya vagy szoftver alapú termékek. Az előre fizetett kártya alapú terméknél az érték egy chipben, míg a szoftver alapú rendszerben egy programban van eltárolva.

Encryption (Kódolás): Tiszta szöveges adatot (plaintext) kriptográfiai algoritmussal kódolnak. Az eredményt ciphertext-nek nevezik.

Home banking (Házibank): Olyan banki szolgáltatás mely telefonvonal, terminál, vagy személyi számítógép segítségével bonyolódok le, nem szükséges hozzá személyes megjelenés.

Internet (Internet): Nyilvános kommunikációs infrastruktúra, összekapcsolt számítógépes hálózat

ISO International Organization for Standardization: Nemzetközi egyezmény, különböző gazdasági, tudományos területekre kifejlesztve az egységes felhasználás érdekében.

Key (Kulcs): Egyedi számkombináció, mely egy kriptográfiai algoritmus eredménye.

Master key (Mester kulcs): Kriptográfiai kulcs, gyakran más kriptográfiai eljárással állítják elő.

Memory card (Memóriakártya): Integrált áramkört tartalmazó kártya, mely csak információtárolásra alkalmas.

Multifunctional cards (Multifunkcionális kártya): több akár pénzügyi, akár más területen felhasználható kártya.

Network money (Hálózati pénz): Olyan elektronikus pénz, amely az interneten áramlik egyik helyről a másikra.

Offline: Kapcsolat nélküli

Online: Állandó kapcsolatot biztosító, igénylő.

Open network (Nyitott, nyílt hálózat): Olyan telekommunikációs hálózat, amely szabadon hozzáférhető.

Operating system: Számítógépek, chipek irányító, vezérlő szoftvere.

PIN Personal Identification Number (Személyes azonosító kód): Egy numerikus kód, mely a kártyabirtokost egyértelműen azonosítja

Plaintext: kódolás nélküli tiszta szöveges adatsor.

Prepaid card (Előre fizetett kártya): Olyan elektronikus értéktároló, melynek elszámolása, kifizetése előre, a felhasználás idejétől függetlenül történik.

Protocol (Protokol): Eljárás, mely elektronikus üzenetek különböző eszközök közötti egyértelmű átvitelét teszi lehetővé.

RAM Random Acces Memory: Egyszer írható, nem módosítható tartalmú adattároló egység.

ROM Read-only Memory: Szabad hozzáférésű, változtatható tartalmú adattároló eszköz.

RSA Rivest, Shamir, Adleman: Mindennapos használatú aszimmetrikus kriptográfiai eljárás.

SAM Security Application Moduls: nem hamisítható számítógépes adattároló egység. Főként titkosítási kulcsok tárolására.

Server (Szerver): Olyan számítógép, amely a hálózat többi gépét kiszolgálja, központi adattároló egység funkcióját tölti be.

Session key:: Olyan kriptográfiai kulcs, amely csak meghatározott ideig érvényes és használható.

Smart card: Integrált áramkörös kártya, mely mikroprocesszort alkalmaz a számítási műveletek elvégzésére.

Time-stamp: Annak az időpontnak a rögzítése, amikor a kártyára érték felírásá történt.

White list (Fehér lista): Az az adatbázis, amely a rendszerhez belépésre jogosult személyek azonosítóit, adatait tárolja.

3.3. Chipkártyák fajtái

A mikroprocesszoros chipkártya jelenleg a legkorszerűbb elektronikus adathordozó kártya. Maga a chipkártya elnevezés széles termékskálát jelöl. Idetartozik minden olyan bankkártya méretű (az ISO 7816 szabvány szerinti) műanyag kártya, amely beépített mikrochipet tartalmaz, ugyanakkor paramétertől függően számos típust lehet megkülönböztetni. A két alapvető csoport az "unintelligens" memóriakártya és az intelligens mikroprocesszoros kártya. Nem lehet elégszer hangsúlyozni a különbséget a memória és a mikroprocesszoros kártyák között, amelyek külső kinézetre hasonlóak és egyaránt hívják őket chipkártyának, ugyanakkor mind tulajdonságaiban, mind felhasználási lehetőségeiben eltérnek egymástól. A memória és a mikroprocesszoros kártya összemosása, összekeverése - sarkítva - hasonló ahhoz, mintha egy floppy lemez és egy komplett PC közé egyenlőségjelet tennénk, mivel mindkettő számítástechnikai eszköz.

3.3.1. Memória kártyák

A memória kártyák egyszerűbb, kevesebb biztonságot igénylő, általában monofunkciós alkalmazásokhoz használhatóak fel. Elsősorban telefonkártyák, törzsvásárlói kártyák (loyalty) tartoznak ide. Magyarországon is ismertek ezek a kártyák: a korábbi MATÁV telefonkártyák illetve üzemanyag-társaságok által régebben kibocsátott törzsvásárlói (pontgyűjtő) kártyák. A memória kártyák is több csoportba sorolhatóak: szabad hozzáférésű illetve védett memóriájú kártyák. Az utóbbiak írási / olvasási joga ugyan titkos kóddal védett, de a kártyainterfész (terminál) közvetlenül ír a memóriába, titkosítási algoritmus használata nélkül. Egyes memória kártyák csak olvashatóak (egyszer írhatóak) mások újratölthetőek.

1. Ábra Memóriakártyák

3.3.2. PIN védelemmel ellátott, tárolt értékű kártyák

Itt az előbb ismertetett memória mellett biztonsági áramkör is van, így a kártya személyre szóló. Ez a kártyarendszer zárt rendszerű, így nem szükséges hozzá bárminemű elszámolóközpont (klíringközpont). Ebbe a kategóriába tartoznak a törzsvásárolói (loyalty) kártyák, amelyek később levásárolható bónuszpontokat tartalmaznak. Memóriakártyákat csak régebben, kezdetleges törzsvásárlói rendszerekben használtak, mert itt nincsenek meg a többpartneres működés biztonsági feltételei.

3.3.3. Huzalozott logikával ellátott kártyák

Az ilyen kártyák meghatározott célra, például beléptető rendszerhez személyazonosításra, vagy célautomaták működtetésére használatosak. Hozzáférési védelemmel (PIN kód) ellátott kártyák. Ez szintén zárt, például egy vállalaton belüli kártyarendszer.

3.3.4. Újratölthető kártyák

Ezek elektronikus pénztárcaként (electronic purse) működnek. Banki terminálról, ATM-ről, vagy speciális telefonkészülékről tölthetők fel. Általában nem nagy összeget tartalmaznak, és egyszerű, olcsó kereskedelmi terminálról használhatók, amelyen megjelenik a vásárolt áru összege, amelyet a kártyatulajdonos OK gombbal hagy jóvá. Ezután az érték a kereskedő terminájába kerül át, amelyet bankja este automatikusan jóváír a kereskedő bankszámláján. Ez már egy nyílt rendszer, mivel kereskedők, vagy egyéb szolgáltatást nyújtók csatlakozhatnak hozzá. Akár nyilvános telefonkészülékben is használható, ha a telefontársaság csatlakozott a rendszerhez. Ezek a szektorközi (interszektoriális) elektronikus pénztárcák. Itt természetesen szükség van banki elszámoló központra, vagy egy megbízható harmadik fél (trusted third party) szolgáltatásaira.

2. Ábra Mikroprocesszoros kártya

3.3.5. Mikroprocesszoros kártyák

A memóriakártyához csak kinézetben hasonlító mikroprocesszoros kártyákat akár a világ legkisebb mikroszámítógépeinek is nevezhetjük. E kártyatípus technológiája teljes mértékben és alapjaiban különbözik a memóriakártyáétól. Fő jellemzője a magas biztonsági szint, amelyet

csak egy mikroszámítógép tud biztosítani. Köszönhetően a programozási lehetőségnek és a viszonylag nagy memóriájának, a kártya multifunkcionális alkalmazása lehetséges. A mikroprocesszoros chipkártyák egyik típusa, a Magyarországon is jól ismert SIM kártyák, amelyek a GSM telefonokban használatosak. Funkcionális szempontból másik kártyacsoport a multifunkciós és pénzügyi alkalmazásokat lehetővé tevő kártyák.

3.3.5.1 A mikroprocesszoros kártyák általános felépítése

A felületi érintkezős kártyák esetében az interfész egy 8 érintkezős fedőlappal kapcsolódik a kártya mikroprocesszorához (8 bites CPU). A 8 érintkezőből jelenleg maximum csak hatot használnak, kettő későbbi alkalmazásra van fenntartva.

A chip további elemei: RAM, az operációs rendszert és a biztonsági algoritmust tartalmazó program memória (ROM) valamint az adatokat tartalmazó EEPROM, amely mérete 32kbyte vagy több is lehet főként az Open Platform-os kártyáknál (JAVA, WIN) Egyes kártyák kiegészülnek még egy matematikai coprocesszorral is, amely a nagy számítás igényű kriptográfiai - elsősorban aszimmetrikus kulcsolású (pl. RSA) - algoritmusok használata esetében szükséges. A memória területek elérése közvetlenül nem lehetséges, csak a mikroprocesszoron keresztül. Ennek révén, a kártyán tárolt adatok, így a bizalmas adatok is (pl. elektronikus pénztárca egyenleg, egészségügyi adatok stb.) csak megfelelő jogosultsággal érhetőek el. A jogosultság ellenőrzése és annak megfelelő válasz kiadása a kártya önálló döntése. A kártya memóriájába az operációs rendszer és a biztonsági algoritmusok letöltése a gyártás során történik, akárcsak a gyári sorozatszám és egyéb gyártási információ beégetése az EEPROM-ba. A kártya sorozatszáma a későbbiekben nem törölhető és nem írható felül, ugyanakkor egyes műveletekhez használható. Mivel ez a szám egyedi, az adott kártyát egyértelműen azonosítja.

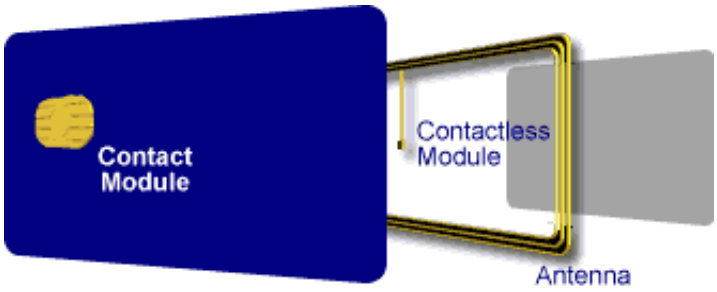
Az adatmemória állományait könyvtár és fájl szerkezetbe lehet rendezni, az egyes memória területeket jól elhatárolva egymástól. A memóriaterület (file) tulajdonságait számos szempont alapján lehet meghatározni: típus (pl. purse), írási - olvasási jog.

3.3.6. Érintkezésmentes (contactless, proximity) kártya

Az érintésmentes vagy érintkezés nélküli (contactless, proximity) kártyák esetében kontaktus helyett a külvilággal való kapcsolat induktív, kapacitív, mikrohullámú vagy rádiófrekvenciás módon jön létre. Ilyenkor az adó-vevő antenna is a szabványos kártya belsejébe van beépítve. A kommunikáció megoldása szerint léteznek néhány milliméteres hatótávolságú, néhány centiméterről olvasható, végül több méteres hatótávolságú kártyák. A hatótávolság az alkalmazás sajátosságainak megfelelően állítható be. Beléptető-rendszereknél ez a távolság általában a nagyobb értéket közelíti. Tömegközlekedési alkalmazásokban – ahol az utasok egymáshoz egészen közel is lehetnek – a hatótávolság általában 5-10 cm, hogy egyértelmű legyen, kinek a kártyájával kommunikál a kártyaelfogadó készülék. Probléma adódhat akkor is, ha két érintésmentes kártya is van az illetőnél, és mindkét kártya tud kommunikálni az elfogadó készülékkel. (Azonos kommunikációs protokollja van mindkét kártyának, vagy mindkét protokollt ismeri a kártyaelfogadó készülék.) Ez ellen úgy védekeznek a cégek, hogy minden készülék csak egyféle kártyát fogad el. Magyarországon és az Európai Unióban a bankok nem tartják kielégítőnek ezt a kommunikációs formát. Az újabb fejlesztésű kártyák emiatt általában érintéses és érintésmentes kommunikációra is képesek. Tömegközlekedési alkalmazásokban mindkét változatra vannak példák, de jóval rövidebb műveleti idő igénye miatt a jövőben az érintkezésmentes kártyák kizárólagossá válása prognosztizálható.

3.3.7. Duális (kétmódú) kártyák

Olyan kártyák, amelyek egyaránt képesek érintkezéses és érintkezésmentes kommunikációra, kielégítve mind a pénzintézetek biztonsággal szembeni elvárásait, mind a szolgáltatók és ügyfeleik gazdaságossággal, praktikummal, kényelemmel, eleganciával szembeni igényeit. A kétféle kommunikációt – a központi egységen, a memóriá(ko)n és a perifériavezérlőn túl – két külön mikroáramkör látja el.



3. Ábra Duális kártya felépítése

3.3.8. Kombi-kártyák

Ezek az újabb fejlesztésű, ún. monochipes kártyák, amelyek a duális kártyák központi egységének, memóriáinak és perifériavezérlőinek egy chipbe való integrálásával jöttek létre. Ezáltal – a duális kártyákkal megegyező módon – kielégítik mind a bankok biztonsági követelményeit, mind a szolgáltatók, felhasználók elvárásait. A monochipek előnye a duális kártyákkal szemben, hogy az összekötő vezetékek elmaradása miatt hosszabb élettartamúak, valamint nagy sorozatban történő gyártás esetén előállításuk olcsóbb. Hátrányuk, hogy a nagyméretű chip mechanikai hatásokkal szemben kevésbé ellenálló. További hátrány, hogy a modul rendszerű kialakítással ellentétben nem mindig az optimális konfiguráció áll rendelkezésre. Az összes smartcard-hoz hasonlóan a kombi-kártyák és a duális kártyák is lehetnek multifunkcionális kártyák. A duális kártya legígéretesebb felhasználási területe a tömegközlekedésben történő felhasználás. Lehetőség van arra, hogy egy kártya egyszerre funkcionálhasson bérletként és gyűjtőjegyként. Ennek megfelelően létezik két külön memóriaterülettel, és van egyetlen memóriával rendelkező változatuk.

3.3.9. Különböző kártyatípusok összehasonlítása

Tulajdonságok, alkalmazási területek	***Memóriakártyák***				***Mikroprocesszoros kártyák***			
	Védelem nélküli memóriakártyák	*PIN védelemmel ellátott, tárolt értékű k.*	*Huzalozott logikájú kártyák*	*Újratölthető kártyák*	*Érintkezéses kártyák*	*Érintkezésmentes (contactless) kártyák*	*Duális kártyák*	*Kombi kártyák*
Saját operációs rendszer					**x**	**x**	**x**	**x**
Védett memória		**x**	**x**	**x**	**x**	**x**	**x**	**x**
Biztonsági szint	**alacsony**	**közepes**	**közepes**	**közepes**	**magas**	**magas**	**magas**	**magas**
Élettartam	**5 év**	**5 év**	**5 év**	**10 év**	**10 év**	**15 év**	**10 év**	**15 év**
Nagy memória kapacitás					**x**	**x**	**x**	**x**
Érintkezéses kommunikáció	**x**	**x**	**x**	**x**	**x**		**x**	**x**
Érintkezés mentes kommunikáció						**x**	**x**	**x**
Multifunkcionalitás		**x**	**x**	**x**	**x**	**x**	**x**	**x**
Zárt rendszerű hasznosítás	**x**	**x**	**x**					
Nyílt rendszerű hasznosítás				**x**	**x**	**x**	**x**	**x**
E-pénztárca funkció				**x**	**x**	**x**	**x**	**x**
Törzsvásárlói pontgyűjtésre alkalmas			**x**	**x**	**x**	**x**	**x**	**x**
Személyazonosítás, beléptetés		**x**	**x**	**x**	**x**	**x**	**x**	**x**
Adattárolás	**x**	**x**	**x**	**x**	**x**	**x**	**x**	**x**
Elszámoló- (klíring) központot igényel				**x**	**x**	**x**	**x**	**x**

3.4. A mikroprocesszoros kártya összehasonlítása a többi kártyatípussal

A mikroprocesszoros kártyák előnye a huzalozott logikájú, valamint a memóriakártyákkal szemben a következő:

- Kisebb kockázati tényező (nagyobb biztonság)
- Szélesebb körű alkalmazási lehetőségek
- Hosszabb élettartam
- Kis üzemeltetési és fenntartási költség a mechanikus alkatrészek nélküli működésből fakadóan
- Rendkívül rövid tranzakciós idő az eladási pontokon
- Távközlési költségek csökkenése az off-line alkalmazás miatt
- Rugalmasság, továbbfejlesztési lehetőségek

3.5. Chipkártyaszabványok

A chipkártyák területén létrehozott szabványokat többféleképpen csoportosíthatjuk. Nem csak a kimondottan szabványosítással foglalkozó testületek által létrehozott leírásokat nevezzük szabványnak, hanem mindazokat a specifikációkat, amelyek követése egy adott területen biztosítja egy eszköz vagy alkalmazás használatát.

3.5.1. Általános szabványok

A chipkártyák világában az alapszabványokat az ISO (International Standard Organization) kezeli. Ezek közül a legszélesebb területet az ISO/IEC 7816 adja, ez tíz részből épül fel. A szabványt alapvetően az érintkezéses kártyák alapszabványaként definiálták. Ennek a szabványnak az első négy fejezete használatos a leggyakrabban, mivel ezek alkalmazása a piacon maradás egyik feltétele. Ezek a fejezetek definiálják ugyanis a kártyák fizikai paramétereit, az elektromechanikai jellemzőket (kontaktusok mérete és elhelyezkedése), a kommunikáció so-

rán használt adatátviteli protokollokat, valamint a kártya és a külvilág között alkalmazható parancs alapkészletet. A fennmaradó hat fejezet az alkalmazások regisztrációs eljárásait fedi le, illetve további utasításokat tartalmaz.

Mindazonáltal nem minden kártya tartalmaz kontaktust a kapcsolat kiépítésére. Az érintkezés nélküli kártyák más jellegű szabványokat igényelnek. Például, kontaktus nélküli kártyák esetében kezelni kell azt, ha egyetlen olvasó hatósugarában egy időben több kártya van. Kontaktusos kártya esetében ilyen az alkalmazás lényegénél fogva nem fordulhat elő. A kis távolságról alkalmazható kártyák (proximity) alapszabványa az ISO/IEC 14443, amelynek négy fejezete a fizikai kiépítést, a használható rádiófrekvenciát, a kommunikációs protokollokat és a már említett kommunikációs ütközések elkerülésének módszereit tartalmazza. Nagy távolságból alkalmazható kártyák (vicinity) esetében az ISO/IEC 15693 az irányadó. Hasonló fejezeteket tartalmaz, mint az ISO/IEC 14443, fontos eltérés azonban a kommunikáció során alkalmazott távolság és az, hogy az ISO/IEC 15693 egész fejezetet szentel az alkalmazások regisztrációjára vonatkozó előírásoknak.

A chipkártyák felhasználásának két legsikeresebb területe a távközlés és a pénzügyi szektor. Nem véletlen hát, hogy elsősorban ezeken a területeken jelennek meg a szabványok.

3.5.2. Távközlés

A távközlésben kiemelt szerepet kap a GSM, amelynek kártyái az ETSI[1] gondozásában lévő GSM 11.11 és GSM 11.14 leírásban szerepelnek. A GSM 11.11 tartalmazza a SIM-en[2] feltüntetett adatobjektumok leírását. Ezek közé tartoznak többek között az előfizető azonosítója, a tárolt telefonszámok, illetve az előfizető hitelesítéséhez kapcsolódó parancsok és algoritmusok. A GSM 11.14 az előző szabványt egészíti ki a SIM Toolkithez kapcsolódó alapkövetelmények definiálásával. A SIM Toolkit

[1] European Telecommunications Standard Institute
[2] Subscriber Itentity Module

lehetővé teszi, hogy a kártya által tartalmazott alkalmazás átvegye a kontrollt a telefon bizonyos területei fölött. Így lehetőséget biztosít menü megjelenítésére a kijelzőn, s esetlegesen második kártyaolvasót is kezel. A GSM 11.14 tartalmazza azokat az utasításokat, amelyek a SIM Toolkit használatához szükségesek.

3.5.3. Pénzügy

A kártyák fizetési célokra történő felhasználása nem új találmány, már eddig is léteztek a jelenlegi technológiához szorosan kapcsolódó szabványok, specifikációk. A chipkártyák megjelenésével a pénzügyi szektor meghatározó szervezetei létrehozták az egységes működést biztosító leírásokat. Ezek közül is kiemelkedően fontos az EMV[3] szabvány, amely definiálja a fizetőkártyákkal és az elfogadásukhoz szükséges eszközökkel szembeni alapkövetelményeket.

A specifikációt az EMVCo. nevű szervezet kezeli. Három fő részből épül fel, az első a kártya, a második a terminál, a harmadik rész pedig az alkalmazással szemben támasztott követelményeket tartalmazta. Tavaly dolgozták ki az EMV2000-et, amelyet négy fejezetre osztottak. Ezek a fejezetek rendre a kártyával szemben támasztott követelményeket, a biztonsági követelményeket (adattitkosítás, kulcskezelés), az adatok és a hitel / betétikártya-alkalmazások specifikációját, valamint az elfogadó terminállal szemben támasztott követelményeket definiálják. Érdemes kiemelni, hogy a szabványt létrehozó szervezetek kidolgozták a szabványnak való megfeleltetés minősítési rendszerét, amely két (hardver és szoftver) szinten hitelesíti a termékeket. Nem elég tehát azt állítani, hogy egy adott kártya megfelel a követelményeknek, a teljes elfogadottsághoz az EMVCo. tagjaitól beszerzett igazolás szükséges.

Az elektronikus pénztárca terjedésével szükségessé vált a különböző gyártók által készített rendszerek keresztelfogadása. Ezen a területen létezik a CEN[4] által létrehozott EN 1546 szabvány is, amely az

[3] Europay – MasterCard – VISA
[4] Európai Szabványosítási Bizottság

elektronikus-pénztárcarendszerek utasításait, az adatokat, valamint az értékátadási folyamat módját adja meg. Mindazonáltal az EN 1546 önmagában nem elég a keresztelfogadás biztosításához. Ezért az elektronikus pénztárca-rendszerek fejlesztői létrehozták a CEPS[5] dokumentumot és a CEPSCo. nevű szervezetet, amely a specifikáció kezelését végzi.

3.5.4. Alkalmazások

Annak érdekében, hogy a chipkártyák által kínált lehetőségek a számítógépeken egységes formában használhatók legyenek, olyan szabványok is létrejöttek, amelyek egységes felületet biztosítanak az alkalmazások fejlesztői számára. Azokat a szabványokat, amelyek ezen területen képződtek, egy szűk csoport (egy adott technológia tulajdonosa) hozta létre. Természetesen lehet vitatkozni azon, hogy ezeket szabványnak nevezzük vagy nem. Jelen esetben az biztos, hogy ezek a specifikációk a gyártók számára követendő definíciókat adnak, és egy adott körben szabványos működést biztosítanak.

A Microsoft a Windows platformon a PC/SC[6] szabvánnyal teremtette meg a annak a lehetőségét, hogy a chipkártyák és a kártyaolvasók egységes módon integrálódjanak az operációs rendszerbe. A specifikáció tartalmazza, hogy az alkalmazás milyen módon veszi fel a kapcsolatot a kártyaolvasóval, valamint hogy az alkalmazások milyen felületen keresztül érhetik el a kártya funkcióit. A specifikáció a Windows rendszerarchitektúrájába illeszkedő DLL-ek[7] feladatait és belépési pontjainak leírását tartalmazza.

Hasonló meggondolásból alakult ki a SUN által vezetett csoport, amely az OCF[8] kialakításával platformfüggetlen specifikációt hozott létre. Az OCF a Java technológián alapul, Java osztályok definiálásával biztosítja a kártyaolvasók és a kártyák funkcióinak elérését. A PS/SC és az OCF

[5] Common Electronic Purse Specification
[6] Interoperability Specifications for Integrated Circuit cards [ICCs] and Personal Computer System
[7] Dinamic Link Library
[8] Open Card Framework

elveit összehasonlítva azt mondhatjuk, hogy a PC/SC teljes szabadságot biztosít az alkalmazásfejlesztő eszköz kiválasztásában, de csak Windows platformon használható; az OCF platformfüggetlen, de csak java nyelven írt programokban alkalmazható. Az alkalmazások fontos csoportját képezik a titkosításokkal foglalkozó megoldások. Az ehhez szükséges kriptográfiai adatok tárolásának specifikációját tartalmazza az RSA által létrehozott PKCS#15, míg a kriptográfiai feladatok eléréséhez szükséges programozói felületet a PKCS#11 írja le. A terminálok számára is van ilyen törekvés: OTA (Open Terminal Architecture; EuroPay)

3.5.5. Kártyaalkalmazások

A szabványok vizsgálata során érdemes visszatérni a kártyán futó alkalmazásokra. Mint korábban látható volt, a kártya és a külvilág közötti kapcsolatra már az ISO/IEC 7816 is ad útmutatást. Mindazonáltal a kártyán futó alkalmazásokkal szemben támasztott követelményekről egyéb specifikációk rendelkeznek. A Java Card, a MULTOS és a Windows for Smart Cards által adott definíciókat operációs rendszerek parancskészleteként lehet értelmezni, még akkor is, ha a Java nem operációs rendszer.

3.5.6. Az ISO 7810-es szabvány

Ez a szabvány határozza meg a plasztikkártyák (chiptől függetlenül) fizikai méreteit.

Jellemző	Méret
Hosszúság (x):	85.6 mm (3.370 in)
Szélesség (y):	58.93 mm (2.125 in)
Vastagság (z):	0.76 mm (0.30 in)

1. Táblázat ISO 7810

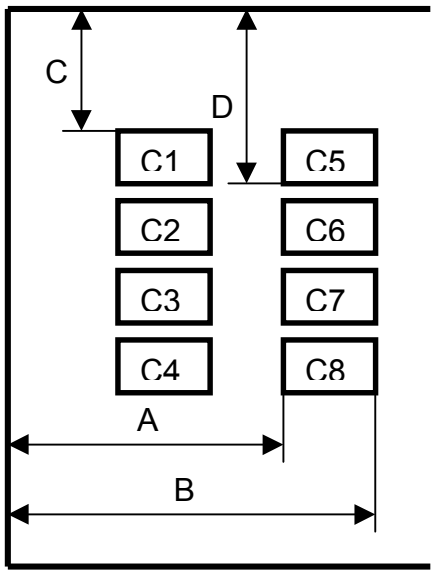
3.5.7. Az ISO 7816-os szabvány

3.5.8. ISO 7816-1

A szabvány ezen pontja a kártya fizikai tulajdonságait, paramétereit határozza meg. Mégpedig az UV fény, Röntgensugárzás, mágneses, és statikus elektromos mezővel, mechanikai behatásokkal szembeni ellenálló képesség nagyságát. Hossz és keresztirányú hajlítgatás károsodás nélküli elviselésének mértékét. Minden egyes tulajdonság paramétereit meghatározva, amelyek pontos ismertetése nem célom, mivel ezek a tulajdonságok csak szélsőséges alkalmazási körülmények esetén kerülnek előtérbe.

3.5.9. ISO 7816-2

A chip érintkező-felületének elhelyezkedését, és lábkiosztását tartalmazza. Ezen paraméterek gyártók általi betartása feltétlenül szükséges a különböző rendszerek átjárhatóságának biztosítása érdekében.

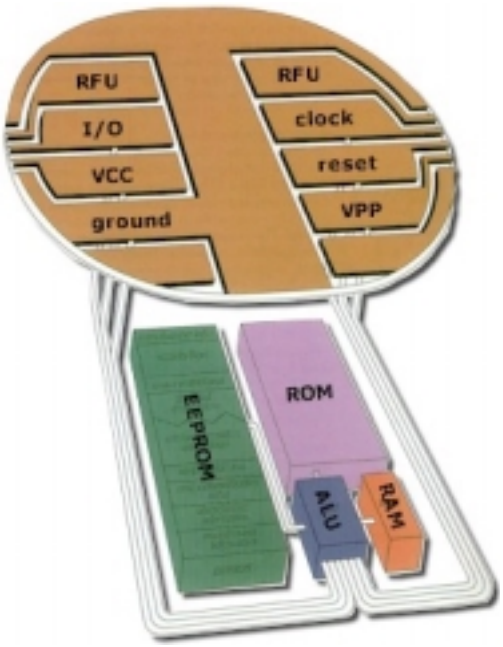


4. Ábra Az érintkezők elhelyezkedése

	A	B	C	D
C1	10.25	12.25	19.23	20.93
C2	10.25	12.25	21.77	23.47
C3	10.25	12.25	24.31	26.01
C4	10.25	12.25	26.85	28.55
C5	17.87	19.87	19.23	20.93
C6	17.87	19.87	21.77	23.47
C7	17.87	19.87	24.31	26.01
C8	17.87	19.87	28.85	28.55

2. Táblázat Az érintkezők elhelyezkedése [mm]

C1 : Vcc (5V)
C2 : RST
C3 : Clock
C4 : RFU
C5 : Gnd
C6 : Vpp
C7: I/O
C8 : RFU



5. Ábra A chip lábkiosztása

3.5.10. ISO 7816-3

A kártyán használt elektronikai jelek leírása

3.6. Titkosítási eljárások

3.6.1. RSA

A nyilvános kulcsú rejtjelezés legelterjedtebb módszere az RSA algoritmus. Ez az algoritmus egy matematikai tételen, *Fermat tétel*[9]én alapul. E szerint a tétel szerint, ha ***p*** prímszám, és nem osztója egy ***a*** egésznek, akkor ***a^(p-1)-1*** osztható ***p***-vel.

A tétel alapján, ha ***p*** és ***q*** különböző prímszámok, és ***a***-nak egyik sem osztója, akkor mind ***p***, mind pedig ***q*** osztója $a^{(p-1)(q-1)}-1$-nek, ami képlettel leírva: $qp \mid a^{(p-1)(q-1)}-1$. Ez nem más, mint a *Fermat tétel*, csak a tételbeli képletben ***a*** helyére egyszer a^{p-1}, egyszer pedig a^{q-1} kerül rendre a ***q***-val, illetve ***p***-vel való oszthatóságot felírva. Mivel ***p*** és ***q*** különböző prímek, ezért a szorzatukkal is osztható $a^{(p-1)(q-1)}-1$. Legyen $n=qp$. Ekkor $a^{(p-1)(q-1)+1}$ pont ***a*** maradékot ad ***n***-nel osztva, ha ***a*** kisebb, mint ***n***. Legyen $ef=(p-1)(q-1)+1$ szorzat alakban felírva. Ekkor az $a^{ef} \bmod n = a$ egyenlethez jutottunk, ahol a ***mod*** a maradékképzést jelenti. Legyen a nyilvános kulcs az ***e,n*** számpáros, a titkos kulcs pedig az ***f*** szám.

A kódolás során az üzenetet először számokká alakítjuk olyan módon, hogy a számok mindegyike kisebb legyen, mint ***n***. Ezután az egyes ***m*** számokat az

$$M=m^e \bmod n$$

képlettel kódoljuk előállítva a rejtjelezett ***M*** üzenetet, és ezt az üzenetet az $m=M^f \bmod n$ képlet alapján lehet dekódolni.

[9] A tétel leírását az 1.sz. melléklet tartalmazza

A felhasznált számoknak olyan nagyoknak kell lenniük, hogy az ***n*** számot ne lehessen prímtényezőkre bontani. Ha ugyanis az ***n*** számot fel tudjuk bontani ***n=qp*** alakra, akkor ***e*** alapján egy osztással meg lehet határozni ***f***-et.

3.6.2. Triple DES (*Data Encryption Standard*)

Egy ideje általánosan elfogadott eljárás, hogy az információk védelmére a Triple DES-t használják a DES helyett. Ez azt jelenti, hogy a bevitt adatokat valójában háromszor titkosítják. Erre sok megoldás létezik, az ANSI x9.52 szabvány határozza meg a Triple-DES titkosítást a k_1, k_2 és k_3 kulcsokkal:

$$C=E_{k3}(D_{k2}(E_{k1}(M))),$$

Ahol az ***Ek*** és ***Dk*** jelenti a DES kódoló (encoding) és visszafejtő (decoding) kódokat a ***k*** kulccsal. Ezt a kódolási módszert néha úgy is nevezik, hogy DES-EDE. Egy másik variáció a DES-EEE, amely három egymást követő kódolásból áll.

Három visszafejtési lehetőség van, amelyet az ANSI x9.52 határoz meg:

- A három kulcs k_1, k_2 és k_3 egymástól független
- A k_1, és k_2 független, de k_1, = k_3
- k_1, = k_2 = k_3

A harmadik eset teszi a Triple-DES rendszert kompatibilissé a DES –sel. Mint minden „jó titkosírás”, a Triple-DES-t is többféleképpen lehet használni. A dupla és a tripla kódolás nem mindig adja meg azt a biztonságot, amit elvárhatnánk tőle.

Van szimmetrikus titkosítási eljárás ***n*** számú kulccsal $E_k(P)$ melyben, ***P*** jelöli a kódolási üzenetet a ***k*** kulccsal. Dupla kódolás két különböző kulccsal ***2n*** számú kódot ad.

Tételezzük fel, hogy képesek vagyunk tárolni $E_k(P)$ –t minden k kulcshoz és a megfejtett szöveget, P-t, és tegyük fel azt is, hogy adott egy visszafejtett szöveg, C, mint $C=E_{k2}(E_{k1}(P))$ a k_1, k_2 titkos kulcsokhoz. Minden egyes I kódhoz csak egy kulcs van, $D_I(C)=E_k(P)$. 2^n lehetséges kulcs van, amely megfelel a (P,C) számoknak, és ezek a kulcsok körülbelül $O(2^n)$ lépésben találhatóak meg. Ha csak $2^p < 2^k$ kulcsokat tudjuk eltárolni, megváltoztathatjuk az algoritmust, és további kulcsokat találhatunk az $O(2^{2n-p})$ lépésben.

Másik eset, ahol a Triple-DES kódolás mindhárom kulcsát figyelembe veszik: legyen $K=(k_a, k_b, k_c)$ és $K'=(k_a \oplus \Delta, k_b, k_c)$ két titkos kulcs, ahol Δ az ismeretlen konstans és $\oplus$ jelöli a **XOR** műveletet. Tételezzük fel, hogy adott egy megfejtett C szöveg, és az ahhoz tartozó visszafejtés P és P' –je a K és K' kulcsokkal. Mivel $P'=D_{ka \oplus \Delta}(E_{ka}(P))$ meghatározható k_a (vagy a lehetséges megoldások k_a helyére) az $O(2^n)$ lépésekben, ahol n a titkos kulcsok száma. Ha feltételezünk egy feltörési kísérletet, akkor a kulcs többi része (k_b és k_c) újabb $O(2^n)$ lépésben határozható meg.

A két kulcsos Triple-DES feltörésével sokan próbálkoztak, közülük is a legnevesebb Merkle és Hellmann, valamint Van Oorschot és Wiener, de az adatigény feleslegessé tette ezeket a próbálkozásokat.

Azonban bármely titkosítást fel lehet törni csak kérdés, hogy megéri-e. A triple DES brute force töréséhez még mindíg sok idő és jelentős számítási kapacitás szükséges. A simple DES-t már 56 óra alatt feltörik.

4. Intelligens rendszerek a nemzetközi gyakorlatban

4.1. Bevezetés

Ebben a fejezetben Magyarország határain kívül üzemelő, intelligens kártyákat felhasználó tömegközlekedési rendszerek kerülnek bemutatásra. De még mielőtt a finn, a szlovák és a cseh rendszerekre térnénk, tisztázzuk mi is az intelligens kártya.

4.2. Az intelligens kártya

Roland Moreno 1974-es szabadalma óta eltelt 27 év, de az intelligens kártyák széleskörű terjedése napjainkban zajlik. Európa egyes országai tapasztalatokban és eredményekben gazdagabbak, melyekből a később csatlakozók is profitálhatnak.

Az ISO 7816-os szabvány határozza meg az intelligens kártyákkal szemben támasztott követelményeket. A szabvány alpontjai (1-től 11-ig) leírják a mai követelményeket kielégítő paramétereket, melyek betartása a különböző fejlesztéseknek ad közös alapot.

Első ránézésre az intelligens kártyák a telefonkártyákra hasonlítanak, de felépítésükben, és ezáltal működésükben is sokban különböznek egymástól. A legfontosabb előnye az intelligens kártyának, hogy memóriarekeszeinek (RAM, ROM, EEPROM) és mikroprocesszorának köszönhetően egy kis számítógépre hasonlít. A kártyának saját operációs rendszere van, mely a kártyán található vagy éppen a külvilágból érkező adatokkal és alkalmazásokkal biztonságos kommunikációra képes.

Ezen felül, a mai korszerű intelligens kártyák fizikai védettsége is magas szinten áll, míg a mikroprocesszor mellett levő kriptoprocesszor a mai privacy igényeket kiszolgáló alkalmazások kezelését is megoldja. Egyes intelligens kártyákon akár 1024 bit-es RSA kulcsok is generálhatóak. Ennek köszönhetően a titkos kulcs sohasem hagyja el a kártyát, de

kiszolgál olyan azonosításra és hitelesítésre kidolgozott alkalmazásokat, mint például egy nyilvános kulcsú titkosírással kódolt és digitálisan aláírt elektronikus levél elkészítése a kapott sima forrásszöveget véve alapul. A kártya védett a jogtalan felhasználás ellen akár a ma még használatos PIN kóddal, akár korszerű és tudományos alapokon nyugvó biometriai eljárásokkal. A fizikai támadások ellen is alkalmazható a kártya önmegsemmisítő (enyhébb esetekben csak önblokkoló) szolgáltatása, mely a kártya elvesztése esetén megvédi a tulajdonost a jogtalan felhasználásból következő károktól.

A smartcardok folyamatirányító mikroszámítógépként, vagyis mikrokontrollerként működő kártyák. A mikrokontroller nem más, mint egyetlen közös egységbe integrált mikroprocesszor, és perifériaáramkörök (órajel-generátor, programtároló (ROM), adattároló (RAM), adatátviteli port, A/D átalakító, sorosvonal-illesztő, időzítő/számláló, stb). A smartcard-ok központi egységgel (8 bites mikroprocesszor), átmeneti tárolóval (RAM), programtárolóval (ROM) a tranzakciók tárolására alkalmas viszonylag nagy kapacitású operatív tárolóval (EPROM és EEPROM részekkel) (open zone, working zone és secret zone részekkel) valamint a külvilággal történő kommunikációt biztosító kontaktusos, illetve induktív, hiper- (HF) vagy rádiófrekvenciás (RF) interfésszel rendelkeznek. A legtöbb változatnál az összes áramkör egy chipbe van integrálva. Ez alól csak a kis sorozatban gyártott, illetve a kétféle kommunikációra képes kártyák egy csoportja képez kivételt. Saját operációs rendszerük van. A működésükhöz szükséges villamos energiát a kommunikáció során kártyaelfogadó berendezésből nyerik. Védelmük PIN kóddal, vagy más fejlett védelmi rendszerrel (biztonsági algoritmussal) van megoldva, amely a harmadik sikertelen próbálkozásnál reteszeli a kártyát. Tehát a smartcardok PIN kód manuális bevitele nélkül (off-line üzemmódban) is képesek alacsony kockázati szintet (visszaéléssel szembeni nagy biztonságot) nyújtani. Hátrányuk a magas kártya előállítási költség. (Képességtől függően 1 – 10 USD.)

4.3. Proximity kártyák Helsinkiben

Helsinki és a környező települések önkormányzatai új utazási adatgyűjtő rendszert vezetett be a tömegközlekedésben. A rendszer alapja a ***Buscom*** technológiájára épülő proximity kártya. Ez a fejlesztés új távlatokat nyitott a térség tömegközlekedésének fejlődésében, ezzel a megoldással Helsinki és környéke csatlakozott a modern nagyvárosok sorába.

A próba üzem (pilot project) 1992 – 93 –ban indult azzal a céllal, hogy felváltsa az addig használt papíralapú jegyeket és bérleteket, valamint sokkal pontosabb adatokat szolgáltasson a tömegközlekedési szokásokról. Az addigi rendszert a rugalmatlanság, magas karbantartási költség és számos különböző járulékos költség jellemezte.

A pilot projekt a Helsinki Fővárosi Önkormányzat (YTV) megbízásából indult el. A projektben érintkezéses és érintkezésmentes kártyákat is teszteltek. Ezek a gyakorlati tesztek vezettek a proximity kártya rendszer megvalósításához, melynek gazdasági és technikai paraméterei messzemenően jobbak voltak a versenytársakénál.

1996 júniusában született az elhatározás a rendszer teljes körű bevezetéséről Helsinki város és környékének tömegközlekedésében. A döntés közösségi elhatározásból született, melyet nemzetközi versenytárgyalás követett, amin a világ vezető rendszerszállítói vettek részt. A nyertes szállító (az Olivetti konzorcium) a Buscomot kérte fel a teljes rendszer intelligens kártyákkal való ellátására. A rendszer jelenleg elérte azt a fejlettséget, hogy a járműveken naponta több mint egymillió kártyatranzakció valósul meg.

4.3.1. A rendszer bevezetésének indokai

A választási kritérium az utazási kártya mellett elsősorban gazdasági előnyökre vezethető vissza, mint a vételár és a fenntartási költség, minőségi tényezőkre, mint pl. a jó irányítási tulajdonságok, technikai megoldások kifinomultsága, szállítói megbízhatóság és tapasztalat, szállítási határidő, tanácsadási és karbantartási szolgáltatások szervezettsége és minősége. Helsinki olyan megbízható, tapasztalt szállítót keresett, amely az igényeknek leginkább

megfelelő rendszert képes kivitelezni. A magas minőségi és gazdasági, gazdaságossági követelményeknek a Buscom-ot látták a legmegfelelőbbnek.

Az intelligens kártyarendszer lehetővé tette a rugalmas jegy- és tarifarendszer alkalmazását, tökéletesítette a jegyértékesítési és érvényességi szinteket, és fokozta a tömegközlekedés iránti igényt. Ezekben a tényezőkben összegezhető a rendszer marketing hatékonysága. Az igények jobb kielégítése, az utazás könnyebbsége elősegítette a tömegközlekedés vonzóbbá válását. Jelentős megtakarításokat értek el a szállítási költségeknél. Mindinkább kiszélesedett a dinamikus utas és járat információs rendszerek felhasználása, mely a gyorsabb, pontosabb tájékoztatást, ez által a kerülőutak és kellemetlenségek elkerülését, tette lehetővé.

A kártyarendszer elősegítette a befektetések mihamarabbi megtérülését, a pénz gyorsabb körforgását. A megtakarítás a bevezetés időszakában volt a legjelentősebb.

4.3.2. A rendszer elemei

Az új rendszer magában foglalja az összes berendezést, a közlekedési rendszert, a járművezetői jegyeladó berendezéseket, a kártyaolvasókat és a jegyvizsgálói olvasókat, kártya feltöltő és értékesítő eszközöket, jegypénztárakat, és az intelligens kártyákat. Szintén a rendszer részét képezi az adatgyűjtő és adatátviteli rendszer, a szoftverek és az egyéb tartozékok, valamint a dolgozók átképzése, betanítása a rendszer használatára.

Az intelligens kártyarendszer rugalmas, nyitott az új alkalmazások, fejlesztések felé. Könnyű az új utasok rendszerbevonása, csak egy kártyát kell számukra kiadni, valamint pontosan felmérhető az utazási szokások időbeni változása. Különböző jegy kombinációk, melyek az időszakos és az alkalmi jegyek tulajdonságaival ruházhatóak fel, mely minden utas igényének leginkább megfelel.

4.3.3. Az adatátvitel

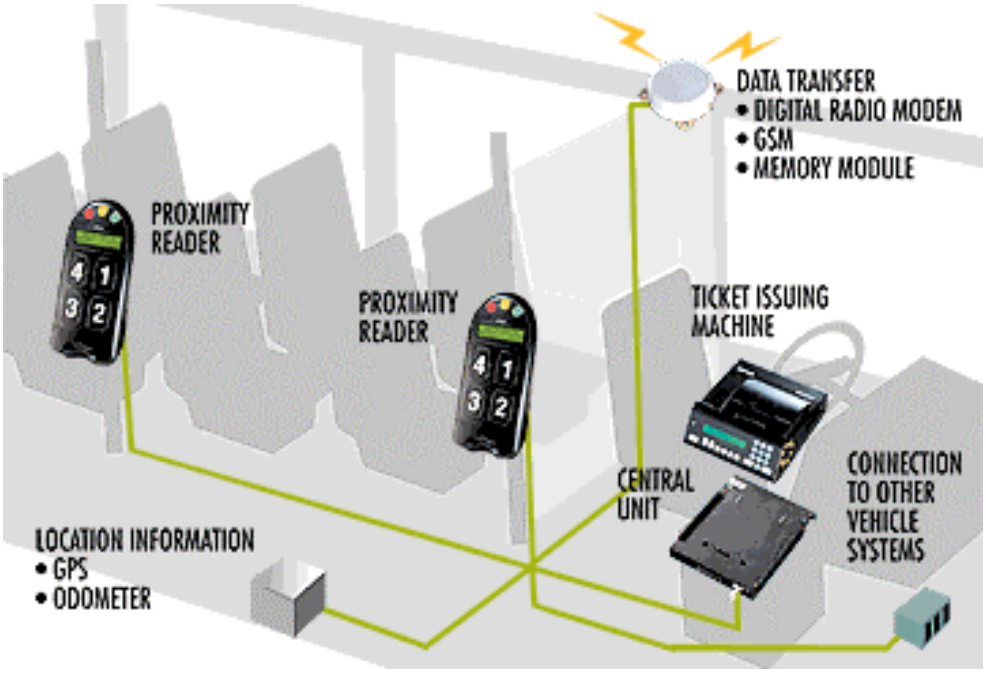
A járműveken szélessávú technológiára épülő digitális rádió modem van elhelyezve, mely az utazási információkat eljuttatja a depóban elhelyezett bázisállomás számítógépébe. Az ellenőrző paraméterek a járműveken vannak tárolva, ilyenek pl. a fekete listák, amelyek átvitele a jegykiadó automatákba csak néhány másodpercet igényel. Az utazási információk és más szintén a rendszerről gyűjtött információk könnyen rendelkezésre állnak, felhasználhatóak napi, heti, havi statisztikák készítésére, de ezeknél rövidebb, illetve hosszabb időintervallumok adatai is lekérdezhetőek.

Legfőbb előnye ennek az adatátviteli technológiának, hogy az adatátvitel sebességét nem befolyásolják az esetleges zajok, zavarások. Ez a tulajdonság érvényesül, amikor nagy számú tranzakcióra van szükség kis idő alatt, itt ugyanis nagy az interferencia valószínűsége. Ez az adatátviteli technológia biztonságos módon képes kezelni, ha az utazó bankkártyával egyenlíti ki a szolgáltatás ellenértékét. A szélessávú átviteli technológia szabadalma nyilvános, könnyen alkalmazható a digitális rádió modemeknél, gyors és akadálytalan a hitelesítése.

4.3.4. A rendszer jelenlegi paraméterei

- egymillió kártyatranzakció naponta
- 1300 busz
- 110 villamos kocsi
- 90 HÉV
- 42 metró kocsi
- 2500 kártyaolvasó
- 1500 jegykiadó automata
- 100 jegyvizsgáló terminál
- 35 depó, bázisállomás
- 320 kártya feltöltő és árusító eszköz

– 300 000 proximity kártya



6. Ábra A Buscom rendszer kiépítése

4.4. EM CARD rendszer szlovák, cseh és lengyel alkalmazása

Ezek a rendszerek teljes egészében megegyeznek a következő fejezet 5.2. pontjában leírt, MicroRaab Rt. által forgalmazott EM CARD rendszerrel, mivel az a cseh, lengyel, és szlovák gyakorlatban használt EM CARD rendszerek hazai megfelelője. Eltérés csupán az üzemeltető társaságok személyében nyilvánul meg.

4.4.1. A rendszer volumene

A rendszer a Szlovák Köztársaságban először 1996 novemberében került bevezetésre, azóta összesen 15 közlekedési társaság 1123 járművére szereltek fel egy-egy olvasó terminált, melyek segítségével mintegy 71 ezer kártyát használnak az utasok nap, mint nap. Ugyanezek a paraméterek Csehország esetében a következőképpen alakultak: a

rendszer bevezetésére 1996 januárjában került sor. A bevezetés óta 14 újabb közlekedési társaság kapcsolódott a rendszerbe 1473 járművel, és körülbelül 240 ezer felhasználói chipkártyával.

5. Intelligens rendszerek a hazai közlekedésben

5.1. Elektronikus utazási kártya-rendszer a Tisza Volán Rt.-nél

A helyi menetrendszerinti közlekedés számára tervezett, gyártott eszközökből több üzemel, így 1997-től Hódmezővásárhely városában teljes körűen használt az előreváltott jegykezelő (érvényesítő vagy érvénytelenítő), és a vonalkóddal ellátott hagyományos bérletjegy-ellenőrző készülék, amely akkor az első üzemszerű felhasználásként indult el Magyarországon. Hasonlóan elsőként indult be az elektronikus utazási kártyarendszer, amelynek bevezetése a helyközi közlekedésben az 5024. számú vonalon 1999. szeptember 1.-én kezdődött. Utazási kártyaként a Texas Instruments gyártmányú, TIRIS rendszerű, aktív chipes elektronikus kártya került felhasználásra.

Az elektronikus utazási kártya a jelenleg használatos havi érvénytartamú bérletjegy-rendszert szolgálja ki. A kialakított belső adattárolása lehetővé teszi eltérő (utazási szám érvényességű, vagy viteldíj összeg tárolásán alapuló) rendszerben való felhasználását. Az utazási kártya elektronikus pénztárca jelleggel is alkalmazható.

Az utazási kártya göngyöleg jellegű, csupán egy begravírozott szám segíti azonosítását. A hosszú élettartam miatt (100.000 db írás – feltöltés jellegű akció) bármiféle – személyiségi jogot nem sértő – adat feltüntetése a későbbiekben korlátozná a felhasználást, kizárja a tulajdonos váltást. A kialakított utazási kártya jelölés biztosítja a visszaváltható-ságot, az ismételt használatba vételt, a közlekedési adatok szabad megválasztását.

Az utazási kártya elektronikusan tárolt adatai a jelenlegi rendszerben: kártyaazonosító szám, az utazási eszköz megnevezése, vonalszáma, relációja, érvényességi tartama, a feltöltő állomás azonosítója. Az utazási kártya felhasználható különféle közlekedési nemek egyedi vagy

tarifaközösségi rendszerében megtestesítve egy, illetve több bérletjegyet.

A kártyakezelő egység a fedélzeti vezérlőtől, jegykiadógéptől elválasztva is használható érvényesség ellenőrzésére, utazási egyenleg közlésére. A kezelőegység az ellenőrzésre felmutatott bérletjegy adatait tételesen tárolja, vagy gyűjtésre adhatja át a jegykiadógépnek, fedélzeti vezérlőnek. A kezelőegység összekapcsolható pénztárgéppel vagy bankterminállal. Ekkor az újratöltéshez (az érvényesítéshez) tartozó bevételnyugtázási feladatokat a kapcsolódó egység végzi el. Az utazási kártya adatai segítségével a kártyakezelő egység a nyugtázó egységet az utas közreműködése nélkül önműködően vezérli.

Az utazási kártya leolvasórész kialakítása biztosítja a jelenleg át nem ruházható bérletjegy és a jegy felhasználójának (felmutatójának) személyzet által történő ellenőrzését (összehasonlítását). A kártyakezelő egység leolvasója 1-2 cm távolságban hatásos, amely lehetővé teszi az érintkező nélküli intelligens kártyákra jellemző, környezetet terhelő, pulzáló nagyfrekvenciás villamosteljesítmény-kibocsátás minimális értékre történő korlátozását.

Az EMKE jegykiadó és jegyérvényesítő rendszer az utazások elektronikus úton történő regisztrációjával minden egyes járatról utazási tényadatokat tárol. A kiadott menetjegyek mellett minden bérletes utazás alapadatként bekerül egy feldolgozó rendszerbe.

5.2. A Microraab Rt. EM Card rendszere

5.2.1. A rendszer általános jellemzése

Az utaskiszolgáló rendszer egy fedélzeti számítógéppel vezérelt, több összetevőkből álló moduláris rendszer. A rendszer alapelve az érintésnélküli kártyával működő utaskiszolgálás.

5.2.2. Az érintésnélküli kártya

A rendszer Mifare típusú chipkártyával működik, amely jelenleg világszerte az egyik legelterjedtebb technológia. A kártya alapja a chip, amely a kártya mentén egy antennával van összekötve. A kártyának nincs szüksége semmilyen külső tápforrásra. Az érintés nélküli kártya használatának előnye a kártya hosszú élettartama – 100 000 felhasználás (Ez a szám az EEPROM írására vonatkozik, tehát ha a memóriába nem történik írási művelet, akkor az nem befolyásolja a kártya élettertamát). Az utas felszálláskor a kártyát a leolvasó berendezés elé helyezi 10 cm-es leolvasási távolságon belül. A kártyáról levonásra kerül az utazás díja, vagy ellenőrzésre kerül az időjegy érvényessége. Az olvasási művelet gyorsasága – 0,2 s – jelentősen felgyorsítja az utas kiszolgálását.

A kártya perszonalizálása: A kártyán tárolásra kerülnek a kártyatulajdonos azonosító adatai is, ezzel kialakításra kerül a kártyatulajdonosok adatbázisa. A kártyán történő adatok tárolásával és adatbázis kialakításával elveszett kártyák esetén megakadályozható a kártyával való visszaélés. Ilyenkor a kártya letiltható és a kártyán fennmaradt összeg átvihető az új kártyára.

Elővétel: Az elővételi árusító helyek végzik a kártyák perszonalizálását, megszemélyesítését, az elektronikus pénztárca és időjegy esetén a pénzösszeg illetve a típus feltöltését a kártyára.

A kártya használata: Az utasok a perszonalizált és megváltott kártyával azonnal utazhatnak.

5.2.3. A rendszer alapkonfigurációja

Az EM 216 gépjármű fedélzeti számítógép[10], a rendszer vezérlő egysége:

- Adatbázisokat tartalmaz (menetrend, díjszabás, tiltott kártyák listája, stb)

- Vezérli a kártyaolvasókat (terminálokat)
- Rádiófrekvenciás úton vezérli a belső és külső információs táblákat, adatokkal látja el a megállók hangos bemondóját, menetjegykiadó pénzérmés automatákat, kártyalyukasztókat, stb.
- Ellenőrzi a menetrend betartását
- Tárolja a statisztikai adatokat

Az adatátvitel a jármű fedélzeti számítógépe és PC közt vezeték nélkül, infraátvitel segítségével történik a kijelölt „kiolvasó" helyeken. Az adatátvitel időtartama az adatok mennyiségétől függ és néhány másodpercig tart. A művelet teljesen automatikus, az átvitel minőségének és hibátlanságának a kiértékelésével. Az adatátvitel eredményes befejezését fényjelzés is jelzi.

EM 316 RD /EM 316 RDP, EM 326/ terminálok[11] kártyaolvasó berendezések: Kommunikálnak a kártyával, így biztosítják a megfelelő tarifa szerint megállapított összeg leolvasását. Operáció eredményességét fény és hangjelzés jelzi. A kártyaolvasó csatlakoztatásával a gépjármű fedélzeti számítógépéhez biztosítva van:

- Az adatátvitel a fedélzeti számítógépből a kártyaolvasóba (árjegyzék, megállók jegyzéke, tiltott kártyák, stb.)
- Statisztikai adatok átvitele a kártyaolvasóból a gépjármű fedélzeti számítógépébe

Az elektronikus menetjegy (kártya) érvényessége ellenőrizhető közvetlenül a járművön az EM 705 R kézi (mobil) leolvasó berendezéssel.

[10] Az EM 216 fedélzeti számítógép technikai paramétereit a 2. sz. melléklet tartalmazza
[11] Az EM 316 RD terminál technikai paramétereit a 3. sz. melléklet tartalmazza

5.2.4. Készpénz nélküli utaskiszolgálás

5.2.4.1 Az elektronikus pénztárca

A kártya memóriájában feltöltésre kerül egy pénzösszeg, amelyből minden utazás alkalmával levonásra kerül a menetjegy ára. A kártyáról megvásárolható az utastárs számára is a menetjegy. A kártyaegyenleg kijelzésre kerül a terminálon (olvasó berendezésen). Nyomtatóval ellátott olvasó berendezés igénybevételével a menetjegy ára és a kártya egyenlege rányomtatásra kerül minden kiadott menetjegyre. Az elektronikus pénztárca újratölthető.

5.2.4.2 Az időjegy (bérletjegy)

A kártya adatbázisába bevihető elektronikus (időre szóló) bérletjegy, amelyet tulajdonosa az előfizetett időszakon belül vehet igénybe. Az utazások száma egy bérleten korlátozható. Minden utazásnál a kártyaolvasó terminál ellenőrzi és kijelzi a bérlet érvényességét. A kártyára többtípusú bérlet váltható.

5.2.4.3 Az elektronikus pénztárca és az időjegy (bérletjegy) kombinációja

A kártya kettősfunkciójú: elektronikus pénztárcaként és elektronikus időjegyként is működik. Ha az utas érvényes elektronikus időjeggyel rendelkezik, a felszállást követő leolvasás után jogosult az utazásra. Az elektronikus pénztárcából megvásárolható az útitárs menetjegye is. Ha az utas nem rendelkezik érvényes időjeggyel, a menetjegy ára levonásra kerül az elektronikus pénztárcából.

5.2.4.4 A szakasz(jegy) – felszállás az első ajtón

A rendszer felépítése: A vezetőnél elhelyezett jármű fedélzeti számítógép és egy, vagy esetleg két az első ajtónál elhelyezett kártyaolvasó terminál. Az elektronikus pénztárcával rendelkező utas felszálláskor a kártyaolvasó terminál előlapján kiválasztja a megfelelő szakaszt, és a

kártyát a leolvasó elé helyezi, így a menetdíj értéke levonásra kerül. A szakasz lehet idő, távolság (km), zóna, stb. Az elektronikus bérletjeggyel rendelkező utas kártyájának érvényesség ellenőrzése a kártya leolvasása után megtörténik. Az érvénytelen kártyát hang- és fénykijelzés jelzi. Következő leolvasással megvásárolható az útitárs menetjegye is.

5.2.4.5 A szakasz(jegy) – felszállás az összes ajtón

A rendszer felépítése: a vezetőnél elhelyezett jármű fedélzeti számítógép és egy, vagy esetleg két kártyaolvasó terminál minden ajtónál elhelyezve. Nagyobb utasforgalomnál ezt a megoldást ajánljuk. Az utaskiszolgálás hasonló az előző pontban leírtakhoz.

5.2.4.6 „Check in – Check out" – felszállás az első ajtón

A rendszer felépítése: a vezetőnél elhelyezett jármű fedélzeti számítógép, egy kártyaolvasó terminál az első ajtónál fel- és leszálláshoz, a többi ajtónál elhelyezett kártyaolvasó terminál csak leszállásra szolgál. Felszállásnál az elektronikus pénztárcából a leolvasó előlegként leolvassa az utolsó megállóhelyre érvényes menetdíj értékét. Leszállásnál a kártyaolvasó terminálon megjelenik a valóságnak megfelelő menetdíj. Ez a módszer megakadályozza az érvényes menetjegy nélküli utazást. A „check in – check out" kiszolgáló rendszer alkalmazásánál az utasnak nincs szüksége a díjszabási feltételek ismeretére, elég, ha a kártyáját felszállásnál és leszállásnál leolvastatja a kártyaleolvasó berendezéssel. Ez a módszer precíz statisztikai adatokat készít a kártyával utazó személyek számáról minden megállóban.

5.2.4.7 „Check in – Check out" – felszállás az összes ajtón

Rendszer konfiguráció megegyezik az előzővel. Az utasok fel- és leszálláshoz igénybe vehetik az összes ajtót. A fel- és leszállási módszerek – eleget téve a gyors utas kiszolgálásnak – szükség szerint variálhatók.

5.2.5. Készpénzfizetés

Kártya nélküli utasok kiszolgálása:

- Menetjegyváltás készpénzért az autóbusz-vezetőjénél
- EM 306 CM érmés jegykiadó automata telepítése a járművön
- Jegyérvényesítő berendezés elhelyezése a járművön

5.2.6. Kiértékelő és információs rendszer

A rendszer lelke része a kiszolgáló szoftver, amely elemei közé tartoznak:

- Alapadatok szerkesztéséhez és tárolásához szükséges programok (menetrendek, díjszabási táblázatok, vezetők adatbázisa, stb.)
- Kommunikációs programok – adatok átvitelére a fedélzeti számítógépekbe és üzemeltetésből származó adatok visszaolvasására
- Kimutatások készítéséhez szükséges programok: utasok mennyisége az egyes vonalakon, bevétel kimutatása vonal-, járat- és megállónként, egyes járatok jövedelmezősége, közlekedési helyzet modellezése, stb.

5.2.7. Egyéb alkalmazási lehetőségek

A rendszer lehetővé teszi a kölcsönös elszámolást több közlekedési társaság között (clearing). Így lehetőség van rá, hogy a kártya tulajdonosa több közlekedési vállalat járatain (vonalain) utazzon ugyanazon chipkártyával. A chipkártya további felhasználásokra is alkalmas, pl. parkoló automaták kezelésére, munkaidő-nyilvántartó és beléptető rendszerekhez, stb.

5.2.8. A rendszer további lehetőségei:

- Lehetőség 10 tarifa definiálására.

- A menetrendek automatikus megváltoztatása – a régi és az új menetrendek a pénztárgép memóriájába kerülnek.
- A jegy árának megváltoztatási lehetősége – ár csúcsidőben és csúcsidőn kívül, éjszakai árak.
- Napi jegy választott ára – amennyiben az egyes jegyek árainak összege túllépi a napi jegy árát, a további utazás ingyenes.
- Időjegy fix időtartamra /tól-ig/, vagy az első felhasználástól számítva.
- Lehetőség az időjegy megszakítására.
- Lehetőség a kártya betét minimumának és maximumának a megadására.
- Akusztikus és fény jelzés a művelet végrehajtásának helyességének /helytelenségének/ a jelzésére.
- Figyelmeztetés az utas számára, amennyiben a kártyán lévő összeg a jegy árának értéke alá esik, időjegy esetén egy nappal a lejárat előtt.
- Az első jegy kiadása automatikusan a kártya típusának megfelelően, további jegy /utastárs számára/ kiadása a kiválasztás után.
- Több jegy vásárlása egy kártyáról – közös felszállás és leszállás.
- Lehetőség van arra, hogy az első ajtón való felszállást az összes ajtón való felszállás módszerével kombináljuk a szükséges utaskezelés szempontjából.

5.2.9. Összefoglalás

A bemutatott utaskiszolgáló rendszer főbb előnyei:

- Utasok gyors elektronikus ellenőrzése
- „Feketén” utazók számának csökkentése
- Szállított utasok pontos statisztikája
- Készpénznélküli kiszolgálás

- A díjszabás rugalmas módosítása
- Kölcsönös elszámolások – clearing
- Rendszer moduláris kiépítése (kibővítés információs táblákkal, hangosbemondóval, műholdas járműkövető rendszerrel, stb.)
- Felhasználóbarát kezelés
- Alacsony üzemeltetési költségek

5.3. comC@rd chipkártyás utaskiszolgáló rendszer az Alba Volán Rt.-nél

Magyarország egyik érintés nélküli chipkártya-alkalmazása valósul meg a tömegközlekedésben, Mór városában, a MatávCom és a Microraab Rt. által kifejlesztett comC@rd chipkártyás utaskiszolgáló rendszer tesztelésével.

A féléves program során Mór lakói az Alba Volán Rt. 6 helyi autóbuszán próbálhatják ki a comC@rd chipkártyás utaskiszolgáló rendszerhez tartozó, elektronikus bérletként és jegyként is alkalmazható intelligens kártyát. A comC@rd rendszer "lelke" az intelligens, érintésnélküli chipkártya (contactless smartcard), mely a meglévő papír alapú bérleteket váltja fel.

Az utaskiszolgáló rendszer egy fedélzeti számítógéppel vezérelt, több összetevőből álló moduláris rendszer, melynek alapelve az érintésnélküli kártyával működő utaskiszolgálás.

A comC@rd ***Mifare***® technológiájú kártyával működik (Smart Card chip). A kártya a chipen kívül egy antennát is tartalmaz. A kártyának nincs szüksége semmilyen külső tápforrásra, ezért rendkívül hosszú élettartamú.

A comC@rd rendszer kivitelezői közül a Microraab Rt. biztosítja az intelligens kártyát és a leolvasó rendszert, míg a MatávCom mobilkommunikációs rendszerén keresztül teszi lehetővé a járművek és az Alba Volán Rt. központja közötti adattovábbítást és -feldolgozást. A comC@rd

intelligens utaskiszolgáló rendszer mindennapi körülmények között zajló tesztelése során a busszal utazó móriak egyelőre csak chipkártyabérletet vásárolhatnak. Az utasoknak jogosultságuknak megfelelően lehetőségük lesz a szokásos felnőtt-, tanuló-, nyugdíjas- és ingyenes bérletek között választani, melyet az Alba Volán móri kibocsátóhelyein feltöltéssel érvényesíthetnek.

5.3.1. A comC@rd rendszer felépítése

A buszon a vezetőnél van elhelyezve a **fedélzeti számítógép** és a **GSM modul**, az első ajtónál pedig egy **kártyaolvasó**.

A fedélzeti számítógép, a comC@rd vezérlő egysége, mely adatbázisokat (menetrend, díjszabás, letiltott kártyák listája…) tartalmaz, vezérli a kártyaolvasókat, ellenőrzi a menetrend betartását, tárolja a statisztikai adatokat.

Az adatokat a comC@rd rendszer fedélzeti számítógépéből GSM DATA kommunikációval töltik le, tekintet nélkül a jármű tartózkodási helyére. A központi számítógépből a járműveken elhelyezett fedélzeti számítógépekbe szintén GSM DATA kommunikációval történik az adatátvitel (árjegyzék, menetrend, letiltott kártyák stb.)

A kártyaolvasó berendezések kommunikálnak a kártyával, így biztosítják a megfelelő bérlettípus, érvényességi idő leolvasását. A művelet eredményességét fény- és hangjelzés jelzi.

Az elektronikus bérlet (kártya) érvényessége ellenőrizhető közvetlenül a járművön kézi olvasó berendezéssel is. Ezt a berendezést közúti ellenőrök használják.

A fedélzeti számítógép lehetőséget teremt a készpénzes utazások biztosítására is, segítségével lehetővé válik a hagyományos, papír alapú menetjegy kiadás is.

A comC@rd rendszer elválaszthatatlan része a kiszolgáló szoftver, amely elemei közé tartoznak az alapadatok szerkesztésére és tárolására szolgáló programok (menetrendek, díjszabási táblázatok, gépko-

csivezetők adatbázisa stb.), a kommunikációs programok az oda-vissza irányuló adatátvitelhez, és a kimutatások készítését lehetővé tévő programok.

A közlekedési vállalat gazdaságos és versenyképes üzemeltetéséhez elengedhetetlen kimutatások készítésére van mód:

- utasok száma az egyes vonalakon, járatokon, megállókban
- bevétel kimutatása vonalanként, járatonként
- az egyes vonalak és járatok gazdaságosságának kiértékelése,
- az egyes autóbuszok és vezetőik teljesítményének az értékelése,
- az egész üzemigazgatóság gazdaságosságának elemzése objektív tényadatok alapján,
- a közlekedési helyzet modellezése és azoknak az intézkedéseknek a szimulálása, amelyek a megcélzott gazdasági eredményeket teremtik meg (járatok megszüntetése, új járatok üzembeállítása)

A comC@rd az utasok számára is igen nagy előnyöket biztosít, hiszen gyors, biztonságos, kényelmes menetdíjfizetést tesz lehetővé, az elveszett kártyát le lehet tiltani és a közlekedési vállalat magasabb szervezettsége komfort érzetet nyújt az utasnak.

Az üzemeltetőnél jelentkező előnyök a comC@rd rendszer használata során:

- komplex, valós statisztikai adatok
- feleslegessé válnak a költséges forgalmi vizsgálatok
- lehetőség a közlekedési rendszer optimalizálására (elemzések alapján a kihasználatlan járatok kivonása ill. ahol szükséges sűrítése stb.)
- alacsonyabb üzemeltetési költségek
- bérlet elektronikus formája - megvéd a visszaélésektől, nincs hamisítás
- rugalmasan, gyorsan lehet változtatni a tarifarendszert

- ellenőrök ellenőrizhetősége (az ellenőrök készüléke jegyzi a leolvasásokat, ezen belül az érvénytelen utazásokat)
- a kártya reklámhordozó (nagyon jó reklámfelület a kártya, melyet értékesíteni lehet)
- korszerű utaskiszolgálás
- felhasználóbarát kezelés
- feketén utazók számának valószínű csökkenése
- a rendszer lehetőséget biztosít a kölcsönös elszámolások megvalósítására - clearing (pontosan lehet követni az utas mely vállalat járatával utazott, így az elszámoláshoz az adatok pontosan rendelkezésre állnak)

A comC@rd rendszer moduláris kiépítése lehetővé teszi a bővítést információs táblákkal, hangosbemondóval, műholdas járműkövető rendszerrel, stb.

5.3.2. A rendszer működése

A rádiófrekvenciás elven működő érintés nélküli kártya használata nemcsak egyszerű és gyors, de olyan hosszú élettartamú is, amely több mint 100 000 leolvasást, vagy akár 25 éves használatot is lehetővé tesz. Az utas felszálláskor a kártyát a leolvasóberendezéshez közelíti, miközben az tizedmásodperc alatt ellenőrzi a bérlet érvényességét, vagy a kártyáról levonja az utazás díját.

5.3.3. A kártya használata

Az utas felszálláskor a kártyát odatartja a leolvasó berendezéshez max. 10 cm távolságra. A kártyáról ellenőrzésre kerül a bérlet érvényessége. A művelet gyorsasága - 0,2 s - jelentősen felgyorsítja az utaskiszolgálást. Az érvénytelen kártya használatát hang- és fényjelzés kíséri.

A kártyán első lépésként tárolásra kerülnek a kártyatulajdonos azonosító adatai, ezzel elkészül a kártyatulajdonosok adatbázisa is. A kártya azonosításával és az adatbázis kialakításával megakadályozható a kártyával való visszaélés. Az elveszett kártyát le lehet tiltani, és az adatbázisban kikereshető, hogy az elvesztett kártya érvényesítve volt-e. Ha igen, a kártyatulajdonos letétdíj ellenében új kártyát kap, melyre a kifizetett érvényességet át lehet vinni, így az utasnak nem kell még egyszer megváltania a bérletét.

A kártyák feltöltését a móri autóbusz-állomáson végzik, az érvényességi idő megújítását ("bérletértékesítést") az autóbusz-állomáson és az autóbuszokon is biztosítják. (A fedélzeti számítógép az olvasón keresztül beírja a kártyába az érvényességi időt.) Az utasok a személyi adatokkal feltöltött és bérletdíj kifizetése ellenében érvényesített kártyával azonnal utazhatnak.

5.3.4. Személyre szóló bérlet

A rendszer működésének további előnye a kártya „perszonalizálása” (személyre szabott kiállítása). A chipkártya megvásárlásakor felkerülnek a kártyatulajdonos azonosító adatai, miközben a közlekedési vállalat számítógépén kialakítható a kártyatulajdonosok adatbázisa is, amely több kényelmi szolgáltatás bevezetésére teremt lehetőséget.

5.3.5. A comC@rd előnyei az utasok számára

A comC@rd alkalmazása gyors fel- és leszállást, illetve készpénzkímélő, kényelmes menetdíjfizetést biztosít. Elvesztése esetén a kártyát a tulajdonos személyi azonosítója alapján le lehet tiltani; megrongálódáskor pedig új chipkártyabérletet lehet kiállítani. Nem elhanyagolható előny, hogy mivel a buszon lévő utasok száma, fel- és leszállásának helye azonnal a központi számítógépbe kerül a mobilkommunikációs rendszeren keresztül, lehetőség van az adatok alapján a tömegközlekedési járatok optimális menetrendjének és útvonalának kialakítására.

5.3.6. A comC@rd előnyei az üzemeltető számára

A tömegközlekedési vállalat az intelligens utaskiszolgáló rendszeren keresztül azonnal megkapja a járattelítettségi és más utazási szokásokat jellemző adatokat, amelyek alapján korábban elérhetetlenül pontos adatokon alapuló komplex statisztikai adatbázist alakíthat ki – ezzel feleslegessé téve a korábbi költséges közlekedési vizsgálatokat. Az így nyert statisztikai adatok alapján lehetőség van a tömegközlekedési rendszer optimalizálására (a kihasználatlan járatok kivonására, zsúfolt vonalakon a járatok sűrítésére, a járatok útvonalának jobb megválasztására).

A tömegközlekedési bérlet elektronikus formája megvéd az esetleges visszaélésektől, mivel hamisítására gyakorlatilag nincs lehetőség.

6. Chipkártyák alkalmazásának szervezési lehetőségei Budapest tömegközlekedésében

6.1. Viteldíjszabási alapok és elvárható jegyválaszték a BKSZ-ben

A BKSz-en belüli díjszabási alapok vonatkozásában - a rendszerrel szemben támasztott követelmények jobb szemléltetése érdekében - a TRANSMAN Kft 1997-ben készült tanulmányában kialakított rendszert vettem alapul, amelynek lényege a következő:

- a Budapest határán belüli terület egyetlen övezet, amelyen belül továbbra is léteznek:
  - bérletek a rendszeres utazók (pl. dolgozók, tanulók, nyugdíjasok, stb.) számára,
  - 1, 3 és 7 napos jegyek az időszakosan utazók (pl. turisták, látogatók) számára,
  - egy útra és több útra érvényes jegyek az eseti utasok számára.
- Budapest határán kívül a városhatár körül 10-12 km-es körsávokban (1,2,3...) és a főközlekedési vonalak közötti szektorhatárok (C,D,E...) által kijelölt övezetekben, szintén léteznek:
  - szövetségi bérletek a rendszeres utazók számára,
  - 1, 3 és 7 napos jegyek az időszakosan utazók számára,
  - egy útra szóló jegyek az eseti utasok számára.
- a jelenlegi rendszerhez képest itt is új elemként jelennek meg a Budapestre és környéke övezetei közötti viszonylataira érvényes egyesített bérletek és időszakos jegyek, amelyek ára feltehetőleg alacsonyabb lesz, mint a hasonló belső és külső bérletek/jegyek együttes ára,
- a teljes árú bérletek és jegyek mellett szociális szempontok figyelembevételével, továbbra is nyújtani kell különböző kedvezményeket, így:

  - a bérletek esetében: Budapesten belül a tanulóknak és a nyugdíjasoknak, a Budapest határát átlépő és a külső övezetek közötti forgalomban tanulóknak és a nyugdíjasoknak, mindkét területen az ingyenesen utazásra jogosultak számára a lehetőséget biztosítani kell (100%-os kedvezmény!)
  - a jegyek esetében: Budapesten belül és kívül az esetenként utazó tanulóknak és nyugdíjasoknak a kedvezményes viteldíjakat szintén lehetővé kell tenni.

- Az elektronikus jegyeladási és jegykezelési rendszerben természetesen a jelenlegi gyakorlattól eltérő megoldások is elképzelhetők, mint például:
  - a bérleteknek a "megvásárolt" érvényességi időszakon belüli, korlátlan számú használati lehetősége helyett, elképzelhető, hogy az elektronikus chipkártyára befizetett összeg az igénybevételtől függően fokozatosan "fogy"; ez egy új díjszabási elvet jelentene, aminek elfogadási valószínűsége kicsi,
  - az utasok bizonyos csoportjai (pl. nyugdíjasok, 65 éven felüliek) számára csak a reggeli csúcsidőszak lejárta (9 óra) után engednék meg a kedvezményes bérletek használatát.

Ezeket az új díjszabási lehetőségeket jelentő kérdéseket nem kívánom eldönteni, csupán azért vetem fel őket, mert egy új, korszerű rendszerrel elvileg ezeket is meg kell tudni oldani.

Ugyancsak nem foglalkozom "egységes" vagy "vegyes" helyközi vasúti ill. autóbusz-viteldíjszintek alkalmazásának kérdésével, tekintettel arra, hogy a két tarifa között jelenleg jelentős eltérések vannak és az "egységesítés" számos problémát vet fel. Abból indulunk ki, hogy az "egységes" viteldíjszintek rendszere bevezethető lesz, ellenkező esetben az elektronikus rendszer adottságait kihasználva, a "vegyes" rendszerre módosító javaslatot kell készíteni.

6.2. Az elektronikus jegyeladási és jegykezelési rendszer javaslata

6.2.1. Bevezetés

Az elektronikus rendszer alapjai azok a viteldíjhordozók, amelyek a különböző használói csoportok számára megfelelő formában lehetővé teszik a szolgáltatások igénybevételét. Az természetes, hogy egy elektronikus rendszer esetén a műszaki lehetőségek és az elvárások is magasabb szintűek lehetnek, mint a hagyományos rendszerek esetében. Az automatizált jegyeladási és kezelési rendszer esetén is az utazás előtti / közbeni / utáni folyamatok szem előtt tartásával a következő főbb tevékenységeket és feladatokat kell megfelelő formában ellátni:

- kártya/jegyeladás ill. feltöltés (pénztárakban, automatákban, egyéb árusító helyeken és a külső járati buszok vezetőinél),
- kártyabérlet- ill. jegykezelés az utazási dokumentumok érvényesítése céljából, utazáskezdéskor a járműveken ill. az állomásokon,
- az érvényesített kártyák (bérletek) és jegyek ellenőrzése az utazás során ellenőrök által,
- statisztikai adatgyűjtés a kártya/jegyeladás és a jegykezelés során.

Ezen folyamatok és funkciók megvalósításához különböző eszközökre van szükség, megfelelő mennyiségben és elrendezésben:

- viteldíjhordozók (chipkártya, mágnescsíkos papírjegy, nyomtatott papírjegy),
- chipkártyakiadó / feltöltő készülékek (pénztárakban, kioszkokban),
- mágnes csíkos jegykiadó és értékadó készülékek (pénztárakban, kioszkokban, egyéb árusító helyeken),
- jegyárusító automaták (állomásokon, csomópontokban, szállodákban stb.),
- érintésmentes jegykezelők (járműveken, állomásokon) a rendszeres chipkártyák (rendszeresen utazók) részére,

- érintéses jegykezelők (járműveken, állomásokon) a mágnes csíkos papírjegyek (időszakos és eseti utasok) részére,
- kártyafeltöltő/kezelő és jegykiadó készülékek (külső járati buszvezetőknél),
- fedélzeti vezérlőegység járműveken/villamos szerelvényeken,- ellenőri készülékek,
- adatkiolvasó készülék / adatátvivő modem (garázsokban, kocsiszínekben, állomásokon),
- számítógépek (garázsokban, kocsiszínekben, egyes állomásokon),
- társasági számítógépek (közlekedési társaságoknál),
- központi számítógép (a szövetségi központban).

6.2.2. Az alkalmazható viteldíjhordozók

Ebből a szempontból a ma ismert és korszerűnek számító rendszerekben a következő viteldíjhordozók jöhetnek számításba:

Érintésmentes chipkártya: a rendszeresen utazók számára bérletszerű használatra, memóriával és belső hurokantennával ellátott, bankkártya-méretű és vastagságú plasztik-kártya, amely a korábbi bérleteket váltja fel és amely a kezelő készülékhez 5-10 cm-re közelítve érintés nélkül aktiválja azt, lehetővé téve a kártya chipjében levő adatoknak az olvasását ill. adatoknak oda való visszaírását a következő tartalommal:

- kártya gyári száma
- a kártyatulajdonos azonosítója (kód, név, cím)
- a kiadó/feltöltő hely azonosítója (BKV, MÁV, Volánbusz-pénztárak stb.)
- díjosztály (teljes árú, kedvezményes)
- a kedvezmény alapja (tanuló, nyugdíjas, 65 éven felüli, társasági alkalmazott, egyéb)

- a kártya területi érvényessége (pl. Budapesten belül (BP), vagy X és Y övezetek között, vagy kombinált "egyesített" formában (BP+XY))
- [a legutolsó pénzfeltöltés időpontja]
- [a legutolsó pénzfeltöltés összege]
- [a befizetés módja (készpénz, bankkártya)]
- a kártya időbeli érvényessége (év, hó, nap)
- a kezelés időpontja/helye (viszonylat), állomás - (visszaírás; az 5 utolsó kezelés adatainak megőrzésével)

A kártya érvényességének megállapításához a szögletes zárójelben levő adatokat nem fontos a kártyán tárolni, azokat elegendő az árusító / feltöltőhely és a központi számítógépen a kártyához tartozó fileban megőrizni, ahol a kártyahasználat havi adatait tárolni lehet.

A chipkártyák jobb azonosíthatósága érdekében a különböző utas csoportok (pl. dolgozók, tanulók, nyugdíjasok, ingyenesek) számára célszerű más-más alapszínű kártyákat alkalmazni. A kártya egyik oldalán a kiadáskor a tulajdonos fényképe is megjeleníthető, a másik oldal reklámcélokat szolgálhat, ami csökkentheti a kártya eladáskori árát (a megfelelő képességű kártyák beszerzési ára, a nagy számra tekintettel, mintegy 2 USD). A chipkártyák csak megfelelő készülékkel, többnyire a személyzet által kezelt jegyárusító kioszkokban, "érintéses" formában tölthetők fel, ugyanis a pénz kezelése megkívánja a nagyobb adatátviteli biztonságot. A legújabb fejlesztések eredményeképpen léteznek már kétmódú (hibrid/duális) kártyák is, ahol a chip egy része érintéses módon "banki" biztonságot ad, és más alkalmazásoknál elektronikus pénztárcaként (pl. telefon, parkolás, töltőállomás) is használható, míg a chip másik része az érintésmentes tömegközlekedési alkalmazást szolgálja. Léteznek olyan rendszerek, amelyek már ma lehetővé teszik a duális kártyákra való későbbi áttérést is. Ez csak abban az esetben lényeges, ha a bankok a későbbiekben hajlandók a jelenlegi mágnescsíkos kártyákról a chipes kártyákra átállni.

Mágnescsíkos papírkártya: az időszakosan utazók számára (egyszeri, többszöri utazásra vagy pl. 1, 3 és 7 napos használatra) ellenállóképes (nagy koercitív erejű) mágnes-csíkkal ellátott viszonylag tartós kartonpapír-kártya, amelynek egyik oldala hőérzékeny nyomtató réteggel van ellátva és amely érintéses kezeléssel használható. A jegy az utascsoportra vonatkozó árért egy vagy több utazásegységgel, vagy ritkábban bizonyos pénzösszeggel föltöltve (pénztárban, automatában vagy külső járatú busz vezetőjénél) adható ki és amelyre az utazás megkezdésekor történő érintéses kezelés

- a kezelés helyét (viszonylat / állomás / társaság)
- a kezelés időpontját (év, hó, nap, óra, perc)
- a megfelelő számú utazásegység/pénzösszeg levonása utáni maradványt nyomtatja rá a vizuális megjelenítés céljából. Ez a fajta adattárolás csak az ISO-szabványméretű kártyáknál valósítható meg. A keskenyebb Edmonson-típusú kártyák ezt nem teszik lehetővé. A mágnescsíkos papírjegyet is - főleg az előzetesen feltöltött értékkel árusítottakat - az egyes utas csoportoknak megfelelő alapszínekkel célszerű árusítani. A kártya első oldala még kedvezőbb reklámfelület, mint a hosszabb életű chipkártya, mivel gyakrabban változtatható (egy kártya ma kb. 6 Ft körüli áron szerezhető be, mely érték a reklámbevétellel arányosan csökkenthető).

Egyedi papírjegy: esetenkénti külső/helyközi utazók számára megfelelő formátumú papírtekercsről letéphető papírjegy, amelyre a helyközi eseti utazások előtt mechanikus nyomtatással kerülnek rá a következő adatok:

- övezetközi érvényesség (X-Y övezetek között, esetleg BP-n belül is),
- a szolgáltató társaság állomás/viszonylat kódja,
- a kezelés időpontja,
- az utascsoportnak megfelelő díjosztály (teljes árú, kedvezményes),
- a viteldíj összege.

Ezek a rendszert kiegészítő papírjegyek csak "azonnali" felhasználással és átszállás megengedése nélkül alkalmazhatók, miközben az állomáson vagy a külső járati buszvezetőnél vásárolt jegyre vonatkozó adatok bekerülnek az elárusító készülék memóriájába, majd a központi számítógépes rendszerbe. A fővároson belül csupán a külső kerületekben közlekedő autóbusz-trolibusz- és villamosjáratokon célszerű a papírjegyek bevezetését megfontolni, ahol az egyszeri vagy többszöri utazásra szolgáló mágnescsíkos jegyekhez való hozzáférés kellően nem oldható meg.

A papírjegyek kiadására alkalmas készülékek a Volánbusz Rt-nél már ma is üzemelnek, amelyek azonban bővítendők/lecserélendők lesznek a chipkártya feltöltését/kezelését, valamint a mágnescsíkos papírjegyeket is kezelő többfunkciós készülékekre.

6.3. A kártya- és jegykezelők használata

A jegykezelés módja a szolgáltatást nyújtó járművek fajtájától függően különböző:

- a gyorsvasúti és nagyvasúti vonalak állomásain és
- a többi eszköz (autóbusz, trolibusz, villamos) járművein.

Az új rendszerben abból kell kiindulni, hogy minden egyes járműre szállásnál az utazási dokumentumokat (bérletkártyák/jegyek) kezeltetni kell.

Az utazási dokumentumok érvényességének megállapításához ill. a díjlerováshoz és a statisztikai adatok gyűjtéséhez a kártya- / jegykezelők következő típusaira van szükség:

- Érintésmentes kezelést lehetővé tevő készülékek, amelyek a személyre és területre érvényes és meghatározott időszakra vonatkozó díjjal feltöltött chipkártyák kezelésére szolgálnak. Az ilyen fajta bérletkártyákkal rendelkezők az autóbuszra, villamosra, trolibuszra célszerűen a hátsó ajtóknál szállhatnak fel és kezelhetik bérletüket minden felszállás során. A kezelőkészülék csupán az utascsoporthoz való

tartozás (pld. dolgozó, tanuló, nyugdíjas stb.), az érvényességi terület és időszak adatait vizsgálva adja a megfelelő jelzést ill. írja vissza a kártyára az érvényes kezelés időpontját a szolgáltató társaság azonosítóját, a viszonylat/állomás kódját.

- Érintéses kezelést lehetővé tevő készülékek, amelyek a mágnescsíkos papírjegyek "érvénytelenítésére" vagy róluk "érték lekönyvelésére" szolgálnak.

A készülékeknek két változata lehetséges:

- övezetek megkülönböztetése nélküli készülékek (Budapesten belül közlekedő járműveken - mivel egész Budapest egyetlen övezet - elvileg elegendőek az ilyen berendezések)
- több övezet megkülönböztetésére alkalmas készülékek; ilyen készülékekre a városhatáron túlra ill. kívül közlekedő járműveken ill. vasútvonalak állomásain lenne szükség, akkor, ha a többövezetes, előreváltható mágnes-csíkos kártyák, többegységes jegyek formájában, lineáris viteldíjrendszert vezetnénk be. Ebben az esetben meg kell oldani a jegykezelőben az övezetváltást, ami történhet a vezető által kézi beavatkozással, de automatikusan is út menti jeladók felszerelésével vagy a GPS-rendszer alkalmazásával is.

A járművek első ajtajánál "kétmódú", mind az érintésmentes, mind az érintéses kártyák kezelését lehetővé tevő egybeépített készülékek célszerűek (ez az ártól függ), hogy a jó szándékú utasoknak a felszállásnál/kezelésnél nagyobb szabadságfokuk legyen. A hátsó ajtóknál elegendő a "bérletkártyás" utasok számára az érintésmentes kezelést lehetővé tevő készülékeket felszerelni. A városhatárt átlépő buszvonalak járművein a kezelő készülékeken az övezet-megadást lehetővé tenni. Mind az érintésmentes, mind az érintéses kezelést szolgáló készüléken célszerűen hang- és fényjelzéssel jelezni az "érvényes" (pl. zöld: teljes árú, kék: kedvezményes) és "érvénytelen" (piros) állapotot.

- A vezetőnél levő kezelőkészüléknek célszerűen a következő hármas funkciót kell kielégítenie:
  - a chipkártya feltöltését/kezelését,

- a mágnescsíkos papírjegy eladását/kezelését,
- egyedi papírjegyek nyomtatását/eladását.

Minden, a készülékkel végzett művelet adatait a fedélzeti irányító egység memóriája tárolja, amely lehet maga a vezetőnél levő többfunkciós készülékben is. Az irányító egység feladata a kezelőkészülékek felügyelete (viteldíjtábla-tárolás, óra-összehangolás, adatátvitel, hibajelzés stb.).

Az állomásokon történő jegykezelés a metró/földalatti bejáratánál, a HÉV- és MÁV-peronokon elhelyezett "kétmódú" készülékekkel a vonatindulás előtt hasonló módon történik, mint a járműveken levő készülékekkel.

E célból a készülékeknek kell, hogy legyen külső, időjárás- és rongálásálló változata is, amelyeket esetenként fedetlen vasúti peronokon helyeznek el (elektromos áram-kapcsolatra ilyen esetekben is szükség van, a hiányzó telefonvonal a készülékek acélból készülő védő dobozában elhelyezkedő kiolvasható memóriával pótolható).

A városhatárt átlépő vasúti és HÉV-vonalak állomásain elhelyezendő készülékeknek az övezeti kezelést is lehetővé kell tenniük (pl. több egységes mágnescsíkos jegy esetében). A készülékek a kártyákra/jegyekre az időpont mellett az állomás azonosító kódját is rögzítik.

Az állomási pénztári kártya / jegyeladó-helyek, amelyeknek a kiadó/érvényesítő készülékei megegyezhetnek a buszvezetőknél elhelyezett készülékekkel, ha vezetékesen összekapcsolhatók a peronon elhelyezett jegykezelőkkel, akkor a jegyeladó készülékek a peronon elhelyezett kezelőcsoport irányítását is elláthatják.

A kisebb állomásokon, ahol nincs lehetőség a jegyárusító hely és a kihelyezett készülékek közötti kapcsolat kiépítésére, célszerű valamelyik kezelőkészülékre bízni az irányítást. Az adatokat a kiolvasható/cserélhető memória gyűjti, amely lehetőséget ad arra is, hogy programozással pótoljuk a hiányzó on-line kapcsolatot (pl. a viteldíjváltozás programozása adott időponttól kezdve).

Az egyes társaság által alkalmazott ellenőrök a hárommódú ellenőri készülékekkel ellenőrzik az utasok jegyeinek érvényességét.

E készülékek láthatóvá teszik a kártyák érvényességét is, ami akkor áll fenn, ha a felszállás után kezelték. Az ellenőrzés során adódó rendellenes jelenségeket az ellenőr a készülékben a kártya/jegytípus kódján és a jelenség okán (pl. lejárt bérletkártya) felül a vonal / viszonylat / jármű azonosítását is rögzíti. Az ellenőri készülék, amely papír-pótjegy kiadására is alkalmas, a szolgálat lejárta után összekapcsolandó valamely jegyárusító hely, vagy garázs/kocsiszín számítógépével, vagy a társaság központi számítógépével. A dokumentum nélkül utazók ill. az át nem ruházható kártyák illegális használata ill. jogosulatlan kedvezmény igénybevétele esetén a szankcionálás módja és mértéke a későbbiekben lenne tisztázandó.

Az elektronikus rendszer egyik előnye a vásárlásnál/feltöltésnél előre megadott érvényességű kártyák egyszerű, érintésmentes és gyors kezelése, vagy kezelése során, az utas által meghatározandó viszonylati érvényesség előállítása és a díjlerovás. A szükséges utas- és bevételstatisztikai adatok gyűjtése érdekében elengedhetetlen, hogy az újszerű bérleteket és jegyeket minden utas (az egyébként ingyenes utazásra jogosult is) minden egyes felszállásnál kezelje. Megfelelő felvilágosító és tudatformáló kampány során rá kell világítani arra, hogy az utastársak általi "megfigyelő ellenőrzés" - amit a hang- és fényjelzés is segít - növelheti a fizetési hajlandóságot, és ezáltal javulhat a költségfedezeti arány, ami csökkentheti a viteldíjak emelésének mértékét.

6.4. Kártyaárusítás/feltöltés és jegyeladás

Az elektronikus rendszerben a viteldíjhordozók árusítása ill. értékkel való feltöltése is megfelelő technikát igényel. Az utasok bérletkártya- és jegyigénye a következő helyeken és módokon elégítendő ki:

- jegypénztárakban, árusító kioszkokban, ahol szakszemélyzet által kezelt készülékkel kerülhet sor a következőkre:

- bérlet chipkártyák eladása (személyi azonosító, érvényességi terület, kedvezmény jogcíme stb. beírásával),
- bérlet chipkártyák fel- és újratöltésével a területi érvényességnek, utascsoportoknak megfelelő egy-, vagy többhavi díj befizetése ellenében egy- vagy többhavi "használhatóságot" lehet megváltani; az utazásra való jogosultság minden felszálláskor a kezeléssel szerezhető meg (fel kell készülni arra, hogy ez vitákat fog kiváltani),
- mágnescsíkos papírjegyek árusítása; gyárilag előre egy, vagy több egységgel feltöltött kártyák a Budapesten belüli utazások, ill. a külső eseti utazások előreváltható jegytípusa (lineáris övezeti viteldíjrendszer esetén).

- kártya- és jegyárusító automaták; különböző műszaki felkészültségű és árfekvésű automaták lehetségesek a következő kívánatos funkciókkal:
  - értékkel/egységekkel előre feltöltött mágnes-csíkos papírjegyek árusítására; érmék, bankjegyek ill. bankkártyák elfogadásával,
  - chipkártyák feltöltésére, hasonlóan három módon (a későbbiekben elképzelhető az ilyen automaták közvetlen banki kapcsolata is; ebben az esetben a duális chipkártyák alkalmazásának is megnő az esélye),
- a járművezetőknél levő többfunkciós készülékek is alkalmasak - mint a korábbi pontban láttuk - a chipkártyák feltöltésére, mágnescsíkos papírjegyek árusítására és papírjegyek kiadására,
- egyéb jegyárusító helyek; az értékkel feltöltött mágnescsíkos jegyek a szolgáltató társaságokon kívül, más kereskedelmi egységekben jutalékos formában, vagy a kártya reklámfelülete fejében - szigorú napi elszámolás mellett - szintén árusíthatók.

A vidéki ingyenes utazásra jogosult személyek - ha a BKSz területére kívülről érkeznek - az érkezési állomásokon (esetleg annak a jár-

műnek a vezetőjénél, amelyikre felszállnak) érték nélküli mágnescsíkos-papírjegyet kaphatnának a felszálláskori jegykezeléshez.

6.5. Az adatkiolvasás és -gyűjtés rendszere

A szövetségi rendszerben történő napi kártya- és jegyeladásokról, valamint a kártya/jegyhasználatról képződő utazási adatok az esti üzemzárás utáni időben különböző módon gyűjthetők össze.

A jegyárusítási adatok a szövetségi területről, az egyes társaságok hatókörének megfelelően, a különböző típusú helyekről, a jegyek típusának, árának megfelelő csoportosításban, a társasági számítóközpontba továbbítandók a következő lehetséges módokon:

- a kártya/jegyárusító pénztárak, kioszkok irányító egységeiből zárás után telefonvonalon,
- a jegyárusító automatákból a memória adatait mikrohullámú telefon-kapcsolattal, vagy a kártyával való feltöltésnél kiolvasással gyűjthetők be az adatok (utóbbi esetben a napi gyűjtési ritmusról esetleg le kell mondani),
- a járművezetőknél elhelyezett árusító/kezelő készülékek eladási adatait a garázsokban/kocsiszínekben a jegykezelő adatokkal együtt olvassák ki,
- az egyéb árusító helyekről a nyitvatartási idő után /telefonon/faxon továbbíthatók az eladási adatok a számítóközpontba.
- A jegykezelési adatok is, az egyes társaságok eltérő közlekedési eszközeinek megfelelően, eltérő módon olvashatók ki, továbbíthatók és gyűjthetők össze:
- autóbuszok, trolik és villamosok fedélzeti irányító egységéből üzemzárás után a garázsokban, kocsiszínekben a infravörös modemmel, ultrarövid hullámú telefon-kapcsolattal, vagy kiolvasóval (retriver) vihetők át a garázs / kocsiszín erre a célra fenntartott számítógépébe,

majd onnan a társaság központi gépébe, végül a BKSz központi gépébe;

- a metró-, kisföldalatti-, HÉV- és MÁV-állomások jegykezelési és utasadatai telefonvonalon, vagy a kisebb állomásokról memóriakiolvasással juthatnak az igazgatósági számítógépbe, onnan a társasági központi gépbe, majd végül a BKSZ-központ gépébe.

A különböző módozatú adatátvitelek megfelelő standardizált, formátumban történjenek.

A chipkártyák utazási adataira tulajdonképpen kezelési eseményenként van szükség, míg a jegyekről elegendőek a helyenként/viszonylatonként, utas csoportonként, jegyfajtánként, övezetenként és óránként csoportosított adatok.

6.6. Az adatáramlást és feldolgozást szolgáló számítógépes rendszer

A szövetségi jegyeladási és jegykezelési rendszert ill. a megfelelő adatáramlást egy hierarchikusan kialakított számítógépes hálózat működteti, amelynek első alapelemei a jegyárusító/feltöltő, valamint a jegykezelőket irányító egységek, amelyek fölött a következő számítógépes szintek találhatók:

- garázsokban/kocsiszínekben ill. állomásokon működő gépek,
- üzemeltetők, társasági központi gépek,
- BKSz-központi gép.

A különböző szinten lévő gépeknek megfelelő módon hálózatba kapcsolva kell működniük. A hálózati kapcsolatok vagy önállóan kiépített vonalakon, vagy bérelt telefon-vonalakon keresztül valósulhatnak meg.

Itt kell szólnunk a kártyahamisítás és az eszközmanipuláció elleni intézkedések fontosságáról, ugyanis az egyes rendszerműveletek mögött mindenütt pénzfolyamatok húzódnak meg. Ezért óvatossági és biztonsági intézkedésekre van szükség a díjhordozók, az eszközök és a számító-

gépes hálózat kialakítása vonatkozásában, a különböző jogosultságok helyes és szigorú meghatározásával is.

A garázsokban/kocsiszínekben levő számítógépek feladatai a következők:

- kapcsolat létesítése az üzemeltetői központi géppel,
- kapcsolat létesítése a garázsban levő járművek irányító egységeivel (adatkiolvasás, adatbetöltés: pl. új viteldíjak),
- kapcsolat létesítése egyes jegyárusító helyekkel és ellenőrökkel, ha azok nem a központi géppel állnak összeköttetésben,
- helyi elemzések.

A garázs- / kocsiszínbeli körülményekre tekintettel célszerű két "ipari" PC-t alkalmazni, amelyek közül az egyik a kapcsolattartást, a másik az elemzéseket és egyéb számításokat végzi.

Az állomásokon levő számítógépek feladata hasonló, mint az előzőekben, azzal a különbséggel, hogy egy-egy metró / HÉV / vasútvonalon az egyik állomáson telepítendő számítógép veszi át a vonal többi állomásáról is az adatokat és továbbítja azokat a vállalati központi számítógépbe.

Az üzemeltetői központi számítógépek feladatai:

- kapcsolat létesítése és adattovábbítás a BKSz központi számítógépének
- kapcsolattartás az üzemeltető garázsbeli / kocsiszínbeli számítógépeivel, valamint a jegyárusító helyek számítógépeivel a következő területeken:
  - a különböző azonosítók karbantartása,
  - a viteldíjtáblázatok karbantartása, a jegykezelő készülékekben a fedélzeti irányító egységen keresztül, valamint az árusító/feltöltő készülékekben,
  - a készülékek fenntartó/karbantartó személyzetének jogosultsági szabályozása,

- jegyeladási adatok fogadása/figyelése,
- a kártyahasználati adatok fogadása/figyelése,
- a különböző készülékek hibabejelentéseinek fogadása,
- különböző készülékek naptárainak és az óráinak szinkronizálása,
- a bevételi és utaskezelési adatok feldolgozásának ellenőrzése az üzemi napon belül,
- adatok szolgáltatása a kártya/jegy-eladásokról és -fogyásokról, valamint feltöltésekről, a bevételi adatok ellenőrzéséhez, kártyák/jegyek beszerzéséhez,
- a napi, heti és havi jelentések készítése az utasszámokról a kártya/jegyeladásokról és feltöltésekről,
- a napi, heti és havi jelentések készítése a készülékek hibáiról, a javítási/karbantartási tevékenységekről és a kieső időkről,
- esetenkénti forgalmi és bevételi vizsgálatok.

A gyűjtött adatok, amelyek a vezetői információs rendszernek is meghatározó alapjai, a következő típusú elemzéseket tegyék lehetővé:

- időpont (év, hó, nap, óra) szerinti összehasonlítások,
- járművek szerint (üzemben/üzemen kívül, utasszámok és bevételek jegytípusonként, övezettípusonként)
- vonalanként/viszonylatonként a járművek száma, menetek száma,
- utasok száma, bevétel nagysága időszakonként,
- érvénytelen kezelések, ellenőrök által feltárt bliccelések,
- megállóhelyenként ahol a megállóhely azonosítható pl. metró, HÉV, MÁV (az utasok száma jegytípusonként, időszakonként stb.)
- vezetőnként (szolgálat kezdete/vége, eladások, műveletek száma stb.)
- jegyárusító helyenként (nyitvatartási idők, eladott kártyák/jegyek és bevételek jegytípusonként),

- általános összegezés (szolgálatban levő járművek száma, napi össz-utasszám és össz-jegyeladás jegytípusonként stb.).

A BKSz központi számítógépe a szolgáltató társaságoktól, az ottani központi számítógépekből minden adatot megkap a vezetői információs rendszer részére, különböző elemzési és tervezési feladatok elvégezhetősége céljából. Ebből a szempontból a BKSz egyik legfontosabb feladata a bevételek felosztása az egyes szolgáltató társaságok között. Tekintettel arra, hogy a szövetségben a kártya/jegyvásárlás ill. feltöltés és a kártya/jegyhasználat társaságilag elválhat egymástól, szükség van az igénybevétellel arányos felosztásra, amely a körvonalazott korszerű rendszer által válik megbízható módon lehetségessé.

A bevételeket kéthetente/havonta, a különböző területeken (pl. Budapesten belül, Budapesten kívül) az eltérő igénybevételi feltételeknek és a jegy/bérlet fajtáknak megfelelően, különböző "bevételi kosarakba" célszerű felosztani. Így legalább négy fő bevételi kosártípus adódik, további "alkosár"-lehetőségekkel (pl. bérlet és jegyfajták szerint, szektorok szerint stb.):

- A Budapest határán belüli bérletkártyás utasok bevételei
- A Budapest határán belüli jegyes utasok bevételei
- A Budapest határát átlépő ill. külső bérletkártyás utasok bevételei
- A Budapest határát átlépő ill. külső jegyes utasok bevételei

Lényeges, hogy ily módon a külső bevételek nem keverednek a Budapesten belül "megtermelt" bevételekkel és az egész felosztás viszonylag megalapozottan végrehajthatóvá válik, ami egyértelműen az elektronikus jegyeladási és kezelési rendszernek köszönhető.

6.7. A rendszer bevezetésének eszköz- és forrásigénye

A Budapesti Közlekedési Szövetség területi hatóköre és utas mennyisége, a szolgáltató társaságok részes járműállományának nagy-

sága, a hálózat kiterjedése, a megállók és átszállóhelyek száma meghatározza a szükséges eszközök mennyiségét.

A felvázolt elektronikus rendszer műszaki tartalmi követelményei határozzák meg az eszközök képességeit és árait.

Ma a piacon találhatók olyan szakmai rendszergazdák (integrátorok), akik az igényekhez igazodó "kulcsrakész" rendszerek kiépítését és szállítását vállalják. Az erre vonatkozó többirányú információgyűjtés alapján az egyes rendszerelemek árai előzetesen becsülhetők.

A hasonló funkciójú berendezések/eszközök között jelentősebb árbeli különbségek lehetnek. A műszaki követelményekből fakadó színvonal, illetve a működtetési körülményekből fakadó elvárások (pl. időjárás-állóság, rongálás-védelem) jelentősen befolyásolják az árakat. Igen lényeges tudni, hogy pályáztatás keretében, versenyviszonyok között néha jelentősen kedvezőbb árak is elérhetők.

Ezek alapján és egyfajta takarékossági szűkítés alapján, előzetesen mintegy 16-18 Mrd -Ft-ra tehető az itt felvázolt elektronikus jegyeladási és jegykezelő rendszer igénye (a későbbiekben az eszközökkel szembeni igények pontosítandók és több árajánlati változat is készítendő).

További mintegy 1,0-1,2 Mrd Ft-ra tehető a megadott összegből a chipkártyák egyszeri ill. a mágnes-csíkos kártyák egyéves költségigénye, amit részben az utasok, részben a reklámozó cégek viselhetnének. A rendszer bevezetése esetén a szükséges szervizhátteret további pályáztatással, vállalkozási alapon célszerű megteremteni. A betanítás és bevezetés költségei néhány százmillió Ft-ot érhetnek el.

Ennek az első látásra jelentős összegnek az előteremtéséhez, a költségvetési források és hitelfelvételi lehetőségek mellett, meg kell fontolni a lízing lehetőségét is. Léteznek már a szakterületen működő olyan cégek, amelyek a beruházási forrásteremtés ezen formájában közreműködési készséget mutatnak. A rendszer kialakítása mint regionális projekt jó eséllyel pályázhat uniós támogatásra is.

6.8. A rendszer bevezetésének előnyei

Az elektronikus jegyeladási- és kezelési rendszer a Budapesti Közlekedési Szövetség létrehozása esetén olyan megoldás, amely számos területen kedvező a hatása.

A korábbi TRANSMAN-vizsgálat alapján született viszonylag kis forrásigényű (mintegy 3 Mrd Ft) egyszerű, többszelvényű papírjegyekre és hagyományos bérletszelvényekre, valamint mechanikus nyomtatós jegykezelőkre alapított rendszernek gyenge pontja az utas- és bevételi statisztika hiányos volta. Ez csak időszakos, mintavételes, a szolgáltató társaságra és a jegyfajta használatára vonatkozó utas felmérésekkel lenne részlegesen pótolható. Az elektronikus rendszer - mint az a korábbiakból látható - mindezeket az igényeket kielégíti, ami a magasabb árat is okozza.

Az új rendszer minden érintettől együttműködést és felkészülést kíván. Az utasoktól még annak belátását is, hogy a megfelelő rend szerint végzendő bérlet/jegyérvényesítés az ő érdeküket szolgálja, mert ezáltal csökkenthetővé válik a bliccelők száma, az így elérhető többletbevétel a díjemeléseket mérsékelheti. Az átállás fokozatosan, esetleg 3-4 hónapon át a kétféle rendszer egyidejű meglétével történhetne (pl. az új jegykezelők felszerelése a metróvonalakon kezdődhetne és először csupán a bérletesekre alkalmazva; majd fokozatosan Budapesten a többi eszközre, végül a többi szolgáltató külső vonalaira is kiterjesztve és a mágnescsíkos papírkártyákat is bevonva).

Az új rendszernek a technológiaváltásból származó hatásait, a különböző érintett csoportok szempontjából, a következőkben foglalhatjuk össze (miközben magának a szövetségnek a bevezetéséből származó előnyöket most nem taglaljuk):

- Az utasoknál
    - a technikai újdonság - a kártya mintegy 5-6 évre szóló megvásárlása következtében keletkező mintegy 500 Ft-os kiadás ellenére - kedvező fogadtatásra találhat, amelynek következtében,

- egyszerűbbé válhat a bérletkártyához/jegyhez való hozzájutás,
- a kötelező jegykezelés révén átláthatóbbá válnak a jogosulatlanul utazók.

- A szolgáltató társaságok számára
  - az új technológia egy lényegesen magasabb szintű munkakultúra lehetőségét hozza, amely a társasági működés egészére kedvező lehet,
  - az utazási igények és bevételek ismeretével automatikusan feleslegessé válik az egyébként szükséges utas felmérések nagy része,
  - a viteldíjemelések olcsóbban, egyszerűbben, akár csúszó módon is megvalósíthatók,
  - az információs rendszer által jelentős létszám-megtakarítás érhető el
  - megteremti a lehetőséget a vezetői információs rendszer javításának, így a szolgáltatások racionálisabb megszervezésének és a hatékonyság növelésének,
  - a bliccelések száma és a bliccelők általi bevételkiesés csökkenthető,
  - a készpénz részarányának csökkenése révén a pénzkezelés biztonságosabbá és követhetőbbé válik
  - a bevételek igénybevétel-arányos felosztásával növeli a gazdálkodás biztonságát, aminek "veszélyeztetése" ma még a félelmek fő forrása.

- Az ellátásért felelős testületek számára
  - a lakosság technikai környezetének jelentős fejlődése a közhangulatban és az élet más területein is kedvező lehet,
  - a szolgáltatások racionálisabb szervezésének lehetősége üzemköltség- és térítéscsökkenést tesz lehetővé,

  - a személyközlekedésben az intermodális kapcsolatok egyszerűbbé válnak, ami által a közösségi közlekedés fokozottabb igénybevételére támaszkodó közlekedéspolitika (pl. P+R rendszerrel kombinálva) könnyebben érvényesíthető,
  - a rendszer újdonsága turisztikai vonzerőt is gyakorolhat; kibővítheti a bankkártyák használati körét és akár többfunkciós citykártya bevezetését is lehetővé teszi.
- A szövetségi társaság számára
  - a rendszer által létrejövő adatrendszer a BKSz vezetői információs rendszernek a fő vázát alkotja, amely lehetővé teszi,
  - a szolgáltatásoknak az utas igényekhez való jobb hozzáigazítását,
  - flexibilisebb viteldíjrendszer kialakítását,
  - a viteldíjak egyszerű változtatását,
  - a szövetségi közös bevételek megalapozottabb, igazságosabb felosztását.

7. Összefoglalás

Összességében megállapítható, hogy a javasolt elektronikus jegyeladási és jegykezelési rendszer magas műszaki színvonalat képvisel, amely emeli a műszaki és gazdálkodási kultúrát a fővárosban és környékén, valamint a szolgáltató társaságoknál. Emellett jelentős változást és javulást hozhat az utasok kiszolgálásában és kezelésében, továbbá a naprakész vezetői információkkal (melyet a rendszer folyamatosan biztosít) a szövetségi szolgáltatások jobb összehangolásában, hatékonyabb működtetésében.

Előzetesen is valószínűsíthető, hogy a feszesebb szervezést lehetővé tevő rendszer által az éves üzemköltségekben ill. a költségtérítési igényekben számottevő megtakarítások érhetők el. Több százmillió forintra tehető az a megtakarítás, amit a bevételfelosztáshoz szükséges mintavételes forgalomfelvételek elmaradása jelent, az adatok megbízhatósága közti különbségről nem is szólva. A bevételnek a bliccelés visszaszorításával elérhető növelése még ennél is nagyobb mértékű lehet.

Végezetül arra is fel kell hívni a figyelmet, hogy egy ilyen technológiaváltás jelentős felkészülést kíván, nem csupán a beszállítóktól, hanem a rendszert a későbbiekben működtető társaságoktól is, amelyek megfelelő átképzési lehetőségek szervezésével tehetik a rendszer bevezetésével együtt járó "emelt szintű" munkakörnyezetet a munkatársi gárda számára vonzóvá.

8. Irodalomjegyzék

- ***Erdős Pál - Surányi János:*** Válogatott fejezetek a számelméletből, Tankönyvkiadó Vállalat, Budapest 1960
- ***MONIGL J. - UJHELYI Z. - NAGY E***. et.al.: A Budapesti Közlekedési Szövetség (BKSz) létrehozását megalapozó vizsgálatok - Zárójelentés Megbízó: BKSz Előkészítő Iroda (TRANSMAN-jelentés 1996.)
- ***MONIGL J. - UJHELYI Z. - KOREN T***. et.al.: A Budapesti Közlekedési Szövetség (BKSz) megalapozó vizsgálata (Városi Közlekedés, XXXVII. évf. 1997/4. p. 209-229).
- ***MONIGL J. - BERKI ZS. - MOLNÁR B.***: Javaslat a Budapesti Közlekedési Szövetség elektronikus jegyeladási és -kezelési rendszerére Megbízó: BKSz Előkészítő Iroda (TRANSMAN-jelentés 1999. április)
- ***BUSCOM:*** Proximity card in Helsinki
- ***MicroRaab:*** EM CARD – tömegközlekedési kártya
- ***Intelligens Kártya Fórum:*** Évkönyv: Naumann János Számítógéptudományi Társaság, Budapest 2000
- ***Europay, MasterCard and Visa (EMV):*** Integrated Circuit Card Specification for Payment Systems, 1998
- ***CompuWorx Rt.:*** CompuWorx Acces Control Reader adatkommunikáció specifikáció, Budaörs 2001
- ***Nemzeti Bankok Szövetsége:*** Definíciók, Basel, 2001

9. Webtár

- ***www.diakbonusz.hu***
- ***www.compuworx.hu***
- ***www.gemplus.com***
- ***www.buscom.fi***
- ***www.bkv.hu***
- ***www.microraab.hu***
- ***www.emtest.sk***
- ***www.ti.com***
- ***www.rsa.com***
- ***www.hirek.com***
- ***www.matavcom.hu***
- ***www.transman.hu***
- ***www.alfagas.hu***

10. Ábra- és táblázatjegyzék

10.1. Ábrajegyzék:

10.2. Táblázatjegyzék:

11. Mellékletek

I. számú melléklet

Fermat tétele

A tétel alapvető jelentőségű a nyilvános kulcsú titkosítások számára.

A hivatkozott ***VI.*** és ***VII.*** tételeket, amelyeket a bizonyítás felhasznál itt nem bizonyítjuk, csak a kimondjuk.

Tétel:

Ha ***p*** prímszám, és nem osztója egy ***a*** egésznek, akkor $a^{p-1}-1$ osztható ***p***-vel.

Bizonyítás:

A bizonyítás abból fog állni, hogy megvizsgáljuk sorra az ***a, 2a, ..., (p-1)a*** számok maradékát ***p***-vel való osztásnál: legyen

$$ka=pq_k+r_k,\ 0<=r_k<p\ (k=1,2,...,p-1).$$

Egyik r_k sem lehet nulla, mert ***k*** nem osztható ***p***-vel, s így relatív prím hozzá, ***a***-ra feltétel szerint ugyanaz áll, s így a ***VII. tétel*** szerint ***ka*** is relatív prím ***p***-hez.

Az összes maradékok különböznek egymástól. Legyen ugyanis $k_1>k_2$ és vonjuk ki a k_1-edik egyenletből a k_2-ediket:

$$(k_1-k_2)a=p(q_{k1}-q_{k2})+(r_{k1}-r_{k2}).$$

Itt a (k_1-k_2) szám p-nél kisebb pozitív egész, és így a bal oldal az előbbiekhez hasonló okoskodás szerint nem osztható p-vel, tehát $r_{k1}-r_{k2}$ sem lehet 0.

Az $r_1,r_2,...,r_{p-1}$ számok tehát az $1,2,...,p-1$ számok közül kerülnek ki, és nincs köztük két egyenlő. Ebből viszont az következik, hogy valamilyen sorrendben az $1,2,...,p-1$ számok mindegyike előfordul közöttük. Szorozzuk össze most az egyenlőségeinket és vizsgáljuk meg a jobb oldalt. Itt, ha tagonként beszorzunk, az $r_1\ r_2\ ...\ r_{p-1}$ tagon kívül csupa p-vel osztható tag keletkezik, e tag pedig utolsó megállapításunk szerint $(p-1)!$-sal egyenlő. Ilyen alakú egyenlőséget kapunk tehát:

$$(p-1)!\ a^{p-1}=pQ+(p-1)!$$

ahol Q valamilyen egész szám. Ezt úgy is mondhatjuk, hogy

$$(p-1)!\ (a^{p-1}-1)$$

osztható p-vel. $(p-1)!$ azonban relatív prím p-hez a ***VII. tétel*** értelmében, mert mindegyik tényezője relatív prím hozzá. Így a ***VI. tétel*** szerint $a^{p-1}-1$ osztható p-vel, és ezt akartuk bizonyítani.

II. számú melléklet

EM 216 fedélzeti számítógép műszaki paraméterei

Az EM 216 fedélzeti számítógép az EM TEST városi tömegközlekedésben használt kiszolgáló rendszer vezérlő egysége, amelyhez saját kiszolgáló berendezések csatlakoznak: az érintésnélküli chipkártyaolvasó terminál hőnyomtató nélkül (EM 316 RD), vagy hőnyomtatóval (EM 316 RDP), és az EM 306 CM pénzbedobó jegykiadó.

A számítógép kezeli a menetrendet, beleszámítva a menetleveleket és turnusokat, árjegyzékeket, a vezetők adatbázisát. Ezek a bemeneti alapadatok az utasok kiszolgálására szolgálnak.

Az EM 216 számítógép lehetővé teszi a készpénzfizetést a vezetőnél, az EM 316 RDP nyomtató segítségével kiadható a menetjegy. Természetesen ezek a készpénzfizetések szigorúan regisztrálva vannak.

A bemeneti és üzemi adatok átvitele az EM 216 fedélzeti számítógépéből adatgyűjtő PC-re automatikusan, optikai úton történik.

A számítógép vezérlő elemként szolgálhat a vezérlő- és információs rendszerek egyéb berendezéseinek irányítására (tájékoztató táblák, digitális kijelzők, GPS). Ezt az RS 485-ös csatlakozó teszi lehetővé.

7. Ábra EM 216 fedélzeti számítógép

Paraméter	Adat
Névleges tápfeszültség	*24 V*
Üzemi tápfeszültség	*18 – 36 V*
Tápáram 20 °C-nál	*400 mA*
Tárolási hőmérséklet	*- 30 °C-tól 70 °C-ig*
Relatív páratartalom	*5 – 95 %*
Méretek (sz x m x v)	*200 x 135 x 50 mm*
Fedél	*IP 40*
Kijelző típusa	*alfanumerikus, LED*
Kijelző mérete	*4 x 20 karakter*
RAM	*512 kB*
FLASH	*512 kB*

3. Táblázat EM 216 fedélzeti számítógép műszaki paraméterei

III. számú melléklet

EM 316 RD chipkártyaolvasó és kijelző terminál műszaki paraméterei

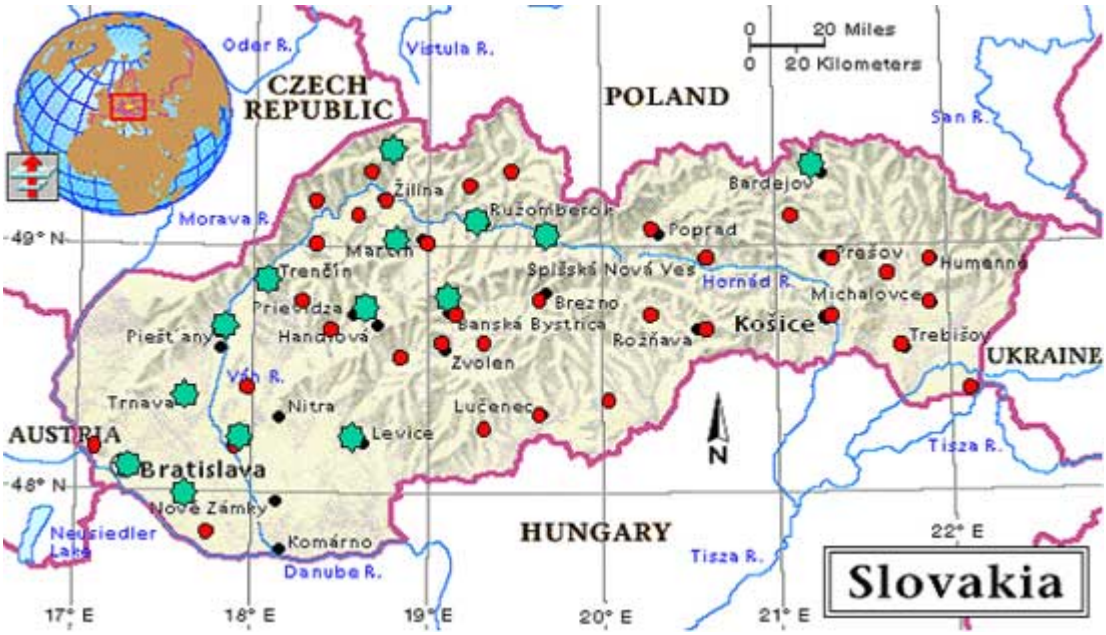
A kártyolvasó a Mifare rendszerű érintésnélküli chipkártyákkal kommunikál 10 cm távolságból. A berendezés elsősorban a tömegközlekedésben az utasok készpénznélküli kiszolgálására szolgál. A terminál előlapján elhelyezett kezelő panel a menetdíj kiválasztására szolgál. A kezelő panel a megrendelő igényei szerint készül el. A berendezés kétsoros LCD kijelző egységgel és LED kijelzővel rendelkezik. Jelzi a kártyával végrehajtott tranzakció helyességét, tájékoztatja az utast a tranzakció végrehajtásáról és a kártyán lévő egyenlegről. A terminál kezelőlapja egyidejűleg a pénzautomata vezérlésére, a menetdíj árának kiválasztására is szolgálhat. Ebben az esetben a kijelző egységen megjelenik a bedobott pénz értéke.

8. Ábra EM 316 RD terminál

Paraméter	Adat
Névleges tápfeszültség	*24 V*
Üzemi tápfeszültség	*18 – 36 V*
Tápáram 20 °C-nál	*400 mA*
Tárolási hőmérséklet	*- 30 °C-tól 70 °C-ig*
Relatív páratartalom	*5 – 95 %*
Méretek (sz x m x v)	*130 x 270 x 50 mm*
Fedél	*IP 40*
Kijelző típusa	*alfanumerikus, LED*
Kijelző mérete	*2 x 16 karakter*
RAM	*512 kB*
FLASH	*512 kB*
Kommunikációs távolság	*10 cm*

4. Táblázat EM 316 RD terminál műszaki paraméterei

IV. számú melléklet



Az EM TEST rendszer szlovák tagjai

- Szoftver és elektronikus eszközök
- Érintésmentes kártya project

9. Ábra EM TEST Szlovákia

Banská Bystrica, Bánovce nad Bebravou, Bratislava, Brezno, Dunajská Streda, Detva, Dolný Kubín, Galanta, Hlohovec, Humenné, Ilava, Košice, Kráľovská Chlmec, Krásno nad Kysucou, Lipany, Lučenec, Malacky, Martin, Michalovce, Modrý Kameň, Nižná, Nováky, Považská Bystrica, Piešťany, Poprad, Prešov, Púchov, Rimavská Sobota, Revúca, Rožňava, Senec, Skalica, Spišská Nová Ves, Stará Ľubovňa, Svidník, Trebišov, Vranov nad Topľou, Zvolen, Žiar nad Hronom, Žilina

Bratislava, Banská Bystrica, Čadca, Bardejov, Liptovský Mikuláš, Levice, Prievidza, Ružomberok, Trenčín, Trnava, Piešťany, Hlohovec, Dunajská Streda, Galanta

V. számú melléklet

Az EM TEST rendszer cseh tagjai

- Szoftver és elektronikus eszközök
- Érintésmentes kártya project

10. Ábra EM TEST Csehország

Cheb, Aš, Kraslice, Tachov, Přeštice, Bělá nad Radbůzou, Babylon, Plzeň, Rokycany, Nezvěstice, Nepomuk, Kněžnou, Opava, Vsetín, Valašské Kralovice, Žlutice, Nejdek, Abertamy, Karlovy Vary, Chomutov, Louny, Žatec, Kadaň, Podbořany, Litoměřice, Teplice, Litvínov, Bílina, Beroun, Vlašim, Příbram, Sedlčany, Tábor, Písek, Milevsko, Strakonice, Blatná, Vodňany, České Budějovice, Český Krumlov, Kaplice, Kutná Hora, Čáslav, Kolín, Jablonec nad Nisou, Liberec, Kosmonosy, Benátky nad Jizerou, Mnichovo Hradište, Semily, Bělá pod Bezdězem, Jičín, Turnov, Hořice, Stará Paka, Dvůr Králové, Zábřeh, Mohelnice, Jeseník, Krnov, Žďár nad Sázavou, Nové Město na Moravě, Tišnov, Bystřice nad Per., Velké Meziříčí, Rosice, Židlichovice, Třebíč, Moravské Budějovice, Pohořelice, Náměšť nad Oslavou, Břeclav, Hustopeče, Uherské Hradište, Uherský Brod, Frýdlant nad Ostravicí, Jablůnkov

Sokolov, Domažlice, Klatovy, Sušice, Mladá Boleslav, Rychnov nad Meziříčí, Zlín, Otrokovice, Luhačovice, Valašské Klobouky, Slavičín, Rožnov, Frýdek Místek, Karviná, Orlová, Havířov, Třinec, Český Těšín, Teplice, Břeclav, Cheb, Karlovy Vary

VI. számú melléklet

Az EM TEST rendszer lengyel tagjai

- Szoftver és elektronikus eszközök
- Érintésmentes kártya project

11. Ábra EM TEST Lengyelország

Bialystok, Bydgoszcz, Elblag, Gdansk, Kalisz Jaworzno, Kielce, Oswiecim, Poznan, Radom, Siedlce, Walcz, Warszawa, Wejherowo, Wroclaw