Kontaktivabade piletisüsteemide ühilduvus: ülevaade ja soovitused hangeteks ning arendusteks

15. detsember 2010

OÜ ELIKO
Tanel Tammet, Alar Kuusik

Sisukord

1. Analüüsi eesmärgid ja eeldused

Käesoleva töö üheks eesmärgiks on kontaktivabadel andmekandjatel põhinevate ühistranspordi piletimüügisüsteemide tehnoloogilise raamistiku kaardistamine ja valdkonna standardite ning erinevate süsteemide liideste analüüs Eesti ühistranspordi vajadustest lähtuvalt.

Töö teiseks eesmärgiks on konkreetsete soovituste andmine kontaktivaba kaarti kasutavate piletisüsteemide hangete ja arenduste jaoks, tagamaks loodavate süsteemide ühiskasutamise võimalikkust. Need soovitused on koos selgituste ja põhjendustega esitatud peatükis 5: nõuded ja soovitused ühilduvatele piletisüsteemidele. Analüüsi lisas tuuakse needsamad soovitused kompaktsel kujul ilma põhjendusteta, eesmärgiga võimaldada soovitusi kasutada vastavate hankematerjalide ühe osana.

Analüüs ja soovitused käsitlevad eeskätt kontaktivabadel andmekandjatel põhinevaid süsteeme. Töö üks siht on esitatavate analüüside ja soovituste kompaktsus ja praktilisus.

Soovitusi koostades on lähtutud eeldusest, et erinevad piletisüsteemid on ja jäävadki olema rajatud küllalt erinevatele tehnoloogiatele ja tööpõhimõtetele, ning ühe ja universaalse piletisüsteemi hankimine või arendamine kogu Eesti ühistranspordi jaoks ei ole praktiline ning ärilistel ja administratiivsetel põhjustel oleks see ka ebareaalne.

Analüüside ja soovituste rõhk on nimelt minimaalse ühisosa leidmisel, mida oleks lihtne erinevates piletisüsteemides järgida ning mille järgimine tagaks süsteemide koosvõime.

Koosvõime all peame silmas eeskätt võimalust, et ühe piletisüsteemi kontaktivaba andmekandjat ehk RFID-piletit saaks kasutada ka teistes piletisüsteemides, mis hõlbustab ja odavdab piletite ostmist, kasutamist ja tootmist.

Lisaks sellele võimaldab koosvõime kergemini saavutada samade riistvarakomponentide kasutamist erinevates süsteemides, mis jällegi muudab süsteemide hankimist, juurutamist ja hooldust odavamaks ning lihtsamaks.

Analüüs ei käsitle küsimust, kuidas erinevad piletimüügisüsteemid (operaatorid) võiksid vastastikku üksteise pileteid müüa, koostada mitmest eri piletist komplekspileteid jms.

2. Kiirülevaade: piletisüsteemid ning kontaktivabad kaardid

Elektroonilisi piletisüsteeme võib jaotada kahte äärmusvarianti:

- Offline süsteemid. Sellistes süsteemides on pileti liik ja pileti kehtivus elektrooniliselt salvestatud otse piletikandjale (füüsilisele kaardile), ning bussi sisenemisel kasutatav või kontrolöri käes olev kontrollseade ei võta piletikontrolliks võrguühendust. Enamus tuntumaid välismaiseid elektroonilise pileti süsteeme, sh näiteks Soomes rakendatavad, on offline süsteemid. Offline süsteemi eeliseks on sõltumatus kvaliteetselt töötavast võrguühendusest (ja sidekulude vältimine), miinuseks aga vajadus rakendada piletile info kirjutamisel (ja sealt lugemisel) keerukat krüptosüsteemi, mis, nagu praktika näitab, võib osutuda suhteliselt kergesti murtavaks. Ilma krüptosüsteemita muutuks piletite võltsimine väga lihtsaks.

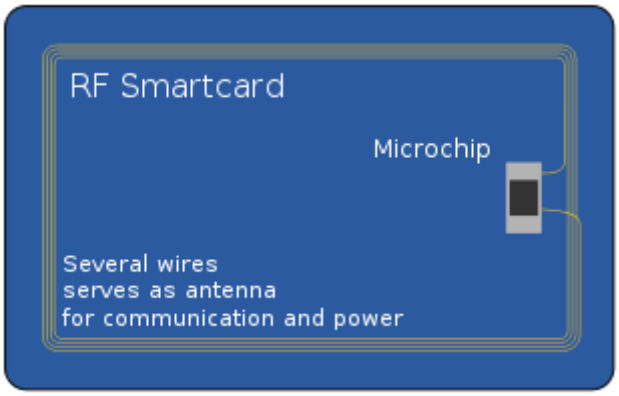
- Online süsteemid. Online süsteemi korral ei ole piletikandjale enamasti salvestatud pileti liiki ega kehtivust, selle asemel on kaardi mikroskeemi tootja poolt piletisse salvestatud unikaalne kood (UID), mis võib olla kas piletiomanikust sõltumatu (anonüümne pilet) või seotud piletiomanikuga või ka otse piletiomaniku identifikaator, näiteks isikukood (personaliseeritud pilet). UID unikaalsuse tagavad kaartides sisalduvate mikroskeemide tootjad, kaardi kloonimine nõuab eritehnikat. Pileti liigi ja kehtivuse kontroll tehakse üle võrgu tsentraalse piletite andmebaasi vastu, kasutades piletikandjal olevat UID-d. Plussiks asjaolu, et mingit krüptosüsteemi ei ole pileti kontrollimisel vaja rakendada ja pileteid ei tule "eeltäita", seega on süsteem fundamentaalselt turvalisem, kui offline süsteem. Miinuseks vajadus regulaarselt võrguühendust võtta, kuigi üldjuhul piisab sagedasest võrguühendusest, võrguühendust igal kontrollikorral vaja ei ole. Näiteks Tallinna/Tartu ID-pileti süsteem ja Tallinna turistikaardi süsteem on online süsteemid, kus küll RFID tehnoloogiat seni ei kasutata. Samuti on online süsteemid erinevad kontserdi/kinopiletisüsteemid, mis võimaldavad veebi kaudu pileti ostu (sebrapilet, Coca Cola plaza piletid jms vöötkoodi lugemisel baseeruvad piletid). Tallinna ID-pileti korral loeb kontrolöriseade ID-kaardilt isikukoodi ja kontrollib kas kontrollseadmesse salvestatud piletite andmebaasist või otse võrgust pileti tüübi ja kehtivuse. Tallinna turistikaardilt loetakse kaardi ID ja liik, külastus salvestatakse/kehtivust kontrollitakse online.

Nagu viimase punkti all kirjas, on online-süsteemi tihti ratsionaalne realiseerida selliselt, et kogu kehtivate piletite andmebaas talletatakse regulaarselt kõigisse kontrollseadmetesse. Selle tulemusena ei ole enamikul kontrollikordadest seadmel vaja võrguühenduses olla. Võrguühendus on vajalik ainult juhtudel, kui kontrollitav pilet on ostetud äsja (näiteks tunnipilet) ning seda ei ole veel kontrollseadmesse salvestatud.

Teiselt poolt sisaldab enamik offline süsteeme erinevaid mahukaid online-komponente, milleks võivad olla näiteks maksekaartidele veebi kaudu raha kandmine, oma ostude/piletite kehtivuse info vaatamine, kaardi-info tagavarakoopiate tegemine, sõidustatistika kogumine jne: funktsioonid, mida saab realiseerida ainult online. Tüüpiliselt realiseeritakse online komponendi info ja RFID-l oleva offline info sünkroniseerimine spetsiaalsetes müügiautomaatides või kontrolliseadmetes.

Kontaktivabad kaardid jagunevad väga paljudesse erinevatesse kategooriatesse. Reeglina kasutavad selliseid süsteemid passiivset RFID tehnoloogiat, mis mh tähendab, et kaart ei sisalda patareid: kaart vastab lugemisseadme raadiopäringule omakorda raadiovastusega, kasutades puhtalt lugemisseadmest kiiratavate raadiolainete energiat. "Kaart" võib, aga ei pruugi olla hariliku plastkaardi kujul: levinud on ka nupukujulised "kaardid" (mitmetes sissepääsusüsteemides), painduval papil olevad "kaardid" (mitmed piletisüsteemid), kleepsuna kasutatavad "kaardid" (tootesildid) jne.

Transpordi- ja maksesüsteemides kasutatakse üle maailma *eranditult* 13.56MHz magnetväljasidestusega tehnoloogiat. Euroopas ja Ameerikas kasutatakse ISO/IEC 14443 A ja B RFID tehnoloogiaid. Allpool kasutatakse NXP tooteperekonna koondnime Mifare ISO/IEC 14443 Type A sünonüümina. Aasias on levinud lähedane (kuid mitte identne) Sony poolt toodetav FeliCa tooteperekond, millel ISO vastavusstandard puudub.



Väga robustselt võttes võiks kaarte jaotada järgmistesse kategooriatesse, alustades lihtsamatest ja lõpetades keerukamatega:

- Lihtsaimad RFID tagid annavad lugejale tagasi kaardi (enamasti) unikaalse kaardi-ID (UID), ning neile ei saa midagi kirjutada. Sellised kaardid on väga odavad ja töökindlad. Toodete sildistamisel kasutatakse enamasti selliseid kaarte. UID lugemine on reeglina kõige kiirem kaardioperatsioon, kaardi kahjustumine pöördumisel ei ole võimalik.

- Veidi keerukamad RFID tagid/kaardid sisaldavad lisaks kaardi UID-le mälu, kuhu saab kirjutamisseadmega andmeid kirjutada. Selline on näiteks Soomes mittelaetava sõidukaardina laialt kasutatav Mifare Ultralight kaart, mis müüakse eeltäidetuna, ning kuhu hiljem uut pileti-infot ei laeta. Kirjutamisprotsessi ajal sideseansi katkestamine (kaardi eemaldamine lugeja juurest) võib kaardi kasutuskõlbmatuks muuta. Kirjutamisoperatsioon on oluliselt (>10 korra) aeglasem kui UID lugemine. Sedaliiki kaardi omahind on 2-5 korda kõrgem lihtsaima kaardi hinnast.

- Keerukuselt järgmised on nn RFID smartcardid, mis sisaldavad lisaks kaardi UID-le ja mälule ka suhteliselt keerukamaid funktsioone täita suutvat mikroprotsessorit. Enamasti on sellises protsessoris realiseeritud krüptofunktsioonid. Kaarte saab kasutada maksesüsteemides, kus makseseade loeb kaardil olevat summat, arvutab sealt ostu maha ja kirjutab sinna uue, väiksema summa. Selline on näiteks Soomes mitmekordselt kasutatav ehk uute piletitega laetav Mifare DESFire kaart. Kaart võib pöördumisprotsessi ajal rikneda, kaardi pöördumisaeg

on oluliselt aeglasem kui UID lugemine. Kaardi tüüpiline omahind ca 10 korda kõrgem kui lihtsaimal kaardil.

- Eraldi kaardiliigi moodustavad RFID liidesega varustatud uuemad krediit- ja pangakaardid (Eeestis selliseid veel ei väljastata, kuid plaanis on nende väljastamise alustamine suhteliselt lähemas tulevikus). Sellistel kaartidel funktsioneerib RFID liides kui alternatiiv kaardiprotsessori vaskkontaktidele: RFID kaudu on võimalik kaarti lugeda ilma teda füüsiliselt lugemisseadmesse paigutamata. Muus osas funktsioneerib selline kaart täpselt nagu standardne protsessoriga krediit/maksekaart ja reeglina ei paku viimasega võrreldes täiendavat funktsionaalsust.

- Lisaks võib välja tuua RFID smartcardi eriliigi, mis ei anna välja kaardi staatilist UID-d ja mis on ette nähtud isikuandmete kandmiseks selliselt, et kaardil olevat informatsiooni ei saa dekrüpteerida, lugemata samas kaardile visuaalselt või vöötkoodi/magnetribaga varustatud informatsiooni (mis ongi siis krüpteerimisvõtmeks). Selliseid RFID smartcarde kasutatakse näiteks uuemates Eesti passides, kus RFID kannab nii passist visuaalselt loetavat infot kui biomeetrilist infot (pilt ja sõrmejäljed), ning plaanis on sellise RFID smartcardiga varustada ka järgmise põlvkonna Eesti ID-kaardid. Iga ühendussessiooni jaoks genereerib selline kaart uue juhusliku UID.

- Hoopis eraldi kategooria ISO 14443A,B ja FeliCa RFID-seadmetest moodustavad nn NFC (near field communication) süsteemid. Enamkasutatavad NFC süsteemid on praegusajal tüüpiliselt integreeritud (st kohe sisse ehitatud) mobiiltelefoniga. NFC süsteemid võimaldavad töötamist kas passiivse RFID tagina või vastupidi, ise aktiivselt RFID tage lugedes/kirjutades. Kuna NFC on reeglina integreeritud telefoni või pihuarvutiga, siis võimaldavad NFC seadmed ka emuleerida/simuleerida RFID tage, mis võib tekitada turvaprobleeme nende kasutamisel tava-RFID-süsteemides. Turul on mitmeid NFC-ga varustatud mobiiltelefone, mh on NFC tugi ehitatud ka uusimasse Androidi operatsioonisüsteemi versiooni (kuid mitte enamikku Androidi kasutatavatesse telefonidesse). Rõhuv enamus turulolevaid mobiiltelefone NFC tehnoloogiat siiski ei sisalda.

Piletisüsteemides oleks põhimõtteliselt rakendatavad kõik eelnimetatud kaardiliigid, mis Euroopa kontekstis peaksid vastama ISO 14443A sidestandardile. Praktikas kasutatakse transpordi-piletisüsteemides aga lihtsamaid kaardiliike, eeskätt mäluga varustatud liht- või smartcarde (vastavalt näiteks Mifare Ultralight ja DESFire).

Oluline on tähele panna, et offline süsteemides on võimalik kasutada ainult selliseid kaarte, mille mällu on võimalik andmeid kirjutada (jällegi näiteks Mifare Ultralight ja DESFire), kuid kaarte, mis annavad välja ainult oma unikaalse kaardi-UID, ei ole arusaadavalt võimalik kasutada. Samuti ei saa offline süsteemides kasutada RFID-ga krediit/maksekaarte ega RFID-ga varustatud ID-kaarte.

Online süsteemides on põhimõtteliselt võimalik kasutada kõiki RFID-kaarte, kuna online süsteemi jaoks on vajalik ainult UID lugemine kaardilt. Selleks UID-ks on üldjuhul kaardi oma UID (seega sobiks tehniliselt ka enamik tootesildistamiseks kasutatavaid RFID tage), võib aga põhimõtteliselt olla ka isikuga seotud ID, näiteks krediit/maksekaardi number või passil/id-kaardil olev isikukood (viimasel juhul tekib küll oluline takistus, nimelt peaks kontrollseade siis lugema ka passis/kaardil olevat masinloetavat visuaalset tekstiala, analoogiliselt passide lugemisele piirikontrollil).

RFID kaardid ei pruugi piletisüsteemides olla ainult piletikandjaks, vaid kanda ka - reeglina väiksemaid summasid - raha, mida saab kasutada piletiostuks. Teisiti öeldes omab RFID piletikandja piletisüsteemis ühte kolmest võimalikust põhifunktsionaalsusest:

- RFID kaardiga on seotud ostetud pilet: kas siis offline, piletile kirjutatuna, või online, süsteemi andmebaasist loetavana. Muid funktsioone RFID kaardil ei ole. Sellised on näiteks Soomes kasutatavad Mifare Ultralight kaardid.

- RFID kaart on maksekaart: kaardile on kantud raha, piletit kaardiga seotud ei ole. Kaardiga maksmine annab tüüpiliselt soodustust, võrreldes sularahaga maksmisega. Seejuures võib soodustus olla seda suurem, mida rohkem raha on kaardile kantud. Selline skeem - küll hariliku, ilma RFID-ta smartckaardi näol - on Eestis kasutusel näiteks Go Busi süsteemis kasutatavate Go In maksekaartidena. Offline süsteemi korral nõuab taoline lahendus sisseehitatud krüptovõimalustega suhteliselt kallima RFID-kaardi kasutamist.

- Kombineeritud variant: kaardiga on seotud pilet ning kui kaardile on kantud raha, siis on kaart samas kasutatav ka maksekaardina. Nõuete poolest kaardi võimalustele ei erine see skeem eelmisest, puhtalt maksekaardi-süsteemist.

3. Olemasolevad süsteemid, standardid ja lahendused

Anname ülevaate nii olulisematest RFID-piletisüsteemide standarditest kui reaalsetest süsteemidest. Tasub tähelepanu juhtida asjaolule, et reaalsed süsteemid erinevad reeglina mingites osades standarditest, eeskätt kas siis pakkudes lisavõimalusi ja/või mitte realiseerides mingeid standardis pakutud võimalusi.

Kõik järgmised standardid on offline piletisüsteemide standardid, st standardite peamine fookus on kaardile kirjutatava info põhimõttelise struktuuri ja seejuures ka olulisemate detailide spetsifitseerimine. Samas näevad standardid ette online-infrastuktuuri näiteks raha kandmiseks kaardile, sõiduinfo tsentraalseks salvestamiseks jne.

- ITSO (http://www.itso.org.uk/) on väga mahukas standard, mille peamine eesmärk on nimelt piletisüsteemide ühilduvuse saavutamine. Tegu on eeskätt Suurbritannia standardiga, kuid seda kasutab eeskujuna ka Soome ühis-piletisüsteemi standard. Süsteem spetsifitseerib eeskätt seda, kuidas erinevaid piletitooteid tuleb offline RFID-kaardi mällu salvestada: koodid, väljad, väljapikkused- ja positsioonid jne. Samuti standardiseerib ITSO mitmed struktureeritud numereerimissüsteemid, detailiseerib PAN numbri kasutamist (mh sätestab, et kasutada tuleb 18-kohalist PAN numbrit) jne.

- CALYPSO (http://www.calypsotechnology.net/) on erinevates eeskätt lõunapoolsetes Euroopa riikides (Prantsusmaa, Belgia, Portugal, Itaalia, samuti mingil määral Saksamaa) kasutatav standard. CALYPSO standardil baseerub ka Riia RFID-ühistranspordi-piletisüsteem. Analoogiliselt ITSO süsteemile spetsifitseerib CALYPSO eeskätt seda, kuidas erinevaid piletitooteid tuleb offline RFID-kaardi mällu salvestada. Tasub tähele panna, et veidi laiema

skoobiga ITSO standard võimaldab omakorda realiseerida ka CALYPSO-l baseeruvaid süsteeme.

- VDV: eeskätt Saksamaa standard.

- Soome YTV E-lippu kontseptsioon: sarnane ITSO standardile, kuid mitte täpselt ITSO standard. Süsteem on ette nähtud piletite hoidmiseks nii lihtsatel RFID kaartidel (Mifare Ultralight), RFID Smartcardidel (Mifare DESFire) kui NFC-telefonidel. Süsteem spetsifitseerib, kuidas salvestatakse pileti-info RFID kaardi mällu. Seejuures kasutatakse süsteemi jaoks loodud/valitud spetsiaalset krüptomehhanismi ja salajasi võtmeid, mis võimaldab krüpteeritud piletiinfo talletamise ka lihtsamatele kaartidele, kus krüptofunktsioonid ei ole realiseeritud kaardi oma protsessoris. Krüptomehhanism kasutab kahte erinevat võtit, üks kaartide tootmiseks/info salvestamiseks ja teine kaardi info lugemiseks. Vaata ka www05.turku.fi/ah/jlk/2009/1105013x/Images/889221.doc ja http://www.sfs.fi/files//alykorttiseminaari09/Jylha-Ollila_2009-09-20.pdf

  E-Lippu kontseptsioon ei ole Soomes tervikuna rakendatud, pigem on tegemist kolme suurema linna - Helsingi, Turu, Tampere - piletisüsteemide ühise arendusplaaniga, mis peaks realiseeritama lähiaastatel. Turus on osa E-lippu kontseptsioonist juba realiseeritud, mh lihtsam Mifare Ultralightil baseeruv mittelaetav RFID-kaart.

Hetkel on käimas projekte eelkirjeldatud piletisüsteemide võimaliku omavahelise ühilduvuse saavutamiseks/analüüsimiseks, vt http://www.ifm-project.eu/ . 2010 suvel demonstreeriti mh eksperimentaalsüsteemi, kus ühele piletikandjale salvestati piletid nii ITSO, Oysteri kui VDV standardite järgi.

Hea ülevaate saamiseks reaalselt kasutusel olevatest elektroonilistest piletisüsteemidest soovitame järgmisi raporteid:

- http://www.emta.com/IMG/pdf/EMTA-Ticketing.pdf

- http://www.emta.com/IMG/pdf/YTV_Fare_and_Ticketing_Systems_in_Europe.pdf

Järgnevas väike ülevaade olulisematest lähipiirkonna välisriikide RFID-süsteemidest. Kõik need süsteemid on offline-süsteemid, kuid sisaldavad ka olulisi online-komponente, näiteks raha salvestamiseks kaardile, kaartide tagavara-infokoopia talletamiseks, sõiduinfo kogumiseks andmebaasi jne.

- Londoni Oyster. Seni ei ole realiseeritud ITSO standardi baasil, kuid on olemas plaan muuta tulevikus ITSO-ga kooskõlaliseks. Kasutatav kaart on võimsamat sorti RFID-smartcard, mis võimaldab nii salvestada piletit (kuni kolm erinevat piletit korraga). Pileti ostmisel kaardile spetsiaalse müügisüsteemi kaudu võtab müügisüsteem piletilt maha vastava rahasumma. Piletit saab kaardile osta ainult spetsiaalse müügiseadmega varustatud müügipunktist. Raha kandmine kaardile toimub on-line, seega on võimalik raha kanda ka näiteks panga püsikorraldusega. Kaardi infot on vastavates seadmetes võimalik laadida online süsteemi, mis võimaldab mh kadunud kaardile kantud piletite/raha taastamist.

- London councils freedom pass: tegu on ITSO/Oyster topeltkaardiga.
- Hetkel käibiv Helsingi RFID-piletisüsteem ei vasta eelkirjeldatud Soome e-Lippu kontseptsioonile. Süsteem väga sarnane Londoni Oyster süsteemile. Kasutatav Travel Card (*Matkakortti/Resekort*) on võimsamat sorti RFID-smartcard, mis võimaldab nii salvestada piletit kui kanda kaardile raha vahemikus 5 - 400 eurot. Pileti ostmisel kaardile spetsiaalse müügisüsteemi kaudu võtab müügisüsteem piletilt maha vastava rahasumma. Piletit saab kaardile osta ainult spetsiaalse müügiseadmega varustatud müügipunktist, mis on Helsingis väga levinud, sh näiteks R-kioskites, samuti müügiautomaatides jne. Raha kandmine kaardile toimub on-line, seega on võimalik raha kanda ka näiteks panga püsikorraldusega.
- Stockholmis on käibel SL-access RFID kaart, mis on samuti väga sarnane Londoni Oyster süsteemile. Kaardi infost on võimalik teha tagavara-online-koopiaid. Täiendavad online-funktsionaalsused, nagu näiteks kasutajakonto, kust saaks näha kogu kaardiinfot, on hetkel arendusjärgus.
- Riia: Calypso baasil RFID-piletisüsteem, vt http://www.calypsonet-asso.org/downloads/cartes09/calypso_Riga_18112009.pdf
- Peterburis arendusjärgus olev süsteem: realiseeritud ITSO baasil.

Kuivõrd enamus lähipiirkonna riike on baseerinud oma süsteemid ITSO standardile või selle mingitele osadele (erandiks Riia), peame Eestis samuti mõistlikuks soovitada pigem ITSO standardi komponente.

4. Eestisisesed vajadused

Kirjeldame kõigepealt suuremate mahtudega elektroonilisi piletisüsteeme ning mõningaid nendega potentsiaalselt seostamis-võimalikke süsteeme eestis.

- Tallinn/Tartu ID-pilet, teostanud Sertifitseerimiskeskus, United Tickets ja Mindstone. Opereerib United Tickets. Tegu on puhtalt online süsteemiga, kus pileti olemasolu on kirjas süsteemi andmebaasis ning ta on seostatud piletiomaniku isikukoodiga. Kontrollimise kiirendamiseks/odavdavamiseks cachetakse kontrollseadmetesse igal öösel kogu piletisüsteemi kehtivate piletite baas, millega välditakse enamikel kontrollimistel online ühendust: online ühendus on vajalik ainult värskelt ostetud piletite, näiteks tunnipiletite korral. Online ühendust teostatakse kiiruse ja töökindluse huvides GSM USSD kanalit kasutades. Süsteem hangib erinevatest registritest automaatselt andmeid soodustuste (pensionärid, õpilased, Tallinna elanikud jne) olemasolu tuvastamiseks. Pileteid saab osta väga paljude müügikanalite (erinevad internetipangad, püsikorraldused, mobiil- ja telefoniost. Rõhuv enamus Tallinna ühistranspordi käibest toimub selle süsteemi kaudu. Süsteemi on suhteliselt lihtne laiendada online RFID-piletite kasutamisele, samuti on lihtne järgnevas kirjeldatud RFID-piletisüsteemide ühilduvuse saavutamine

- Kalastaja ID-pilet, loomaaia jms ID-piletid: realiseeritud ja hallatud eelnevalt kirjeldatud ID-pileti süsteemi raames.

- Tallinn Card turistidele, teostanud Sertifitseerimiskeskus, United Tickets ja Mindstone. Opereerib UnitedTickets. Süsteem baseerub magnetribaga kaartidel, mida müüakse väga paljudes majutusasutustes, süsteemiga liitunud muuseumites jms soodustust pakkuvates asutustes. Tegu on online süsteemiga, mis võimaldab kaardilugemiste cachemist lugemisseadmetes juhuks, kui online side on häiritud või kui online sidet soovitakse teostada perioodiliselt. Peamised tehnilised eesmärgid: (a) kontrollida, et sama kaardiga ei sisenetaks ühte soodustust pakkuvasse asutusse korduvalt, (b) salvestada kõik külastused süsteemi andmebaasi, mida omakorda kasutatakse müügist laekunud summade jaotamiseks soodustust pakkuvate asutuste vahel. Süsteemi on suhteliselt lihtne laiendada online RFID-piletite kasutamisele, samuti on lihtne järgnevas kirjeldatud RFID-piletisüsteemide ühilduvuse saavutamine

- Elektriraudtee RFID-kaardi-piletid, teostanud WebMedia. Opereerib Elektriraudtee. Tegu on ainsa aktiivselt opereeritava RFID-piletisüsteemiga Eestis. Elektriraudtee piletisüsteem tervikuna on multifunktsionaalne mitmes mõttes:

    - Võimaldab kasutada nii ID-piletit (liidesega Tallinna ID-pileti süsteemi) kui Elektriraudtee oma RFID-kaardi-piletit.

    - RFID kaart on korraga kasutusel nii piletikandjana kui maksevahendina, kuhu kasutaja saab online raha kanda.

    - Pileti olemasolu info talletatakse nii RFID-kaardile (offline) kui teatud sagedusega kontroll-müügiseadmete sünkroniseerimise järel ka süsteemi andmebaasi (online).

  Järgnevas kirjeldatud RFID-piletisüsteemide ühilduvuse saavutamine süsteemiga on lihtne.

  Mitmetes maakondades, sh Tartu maakonnas kasutatavad Go Busi smartcard tehnoloogia ettemaksu-kaardid, teostanud WebPartner ja opereerib GoBus. Nimetatud kaardid on puhtalt raha kandvad ettemaksu-kaardid, mis ei sisalda piletit ja ei kasuta RFID-d. Üleminek RFID smartcardidele ja järgnevas kirjeldatud RFID-piletisüsteemide ühilduvuse saavutamine süsteemiga on tõenäoliselt suhteliselt lihtne.

- RFID-ga kaardid üksikute Tallinna koolide sissepääsusüsteemides, teostanud InDeal. Opereerib In Deal. Kaarte oleks võimalik kasutada piletikandjatena järgnevas kirjeldatud ühilduvusstandardis.

- RFID-ga ISIC kaardid koostöös SEB-ga. RFID reaalse kasutuse kohta sellistes kaartides ei ole analüüsi teostajatel andmeid. Kaarte oleks võimalik kasutada piletikandjatena järgnevas kirjeldatud ühilduvusstandardis.

- Mifare RFID pääslasüsteemid, näiteks Tallinna Tehnikaülikool (Hotronic), kasutatakse UID-d. Lahendused on kiiresti populaarsust kogumas kuna pääsukaardi hind on oluliselt odavam kui varasemate 100-300kHz tehnoloogial põhinevate kaartide korral.

Hetkel on Eestis käimas mitmed hanked ühistranspordi piletisüsteemide moderniseerimiseks, reeglina nähakse neis ette RFID kaartide kasutuselevõttu. Peamised moderniseerimise eesmärgid on:

- Mitte-elektrooniliste piletite kasutamise minimeerimine.
- Kasutajate suurem mugavus: online piletiostude võimaldamine, kiirem ja mugavam piletikontroll.
- Võimalus registreerida kõiki sõite (eeskätt transpordivahendisse sisenemisi) andmebaasidesse (kas online või - üldjuhul - lugemisseadmesse cachetud kaardilugemiste regulaarse ülekandmisega online andmebaasi). Registreerimise üks peamisi eesmärke on reisiliinide parema planeerimise ja optimeerimise võimaldamine, maaliinidel ka dotatsioonide senisest täpsema jaotamise võimaldamine.

Käesoleva analüüsi koostamise ajal on hangete osas:

- Käimasolev Tallinna / Harjumaa RFID-põhine piletisüsteemi hange. Analüüsi kirjutamise hetkel võitjat välja kuulutatud ei ole.
- Käimasolevad Tartumaa ja Jõgevamaa RFID-põhised piletisüsteemi hanked. Analüüsi kirjutamise hetkel on Tartumaa võitjaks kuulutatud WebPartner.
- Analoogilisi RFID-piletisüsteemi hankeid on plaanis välja kuulutada mitmetes maakondades.

5. Nõuded ja soovitused ühilduvatele piletisüsteemidele

Käesolevas peatükis esitatakse lihtne ning valdavale enamikule kontaktivabadele meediumitele sobilik ühildumisstandard. Ühildumisstandard on orienteeritud piletisüsteemide jaoks, kus piletite infot ei hoita piletikandjal, ehk siis online süsteemidele.

Puhtalt offline süsteemide jaoks käesolev standard lahendust ei paku. Offline süsteemi standardiseerime on väga oluliselt keerukam, kui online süsteemi standardiseerimine, ning vastava huvi korral soovitame eelistada ITSO süsteemi, mis on mh Soome E-Lippu kontseptsiooni inspiratsiooniks.

Tasub tähele panna, et käesolevas esitatav standard ei keela ega takista offline süsteemide ehitamist, vaid näeb online süsteemi kasutamise võimaluse ette ühilduvuse mehhanismina. Erinevate offline süsteemide ühilduvuse tagamist ilma online ühilduvus-komponendita peame ebareaalseks, kuna see eeldaks offline süsteemides kasutatavate krüptovõtmete pidevat vahetamist eri offline süsteemide vahel, mis oleks korraga nii keerukas, äriliselt problemaatiline kui vähese turvalisusega meetod. Muuhulgas ei ole ühildumist saavutatud ka Soomes eri linnades (näiteks Helsingi/Turu) kasutatavate (offline) süsteemide vahel, ning seda vaatamata asjaolule, et mõlemad süsteemid kasutavad samu kaarditüüpe ja standardeid.

Standardis kasutatakse ära fakti, et iga kontaktivaba kaart omab unikaalset identifikaatorit, mis on tootja poolt juba kaardile omistatud. Standard arvestab turvalisuse poolelt asjaoluga, et kaardi

unikaalse identifikaatori muutmine on väga raske ning antud rakenduste valdkonnas – ühistranspordi piletikandjana – ei tasu selline tegevus ennast ka rahaliselt ära.

Standardis soovitatakse, et kasutatavate piletikandjate (üldjuhul RFID-tehnoloogiat kasutavad kaardid) üle toimub visuaalne kontroll (kas siis kontrolöride poolt teostatav pisteline kontroll või ühissõiduki juhi poolt teostatav pidev kontroll kõikide piletikasutuste kohta). See välistab piletite elektroonilise võltsimise tehnoloogiliste vahendite (näiteks spetsiaalse lühimaasidestusega raadioseadme abil).

UID võltsimine turulolevatel RFID kaartidel on kõrgtehnoloogia abil teoreetiliselt võimalik, kuid praktiliselt väga keerukas ja kallis (RFID kaardid ei võimalda UID-d üle kirjutada), ning tema massiline teostamine eeldaks võltsija poolt pidevat ligipääsu online-piletiandmebaasile. Seega peame sellise teoreetilise võimaluse äriotstarbel kuritarvitamist majanduslikult väga ebaotstarbekaks.

Jaotame esitatava ühilduvusstandardi kahte kihti:

- Esimese (madalama) taseme kiht ehk tehniline ühilduvus võimaldab eri süsteemide seadmetel kaarte lugeda ja pileti olemasolu kontrollida, kuid ei piisa selleks, et kasutaja saaks veebiostu, mobiiliostu vms maksekanali kaudu oma kaardile laadida teiste süsteemide pileteid. Teiste süsteemide pileteid saab küll kaardile laadida vastava RFID-lugejagaga varustatud müügipunktis.

- Teise (kõrgema) taseme kiht ehk online-ostu ühilduvus võimaldab kasutajal laadida oma kaardile pileteid ka veebiostu, mobiiliostu vms kanali kaudu, minemata selleks RFID-lugejaga müügipunkti.

Kokkuvõtlikult võib öelda, et käesolev ühildumisstandard võimaldab:

- kasutada ühe offline või online süsteemi piletikandjat (RFID kaarti) teises online süsteemis.

- disainida offline-süsteeme, mis on võimelised online müügisüsteemi kaudu ostetud pileteid oma teeninduspunktides oma (offline süsteemi) piletikandjale peale kandma.

Käesolev standard ei paku lahendusi, mis võimaldaksid:

- kasutada ühe puhtalt offline süsteemi piletikandjat (RFID kaarti) teises tehnoloogiliselt ja äriliselt erinevas puhtalt offline süsteemis. Nagu eelnevas selgitatud, ei pea analüüsi koostajad sellist võimalust majanduslikult ja administratiivselt realistlikuks, kuigi tehnoloogiliselt oleks selline võimalus muidugi saavutatav.

5.1 Piletikandja spetsifikatsioon ning tehnilise taseme ühilduvus

Nagu varasemas öeldud, võimaldab tehnilise taseme ühilduvus eri süsteemide seadmetel teise süsteemi ISO 14443A RFID kaarte lugeda ja (online) pileti olemasolu kontrollida, kuid ei piisa selleks, et kasutaja saaks veebiostu, mobiiliostu vms maksekanali kaudu oma kaardile laadida teiste süsteemide pileteid. Ainult tehnilise taseme ühilduvuse korral seostatakse pileti olemasolu puhtalt

RFID kaardi UID numbriga, kasutamata muid identifikaatoreid, nagu näiteks järgmises peatükis kirjeldatud PAN-i.

Tehnilise taseme ühilduvus on eelduseks järgnevas kirjeldatud online-ostu taseme ühilduvusele, mida me soovitame ühilduvusel eesmärgiks seada: ainult tehnilise taseme ühilduvus ei paku kasutajatele mugavat võimalust piletiostuks teise süsteemi kaardile.

Piletikandja (RFID tehnoloogiat kasutav kaart) peab tehnilise taseme ühilduvuse jaoks vastama allpool kirjeldatud nõuetele.

Nõuded piletikandja füüsilisele meediumile

Piletikandja peab olema ISO/IEC 7810 standardi ID-1 formaadis kaart (kõik tavalised krediitkaardi-mõõdus kaardid vastavad sellele standardile).

Piletikandja peab omama ISO/IEC 14443 Type A (nn. MIFARE standard, kõige levinum, väga paljud standardid toetavad seda – ITSO, VDV) nõuetele vastavat RFID-kiipi. Type B standardit kasutab Calypso. Type B-d käesolev standard ei soovita, kuna nende kaartide tehniline suhtlus on erinev Type A süsteemist ning Type B on vähem levinud. Tüüpilised kaardilugejad suudavad lugeda nii Type A kui Type B kaarte, ning põhimõtteliselt oleks käesoleva standardi raames võimalik kasutada ka Type B kaarte.

Mitte-pangakaardi korral peab RFID-kiip omama staatilist unikaalset UID-i. Rõhuv enamus RFID-kaarte ja -tage sellist UID-i sisaldavad. Vastupidise näitena hakkab uus ID-kaart sisaldama dünaamilise UID-iga kiipi ja seega ei sobi RFID-piletiks.

Pangakaartide korral on nõutav EMV Contactless standardile vastava kaardi kasutamine. On põhjust arvata, et lähiajal hakatakse ka Eestis pankade poolt selliseid kaarte väljastama.

5.1 Piletikandja numeratsioon ning online-ostu tasemel ühilduvus

Online-ostu tasemel ühilduvus võimaldab kasutajal RFID-kaardile laadida teiste süsteemide online-pileteid, kasutades selleks veebiostu, mobiiliostu vms kanaleid. Selleks peab kaardil olema kasutaja jaoks visuaalselt loetav number, mida piletiostul veebivormi või mobiiliostul mobiili kaudu sisestada. Eriti mobiiliostu jaoks on väga soovitav, et tegu oleks nimelt numbriga, mitte aga suvalise tähejadaga.

Taoline kaardile kantud visuaalne number (või selle numbri piisavalt mahukas osa) on allpoolkirjeldatud kaardinumber PAN.

Võib tekkida õigustatud küsimus, miks ei või visuaalse numbrina kasutada lihtsalt RFID UID-d, millega kaart niikuinii seotud? Peamisi põhjuseid on kaks:

- RFID UID number on välja kirjutatuna väga pikk ning seetõttu oleks tema korrektne tippimine veebivormi või mobiili äärmiselt vaevarikas.

- RFID UID numbrid ei lange kokku laialtkasutatavate kaardinumeratsiooni-strandarditega (pangakaardid, kliendikaardid jne jne), mis muudakse nende kasutamise ühises süsteemis väga vaevarikkaks.

Nõuded piletikandjate numereerimisele

Piletikandjale peab olema määratud unikaalne ISO/IEC 7812 standardi kohane kaardinumber – PAN.

Sellist standardit järgib ITSO ühistranspordi kaartide standard, soome YTV standard, kõik pangakaardid, pea kõik lennufirmade kliendikaardid, valdav enamus mangetribaga kliendikaarte, Tallinn Card.

PAN peab olema piletikandjale trükitud ja visuaalselt loetav. Pealetrükitud PAN on kasutatav üldjuhul selleks, et tippida number sisse kaardile pileti elektroonilisel laadimisel või ka - erijuhtudel - piletikontrolliks, kui kontrolöriseadmel ei ole kaardi elektroonilise lugemise võimalust: näiteks kalastuspileti kontroll mobiiltelefoniga.

PAN võib, aga ei pea olema kaardile elektrooniliselt kirjutatud ja elektrooniliselt loetav. Tuleb tähele panna, et PAN on erinev RFID-kaardile tootmisel salvestatavast ja elekrooniliselt loetavast UID-st, mis sisaldab väga palju numbrikohti ning reeglina ei ole kaardil visuaalselt esitatud.

Samuti on kasulik PAN-i kirjutamine kaardile ribakoodina, mis võimaldab mugavate müügisüsteemide ehitust ilma RFID-lugejat müügiseadmele lisamata, kasutades siis harilikke olemasolevaid ribakoodilugejaid.

PAN kaardinumber peab olema piletikandjal visuaalselt esitatud ehk peale trükitud ühel järgmistest kujudest:

a) Kaardinumbri esitus täispikal kujul

Kaardinumber esitatakse piletikandjal täispikalt kuni 19 numbrikohaga – st kujul, nagu seda näeb ette ISO/IEC 7812 standard:

$$i_1 i_2 i_3 i_4 i_5 i_6 n_1 \dots n_k c$$

Kus:

- $i_1 i_2 i_3 i_4 i_5 i_6$ – 6-kohaline kaardi väljaandja IIN (*issuer identification number*).
- $n_1 \dots n_k$– piletikandja unikaalne identifikaator antud väljaandja juures, k võib olla maksimaalselt 12 (st piletikandja identifikaatori pikkus võib olla maksimaalselt 12 kohta, minimaalsele pikkusele piirangut pole)

- c – piletikandja numbri kontrolljärk, mis on arvutatud kõikidest selle ees toodud numbritest $i_1 i_2 i_3 i_4 i_5 i_6 n_1 \dots n_k$ Luhni algoritmi järgi (vt http://en.wikipedia.org/wiki/Luhn_algorithm)

Märkused:

Piletikandja (RFID kaardi) väljaandjad peavad kasutama kas rahvusvahelist IIN-i, taotledes rahvusvaheliselt organisatsioonilt (haldushierarhia, mille tipmine organisatsioon on American Bankers Association) oma IIN-i või kasutama Eestis kokkulepitud IIN määramise põhimõtet (vt detaile järgnevas).

Ühistranspordi piletite ITSO standard kasutab mitte maksimaalset võimalikku 19 numbrikohta, vaid 18 numbrikohta. Käesolev standard lubab ITSO 18 numbri kasutamist, kuid ei keela ka 19 numbrikoha kasutamist.

ITSO standard näeb ette kõigil ITSO-t järgivatel kaartidel ühe ja sellesama ITSO poolt määratud IIN-i kasutamist. Selline IIN on käesoleva ühilduvusstandardi poolt lubatud, kuid ei ole kohustuslik.

Eesti isikukood on üks võimalik unikaalse identifikaatori $n_1 \dots n_k$ erijuht personaliseeritud kaartidel. Isikukood on 11 numbrikohta pikk. Tuleb tähele panna, et isikukoodi viimane koht on kontrollsumma üle isikukoodi, kuid PAN numbril lisandub viimaseks kohaks täiendav kontrolljärk c üle kogu PAN numbri.

Kontrolljärk c peab olema visuaalselt esitatud unikaalse identifikaatori viimane numbrikoht, seda ära jätta ei tohi.

Vastavalt ISO/IEC 7812 standardile ja Eestis kokku lepitud põhimõtetele (vt: http://www.ids.ee/index.php/iin-register.html) esitatakse Eestisisese IIN-iga kaardinumber järgmiselt:

$$9233 i_1 i_2 i_3 i_4 n_1 \dots n_k c$$

Kus:

- $i_1 i_2 i_3 i_4$ – 4-kohaline Eestisisene kaardi väljaandja eraldusnumber.
- $n_1 \dots n_k$ – piletikandja unikaalne identifikaator antud väljaandja juures, k võib olla maksimaalselt 10 (st piletikandja identifikaatori pikkus võib olla maksimaalselt 10 kohta, minimaalsele pikkusele piirangut pole)
- c – piletikandja numbri kontrolljärk, mis on arvutatud kõikidest selle ees toodud numbritest Luhni algoritmi järgi (vt http://en.wikipedia.org/wiki/Luhn_algorithm)

Eestisisese IIN kaardinumbri järgmine ei ole ühilduvuseks kohustuslik (võib kasutada ka muid ISO/IEC 7812 standardi järgseid IIN numbreid, näiteks välisfirmade IIN numbrit), kuid oleks Eesti turule suunatud kaartide puhul väga selgelt mõttekas valik.

b) Kaardinumbri esitus lühikujul

Kasutusmugavuse suurendamiseks on võimalik esitada piletikandjatel kaardinumber visuaalselt lühikujul. Sellisel juhul peab piletikandja väljaandja määratlema enda väljaantavatele piletikandjatele kaardinumbri prefiksi, mis tuleb liita piletikandjal esitatud kaardinumbrile ette, et saada täispikk PAN.

Prefiks peab sisaldama väljaandja IIN-i ning võib ka täiendavalt sisaldada piletikandja unikaalse identifikaatori algusosa mingeid kohti. Sellistel piletikandjatel peab olema esitatud pileti väljaandja poolt antud kaarditüüpi identifitseeriv logo.

Logo järgi saab kaardi laadimise korral kaardinumbri käsitsisisestamisel valida kaardi tüübi/väljaandja, mille järgi süsteem saab ise üheselt tuvastada vastava prefiksi, saamaks kokku tervikliku kaardinumbri. Süsteemides tuleb selliste kaartide korral siseselt alati kasutada kaardi täispikka numbrit.

Muus osas vastab lühinumbri esitus eelnevalt kirjeldatud pika numbri esitusele, kehtivad samad nõuded kontrolljärgu c arvutusest, visuaalse esituse kohustuslikkusest jne.

Piletikandjal hoitav elektrooniline info

Piletikandja PAN võib olla (kuid ei pea olema) esitatud ka elektrooniliselt. Elektroonilise esituse jaoks soovitame kasutada ITSO standardit, mille juures tuleb küll tähele panna, et ITSO standard nõuab kõigil kaartidel ühe ja sellesama IIN kasutamist, mida praegune standard kohustuslikuks ei tee.

Sellist tüüpi piletikandjate korral, kus ITSO standard ei näe ette PAN elektroonilist kirjutamist kaardile (näiteks Mifare Ultralight), kasutatakse piletikandja PAN numbri elektroonilise esitamise jaoks spetsiaalselt kodeeritud piletitoote infot, mille formaatimine/esitamine on piletisüsteemi arendaja ülesanne. PAN elektroonilise kirjutamise standardiseerimine võiks olla edaspidise standardimistöö üks eesmärke.

Pangakaartide korral ITSO standardi põhist täiendavat rakendust kandjale ei lisata, vaid piletikandja tuvastamiseks kasutatakse selle EMV rakenduses leiduvat infot. Pangakaartide kasutamise puhul piletikandjana tuleb kogu suhtlus kaardiga realiseerida EMV spetsifikatsioonidele vastavalt. Käesolev standard neid spetsifikatsioone eraldi välja ei too.

Elektroonilist PAN-i lugevad piletisüsteemid võiksid ühilduvuse laiendamiseks realiseerida piiratud arvu enimkasutatavate RFID kaartide tuvastamise ja neilt - igaühelt erinevast asukohast - PAN numbri lugemise. Suhteliselt lihtne on seda näiteks realiseerida Soomes kasutatavate YTV standardijärgsete kaartide puhul, kuhu on PAN number kirjutatud konkreetselt spetsifitseeritud asukohta.

Piletikandjate numbrite säilitamine ja töötlemine infosüsteemides

Ühilduvates infosüsteemides ja nende andmebaasides säilitatakse/kasutatakse piletikandjate määratlemiseks täispikka PAN-i.

Erandina identifitseeritakse piletikandjana kasutatavad RFID-pangakaardid turvalisuse huvides mitte PAN-i, vaid PAN numbrist SHA512-algoritmiga koostatud räsi abil (räsi pikkus on 64 baiti). Põhjus asjaolus, et pangakaardi PAN-i loetakse salajaseks infoks ning selle lahtine säilitamine näiteks kaardimaksete teostajate poolt ei ole lubatud.

5.2 Piletimüügi ja kontrollimise mehhanismis ühilduvas süsteemis

Järgnevas kirjeldatud mehhanism võimaldab erinevate piletisüsteemide poolt välja antud kandjate ristkasutust. Ühe konkreetse piletisüsteemi siseselt on samas süsteemis väljaantud piletite kontrolli võimalik teostada ka süsteemi oma vahenditega, mis ei pea vastama esitatud mehhanismile ja mida standardiseerida ei ole otstarbekas: taolisi erilahendusi edasine tekst ei käsitle.

Nagu eelnevas selgitatud, on piletikandja visuaalselt loetav ja infosüsteemides kasutatav number PAN erinev RFID-kaardile tootmisel salvestatavast ja elektrooniliselt loetavast UID-st.

Jällegi, osadel kaartidel võib PAN olla kaardile elektrooniliselt kirjutatud, kuid selline kirjutamine ei ole ühilduvuse jaoks kohustuslik. Vaatame järgnevas elektrooniliselt loetavast UID-st PAN leidmise protsessi.

UID on vanematel RFID kaarditüüpidel pikkusega 4 baiti, uuematel 7 või 10 baiti. Siinkohal tegu siis baitide arvuga, mitte numbrikohtadega.

Piletikasutaja ostab (laeb) oma piletikandjale uue pileti PAN-i baasil, veebisüsteemides reeglina tippides kas täispika PAN-i või tema lühiesituse veebilehe vormile.

Pileti kontrollimisel kasutatakse reeglina, vastupidi, elektrooniliselt loetavat RFID UID-d.

Seega on kontrollimisel vaja tuvastada RFID UID järgi, kas antud piletikandjaga on seotud kehtiv sõiduõigus.

Selleks peab online piletisüsteem andmebaasis seostama kehtiva pileti nii visuaalse PAN-i kui RFID UID-ga, isikustatud pileti korral ka isikukoodiga (mis võib, aga ei pruugi olla PAN-i osa).

Piletiostul edastatakse baasi PAN. Baasi salvestamisel peab süsteem tuvastama PAN-ga seotud RFID UID ja selle samuti piletiga siduma.

Selleks peavad kõik ühilduvate piletite väljaandjad siduma tsentraalse serveri kaudu teistele süsteemidele kättesaadavas LDAP serveris kõigi oma väljaantavate kaartide RFID UID-d PAN-ga. Seda seostamist on mõttekas teha kaartide tootmise/tellimisega paralleelselt, kasutades piletisüsteemi haldajale sobivamat mehhanismi/algoritmi. LDAP server realiseerib kaks päringut:

- annab päringu sisendiks antud PAN-le vastuseks RFID UID-i (kohustuslik funktsionaalsus) ja isikustatud kaartide korral lisaks ka seotud isikukoodi (võimaldab pileti hinna arvutamisel kasutada soodustusi).
- annab päringu sisendiks antud RFID UID-i järgi PAN-i (vajalik ühilduvate piletite müügil piletikandja RFID UID-i järgi)

Vastava LDAP serverite infrastruktuuri ja väljade nimede spetsifitseerimine oleks edasise standardiseerimistöö üks ülesanne.

Ühilduvuse tagamiseks tuleb ehitada tsentraalne, kõigile ühilduvatele piletisüsteemidele kättesaadav LDAP server, mis seob eri väljaandjate oma LDAP serverid.

Konkreetse väljaandja server leitakse pileti PAN järgsel salvestamisel PAN-s sisalduva IIN (või soovi korral pikema prefiksi kaudu, mille esimene osa on IIN): prefiks (mis võib, aga ei pruugi ise olla terviklik IIN) määrab konkreetse väljaandja serveri.

Pileti kontrollimisel loeb kontrollseade pileti RFID UID ja tuvastab kas süsteemi online andmebaasist (mis on üldjuhul igal piletisüsteemil oma) või seadmesse laetud piletite andmebaasist, kas selle RFID UID-ga on seotud antud süsteemis kehtiv pilet.

Pileti müügil on kaks erinevat võimalust: pilet müüakse kas visuaalse PAN-ga seotuna, või - kui müügiseadmes on RFID-lugeja - kaardi RFID UID järgi.

6. Infoturbe küsimused

RFID piletitega seotud infoturbe küsimused jagunevad kahte põhikategooriasse: kasutajate võimalik salajane (mass)jälitamine ja kaartidele salvestatud info võimalik lahtimurdmine ja kopeerimine teistele kaartidele.

Salajase mass-jälitamise oht on olemas kõigi RFID kaartide korral, mis sisaldavat unikaalset staatilist infot, näiteks isikukoode või ka lihtsalt harilikku anonüümset RFID UID-d. Hea ülevaate ohtudest leiab artiklist http://www.springerlink.com/content/m177234t0162u420/ , samuti käesoleva analüüsi autorite varasemast analüüsist http://www.lambda.ee/images/7/7a/Rfid_id_analyys_2.pdf . Väga detailse analüüsi kaartide salajase lugemise aspektidest annab magistritöö http://dspace.uta.edu/bitstream/handle/10106/4948/Chopra_uta_2502M_10684.pdf?sequence=1

ID-kaartide ja RFID-ga passide puhul välistatakse jälitamine sel viisil, et RFID-lt loetav info ei ole staatiline (iga lugemiskord on erinev) ning dekrüpteerimiseks on vaja lugeda ID-kaardil või passis visuaalselt kirjutatud infot.

Isikuga sidumata RFID kaartide salajane lugemine jälgimise eesmärgil on arusaadavalt väiksem probleem, kui isikustatud kaartide puhul. Seetõttu on isikustatud kaartide puhul väga soovitav mitte

esitada kaardil otsest isikuinfot, näiteks isikukoode: selle vältimisel eeldab lihtne jälitamine piletisüsteemi isikustatud piletite andmebaasi leket kolmandatele osapooltele.

Kaartidele kirjutatud info kopeerimise oht on praktikas arusaadavalt olulisem ja kriitilisem, kui jälitamisvõimaluse minimeerimine.

Siin tuleb eristada kahte võimalust:

a) RFID UID massiline kandmine teistele kaartidele. Nagu eelnevas kirjeldatud, ei ole tööstuslikult toodetavate RFID kaartide puhul selline toiming praktiliselt võimalik, ehk täpsemalt, ei ole majanduslikult tasuv. Ohuna toome välja n.n. relay rünnakud näiteks NFC telefoni kaudu: kontrollsüsteemile esitatakse NFC-telefon, mille tarkvara emuleerib mõne olemasoleva kaardi UID-i. Sellise kuritarvituse vastu on praktikas vaja lubada RFID UID-põhist piletimüüki ainult kaartidele, mitte aga telefonidele või eriseadmetele. Kuritarvituse alternatiivse vältimise viis oleks keerukate PKI-põhiste kaartide kasutamine, näiteks MIFARE SmartMX.

b) RFID kaardi mällu kirjutatud krüpteeritud andmete (mis on kasutusel offline süsteemides) lahtimuukimine ja teistele kaartidele ülekandmine. Erinevalt RFID UID-st on kaardi mälu RFID seadmete abil lihtsalt kirjutatav, seega on põhiküsimus krüpteeritud andmete lahtimuukimise ohus. Selline oht on väga reaalne, nagu on kirjeldatud näiteks järgmistes publikatsioonides:

Artiklites http://www.cs.virginia.edu/~kn5f/pdf/Mifare.Cryptanalysis.pdf , http://www.nicolascourtois.com/papers/mifare_rump_ec08.pdf ja http://sar.informatik.hu-berlin.de/research/publications/SAR-PR-2008-21/SAR-PR-2008-21_.pdf esitatakse võimalus murda massiliselt kasutusel oleva Mifare Classic krüptofunktsioonidega smartcardi infot paari sekundiga. Nimelt sellist kaarti kasutab näiteks Londoni Oyster süsteem. Samuti väidetakse, et kaardi "pealtkuulamise" järel on võimalik kaarti kloonida alla minutise ajakuluga. Kaardi pealtkuulamine eritehnikaga on võimalik 2-5 meetri kauguselt.

7. Ettepanekud edasise uurimistegevuse ja standardimise algatamiseks

Eeltoodud standardi kontekstis on olulisemad lähiajal uurimist ja standardimist vajavad küsimused järgmised:

- Online-ühilduvuskomponendi jaoks vajalik LDAP infrastruktuur. Siinkirjeldatud standardi kasutuselevõtmisel on tingimata vaja spetsifitseerida päringud ja vastused, ligipääsude haldamine, ning erinevate LDAP serverite omavaheline suhtlus. Samuti oleks kasulik töötada välja kõigile osapooltele levitatav ühine LDAP-tarkvarapakett, mis hõlbustaks ühilduva online-süsteemi juurutamist.

- PAN numbri turvaline kirjutamine kaardile, mis hõlbustaks ostu- ja kontrollimehhanisme. Selleks oleks eeskätt kasulik tuvastada sobiva offline-standardi, näiteks ITSO, poolt soovitatavaid põhimõtteid PAN numbri salvestamiseks ja uurida, kuidas need põhimõtted võiksid sobida võimalike arendusjärgus RFID-piletisüsteemidega Eestis.

- Suurima lähinaabri - Helsingi - piletisüsteemi hetke arendusseisu ja -plaanide täpsem uurimine ning vastavalt sellele tehniliste nüansside kontrollimine ühilduvuse saavutamiseks Helsingis praegu ja lähiperspektiivis ning Tallinnas lähiperspektiivis kasutusel olevate RFID piletisüsteemide vahel.
- Täiendavad uuringud eelpool mainitud turvaküsimuste osas.
- NFC telefonide turuletuleku prognoosid ja nende kasutamise võimalused piletisüsteemides.

LISA: Tehnilised tingimused hangete läbiviimisel

Käesolevas lisas esitatakse kompaktne, hangete koostamiseks sobivam versioonis eelnevas detailsemalt kirjeldatud ühilduvusstandardist. Ära on jäetud näiteks põhjendused esitatud soovitustele. Kompaktse kirjelduse kasutamisel oleks väga soovitav esitada täiendava taustamaterjalina terve käesolev analüüs või vähemalt standardi detailne variant ülalt.

1 Piletisüsteemide ühilduvusstandard

Käesolevas esitatakse lihtne ning valdavale enamikule kontaktivabadele meediumitele sobilik RFID-piletite ühildumisstandard. Ühildumisstandard on orienteeritud piletisüsteemide jaoks, kus piletite infot ei hoita piletikandjal, ehk siis online süsteemidele.

Tasub tähele panna, et standard ei keela ega takista offline süsteemide ehitamist, vaid näeb online süsteemi kasutamise võimaluse ette ühilduvuse mehhanismina.

Standardis eeldatakse, et kasutatavate piletikandjate (üldjuhul RFID-tehnoloogiat kasutavad kaardid) üle toimub visuaalne kontroll (kas siis kontrolöride poolt teostatav pisteline kontroll või ühissõiduki juhi poolt teostatav pidev kontroll kõikide piletikasutuste kohta). See välistab piletite elektroonilise võltsimise tehnoloogiliste vahendite (näiteks NFC mobiiltelefoni) abil.

2 Piletikandja spetsifikatsioon ning tehnilise taseme ühilduvus

Tehnilise taseme ühilduvus on eelduseks järgnevas kirjeldatud online-ostu taseme ühilduvusele, mida me soovitame ühilduvusel eesmärgiks seada: ainult tehnilise taseme ühilduvus ei paku kasutajatele mugavat võimalust piletiostuks teise süsteemi kaardile.

Piletikandja (RFID tehnoloogiat kasutav kaart) peab tehnilise taseme ühilduvuse jaoks vastama allpool kirjeldatud nõuetele.

Nõuded piletikandja füüsilisele meediumile

Piletikandja peab olema ISO/IEC 7810 standardi ID-1 formaadis kaart.

Piletikandja peab omama ISO/IEC 14443 Type A (nn. MIFARE standard, kõige levinum, väga paljud standardid toetavad seda – ITSO, VDV) nõuetele vastavat RFID-kiipi. Type B standardit kasutab Calypso. Type B-d käesolev standard ei soovita, kuna nende kaartide tehniline suhtlus on erinev Type A süsteemist ning Type B on vähem levinud. Tüüpilised kaardilugejad suudavad lugeda nii Type A kui Type B kaarte, ning põhimõtteliselt oleks käesoleva standardi raames võimalik kasutada ka Type B kaarte.

Mitte-pangakaardi korral peab RFID-kiip omama staatilist unikaalset UID-i.

Pangakaartide korral on nõutav EMV Contactless standardile vastava kaardi kasutamine.

3 Piletikandja numeratsioon ning online-ostu tasemel ühilduvus

Online-ostu tasemel ühilduvus võimaldab kasutajal RFID-kaardile laadida teiste süsteemide online-pileteid, kasutades selleks veebiostu, mobiiliostu vms kanaleid. Selleks peab kaardil olema kasutaja jaoks visuaalselt loetav number, mida piletiostul veebivormi või mobiiliostul mobiili kaudu sisestada.

Taoline kaardile kantud visuaalne number (või selle numbri piisavalt mahukas osa) on allpoolkirjeldatud kaardinumber PAN.

Nõuded piletikandjate numereerimisele

Piletikandjale peab olema määratud unikaalne ISO/IEC 7812 standardi kohane kaardinumber – PAN.

PAN peab olema piletikandjale trükitud ja visuaalselt loetav. Pealetrükitud PAN on kasutatav üldjuhul selleks, et tippida number sisse kaardile pileti elektroonilisel laadimisel või ka - erijuhtudel - piletikontrolliks, kui kontrolöriseadmel ei ole kaardi elektroonilise lugemise võimalust.

PAN võib, aga ei pea olema kaardile elektrooniliselt kirjutatud ja elektrooniliselt loetav.

Samuti on kasulik PAN-i kirjutamine kaardile ribakoodina.

PAN kaardinumber peab olema piletikandjal visuaalselt esitatud ehk peale trükitud ühel järgmistest kujudest:

a) Kaardinumbri esitus täispikal kujul

Kaardinumber esitatakse piletikandjal täispikalt kuni 19 numbrikohaga – st kujul, nagu seda näeb ette ISO/IEC 7812 standard:

$i_1 i_2 i_3 i_4 i_5 i_6 n_1 \dots n_k c$

Kus:

- $i_1 i_2 i_3 i_4 i_5 i_6$ – 6-kohaline kaardi väljaandja IIN (*issuer identification number*).
- $n_1 \dots n_k$– piletikandja unikaalne identifikaator antud väljaandja juures, k võib olla maksimaalselt 12 (st piletikandja identifikaatori pikkus võib olla maksimaalselt 12 kohta, minimaalsele pikkusele piirangut pole)
- c – piletikandja numbri kontrolljärk, mis on arvutatud kõikidest selle ees toodud numbritest $i_1 i_2 i_3 i_4 i_5 i_6 n_1 \dots n_k$ Luhni algoritmi järgi (vt http://en.wikipedia.org/wiki/Luhn_algorithm)

Piletikandja (RFID kaardi) väljaandjad peavad kasutama kas rahvusvahelist IIN-i, taotledes rahvusvaheliselt organisatsioonilt (haldushierarhia, mille tipmine organisatsioon on American Bankers Association) oma IIN-i või kasutama Eestis kokkulepitud IIN määramise põhimõtet (vt detaile järgnevas).

Eesti isikukood on üks võimalik unikaalse identifikaatori $n_1 \dots n_k$ erijuht personaliseeritud kaartidel. Isikukood on 11 numbrikohta pikk. Tuleb tähele panna, et isikukoodi viimane koht on kontrollsumma üle isikukoodi, kuid PAN numbril lisandub viimaseks kohaks täiendav kontrolljärk c üle kogu PAN numbri.

Kontrolljärk c peab olema visuaalselt esitatud unikaalse identifikaatori viimane numbrikoht, seda ära jätta ei tohi.

Vastavalt ISO/IEC 7812 standardile ja Eestis kokku lepitud põhimõtetele (vt: http://www.ids.ee/index.php/iin-register.html) esitatakse Eestisisese IIN-iga kaardinumber järgmiselt:

$9233 i_1 i_2 i_3 i_4 n_1 \dots n_k c$

Kus:

- $i_1 i_2 i_3 i_4$ – 4-kohaline Eestisisene kaardi väljaandja eraldusnumber.
- $n_1 \dots n_k$– piletikandja unikaalne identifikaator antud väljaandja juures, k võib olla maksimaalselt 10 (st piletikandja identifikaatori pikkus võib olla maksimaalselt 10 kohta, minimaalsele pikkusele piirangut pole)
- c – piletikandja numbri kontrolljärk, mis on arvutatud kõikidest selle ees toodud numbritest Luhni algoritmi järgi (vt http://en.wikipedia.org/wiki/Luhn_algorithm)

Eestisisese IIN kaardinumbri järgmine ei ole ühilduvuseks kohustuslik (võib kasutada ka muid ISO/IEC 7812 standardi järgseid IIN numbreid, näiteks välisfirmade IIN numbrit), kuid oleks Eesti turule suunatud kaartide puhul väga selgelt mõttekas valik.

b) Kaardinumbri esitus lühikujul

Kasutusmugavuse suurendamiseks on võimalik esitada piletikandjatel kaardinumber visuaalselt lühikujul. Sellisel juhul peab piletikandja väljaandja määratlema enda väljaantavatele piletikandjatele kaardinumbri prefiksi, mis tuleb liita piletikandjal esitatud kaardinumbrile ette, et saada täispikk PAN.

Prefiks peab sisaldama väljaandja IIN-i ning võib ka täiendavalt sisaldada piletikandja unikaalse identifikaatori algusosa mingeid kohti. Sellistel piletikandjatel peab olema esitatud pileti väljaandja poolt antud kaarditüüpi identifitseeriv logo.

Logo järgi saab kaardi laadimise korral kaardinumbri käsitsisisestamisel valida kaardi tüübi/väljaandja, mille järgi süsteem saab ise üheselt tuvastada vastava prefiksi, saamaks kokku tervikliku kaardinumbri. Süsteemides tuleb selliste kaartide korral siseselt alati kasutada kaardi täispikka numbrit.

Muus osas vastab lühinumbri esitus eelnevalt kirjeldatud pika numbri esitusele, kehtivad samad nõuded kontrolljärgu c arvutusest, visuaalse esituse kohustuslikkusest jne.

Piletikandjal hoitav elektrooniline info

Piletikandja PAN võib olla (kuid ei pea olema) esitatud ka elektrooniliselt. Elektroonilise esituse jaoks soovitame kasutada ITSO standardit.

Sellist tüüpi piletikandjate korral, kus ITSO standard ei näe ette PAN elektroonilist kirjutamist kaardile (näiteks Mifare Ultralight), kasutatakse piletikandja PAN numbri elektroonilise esitamise jaoks spetsiaalselt kodeeritud piletitoote infot, mille formaatimine/esitamine on piletisüsteemi arendaja ülesanne.

Pangakaartide korral ITSO standardi põhist täiendavat rakendust kandjale ei lisata, vaid piletikandja tuvastamiseks kasutatakse selle EMV rakenduses leiduvat infot. Pangakaartide kasutamise puhul piletikandjana tuleb kogu suhtlus kaardiga realiseerida EMV spetsifikatsioonidele vastavalt. Käesolev standard neid spetsifikatsioone eraldi välja ei too.

Elektroonilist PAN-i lugevad piletisüsteemid võiksid ühilduvuse laiendamiseks realiseerida piiratud arvu enimkasutatavate RFID kaartide tuvastamise ja neilt - igaühelt erinevast asukohast - PAN numbri lugemise.

Piletikandjate numbrite säilitamine ja töötlemine infosüsteemides

Ühilduvates infosüsteemides ja nende andmebaasides säilitatakse/kasutatakse piletikandjate määratlemiseks täispikka PAN-i.

Erandina identifitseeritakse piletikandjana kasutatavad RFID-pangakaardid turvalisuse huvides mitte PAN-i, vaid PAN numbrist SHA512-algoritmiga koostatud räsi abil (räsi pikkus on 64 baiti).

4 Piletimüügi ja kontrollimise mehhanismid ühilduvas süsteemis

Järgnevas kirjeldatud mehhanism võimaldab erinevate piletisüsteemide poolt välja antud kandjate ristkasutust. Ühe konkreetse piletisüsteemi siseselt on samas süsteemis väljaantud piletite kontrolli võimalik teostada ka süsteemi oma vahenditega, mis ei pea vastama esitatud mehhanismile ja mida standardiseerida ei ole otstarbekas: taolisi erilahendusi edasine tekst ei käsitle.

Piletikandja visuaalselt loetav ja infosüsteemides kasutatav number PAN on erinev RFID-kaardile tootmisel salvestatavast ja elektrooniliselt loetavast UID-st.

Kaartidel võib PAN olla kaardile elektrooniliselt kirjutatud, kuid selline kirjutamine ei ole ühilduvuse jaoks kohustuslik. Vaatame järgnevas elektrooniliselt loetavast UID-st PAN leidmise protsessi.

Piletikasutaja ostab (laeb) oma piletikandjale uue pileti PAN-i baasil, veebisüsteemides reeglina tippides kas täispika PAN-i või tema lühiesituse veebilehe vormile.

Pileti kontrollimisel kasutatakse reeglina, vastupidi, elektrooniliselt loetavat RFID UID-d.

Seega on kontrollimisel vaja tuvastada RFID UID järgi, kas antud piletikandjaga on seotud kehtiv sõiduõigus.

Selleks peab online piletisüsteem andmebaasis seostama kehtiva pileti nii visuaalse PAN-i kui RFID UID-ga, isikustatud pileti korral ka isikukoodiga (mis võib, aga ei pruugi olla PAN-i osa).

Piletiostul edastatakse baasi PAN. Baasi salvestamisel peab süsteem tuvastama PAN-ga seotud RFID UID ja selle samuti piletiga siduma.

Selleks peavad kõik ühilduvate piletite väljaandjad siduma tsentraalse serveri kaudu teistele süsteemidele kättesaadavas LDAP serveris kõigi oma väljaantavate kaartide RFID UID-d PAN-ga. Seda seostamist on mõttekas teha kaartide tootmise/tellimisega paralleelselt, kasutades piletisüsteemi haldajale sobivamat mehhanismi/algoritmi. LDAP server realiseerib kaks päringut:

- annab päringu sisendiks antud PAN-le vastuseks RFID UID-i (kohustuslik funktsionaalsus) ja isikustatud kaartide korral lisaks ka seotud isikukoodi
- annab päringu sisendiks antud RFID UID-i järgi PAN-i (vajalik ühilduvate piletite müügil piletikandja RFID UID-i järgi)

Ühilduvuse tagamiseks tuleb ehitada tsentraalne, kõigile ühilduvatele piletisüsteemidele kättesaadav LDAP server, mis seob eri väljaandjate oma LDAP serverid.

Konkreetse väljaandja server leitakse pileti PAN järgsel salvestamisel PAN-s sisalduva IIN (või soovi korral pikema prefiksi kaudu, mille esimene osa on IIN): prefiks (mis võib, aga ei pruugi ise olla terviklik IIN) määrab konkreetse väljaandja serveri.

Pileti kontrollimisel loeb kontrollseade pileti RFID UID ja tuvastab kas süsteemi online andmebaasist (mis on üldjuhul igal piletisüsteemil oma) või seadmesse laetud piletite andmebaasist, kas selle RFID UID-ga on seotud antud süsteemis kehtiv pilet.

Pileti müügil on kaks erinevat võimalust: pilet müüakse kas visuaalse PAN-ga seotuna, või - kui müügiseadmes on RFID-lugeja - kaardi RFID UID järgi.