RFID kasutusvõimaluste analüüs ning soovitused eesti ID-kaardi täiendamise kontekstis

Tallinna Tehnikaülikool

Elmer Joandi, Alar Kuusik, Tanel Tammet

versioon 2

jaanuar 2008

Sisukord

1. Sissejuhatus

Käesoleva analüüsi eesmärgiks on tuvastada, milliseid rakendusvõimalusi võiks RFID-identifikaatoriga varustatud eesti ID-kaardil peale esmase piirikontrolli-rakendusi veel olla, ning kas ja kuidas saaks neid täiendavaid rakendusi kombineerida Kodakondus- ja Migratsiooniameti jaoks vajalike lahendustega. Küsimuste fookuseks on laiemate rakendusvõimaluste ja ülestõusvate turvalisusküsimuste vahel võimalike kompromisside otsimine.

Analüüs jaguneb järgmisteks peatükkideks:

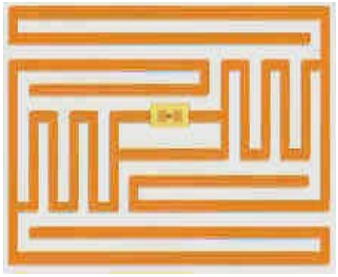
- Ülevaade võimalustest, vajadustest, rakendustest ja problemaatikast
- Peamised analüüsi kontekstis olulised rakendused
- Detailsem ülevaade RFID tehnoloogiatest
- Turvaprobleemid ja nende võimalikud lahendusviisid
- Kokkuvõtvad järeldused, soovitused ja edaspidised uurimissuunad
- Lisa: Mifare SmartMX perekond

Töö baseerub:

- autorite varasemal kogemusel RFID süsteemide loomise, rakendamise ning sideküsimuste valdkonnas,
- autorite varasemal kogemusel turvaküsimuste valdkonnas,
- käesolevat teemat puudutava kirjanduse läbitöötamisel,
- intervjuudel Kodakondsus- ja migratsiooniametiga, Sertifitseerimiskeskusega, RFID-põhiste uksesüsteemide tarnijaga ning juurutajaga, lisaks RFID-tehnoloogiat juurutava SEB Eesti Ühispangaga.

Analüüs ei too eraldi loeteluna välja soovitavaid artikleid RFID standarditest, rakendustest ja turvaküsimusest: mitmekesist ja detailset taust- ning lisamaterjali on asjasthuvitatutel lihtne leida võrgust. Alustuseks tasub tutvuda wikipedia lehega http://en.wikipedia.org/wiki/RFID, kus on toodud nii suur hulk viiteid eraldi materjalidele kui spetsiifilisemaid küsimusi käsitlevatele lehtedele ja portaalidele.

2. Ülevaade RFIDi võimalustest ja problemaatikast



RFID (Radio Frequency Identification) *tagid* on väga väikesed ja odavad pisiarvutid, millega võetakse ühendust raadiosagedusel, st juhtemeta. RFID tag koosneb niisiis pisiarvutist ja sellega seotud antennist.

Enamasti on tegu väga odavate, erinevatele toodetele pealekleebitavate nn tagidega, mille tüüpiliseks eesmärgiks on toote mugav identifitseerimine.

RFID tagide eestis levinuimad rakendused on vargusvastased riputid/kleepsud kauplustes müüdavatel toodetel ning kontaktivabad ukseavamis-kaardid (pääslasüsteemid). Eestis veel vähelevinud, kuid maailmas üks olulisemaid, kasvavaid ja samas vastuolulisemaid rakendusi on pealekleebitavate või trükitavate ribakoodide asendamine: RFID tag vastab RFID lugejale oma identifitseerimisnumbri.

Enamus RFID tage on nn *passiivtagid*: neil ei ole oma toidet (patareid), ning töötamiseks saavad nad voolu tagi lugemise seadme raadiokiirgusest. On olemas ka omaette toitega varustatud *aktiivtagid*, kuid taolisi me antud töös ei vaatle. Enamuse siin töös käsitletavate küsimuste jaoks ei ole küsimus oma toite olemasolust ka kuigi oluline.

Passiivtagide lugemiskaugus on suhteliselt väike: mõned sentimeetrid kuni mõned meetrid, sõltuvalt lainealast, tagi ja lugeja tüübist ning lugemisvõimsusest. Tagide lähedal asuvad metallesemed võivad tagide lugemist oluliselt häirida või võimatuks muuta.

Tootmises ja kasutuses on väga palju ja väga erinevaid tagitüüpe, mida võib jagada nii funktsionaalsuse ja mälumahu kui kasutatava raadiosageduse järgi. Detailsem ülevaade nendest tüüpidest antakse ülejärgmises peatükis. Lühiülevaatena toome välja järgmised olulisemad funktsionaalsuse variandid, alates lihtsamatest ja jätkates keerukamatega (keerukad sisaldavad enamasti ka lihtsama variandi funktsionaalsust). Igal variandil on mitmeid erivariante, nende erisusi me siinkohas ei vaata.

- Tag, mis vastab ühe biti informatsiooni: ei/jah. Sellised tage kasutatakse kauplustes vargusvastaste vahenditena. Aktiivse tagiga väravast läbiminek käivitab alarmi.
- Tag, mis on suuteline lugejale vastama talle peale salvestatud *unikaalse ID-numbri*. Sellised numbrid on reeglina suhteliselt pikad (kas 64 või 96 bitti) ning kannavad eri numbriosades (väljadel) kas EPC standardi järgi unikaliseeritud tootja ning tootetüübi kategoriseeritud informatsiooni. ID-numbri üks osa kannab ka unikaalset ID numbrit, mis on siis erinev igal üksikul ID-tagil. Niisuguseid tage kasutatakse eeskätt kaupade identifitseerimisel, ribakoodi asemel. Kasutatakse selliseid tage näiteks mh toodete identifitseerimiseks ribakoodi asemel, samuti mõnedes ühistranspordisüsteemides sõiduõiguse kinnitamiseks.
- Tag, mis lisaks mainitud ID-numbrile sisaldab *täiendavalt mälu*, tüüpiliselt vahemikus 128-1024 baiti (kuid mälumahud kasvavad pidevalt), mis on RFID-kirjutaja abil vabalt kirjutatav ning mida RFID-lugeja saab lugeda, lisaks eelmainitud ID-numbrile. Tüüpiliselt salvestatakse mällu täiendavat informatsiooni eseme kohta, millele RFID tag on kleebitud. Näiteks kasutatakse selliseid tage lennukiosade kontrollimis- ja hooldusinfo salvestamiseks, samuti mitmtes transpordisüsteemides piletina.
- Tag, mille erinevad mälupiirkonnad on *kaitstud salajase võtmega/võtmetega*: lugeda või kirjutada saab ainult võtit (parooli) teades. Muuhulgas võib ilma võtit teadmata olla võimatu ka tagi ID numbri lugemine. Enamus niisugust tüüpi (samuti keerukamad, vt järgmist lõiku) RFID tage järgib ISO 14443 standardit.

- Tag, mis sisaldab *komplekssetmikroprotsessorit*, mis võimaldab realiseerida keerukaid ja kindlaid krüptoalgoritme, lisada tagile täiendavat tarkvara jne. Selliseid tage kasutatakse näiteks elektrooniliselt loetavates passides (e-passides), mh ka uues eesti passis, mille väljaandmist alustati 2007 aastal.

Tagidel on väga palju erinevaid rakendusi, ning rakendusvõimaluste ring, nagu ka tagide funktsionaalsus, üha laieneb. Kõiki rakendusi me siinkohal üles lugema ei hakka, järgmises peatükis toome ära antud töö kontekstis olulisemad tüüprakendused.

Juhime kohe tähelepanu, et sõltumata tagi tüübist on tagidega seotud aktiivselt uuritav ja sagedasi proteste ja tõsiseid probleeme tekitav turvatemaatika, mis jaguneb kahte ossa:

- Tagide sisu kopeerimine või muutmine, mis on kasutatav pettusteks (näiteks võimaldamaks õigustamata isikutel läbipääsu pääslast, sõitu ühistranspordis vms) või identiteedivarguseks (sisestada oma RFID tagi teise isiku info).
- Jälitustegevus. kuna tage loetakse raadio teel, saab neid lugeda märkamatult. Unikaalset ID-i või mõnda muud sisulist informatsiooni kandavat tagi saab niisiis kasutada esialgsest ettenähtud rakendusest sõltumatult mitmekesiseks jälitustegevuseks ja informatsiooni korjamiseks nii esemete kui neid kasutavate inimeste kohta.

Antud töö kontekstis on põhiohuks jälitustegevus. Jälitusvõimaluste kontekstis on olulisemad kaks ohustsenaariumit:

- **Ribakoodi asendajana kasutatavate tagide kinnitamine laiatarbekaupadele** (eestis veel ei praktiseerita, maailmas mitmel pool küll). Sellistel tagidel võib olla sees unikaalne id-number, mida ostmis- ja maksmisprotsessi käigus saab põhimõtteliselt andmebaasis siduda konkreetse inimesega.

  Oletame, et kauba ostja jätab tagi kogemata kauba külge, tag ei ole deaktiveeritud, ostja kannab tagi edaspidi tihti endaga kaasas (riietuseseme, raamatu, koti vms küljes).

  Analoogilise probleemi tekitavad ka bussipiletitena/kuukaartidena kasutatavad RFID kaardid, juhul, kui neid on ostetud pangakaardi abil, mis muudab teoreetiliselt võimalikuks RFID kaardi seostamise konkreetse inimesega.

  Kui nüüd paljukäidavates või muidu huvipakkuvates kohtades - tüüpiliselt ustel, kus inimesed astuvad läbi kitsa täpselt määratud ala, mille külge on hea paigutada lugejat - märkamatult lugeda kõiki lugeja nähtavusse ilmuvaid tage, saab osa neist andmebaasi kaudu siduda konkreetsete inimestega. Sellisel viisil on põhimõtteliselt võimalik suurte inimhulkade märkamatu jälgimine/kaardistamine.

  Arusaadavalt nõuab taoline tegevus tõsist organisatsiooni ja kokkuleppeid kauplustega, ning ei ole seetõttu praktikas kuigi kerge läbi viia. Sellegipoolest valmistab see esialgu pigem teoreetiline võimalus paljudele inimestele tõsist muret. Riskide maandamiseks toodetakse osa tage kergesti deaktiveeritavatena (pooleksmurtavad), neid deaktiveeritakse eriseadmete abil taolisi tooteid müüvates kauplustes, tagi otsijaid/deaktivaatoreid müüakse jne.
- RFID tagi mälus kasutaja isikuinfot hoidva e-passi, e-töötõendi või e-id-kaardi kasutamine. Jällegi, kui kinnitada paljukäidavatesse või muidu huvipakkuvates kohtadesse märkamatud RFID lugejad, saaks inimeste liikumist jälgida otse, ilma mingi keeruka tagi-inimese seostamiseta ja organisatsiooniliste ettevalmistusteta.

Taolise ohu pärast talletatakse otsene isikuinfo alati ainult sellistesse tagidesse, mis sisaldavad kompleksset krüptoprotsessorit ja võimaldavad informatsiooni lugeda ainult võtme olemasolu korral. Võtmena kasutatakse konkreetselt e-passil (selline on ka uus, alates 2007 aastast väljaantav eesti pass) passis olevat masinloetavat, mittelektroonilist, trükitud alas olevat informatsiooni: passi rfid-s olevat isikuinfot ei saa lugeda muidu, kui ei ole enne teada passis mitte-elektrooniliselt kirjas olevat informatsiooni. Ilma võtmeta ei anna e-pass välja ka mitte unikaalset idi, samuti muutub (juhuslike arvude generaatorit kasutades) tema poolt väljastav krüpteeritud info iga kasutuskorra järel.

Varjatud jälitustegevuse vastu on võimalikud järgmised kaitsed:

- Mittevajalike RFID tagide (näiteks toodetel) hävitamine või deaktiveerimine: kas kohe poes või inimese poolt ise (soovitav eeldus on tagide tuvastamist võimaldava lugeja kasutamine).
- Selliste RFID tagide kasutamine, mis hoiavad informatsiooni kindlalt krüpteerituna, näiteks e-passi tehnoloogiat kasutades.
- RFID tagi varjestamine, kasutades kas lihtsast fooliumist ümbrist või veidi paksemast ja tõhusamast õhukesest metall-lehest ümbrikku.

Vaatamata krüptovahendite olemasolule ja laiemale kasutusele, ei ole paljud eksperdid siiski veendunud, et praegu kasutavad krüptolahendused, näiteks e-pass, on RFID tagide kontekstis piisavalt kindlad, eriti pikema aja perspektiivis. Ohtliku näitena tuuakse välja kasvõi asjaolu, et RFID tagide on omavahel eristatavad ka raadioühenduse nüansside alusel, samuti asjaolu, et e-passi võtmed on teatud info omamisel isiku kohta realistlikult ennustatavad/läbi proovitavad (variantide arv ei ole väga suur).

Viimased ohud on problemaatilised eeskätt jälitusvõimaluste kontekstis. Täiesti kindlat kaitset saab pakkuda ainult tagi varjestav ümbrik. Olulise argumendina toome siinkohas välja asjaolu, et USAs on juurutatud krüptomeetoditega kaitstud, RFID põhine ametiisikute töötõend (PIV). USA justiitsminis 2007 suvel tehtud uuring/juhend sätestab siiski, et seda kaarti tuleb üldjuhul kanda nimelt varjestatud ümbrikus.

3. Peamised töö kontekstis olulised rakendused

Anname ülevaate pääslasüsteemidest, transpordisüsteemides kasutatavatest piletisüsteemidest, elektroonilistest maksevahenditest ja e-passi süsteemist. Käsitleme neid süsteeme muuhulgas potentsiaalse RFID-iga varustatud eesti-ID-kaardi kontekstis.

3.1 Pääslasüsteemid

Pääslasüsteemid on hetkel Eestis üks peamisi, kui mitte kõige laiemalt levinud RFID kaardi rakendus.

Pääslasüsteemid töötavad üldiselt järgmisel põhimõttel: ustel on RFID kaartide lugejad, mille juures on keskselt juhitav/uuendatav andmebaas RFID kaartide ID-numbritest, millega on õigus ust avada. Kasutajatele väljastatakse RFID kaardid ja registreeritakse nende isik andmebaasi koos väljastatud RFID kaardi ID numbriga. Seejärel määratakse, mis ustest/ustekategooriatest mis aegadel isik tohib läbi pääseda. Uuendatud info kantakse ustel asuvatesse lugejatesse.

Analüüsi käigus on tehti intervjuu Jaan Ojarannaga, kellel on 12 aastat RFID pääslasüsteemide välja töötamise (s.h. kontrollerid) ja paigalduse kogemust (Mikrotehnika OÜ). Suuremad püsikliendid: Alarmnet, üks telefoni püsivõrkude ja konteinerkeskjaamade omanikfirma.

Tüüpiliselt kasutatakse süsteemides 125kHz ja 134kHz madalsageduslikku RFID-d. Mittekirjutatavas (read only) kaardis sisaldub unikaalne kood, tüüpiliselt 40 bitti, andmevahetusprotokollid on EM Marine EM41001 ja EM41002 mikroskeemidega ühilduvad. Kontrollerisse edastatakse kood, mida võrreldakse kontrollerisse salvestatud andmebaasi kirjetega.

Kontrolleris hoitakse ainult võtmekoode. Andmevahetus ei ole krüpteeritud, aeglase traadita side tõttu oleks see ka keerukas. Erinevate tootjate kaardid ei ole sageli turukaitse põhjustel ühilduvad (kontroller toetab ainult teatud koodipiirkonna ID-sid). Põhimõtteliselt on võimalik piisavalt paindliku seadme abil lugeda kõiki kaarte ja neid kopeerida. Kaardi kauglugemine (üle 50 cm) on võimalik, kuid keerukas ja nõuab spetsiaalriistvara.

Eksperdi arvamuse kohaselt oleks ID-kaardi kasutamine pääslakaardina hea idee.

Potentsiaalse kombineeritud ID-kaardi/pääslakaardi head küljed:

1) Mugav ja odav. Üks kaart sobib mitmele uksele, olemasolevate süsteemide puhul ei tööta firmadevahelise konkurentsi tõttu (suuremat kasumit teenitakse hetkel kaartide müügist).

Halvad küljed:

1) Kaarti kasutatakse rohkem, suureneb kaardi kaotamise tõenäosus.
2) Kaotatud kaardile trükitud andmete (nimi) alusel on lihtne tuletada, milliseid uksi sellega avada saab (töökoht, võibolla ka kodu).

Soovitused:

Side peaks olema krüpteeritud, näiteks muutuva koodiga vms suhteliselt lihtsa meetodiga, sest:

1) 13,56MHz raadiosignaal levib hästi ja seda saab pealt kuulata,
2) kui lahendus on laialt kasutuses, on ka lugemise seadmed levinud ning järelvalveta unustatud kaardi saab hõlpsasti kopeerida.

Võtmete vahetus teeb kaardisüsteemi paigaldamise installeerijale mõnevõrra keerukamaks. Mõistlik oleks kaardi pääsla-ala samal mälukiibil hoida ID-kaardi rakendusest eraldi, see võiks olla loetav-kirjutatav et saaks muuta vastavat pääsla ID-d. Sobiva andmevahetuse protokolli kohta andmed puuduvad, võiks vaadelda näiteks Idesco seadmeid ja kasutada sarnast protokolli (kui see kasutab krüpteeritud sidet). Teine võimalus on luua teadlikult muu maailmaga mitteühilduv lahendus, mille välja töötamisel kaasata Eesti turvafirmasid (näit Turvafirmade Assotsiatsiooni kaudu). Võimalik, et kaksikinterfeisiga kaardi (kiipkaardi ja RFID interfeisiga) kasutamine võimaldab vähendada turvariske.

Autori (Alar Kuusik) enda koostöökogemusest Visari Metall jt uksetootjatega:

Klient valib sobiva lukusüsteemi, olulisem ja sageli kallim osa on (elektriline) lukk või lukuvastus. Uksefirmad enamasti lukusüsteeme ise ei paigalda, ukse valmistamise käigus lepivad lukusüsteemi tarnija ja ukse valmistaja kokku vajalikud avad, kaablikanalid, jms. Lukusüsteem paigaldatakse kohale pandud uksele, ukse hind lukusüsteemi tüübist ei sõltu (võibolla sõltub erilahenduste korral) Elektriline vasturaud maksab alates 1500 kroonist, elektriline lukk 2500 kroonist, elektromagnetsulgur 1500 kroonist. Side uksekontrolleri ja lukumehhanismi vahel ei ole tavarakendustes elektrilises mõttes kaitstud. Madalsageduslik RFID kontroller ühele uksele koos uksesensoriga maksab 500-1500 krooni, koos toiteploki ja paigaldusega ca 3000-5000 krooni. Selline kontroller talletab 500-1000 kaardi ID. Süsteemid, kus andmebaasi saab mugavalt modifitseerida arvuti kaudu maksavad 10000-15000 krooni, kuid neid kasutavad peamiselt büroohooned. Proxikaarte müüakse lõpptarbijale 50 kr/tk. 50 korteriga kortermajas on kulutus kaartidele (3 kaarti igasse perre) 150x50= 7500 krooni, mis on suurem kui muu soetus- ja paigalduskulu. Kui süsteem töötaks ID-kaardiga, oleks kulutus kortermajale kuni 50% väiksem.

3.2 SEB Eesti Ühispanga RFID rakendus ISIC kaardil

Ülevaateks vajaliku informatsiooni saime intervjuust SEB Eesti Ühispanga vastava valdkonna töötajatega: Kaido Raiend ja Tarmo Tikan. Tegu on Eesti konteksis huvipakkuva süsteemiga, kus laialt kasutuses olevale kaardile (pangakaart) on täiendavalt lisatud suhteliselt universaalselt kasutatav RFID funktsionaalsus. Teatud mõttes on tegemist potentsiaalse ID-kaart+RFID kombinatsiooni lihtsama analoogiga.

SEB EÜP väljastab hulgaliselt erinevat sorti makse- ja krediitkaarte. Õpilastel ja üliõpilastel on võimalik SEB EÜP-st saada pangakaarte, mis on samaaegselt ka õpilastele mitmesuguseid soodustusi võimaldavad, isikut identifitseerivad (mh on kaardil omaniku pilt) ja tema õpilase staatust kinnitavad ISIC kaardid.

Taolistele pangakaart/ISIC kaartidele on SEB EÜP paigutanud ISO 14443 standardi kohased Mifare Atmeli RFID tagid, mis

- Väljastavad lugejale 4-baidise seerianumbri (3 sisubaiti + 1 kontrollbait) (mitte isiku ID) ja

täiendavat informatsiooni RFID mälust (kokku kaardil üks kilobait mälu).
- Võimaldavad osade andmeareaalide krüpteerimist.
- Võimaldavad krüpteeritud sidet kaardilugejaga.

Kaardile lisatud RFID tagid ei ole seotud kaardi muude võimalustega, muuhulgas ei ole nende RFID tagide abil mitte kuidagi võimalik läbi viia pangaoperatsioone. Tage saab kasutada kaartide identifitseerimiseks, analoogiliselt eelmises peatükis kirjeldatud pääslasüsteemidega, sellisena on tegemist lihtsalt täiendava, sõltumatu funktsionaalusega, mis on kaardile lisatud (kaardil seega kolm funktsionaalsust: pangakaart, ISIC kaart, RFID tag).

Kaardile on kantud omaniku nimi, sünnipäev, ISIC number, kooli nimi, kirjutamisaeg, kaardi ID.

Pääslasüsteemid ongi olnud nimetatud SEB EÜP RFID-ga varustatud ISIC kaardi pilootrakenduseks. Konkreetselt kasutab neid kaarte Gustav Adolfi gümnaasium Tallinnas, kus nimetatud kaartide abil on realiseeritud kaks rakendust:
- Kooli sisse- ja väljapääs (pääslasüsteem) ja sisenemiste- väljumiste registreerimine, võimaldamaks koolil ja vanematel jälgida õpilaste kooliskäimist.
- Sööklakülastuse käigus söömise registreerimine, mille alusel hiljem söögi eest makstakse. Tegu ei ole niisiis pangakaardi funktsionaalsusega seotud maksevõimalusega, vaid lihtsalt registreerimisega RFID kaardi abil.

Nimetatud RFID-l olevad andmed on kaitstud/avatud järgmiste põhimõtete alusel:
- Osa andmeid RFID-l on kaitstud kirjutamisparooliga mida omavad TRÜB kui kaartide valmistaja ning Idnetwork kui süsteemi autor. Paroole saab uuendada enne iga uue partii valmimist.
- Falck piletikontrolörid omavad parooli osade andmete lugemiseks kaardilt.
- Pääslasüsteemi lugejad ei kasuta paroole, loevad ainult kaitsmata andmeid, kaardi ja lugeja vaheline side krüpteerimata, kaart ei tuvasta ka terminali.

SEB EÜP töötaja hinnangul oli süsteem vastuvõtt Gustav Adolfi Gümnaasium positiivne, samuti soovitas ta perspektiivis analoogiliste süsteemide sisseviimist teistessegi koolidesse, mis, liidestatuna näiteks E-kooli süsteemiga, võimaldaks lapsevanematel kergemine kontrollida laste kooliskäimist.

Juhime siinkohas tähelepanu, et potentsiaalse ID-kaart+RFID kaardi kombinatsiooni peamised jälitusvõimaluse-ohud on vähemalt samavõrra olemas juba praegu ka SEB EÜP ISIC + RFID kaardi kombinatsioonil.

3.3 Ühistransport

Kuivõrd ühistranspordi problemaatika on sisuliselt sarnane pääslasüsteemide problemaatikaga, ei hakka me seda valdkonda eraldi pikemalt käsitlema. Juhime tähelepanu järgmistele asjaoludele:

Nagu varem mainitud, on ühistranspordis ID-kaardi kasutamine Eestis peamine krüpteerimata, PIN-I vaba laiatarbe-funktsionaalsus ID kaardile. Juba lähiperspektiivis on näha vajadust asuda ühistranspordis kasutama ka RFID-kaarte. RFID on perspektiivis vältimatu näiteks maakonnaliinidel kaardipõhise maksesüsteemi sisseviimisel. ID kaardi kasutamine RFID-ga varustatult selles kontekstis

võimaldaks kaardikasutust tarbijatele oluliselt mugavamaks ja odavamaks teha.
Ühistranspordisüsteemis piisab miinimumtasemel ka sellest, kui kaardil on laiatarbe seadmete poolt loetav unikaalne ID, mis ei pea tingimata olema isegi seotud isikuandmetega: ka anonüümne unikaalne ID ja konkreetsete sõiduõiguste mitte kaardile kirjutamine, vaid serveri andmebaasis hoidmine on piisav funktsionaalsus.

Teiseks, maailmas on RFID põhised sõidukaardid juba preagu väga levinud ning nende levik üha laieneb. Maailmas levinumatest süsteemidest märgime ära Octopus süsteemi (vaata http://en.wikipedia.org/wiki/Octopus_card) ja Euroopas enimkasutatud Calypso süsteemi (vaata http://en.wikipedia.org/wiki/Calypso_%28RFID%29).

3.4 Maksekaardid

RFID-i kasutamine pangastandarditele vastava maksekaardina ei ole töö kontekstis kuigi oluline teema, kuna taolise funktsionaalsuse lisamist ID-kaardile peame vähetõenäoliseks. Juhime lihtsalt tähelepanu kahele aspektile:
Esiteks, krediitkaardi firmade Visa ja Mastercardi ettevõttel on loodud piiratud (mikro)makseteks sobiv EMV standard ja süsteem. Visa on andnud välja (kuigi mitte Eestis) hulgaliselt pangakaarte, kus taoline RFID funktsionaalsus on olemas ja Visa seisukohast piisavalt turvatud. Soovitame vaadata EMV konsortsiumi portaali www.emvco.com

Teiseks, perspektiivis on väga tõenäoline selle protsessi edasiminek, RFID lisamine uutele pangakaartidele ka eestis, samuti EMV standardiga sobivate kaardilugejate levik. Seega on perspektiivis oluline, et EMV standardi järgseid maksekaarte lugeda suutvad RFID lugejad suudaks – vähemalt riistavara mõttes – lugeda ka ID kaardile potentsiaalselt lisatavat RFID tagi.

3.5 E-pass ja tema võimalik laiendus Eesti ID-kaardile

E-passist kõneldakse käesolevas töös mitmes peatükis, eri kontekstides. Anname siinkohal tervikliku lühiülevaate süsteemist ja tema juurutusest Eestis, samut potentsiaalsest laiendusest ID kaardile. Informatsiooni osas Eesti E-passi (ja potentsiaalse laienduse osas ID-kaardile) kohta toetume intervjuudele Sertifitseerimiskeskuses ja eeskätt intervjuule Kodakondsus- ja Migratsiooniameti vastava eriala spetsialisti, Ivar Jungiga.

E-passi all peame üldisemalt silmas passe (ja ID kaarte), millel on passiandmeid sisaldav RFID tag, mis siis võimaldab passiandmeid RFID lugeja abil kontaktivabalt lugeda. Maailmas on E-passe väljastanud suhteliselt paljud riigid. E-passi funktsionaalsust sisaldaval passil on esikaanel paremal nähtav tingmärk.

E-passide kasutuselevõtu soov on osaliselt tingitud USA murest terrorismiohu osas, samuti lennundusfirmade soovist tõhustada ja efektiviseerida passikontrollimisprotsesse lennujaamades.

Euroopa liit kas näeb oma liikmesriikide passidel taolise funktsionaalsuse otseselt ette või peab seda tungivalt soovitavaks. Euroliidu riigid on kõik taolised passid juba sisse viinud või kohe viimas.

Muuhulgas varustatakse ka Eestis alates 2007 kevadest väljaantud passe RFID tagiga, mis realiseerib E-passi funktsionaalsust.

Euroopa liidu vastavat suunist saab eestikeelsena lugeda järgmisest failist:

http://ec.europa.eu/justice_home/doc_centre/freetravel/documents/doc/c_2006_2909_et.pdf

3.5.1 Andmed E-passis ja nende lugemine

E-passi kontekstis kõneldakse Eestis ja mujal tihti "biomeetrilistest andmetest". Konkreetselt peetakse seejuures silmas inimese digitaalkujul fotot, lähiperspektiivis ka sõrmejälgi.

Kõik euroopa liidu e-passid ja enamus teiste riikide e-passe kasutavad andmete hoidmiseks, lugemiseks ja turvamiseks sama standardit. Standard koosneb kahest sõltumatust osast:

- RFID tagi tüübist: kasutatakse ISO 14443 tüüpi tage, variante A ja B (eesti e-pass võimaldab kasutada mõlemit). Sama tagitüüpi kasutatakse maailmas ka paljudes teistes nn smartcard RFID rakendustes, nagu näiteks pangakaartides ja ühistranspordi piletites.
- Kaardile kantud info kodeeringust ja krüpteeringupõhimõtetest: kasutatakse rahvusvahelise tsiviillenduse organisatsiooni (ICAO) standardit. See standard on siis sisuliselt E-passi spetsiifiline.

Eesti e-passile on vastavate standardite alusel kantud passis trükituna näha olevad andmed, samuti digitaalsel kujul passipilt.

Kõik andmed on krüpteeritud RFID tagis oleva kompleksse krüptoprotsessoriga: ilma võtit teadmata on tagi poolt lugejale väljastatav info sisuliselt juhuslik müra (vastusinfo muutmiseks lugemiskordade vahel kasutab tagi protsessor juhuslike arvude generaatorit). Mingit unikaalset, muutumatut ID numbrit võtit mittevaldavale lugejale tag ei väljasta.

Dekrüpteerimise võtmeks ICAO standardi järgi passis olev masinloetav, mittelektrooniline, trükitud alas olev informatsioon: seega ei saa passi rfid-s olevat isikuinfot ei saa lugeda muidu, kui ei ole enne teada passis mitte-elektrooniliselt kirjas olevat informatsioon. e-passi lugejad on reeglina komplektis visuaalse masinloetava ala lugejatega.

Taolist ligipääsukontrolli nimetatakse BAC (Basic Access Control). Muuhulgas on RFID-l olevad andmed ka krüpteeritud: 4096 bitise RSA võtmega, mis välistab nende suvalise muutmise.

On olemas ka vabavaraline teek ja rakendus ICAO standardi järgsete passide lugemiseks: selle võib rfid-lugejaga ühendada igaüks, vt http://www.waazaa.org/wzpass/

Osa e-passi väljastavaid riike lisab passi kaane sisse varjestava fooliumi, mille tõttu passi RFID tagi saab lugeda ainult juhul, kui pass on avatud. Eesti passile taolist varjestust lisatud ei ole, pass on loetav ka kinnisena (muidugi eeldusel, et võti on passist enne välja loetud/teada).

Eesti e-pass ei sisalda hetkel sõrmejälgi, kuid sõrmejälgede perspektiivne passis hoidmise nõue on kas Euroliidu või Schengeni organisatsiooni poolt antud, ning vastavate Euroliidu standardite lõpliku valmimise järel käivitab KMA projekti, mille järel varustatakse edaspidised passid juba uute, modernsemate RFID tagidega, ning lisatakse tagi infosse ka sõrmejälgede digipildid.

Sõrmejälgede lugemise krüptograafiline kaitstus saab olema tugevam, kui seniste infoväljade kaitstus. Rakendatakse asümmeetrilise võtme krüptograafiat, lugejal peab olema lugemiseks võti, mida passist endast välja lugeda enam ei saa. Võõrriikide vastavatele asutustele antakse vajalik võti ainult nende taotluse alusel.

Taolist ligipääsuskeemi nimetatakse laiendatud juurdepääsu kontroll (EAC: Extended Access Control): nii lugeja kui RFID autendivad teineteist vastastikku, erinevalt lihtsamast BAC-s (vt varasemaid lõike), mille järgi saab RFID-i lugeda suvalise lugejaga, kui lugejal on teada RFID-i krüptovõti.

Nagu mainitud, sõrmejälgede salvestamise/krüptokaitse standard ei ole päris lõplikult valmis, kuid peaks valmis saama lähiajal. Saksamaal on juba käivitatud sõrmejälgede passis hoidmise projekt, mis baseerub mainitud standardi eelversioonile: antakse välja e-passi 2 tüüpi biomeetriaga; nägu ja 2 sõrmejälge. Kasutatakse laiendatud juurdepääsu kontrolli (EAC). Piloodiks on nende passide kontrollimine piiripunktides.

3.5.2 Eesti ID-kaart ja RFID

Eesti ID-kaart on mitmeti sarnane passile: talle on kirjutatud sarnased isikut identifitseerivaid andmed, kaardil on pilt, tal on sarnane optiliselt masinloetav riba.

Erinevalt passist on ID-kaardil kontakt-mikroprotsessor, mis

- sisaldab samu isikuandmeid digitaalselt ja krüpteerimata, kaardilugejaga vabalt loetavaid;
- sisaldab tuge (sh krüptograafia-arvutusi tegevat mikroprotsessorit) avaliku võtme krüptograafiale, seotuna PIN koodidega: selle funktsionaalsuse abil saab kaarti kasutada turvaliseks, mittekopeeritavaks identifitseerimiseks (näiteks internetipankades), samuti digiallkirja andmiseks (näiteks digiDoc portaalis). Kumbki rakendus nõuab kasutajalt PIN koodi sisestamist, PIN kood liigub kasutaja arvutist ID-kaardi sees olevasse mikroprotsessorisse, mis siis teostab vajalikud arvutused.

Väljapool kasutaja autentimist ja digiallkirja võimaldamist kasutatakse Eesti ID-kaardi elektroonilist funktsionaalsust praegu kõige rohkem Tallinna ja Tartu ühistranspordis, kus on realiseeritud ID-pilet. Viimane kujutab endast keskserveris olevat andmebaasi, kus isikukoodidega on seostatud vastavad sõiduõigused, enamasti teatud tüüpi kuukaardid. Sõiduõiguse kontrollimisel kasutatakse ID-kaardi lugejaid selleks, et kiiresti ja mugavalt tuvastada reisija isikukoodi: ID-kaart ise ei sisalda mingit infot sõiduõiguse kohta. Isikukoodi lugemine kontaktiga seadmes on, nagu eespool mainitud, krüpteerimata ja kõigile vaba, PIN koodi sisestada ei tule.

Lähiperspektiivis on nii Tallinna linnal kui süsteemi haldaval Sertfitseerimiskeskusel plaanis ID-pileti kasutusala laiendada, nii teatri-, kontserdi- kui muuseumipiletite võimaldamiseks sama põhimõtte alusel.

Tehnoloogiliselt ja organisatoorselt oleks täiesti mõeldav ka Eesti ID-kaardi täiendamine RFID tagiga. See laiendus täidaks lähiperspektiivis eesmärki:

- ID kaardi kasutamine analoogiliselt E-passiga reisimisel, juhtudel, kus nõutakse reisidokumendi elektroonilist loetavust. Praegust kontaktiga ID-kaarti teiste riikide piirikontrollisüsteemid reeglina ei loe.
- ID kaardi mugavam kasutamine ID-piletina: kaardi lugejasse sisestamise asemel saaks ta panna lihtsalt lugeja vastu või lähedale, mis samamoodi loeks omaniku isikukoodi või muud hädatarvilikku identifikaatorit (ei pea olema isikukood!)
- ID kaardi kasutamine pääslates ja muudes rakendustes, kus praegu kasutatakse või plaanitakse kasutada isikut identifitseerivaid RFID tage.

Esialgsed kavad RFID tagi paigutamiseks uue põlvkonna ID-kaartidele olid olemas juba 2006 sügisel, kuid tol hetkel ei tunnetatud selget vajadust äsjamainitud funktsionaalsuse järele, ning arvestades tekkivad turvaprobleeme ja suuremat ID kaardi hinda jäeti kavad välja arendamata.

Juhul, kui soovitakse ID kaarti edaspidigi reisidokumendina kasutada, kasvõi ainult Euroliidus, võib osutuda vajalikuks E-passi funktsionaalsuse lisamine ID-kaardile.

Siseriiklikuks tarbimiseks E-passi funktsionaalsusel ID-kaardil mõtet ei ole, kuna E-passi andmete lugemine on võimalik ikkagi ainult optiliselt masinloetava riba lugemisel, mis on oluliselt keerukam, kui olemasoleva kontakt-mikroprotsessori kasutamine.

Seega oleks RFID tagi lisamine ID kaardile mõtestatud eeskätt juhul, kui tagi saaks kasutada näiteks pääslates ja piletisüsteemides harilike RFID lugejatega. Niisugune võimalus oleks ühest küljest väga mugav – paljude erinevate pääsla- ja piletikaartide asemel saaks kasutada sedasama ID kaarti, tekitab aga teatud turvariski eeskätt jälitusvõimaluse osas: ID kaart on inimestel üldjuhul kogu aeg või enamik aega kaasas, ID kaardi RFID tagile kantud informatsiooni saaks suhteliselt lihtsalt seostada isikuga.

Turvaküsimuste detailsem ülevaade antakse käesoleva töö ülejärgmises peatükis. Tööd lõpetavates soovitustes antakse ideid RFID tagi ohutuma lisamise võimaldamiseks ID kaardile, mis meie hinnangul on põhimõtteliselt võimalik, kuid nõuab tähelepanu ja läbimõeldust.

4. Detailsem ülevaade RFID tehnoloogiatest

Järgnev ülevaade fokuseerub RFID baastehnoloogiatele, grupeerituna sagedusalade kaupa.

4.1 ulRFID tehnoloogiad

Meeldetuletuseks: RFID tehnoloogia puhul toimub objektide identifitseerimiseks kasutatava informatsiooni edastamine raadiosagedusliku elektromagnetilise sidestuse abil. Tüüpiline RFID süsteem koosneb lugejast (ingl. k. "reader" või "interrogator") ja märkidest (ingl. k. "tag", "transponder" või "label").

Erinevad RFID süsteemid töötavad sagedusvahemikus 100 kHz kuni 5,8 GHz, töösagedus määrab süsteemi peamised omadusedkusjuures töösagedusest olenevad ka süsteemi omadused, vastavad ISO/IEC klassifikaatorid on järgmised:

- 18000-2 < 135 kHz madalsageduslik
- **18000-3 13,56 MHz kõrgsageduslik**
- 18000-6 860-960 MHz ülikõrgsageduslik
- 18000-7 433 MHz ülikõrgsageduslik
- 18000-4 2,45 GHz mikrolaine
- 18000-5 5,8 GHz mikrolaine

Valdav enamus kasutatavatest märkidest on "passiivsed", st. neil puudub sisemine toiteallikas ning need tarbivad lugeja poolt tekitatava elektromagnetvälja energiat, st passiivne märk on töövõimeline (andmetöötlus, andmeedastus) ainult lugeja elektromagnetväljas. Aktiivsetel ja semipassiivsetel märkidel on sisseehitatud energiaallikas või energia kogumise süsteem ning need on töövõimelised ka ilma lugejapoolse ergutuseta.

- Olukordades, kus ei ole vaja objekti pidevalt jälgida (s.h. inimeste identifitseerimisrakendustes) kasutatakse reeglina passiivmärke.
- Passiivtehnoloogi korral on märgi andmevahetuskaugus 1 cm kuni 10 m sõltuvalt tehnoloogiast, kuni 15MHz korral on keerukas märki aktiveerida kaugemalt kui 1m.
- Aktiveeritud märgi ja lugeja vahel toimuvat kommunikatsiooni saab pealt kuulata kümnete meetrite kauguselt.
- Kõiki RFID märke saab varjestada metalli ja näiteks fooliumiga.

Üks põhjalik RFID standardeid käsitlev nimekiri on on avaldatud allikas [5]. Andmevahetus märgi ja lugeja vahel võib olla ühesuunaline - ainult märgis sisalduva koodi lugemine kui ka kahesuunaline - märgi mälusse saab lugeja kaudu salvestada andmeid (ja neid muuta). Andmevahetus lugeja ja märgi vahel võib toimuda nii avatud kui ka krüpteeritud kujul.

Piirangud töösageduste ja lugeja kiirgusvõimsuse suhtes on määratud piirkondlike raadioeetri piirnormatiividega (Euroopas ETSI, USA-s näiteks FCC standardid) ja inimesele ohutu kiirgutasemega (näiteks standardid IEEE C95.1-1991 ja BS EN 50357, BS EN 50364, EN 300 330, FCC 47 CFR osa 15.209) [3, 4]. Lihtsustatult, ülikõrgsagedustehnoloogia korral on maksimumvõimsuse piirajaks eetrinormatiivid, suure töökaugusega (1 m ja rohkem) kõrg- ja madalsagedustehnoloogia korral

ohutuspiirangud.

4.2 Ülikõrsageduslik ja mikrolaine RFID: logistika ning pääslasüsteemid

Ülikõrgsageduslik (ÜKS) passiivne RFID tehnoloogia on optimaalne rakendustes, mis eeldavad tegevuskaugust üle 0,5 m, või kus märgi madal hind on esmatähtis – eeskätt logistikas. Praktikas levinud standardid on ISO 18000-6B (tähtsuselt kahanev) ja ISO 18000-6C (valdav). ÜKS RFID töösagedused on valitud suurima lubatud võimsusega vabakasutuspiirkondadesse, peamiselt vahemikku 860-960MHz (Euroopas ETSI EN 302 208, 865-868MHz, 2W ERP ja EN 300 220-1, 869.4-869.65MHz, 0.5W ERP, USA-s FCC osa 15 sektsioon 247 902-928MHz, 4W EIRP (ehk 2.4W ERP). Nimetatud saatevõimsustel on võimalik märgi tuvastamine kuni 10 m kauguselt. 433MHz ja mikrolaine piirkondades on lubatud saatevõimsus väiksem, seetõttu ka kasutatakse neid vähem, ülemaailmselt aktsepteeritud standardid puuduvad. Kuna ÜKS RFID eesmärgiks on märgi minimaalne omahind, hetkel ca 0,5-1 kr ja sellest tulenevalt ka minimaalne keerukus, siis hetkel kasutatavad sideprotokollid krüpteeritud sidet ei võimalda. Suure sidekauguse tõttu on ÜKS RFID märkide pealtkuulamine suhteliselt lihtne. Samuti võib kergesti ette kujutada teenuste mittevajalikku aktiveerumist kauglevi tõttu. Vähemalt lähiaja perspektiivis (3-5 aastat) ÜKS RFID kasutuselevõtt kriitilistes turva-, pääsla- ja makserakendustes ei ole tõenäoline. Võimalikud on mittekriitilised pääslarakendused, näiteks haiglauste juhtimine, kuid on raske näha RFID eelist tavapäraste liikumisandurite ees.

4.3 Madalsageduslik RFID: pääslasüsteemid

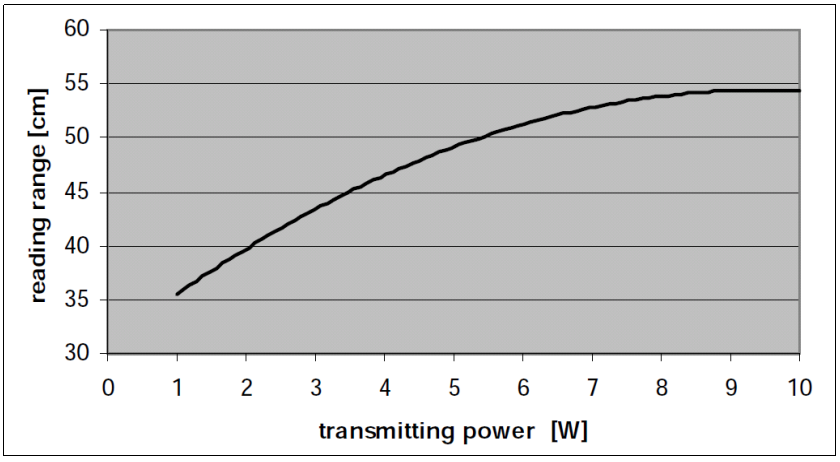
Madalsageduslikud RFID süsteemid (ISO 18000-2) töötavad sagedustel alla 135 kHz, (enimlevinud sagedused 125 kHz ja 134,2 kHz), selle tehnoloogia peamised rakendused on pääslasüsteemid (nn levinud proxi kaardisüsteemid), autouste automaatse avamise lahendused ja loomade nahaalune märgistamine. Madalsagedusliku tehnoloogia eeliseks võrreldes kõrgsageduslike ja ülikõrgsageduslike süsteemidega on väiksem tundlikus ümbritseva keskkonna mõjutustele, madal kiirgussagedus on inimesele ohutum. Kuna tehnoloogia on tootmises ca 15 aastat, on seadmed (lugejad) odavad – umbes 1000 krooni. Puudusteks võrreldes kõrgsagedusliku tehnoloogiaga (13,56 MHz) on suurem antennipooli keerdude arv (s.t. keerukam ja põhimõtteliselt kallim märk), väiksem andmevahetuskiirus (tavaliselt 1-4 Kbaud) ja mõnevõrra väiksem tööraadius - tüüpiliselt 2-5 cm („proximity“) ja suurema lugemiskaugusega ("vicinity") süsteemides kuni 1 m (magnetvälja tugevuse piirang, nõuab lugejalt kiirgusvõimsust ca 20-40W). Märgi hind on 20-50 krooni, lugeja hind alates 1000 kroonist. Suhteliselt kõrge märgihinna tõttu on selge tendents pääslaseadmete turul asendada madalsageduslik tehnoloogia kõrgsageduslikuga. Krüpteeritud sidet ei kasutata. Madalsageduslikku RFID-d reeglina ei kasutata makse- ja kõrge riskiastmega identifitseerimissüsteemides. Madalsagedusliku märgi (salajaseks) kauglugemiseks (üle 1 m) on tarvis lubatud kiirgustaseme piirnormatiive ületavat seadet võimsustarbega alates 100W.

4.4 Kõrgsageduslik RFID: pääsla- ja maksesüsteemid

Kõrgsagedusliku (KS) RFID (Contactless Smart Card) töösagedus on 13,56 MHz. Kõrgsageduslik

RFID kogub populaarsust pääslarakendustes, seoses tehnoloogilistel põhjustel saavutatud madalama märgi hinnaga (ca 10-17 kr/tk, ka väikestes kogustes). Hetkel on siiski 13,56 MHz lugejad ca 2-3 korda kallimad kui madalsagedusliku tehnoloogia seadmed, näiteks Idesco Access 7C lugeja maksab 250 EUR, analoogiline 125kHz seade 100 EUR [6], majanduslikku põhjendust sellel pole ning hinnad eeldatavasti võrdsustuvad 2-3 aasta jooksul. 13,56MHz töösagedusel kasutatakse kahte peamist andmeedastusprotokollide perekonda: ISO 15693, ISO 14443, mis kasutavad identset füüsilist signaliseerimiskihti ning seega on loetavad sama riistvaraga. Valdav enamus kõrgsagedusliku RFID lugejaid ka toetab mõlemat standardit. ISO 15693-2,3 (sertifitseeritud juba 1999) on välja töötatud kontaktivabade pääslakaartide jaoks (madalsagedusliku proxikaardi asendusena), selle andmevahetusprotokoll on lihtne ja ei toeta krüpteeritud sidet ega kommunikatsiooni kahe aktiivseadme vahel. Erinevad tootjad kasutavad kaubamärke TagIT (Texas Instruments (TI)), ICode (Philips). Tänu robustsusele ja suhteliselt madalale andmeedastuskiirusele 26 kbs tagab ISO 15693 hea töökindluse ja sidekauguse. Tegevuskaugus sõltub saatevõimsusest, ja mõlema antenni (lugeja, märk) suurusest. TI andmetel on võimalik saavutada tegevuskaugus 120 cm, kui krediitkaardi suurune märk on kahest antennist formeeritud väravas. Ühe lugejaantenniga (80x60cm) ja saatevõimsusega 10W on võimalik tootja andmetel saavutada tegevuskauguseks 80 cm krediitkaardi suuruse märgi korral. Kui mõlema antenni mõõdud suurenevad, kasvab ka tegevuskaugus ligikaudu ruutjuurga mõõtmete kasvust. 10W ergutusvõimsus on saavutatav laiatarbekasutuses olevate seadmetega, näiteks Texas-Instrument S6500 Long Range Reader Module, või firma Feig seadmetega, mis tarbivad tööolukorras võimsust ca 50-60W ja maksavad ca 1000 EUR. On oluline, et kirjeldatud seadmestikku saab põhimõtteliselt kasutada ka ISO 14443 märkide (pahatahtlikuks) kauglugemiseks.

Joonisel 1 on toodud autorite partnerite INRIA-Rennes (Prantsusmaa) mõõtetulemused 45x76mm ISO 15693 märgi tegevuskauguse kohta sõltuvalt saatevõimsusest kasutades 32x33cm Texas-Instrument antenni (ref. RI-ANT-T01A).



Joonis 1: ISO15693 „vicinity“ märkide tegevuskaugus sõltuvalt saatevõimsusest

ISO 14443 märke kasutatakse lühikese tegevuskaugusega (2-10 cm) käsilugejarakendustes ergutusvõimsusega 0.1-0.2W, lugemiskiirus on 106-424 kbs. ISO 14443 on standard, mida kasutatakse nii pääslasüsteemides, RFID loetavates passides ning maksekaartides. ISO 14443 A ja B erinevus on füüsilises kihis, täpsemalt modulatsioonisügavuses. ISO 14443 on paremini spetsifitseeritud Mifare sideprotokollide perekonnaga (ISO 14443A implementatsioon, mille teostas Philips, nüüdne NXP), tagavad andmevahetuskiiruse kuni 424 kbs ning toetavad krüpteeritud sidet. Olemasolevad alamperekonnad Mifare Standard 1K/4K, Mifare DESFire, Mifare UltraLight, Mifare SmartMX. Mifare Standardis kasuitatakse sideprotokolli T=CL, mis erineb ISO 14443-4 standardist. ISO 14443A (Mifare) on kahtlemata enimlevimud standard, ISO 14443B märke toodavad Atmel jt, see on vähemlevinud. Võrreldes ISO 15693 protokolliga on ISO 14443 keerukam ning võimaldab kahesuunalist sidet. Vastavaid märke kasutatakse laialdaselt

- ravimite märgistamisel,
- ühistranspordisüsteemides, kuuldavasti lähiajal ka Moskvas,
- krediit- ja maksekaartides,
- kontaktivabaks andmeedastuseks mobiiltelefonide ja makseterminalide vahel.

Tuntumad RFID maksekaardi tehnoloogia brändid on Jaapanis: FeliCa. ISO 14443 RFID võimalusega maksekohtade arv aastal 2006 oli Jaapanis ca 20000.

ISO 14443 tehnoloogia

Eksisteerivad lahendused kasutavad valdavas enamuses Philips/NXP Mifare mikroskeeme. Kõrgete turvanõuete korral kasutatakse järgnevaid:

Mifare Standard 1k, 4k märkide andmeala on jagatud blokkidesse, pöördumisõigus individuaalsetele blokkidele määratakse vastavalt võtmele, mida lugeja kasutas ühenduse loomisel. 1k, 4k kirjeldab kiibi mälumahtu kilobaitides. Mifare Standard kiibid ei sisalda rakenduste kontrollerit.

Mifare DESFire märgid omavad 56 bitilist unikaalset ID-d ja on failisüsteemi struktuuriga: kuni 28 rakendust märgil, kuni 32 faili rakenduse kohta, 14 erinevat võtit rakendustele, lisaks võtmed järjekorranumbriga 15 ja 16: 0xE – kõigile avatud rakendus ja 0xF – kõigile keelatud rakendus. Mälumaht DESFire kiipidel on 4 kilobaiti, andmevahetuskiirus kuni 424 kbs. Sisaldab PKI ko-protsessorit.

SmartMX on Mifare uusim perekond, mis sisaldab mikrokontrollerit ja mille mõned mikroskeemid vastavad CC EAL5+ turvanõuetele. C51 mikrokontrolleri käsustikuga ühilduvad komponendid toetavad RSA, ECC, dual/triple key DES ja AES (sisaldab PKI ko-protsessorit). Olemas kaksikinterfeisidega mikroskeemid: ISO 7816 kontaktliides (1 Mbs) ja ISO 14443A 13.56MHz RFID liides (800 kbs), 4096 baiti RAMi. Rakenduste ja turvatehnika struktuur sarnane nagu Mifare DESFire-l, (mõnede allikate kohaselt on DESFire eelprogrammeeritud süsteemitarkvaraga SmartMX). Toetatud avaliku võtme lahendused RSA, El'Gamal, DSS, Diffie-Hellmann, Guillou-Quisquater, Fiat-Shamir ja elliptiline. SmartMX toetab nii ISO 14443-4, T=CL (Mifare 1k, 4k) protokolle ja kasutaja poolt defineeritavaid protokolle (kasutades sisseehitatud C51 mikrokontrollerit).

Kuna Mifare mikroskeemid kasutavad: a) lihtsamal juhul erinevate salasõnadega kaitstud mälualasid, b) erinevate salasõnadega kaitstud rakendusi ja seotud faile, on võimalik luua lisafunktsioonidega ID-kaart põhifunktsionaalsuse turvalisust vähendamata (erineva informatsiooni hankimiseks kaardilt saab

kasutada erinevaid salasõnu).

Mifare/ ISO 14443A edasiarendus on NFC (Near Field Communication) standard, mis võimaldab sidet kahe aktiivseadme (ehk RFID aktiivmärgi), näiteks mobiiltelefoni, vahel. NFC protokollistandardid on NFC IP-1 (ECMA 340), ISO süsteemis tuntud kui ISO 18092. NFC standardit kasutatakse mobiiltelefoni kasutamisel maksevahendina ja pääslakaardina. Konkreetse NFC realisatsiooni turvalisus on määratud konkreetse realisatsiooniga, see ei ole ilmselt väiksem kui MobiilID lahenduse korral, sest sertifikaate hoitakse samal SIM kaardil.

4.5 Kõrgsageduslik RFID: ePass ja ID kaart

Biomeetriliste andmetega ePass peab vastama ICAO 9303 ePassport standardile, mille füüsiline kommunikatsioonikiht põhineb ISO 14443. Minimaalne andmemälu on 32kB, erinevaid andmealasid kaitstakse eri turvalisusega (Extended Access Control (EAC)). Tundub, et kasutatakse mõlemat standardi A ja B versiooni. ID kaardi puhul oleks mõistlik ühilduvus olemasolevate e-passidega (Taani, Rootsi, UK, Saksamaa), mida on välja antud üle 100 miljoni. (Eesti ID kaart ei ühildu näiteks Saksamaa analoogiga.) NXP andmetel kuulub sellele firmale (Mifare tehnoloogiale) 80% e-passide turust [1]. Mifare SmartMX (80 kB versioon) on valitud kasutamiseks Saksamaa RFID passides, valiku põhjuseks on ilmselt suurim võimalik mälumaht. Kasutades *dual interface* RFID mikroskeemi on võimalik tagada ID-kaardi ühilduvus olemasolevate seadmetega (kiipkaardilugejatega).

Passide turvalisus on tagatud eeskätt krüpteeritud side ja võtmetega. Nagu märgitud, võimaldavad keerukamad ISO 14443 mikroskeemid arvestatavat krüptograafiat. Peamine e-passide turvarisk on side pealtkuulamine, varastatud salasõnaga andmete kauglugemine. Seetõttu kasutatakse minimaalset lugemisseadmestiku võimsust, passi lugemisseadmed on tavaliselt konstrueeritud kinnise kujul, mis piirab infot kandva elektromagnetvälja levikut ja takistab pealtkuulamist, siiski on ka avatud seadmeid [2].

Arcontia ARC1003-B e-passi lugeja, www.arcontia.se

Passi üks kaan sisaldab varjestavat fooliumi, st suletud passi loetavus on halvem (ei pruugi siiski võimatu olla). Nagu märgitud, ISO 14443 märke saab füüsiliselt lugeda ISO 15693 jaoks konstrueeritud seadmetega, legaalse saatevõimsuse korral on realistlik andmeid kätte saada 20-50 cm kauguselt. Andmete kontaktivaba varastamise vältimiseks soovitatakse hoida passe fooliumümbrises (ilmselt keerukam realiseerida ID-kaardi puhul). *Relaying* meetodil RFID märgi pealtkuulamise

keerukus on suurem kui kiipkaardi pealtkuulamise keerukus (hetkel kasutatava ID kiipkaardi andmevahetuse pealtkuulamiseks modifitseeritud terminali loomine on oluliselt lihtsam kui vastava RFID pealtkuulamisterminali loomine).

4.6 Kõrgsageduslik RFID: Maksekaart ja mobiiltelefon

ISO 14443A/B? standardeid kasutatakse VISA, MC/EC RFID kaardilahendustes analoogiliselt ePassile. Turvalisuse tagavad sarnaselt passidega võtmete süsteem, krüpteeritud side ja lühike kommunikatsiooniraadius. Euroopasse on jõudmas NFC toega mobiiltelefonid, näiteks Nokia 6131NFC, mis võimaldab maksekaardi funktsiooni mobiiltelefoni abil kasutades RFID kommunikatsiooni. Rakendus on sarnane MobiilID-ga, kus kasutaja turvasertifikaate hoitakse SIM-kaardil, kuid andmevahetus toimub kaupmehe NFC/RFID makseterminali kaudu. Samuti oleks põhimõtteliselt võimalik näiteks RFID ID-piletit (ID-kaarti) kontrollida suvalise RFID mobiiltelefoni abil. Valdav enamus Jaapanis turustatavaid vähemalt keskmise hinnaklassi telefone (nn. *o-saifu-keitai*) toetavad RFID pääsla ja maksefunktsiooni.

4.7 RFID tehnoloogiate lähiaastate arengusuunad

- NFC/RFID mobiiltelefonide laialdane levik Euroopas ja USAs.
- Magnetribaga ühistranspordipiletite asendumine kõrgsagedus RFID piletitega.
- Kõrgsagedus RFID maksekaartide kasutuselevõtt.
- Ülikõrgsagedus RFID märkide kasutuselevõtt kaupade märgistamisel, lugemisseadmete hinnalangus ca 500 USD-ni.
- Võimalik, et ÜKS RFID suundumine mobiiltelefoni, kui tekivad reaalsed rakendused.

4.8 Peatükis viidatud allikad:

[1] http://www.theregister.co.uk/2007/11/01/german_g2_epassport/
[2] http://www.arcontia.se/content/products.aspx?id=1
[3] "Understanding RFID Compliance Standards". A WHITE PAPER BY DATA SYSTEMS INTERNATIONAL. [WWW] http://www.dsionline.com/collateral/pdf/software/wp_RfidStandards.pdf (30.06.07)
[4] "Proof of ETSI and FCC Compliance of RFID Reader and Wake-Up Driver ICs." Atmel U2270B Application Note. 4667A-RFID-06/03. [WWW] www.atmel.com/dyn/resources/prod_documents/doc4667.pdf (30.06.07)
[5] [WWW] http://engineers.ihs.com/news/topics/rfid-standards-news.htm (30.06.07)
[6] http://www.micromade.pl/micromade/?p=cennik

5. Turvaprobleemid ja nende võimalikud lahendusviisid

Järgnev peatükk vaatleb turvaküsimusi laiemalt/pikema perspektiiviga, kui ainult e-passi standardile vastava, võimalik, et lihtsate täiendavate vahenditega varustatud RFID süsteemi probleemi. Muuhulgas vaadeldakse ka põhimõttelist võimalust kasutada taolist ID-kaarti maksevahendina ja/või anda tema abil, RFID tehnoloogiat kasutades, digitaalset allkirja.

5.1 Olulised turvalisuse murdmise stsenaariumid

Kogu järgneva turvateema kontekstis on läbivalt olulised paar turvalisuse murdmise stsenaariumi.

5.1.1 Remote replay, "kaugele taasesitamine".

Täna loetakse RFIDe turvaliseks kuna nendega suhtlemiseks tuleb neile läheneda pea isikliku kontakti piires (5cm -2 meetrit).

Samas, kaardiga võib suhelda läbi varjatud duplex raadiosaatja (eeldusel, et kaarti ergastatakse läheduses kas legaalse või salajase energiaallika poolt) ja edastada oma signaale väga kauge maa taha. Mõnede kaartide puhul piirab suhtluse protokolli ajalimiit säärase "raadiotasemel salajase pikenduse" sama asumi piiresse, mõnedel mitte. Seega, turvalisuse analüüsi mõttes võib >1000EUR väärt juhtumite puhul käsitleda RFID kaarti kui seadet, mis on omaniku taskus olles potentsiaalselt ühendatav ja kasutatav kõigi samas linnas viibivate lugejatega(terminalidega).

See tähendab, et ka kõige kõvema krüpteerimistarkvaraga kaart on "salaja ajutiselt teisaldatav" juhul, kui tema aktiveerimiseks ei kasutata isiku tahteavaldust (kas kontaktkaardi füüsilist sisestamist terminalavasse või PIN koodi sisestamist). Kui salajane lugeja paigaldatakse ohvri lähedusse, siis on lugemisvõimalus ajaliselt piiramatu. Kui ohver või seade kasutab varjestusmehhanisme, siis jäävad ikkagi etteaimatavad momendid ajas (näiteks rahakoti tõstmine ukseavamissüsteemi RFID lugeja juurde), kus kaugele taasesitamine on võimalik.

Teema pole seni olnud oluline, kuna RFIDide rakendused ei ole tüüpiliselt väga kõrge tehingu väärtusega või on vastutus/risk hajutatud muudel viisidel. See tähendab muuhulgas, et kõik kohad, kus seni on saanud end tuvastada ID kaardi sisestamise(ilma PINita) teel, peavad RFIDi lisandudes hakkama nõudma ka PIN koodi ja allkirjastamismehhanismi kasutust.

5.1.2 PIN koodi vargus.

PIN koodi vargus iseenesest on lihtne. Kõige elementaarsem on see ära lugeda kasutaja sisestamise käigus mõnes avalikus terminalis. Natuke lihtsam/keerulisem on ohvri arvutisse trooja hobuse paigaldamine. Massiliseks PIN koodide hankimiseks tuleb leida moment ja lisada teenindussaalis kaarditerminalile lutikas. Teema pole seni olnud oluline, kuna PIN koodi tarbimiseks smartcardiga

tuleb ka kaart kätte saada ja toimetada kohta kus sobival momendil tehing teostada.

5.1.3 Kombinatsioon eelmisest kahest

Eelnevad kaks koos avavad täiesti uue võimaluse - varastada PIN kood ja kasutada kaarti omaniku teadmata kus iganes(sama asumi piires) millal iganes. Teema pole seni olnud oluline RFID Smartcardide juures, kuna peamiselt kasutatakse neid panganduses ja panganduses on tehingulimiidid, hajutatud vastutus ja kontroll, mis kõik kokku teevad säärasel viisil elatise teenimise küllaltki tänamatuks.

Kui tehnoloogia kantakse kontrollimatult üle piiramatu vastutusega tehingutele (näiteks kriminaalsusi sisaldava võltslepingu allkirjastamine) ja mõõtmatu väärtusega tehinguteni (näiteks kasutaja isikuandmetele ligipääs), muutuvad need juhtumid oluliseks.

5.2 RFID kaartide kasutusloogikad

RFID kaartide laiema juurutamise strateegia valikuteks vaatleme erinevaid kasutusloogikaid, mis võiks kõne alla tulla keskse(riikliku) RFID-ID kaardi kasutusaladena.

5.2.1 Anonüümne läbipääsuseade

Kaart, mille eesmärk on olla anonüümne, või mis on anonüümne oma tehnoloogilise lihtsuse tõttu. Täiesti anonüümne seade on keerulisem, kuna tema tunnus peab olema ka juhuslik. Siia klassi kuuluvad igasugu ühekordsed ja hooajalised läbipääsuload avalike teenuste kasutamisel. Osadel kasutusjuhtudel on anonüümsus taotluslik ja nõutud eeltingimus.

5.2.2 Anonüümne maksekaart

Kaart, mille peale kantakse hulk anonüümset e-raha - sertifikaate raha omamise kohta või mis suhtleb anonüümse kontoga keskserveris. Kasutuseesmärk on mitte võimaldada müüjal ostja jälgimist.

5.2.3 Anonüümne rahakott

Anonüümne maksekaart, mis on uuesti laetav ja võib teostada teise rahakotiga rahavahetusoperatsioone ilma keskse infrastruktuuri abita.

5.2.4 Trükkimise asendaja

Turvamata ligipääsuga seade võimaldamaks kandja kohaseid andmeid arvutisse sisestada automaatselt. Siia kuulub laotarkvara ja ka e-passi üldkasutus. Juhul, kui RFID kaardi "kauge maa taha taasesitamist" võimaldavad seadeldised muutuvad kergelt omandatavateks toodeteks, siis ka ID-kaart koos oma võimaliku RFID liidesega nendes kasutustes, kus PIN koodi ei sisestata. E-pass on turvatud passist optiliselt loetava PIN koodiga ja seega kaitstum, kuid tema kasutuseesmärk on siiski vaid andmesisestuse kiirendamine(versus samade andmete otsimine võimalikust üleilmsest isikuandmebaasist), mitte kasutaja identifitseerimine.

5.2.5 Isikustatud ja kiire läbipääsuluba

Hetkel kasutatakse RFID kaarte isikustatud läbipääsulubadena (mugavusväärtusega uksesüsteemid).

5.2.6 Mehaanilise kulumiskindlusega andmeedastuskanal

RFID liidest kasutatakse suure kasutuskordade arvuga kaartide või kaardilugejate juures, kuna kontakühenduse eluiga on oluliselt lühem. ID-kaardi hind ja kontaktide eluiga on seni olnud oluline argument suure kasutuskordadega väikesemahulistes tehingutes rakendamise vastu.

5.2.7 Maksekaart

Tavaline pangakaart, kus smartcard suhtleb kas ainult või lisaks ka RFID liidese läbi. USAs juba laial levinud pangakaardina.

5.2.8 Isikustatud rahakott

Isikustatud smartcard mis opereerib e-rahaga. Hetkel laiemat kasutust ei tea. Põhimõtteliselt on sama kasutusloogika ka täna laiatarbekasutuses oleval ühistranspordi maksekaardil, kuid arvatavasti ei opereeri ta oma sisuga nii keeruliselt, kui e-raha puhul vaja oleks.

5.2.9 Digitaalallkirjastamise vahend

Eesti ID-kaart kui seadustatud allkirja andmise vahend. Pangakaart, mille kasutamisel sisestatakse PIN kood on samuti tehingut kinnitava digitaalallkirja loogikat kasutav seade.

5.3 Turvamise tasemed

5.3.1 Alati taasesitatav

Täna kuuluvad siia kaardid, mis ei kasuta krüpteerimisvahendeid ja tehingute arvu lugemist. Kasutatakse juhtudel, kui turvalisus pole oluline või info õigsuse kontroll toimetatakse sõltumatult elektroonilisest infost (mida kasutatakse info sisestamise kiirendamiseks). Oluline probleem on terminali operaatori arusaam kasutuse turvalisusest - operaator võib harimatusest eeldada, et laetav info on kaitstud. Kauge taasesitamise seadmete levides kukuvad siia klassi ka kõik krüpteerimist kasutavad RFID kaardid, mille aktiveerimiseks ei ole vaja omaniku tahteavaldust (PINi sisestamist) ja mis on raadioeetri kaudu alati ligipääsetavad.

5.3.2 Probleemidega taasesitatav

Kaardid, mille sees on tehingute (isikutuvastuste) kordade lugeja ja kaardikasutusel on keskne andmebaas kus statistiliste või loogiliste meetoditega tuvastatakse kahtlaseid kasutusi, tõstes sellega pahatahtlikul taasesitamisel vahelejäämise riski.

5.3.3 lugeja tuvastab kaardi

Kaardid, mille turvalisus põhineb lugeja teadmisel, milliste sertifikaatidega kaarte usaldada. Kauge taasesitamise seadmete levides muutuvad need kaardid alati (kohati) salaja taasesitavateks.

5.3.4 lugeja ja kaardi vastastikune tuvastus, krüpteeritud side

Kaardid mille turvalisus põhineb vastastikusel tuvastusel. S.t. ka kaart teab, milliste sertifikaatidega lugejat usaldada. Nende kaartide probleemiks on lugeja sertifitseerija sertifikaadi kompromiteerumine, kompromiteeritud terminalide/kaartide eiramise võimatus ja kauge taasesituse võimaluste avardudes ka alati taasesitatavus.

5.3.5 lugeja ja kaardi vastastikune tuvastus, krüpteeritud side, PIN sisestamine

Kaardid mille turvalisus põhineb vastastikusel tuvastusel ja sellele järgneval kasutaja tahteavaldusel. Nende kaartide probleemiks on, et esimese kompromiteeritud terminali kaudu PIN sisestamise järel muutuvad nad alati taasesitavateks kuni PINi muutmiseni. Siia kuulub ka E-Pass, mille PIN on optiliselt loetav passi sees. Kuna see PIN pole muudetav, siis on E-Pass peale esmast kompromiteeritud terminalis viibimist "kaugele taasesitatav" kuni oma eluea lõpuni.

5.3.6 mobiilidele lisatud RFID smartcardid

Tuleb tähele panna, et tänapäevased mobiilid ei erine eriti kasutajate koduarvutitest, sertifikaadid +krüpteerimine asuvad tüüpiliselt SIM kaardil ja PIN koodi sisestamise sõrmistik on "mobiilarvuti" järjest lihtsamini asendatava ja kompromiteeritava tarkvara kontrolli all. Samas on see tõenäoliselt kõige turvalisem RFID kasutusrakendus mis lähiajal laialdast praktilist kasutust leiab.

5.3.7 Kaart ja lugeja tuvastavad teineteist vastastikku ja kontrollivad on-line teineteise kehtivust

Siia kuuluvad patareitoite ning infokanaliga varustatud seadmele lisatud smartcard+RFID moodulid. Kuna seadmed on suuremate gabariitidega, siis eeldame, et neil on enamasti peal ka turvalisemate rakenduste tarbeks kasutaja tahteavalduse sisestamise vahendid (PIN sõrmistik) ja seega nad ei ole "kaugele taasesitatavad". Siia võiks kuuluda võimalikud erilahendused isikutuvastuseks ja ka mobiiltelefonid, millel on eraldiseisev, tarkvaraliselt juhitamatu smartcard+RFID.

5.3.8 PINiga varustatud seade

Põhimõtteliselt on tänasel tehnoloogia tasemel võimalik ka toota traditsioonilises plastikkaardi gabariitides arvuti, mis nende operatsioonidega hakkama saab, omades puutetundlikku sõrmistikku PIN sisestamiseks ja kontrollides terminali kehtivust keskserverist läbi sama terminali võimaldatud võrguühenduse. Selle taseme seadmed on ka ainukesed mis on jätkusuutlikult sobivad piiramatu ja määramatu vastutusemääraga tehingute teostamiseks, kuid on majanduslikus plaanis ebarealistlikud.

5.4 Ühiskondlik mõõde

Kui ID-kaart on veel inimesele subjektiivselt kuidagi "oma kontrolli all", siis RFID kaart ei ole seda enam isegi näiliselt mitte. Ühiskonna vastuvõtlikus selles küsimuses ei ole prognoositav.

Inimesi kulutatakse liigse tehnoloogiaga. Iga muutus ja lisanduv võimalus/seade nõuab paratamatult inimestelt lisatähelepanu ja õppimist. Tuleks kaaluda, kas väheste inimeste kaardikasutus kaalub üles paljude mittekasutajate tähelepanu mõttetu kulutamise. Soovitav oleks kaaluda eraldiseisva mini-ID kaardi loomist mini ja mikrotehinguteks, sel juhul võiks kasutus hüppeliselt suureneda ja kaardiomaniku õppimis/tähelepanu vajadus, personaalne vastutus ja risk väheneda tasemeteni, kus keskmise kodaniku tulu ja kulu koguprotsessist on adekvaatses seoses.

RFID kaartidel on tuleviku ühiskonda oluliselt muutev roll. Kindlasti saab iga inimene paari RFID kaarti oma rahakotis kandma. Seega pole küsimus riikliku standardiseeritud RFID liidesega kaardi tekkimisest mitte kas, vaid millal.

ID-kaardi kuluefektiivsus. Säärased vahendid on mõeldud elektroonse abivahendina asjaajamiskulude kokkuhoidmisel. Täna hoiab enamuse asjaajamiskulusid meile kokku panga paroolikaart või PIN-generaator. ID-kaardi tehnoloogial põhinevalt - uksekaardid ja välismaal ka reaalset masskasutust leidnud spetsialiseeritud ühistranspordi kasutuskaardid. ID-kaardi elektrooniline osa ei ole siinkohal esirinnas.

Eesti eripära digitaalallkirjanduse pioneerina seisneb väikeses riigis, poliitilises ja meediavõimekuses suruda läbi tehnoloogiliselt küsitavaid projekte ja riigisiseses suures sotsiaalses sidususes, mis võimaldab sääraste projektide, maailma mõistes pilootprojektide, vigu parandada ilma suuremate mainekahjustusteta. See ei ole jätkusuutlik lähenemine - esialgne kulude kokkuhoid ja tehnoloogiate enneaegne rakendamine võivad toota hiljem probleeme. Kogemuse ülekandmine suurema rahvaarvuga ja/või väiksema sotsiaalse sidususega maadesse võib osutuda vastutustundetuks.

Tänane sertifitseerimise infrastruktuur eeldab, et kõik üht tüüpi kaardi kasutajad peavad usaldama üht keskust. Demokraatlikus ühiskonnas ei ole inimestel seni seda vajadust olnud - kõigi riiklike struktuuride puhul on võimalik usaldada vaid osa neist. Siinkohal tihti kõlanud vastuväide - mitteusaldajad elagu ebamugavamalt kui soovivad ja küll nad hakkama saavad - see väide võiks asenduda tehnoloogiliste lahendustega kus puuduvad vältimatud keskse inimgrupi usaldamise nõuded.

RFID+ID kontekstis on peamiseks laialtlevinud ühiskondlikuks arutlusteemaks inimeste jälgitavus. See tõuseb reaalselt oluliseks teemaks juhul, kui riiklikud või üleriigilised erastruktuurid loovad mingi superandmebaasi, kuhu vastav info koondub. Erastruktuuride säärase tegevuse vastu saab koostada seadusi. Riiklike kesksete jälgimisbaaside teema vajab aega ühiskonnas selgeks rääkimiseks. Londoni ühistranspordi süsteem sai 2006 aasta kevadel politseilt 250 jälituspäringut kuus. Inimeste geograafilist jälitamist võimaldavate andmete säilitusaeg vajab tulevikus reglementeerimist.

5.5 Kontaktkaartide versus RFIDiga kaartide turvavõrdlus

Kontaktkaardid omavad sisseehitatud kaitset elektromagnetväljaga mõjutamise vastu. Raadiokaardid peavad seejuures saama kätte oma tööks tarviliku EM välja. Seega on nad selle koha pealt olemuslikult veidi kaitsetumad.

Vastutus tehingute eest - kontaktkaartidel võib vastutuse ja otsustuse jätta üksnes kasutajale, appelleerides tema vabale tahtele sisesta kaarti terminali. RFID kaartidega võib juhtuda, et kohus ei pea riikliku või täis- ja poolmonopolistlike struktuuride poolt "de facto" pealesurutud lahendust ja selle turvamist kasutaja ainuvastutuseks, kuna keskmine kasutaja ei oma selleks ei teadmisi ega füüsilise sekkumise võimalusi. Pangakaartidel, erinevalt ID-kaardist on vastutusmäär piiratud ja pangad on nõus enamustel juhtudel ise vastutama. Järelduvalt - RFID kaartidega piiramatu vastutusega digitaalallkirjade andmine on täielikult kasutaja vastutusalas vaid esimese tõsise kohtulahendini.

RFID kaardid on sobilikumad avalikesse järelvalveta kohtadesse terminalide paigutamiseks - terminali on raskem rikkuda kui kontaktkaardi puhul.

Kaardi lõhkumine liigse elektromagnetvälja abil (tehniliselt oluliselt keerukam mehaanilisest (s.h. ID-kiipkaardi) kahjustamisest, kuid teostatav omaniku tahtest sõltumatult) . Säärane võimalus loob kolm peamist väärkasutusjuhtu -

1. tahtlik anonüümne vandalism võõraste kaartide kallal
2. tahtlik oma kaardi rikkumine eesmärgiga saada tasuta uus kaart.
3. tahtlik oma kaardi rikkumine eesmärgiga appelleerida oma mittetahtlikule võimetusele teha tehinguid. Seda siis igapäevasel tasemel(ei saanud tööle tulla kuna ID-kaart läks katki) kui ka suurte juhtumitega (ei saanud üle piiri oma kahtlaselt poolkatkise ID-kaardiga ja seetõttu jäi väga kallis tehing sõlmimata).

Kaartide varguse suhtes on RFID kaardid eelistatud - neid ei pea ajutiselt võõrastesse kätesse andma ega ka taskuvarastele hõlpsates kohtades kandma.

Kaartide kopeerimine - RFID jääb siin kontaktkaartidele alla, kuna on võimalik esitada üks kasutuskõlbmatu RFID osaga füüsiline kaart ja samas käe varrukas hoida teist RFID saatjat või kaugemal asuva identiteedivarguse ohvri reaalse ID-kaardi juurest signaale edastavat süsteemi. ID kaardi esitamine RFID liidesele ei oma seega teoreetiliselt mitte mingit tõendavat jõudu enne kasutajapoolset PINiga kinnitamist.

RFID on võrdluses nõrgem ka teenusega petmise - topelttehingute juhtumitel. Tehing võib jääda pooleli kõigil võimalikel ajahetkedel. Kontaktkaardil on kaardi sisestamine ja väljastamine üsna arusaadavad punktid ajas, RFID puhul täpselt määratletud piiri pole. See on kõigile osapooltele (müüja(kontrollija),ostja(kontrollitava), terminal, kaart) lisanduvat segadust tekitav, avades uusi võimalusi tahtlikeks ja tahtmatuteks topelttehinguteks ning küsitavaks vastutuseks nende eest.

Raadiotaseme suhtlus on olemuselt ebaselgem. Seega on üks risk ka olulist kõlapinda leidvatest üksikjuhtumitest tekkivad skandaalid. Näiteks kui keegi ühistranspordis mingi segaduse tõttu ilma suurema süüta "jäneseks" tunnistatakse. Neid juhtumeid ei pruugi olla olulisel määral, kuid neid on statistiliselt veidi rohkem ja seega on suurem ka risk saada üksikindiviidi õigustatud pahameelest oluline tagasilöök tegevuse mainele.

Väga oluline arusaamatus tänaste RFID kaardi kasutajate seas on kauge taasesituse küsimuses. Uksesüsteemides eeldatakse, et sisenemiseks on vaja füüsilist kaarti. Samas, ükskõik kui turvalise, ilma PIN koodita kasutatava kaardiga on võimalik lihtsalt signaale raadiotasemel edastada, s.t. kahe ründaja koostöös tuua rünnatav pahaaimamatult raadio teel terminalile virtuaalselt lähedale.

5.6 Digitaalallkirjastamise eripärad

Digitaalallkirjastamise eripära võrreldes muude kaartidega on kõrgendatud tehingumäärades ja kasutajale seatud vastutuses. Kaardisüsteemid on arenenud peamiselt panganduses, kus kaartidel on tehingupiirid ja vastutus on hajutatud ostja, müüja ja panga vahel. Säärane vastutuse jagunemine ja limiteeritud tuluvõimalus lõikab ära motivatsiooni paljudeks keeruliseks turvarünnakuteks. Seadustatud digitaalallkirjaga kaardid on leidnud vähest rakendamist ja on täna arenenud välja pangandussektori tehnoloogiatest. Seadusega on vastutus tehingute eest pandud lõppkasutajale. Paljudes arenenud riikides on ID-kaardi laadsete plaanide vastu suured protestid ja seda üsna õigustatult. Kasutajale on seatud ebaproportsionaalselt suur vastutus, kasutades tehnoloogiat mis on välja arenenud teistsuguse loogilise mudeli järgi toimides. Tehnoloogia ei ole selleks veel küps. Tehnoloogia saab olema valmis siis, kui PIN koodi sisestamine vms kasutaja vaba tahte väljenduse kontrolli mehhanism on samavõrd kasutaja kontrolli all kui kaart isegi - seda võib oodata elektrooniliste identifitseerimisvahendite järgmiselt põlvkonnalt.

Kasutajad on tänase ID-kaardi puhul leppinud, et nende PIN kood läbib ebaturvalisi kanaleid (arvutitarkvara, kaarditerminal). Lisanduvalt PIN koodi igakordne raadioeetrisse edastamine ei pruugi enam nii vastuvõetav olla. Täna enamus kasutajaid ei saa aru füüsiliste PIN koodi sisestuskanalite ebaturvalisusest. Võib juhtuda, et "raadio kaudu" edastamise pealesundimisel aga enamusel tekib tõrge ja kahtlus ka juhul kui tegelikult on tegemist väga usaldusväärse süsteemiga.

PIN koodi sisestamisel kasutaja ühtaegu a) usaldab terminali b) eeldab, et kui terminal siiski on ebausaldusväärne, siis ta järgmine kord ei pane oma kaarti terminali, kust esimesest kohast varastatud PIN koodiga võidakse teha tema tahtest sõltumatuid tehinguid. RFID kaartide puhul need kaks asjaolu ei toimi enam koos - murtud turvalisusega terminalist teada saadud PIN koodiga võib teha edasisi tehinguid kasutaja käitumisest sõltumatult. Kõrgendatud tehingumäärade puhul on sääraste juhtumite esinemine kindlustatud.

Raadiokaartide puhul võib kasutaja kohtus appelleerida asjaolule, et ta ei saanud toimuvast aru ja tal ei olnud ka võimalust sündmuste kulugu mõjutada (füüsiliselt kaarti paremini hoides). Seni on RFID kaarte kasutatud vaid piiratud ja hajutatud vastutusega rakendustes. Piiramatu vastutusega rakendustes, suuremate tehingumäärade juures, võidakse teha tehing, kuulutada see hiljem tühiseks ja nõuda tekkinud segaduse hüvitamist kas kaardisüsteemi operaatori või riigi vastutusel.

5.6 E-Passi eripärad

E-Pass on üleilmne standard. Tegu on RFID smartcardiga, mille PIN on kirjutatud passi optiliselt loetavana. Seadme kasutuseesmärk on piiriületuste kiirendamine lennujaamades, standardi algataja oligi rahvusvaheline tsiviillennunduse organisatsioon. Selleks konkreetseks kasutuseks on E-Pass ka adekvaatselt turvatud. Eesti E-Pass on väidetavalt veidi vähem turvatud, kuna puudub kaitsev fooliumikiht. E-Passi funktsionaalsus on uuel Eesti passil. Infrastruktuur ja standardid on arendatud välja suunatuna mitte tehingutele või isikutuvastusele, vaid andmete kiirele sisestamisele kontrollpunktis.

E-Passi PIN on pikk ja selle lugemiseks kasutatakse optilist kallist skännerit. E-Pass tuleb esitada reisidest EU'st välja. PIN sisestamine on kulukas ja seega kodumaised kasutused vähemolulistes kohtades ei saa olema populaarsed.

Kokkuvõtvalt jätab see ID-kaardile lisatavale (ID-kaardiga elektriliselt sidumata) E-Passile väga vähe kasutusotstarvet - juhul kui EU lennujaamades suudetakse optilist koodi masinlugeda, siis EU sisene piiriületus oleks peamine ja ainukene võimalik rakendus monofunktsionaalsele E-Passile ID-kaardil.

Multifunktsionaalse E-Passi lisamine ID-kaardile - see valik on mõtestatum, kuid sel juhul(arvestades ID-kaardil asuva E-Passi väikest kasutust oma peaeesmärgil) ei puutu E-Pass asjasse muul moel, kui et kasutatakse selle suhtlus ja andmesalvestusstandardit kui esmast arenguplatvormi. Võimalik tehniline lahendus võimaldaks sel juhul osasid funktsioone kasutada ilma PIN koodita või inimesele harjumuspärase lühikese PIN koodiga.

5.7 Multifunktsionaalse kaardi eripärad

Multifunktsionaalne kaart peab arvestama erinevaid kasutuse ja turvamise loogikaid. See tähendab, et kaardil oleva pisikese arvuti programm peab olema keerulisem - etendama kaardil asuvat mitut eri virtuaalset kaarti - anonüümset, lihtloetavat, terminalis asuva võtmega loetavat, PIN koodiga kaitstut, on-line kontrollitud sertifikaatidega kaitstut.

Areneva tehnoloogia tingimustes juurutavad erinevad riigi ja erastruktuurid omi kaarte, nende koostöövalmidus on sellest lähtuvalt kõikuv.

Riik võiks väljastada avatud platvormiga multifunktsionaalse kaardi pilootprojektina, võimaldades erinevatel erainitsiatiividel liituda.

Turvalisuse osas on multifunktsionaalse kaardi suurim eripära "turvalisuse ristleke". See tähendab olukorda, kus erinevad kasutusjuhud on erineva nõutava turvalisusega, kuid kasutaja/operaator/terminalivõrgu omanik ei saa sellest aru ja kasutab kaarti samal viisil mõlemas kohas. Näiteks juhtum, kui üht ja sama kaardi kaitstud osa kasutatakse nii isikuandmete hoidmiseks kui bussipiletina, võimaldades nõrgema turvalisusega terminalis kasutada tugeva turvalisuse andmeid. Seega peab multifunktsionaalse kaardi rakendamisel väga täpselt kaardistama erinevad kasutusjuhud ja läbi analüüsima nende nõutud turvalisusvajadused.

Multifunktsionaalsel kaardil on ka käideldavuse osas üks, tänaseks juba praktiline probleem - kui kaotad kaardi, kaotad kõik. Suurorganisatsioonid, mis on oma töö ja arvutiturvalisuse seadnud ID-kaardi järele toimima, kaotavad järjest tööpäevi kui kasutaja ID-kaart kaduma läheb, olukord küll lihtsustub KMA ajutise ID-kaardi lahenduse juurutamisel. See on üks oluline argument ID-kaardile "kahe väiksema venna" loomiseks.

6. Kokkuvõtvad järeldused, soovitused ja edasised uurimissuunad

6.1 Järeldused

- Universaalse riikliku RFID liidesega isikutuvastust võimaldava seadme laialdane kasutusvõtt on tulevikus paratamatu. Seega tuleb teemaga riiklikul tasandil kindlasti aktiivselt edasi tegeleda ja otsida kompromisse erinevate kaarte kasutavate majandussektorite vahel - pangandus, transport, ligipääsusüsteemide tarnijad, riiklikud pisitoimingud.
- ID-kaart võiks teatud tingimustel sisalda E-Passi laadset avalikku andmeosa. Kui E-Pass ja ID-kaart oleks ühel plastikutükil kuid ilma omavahelise ühenduseta, siis E-passi osal võiks olla RFID liides. Tõenäoliselt ei ole see kombinatsioon multifunktsionaalse kaardi rollis parim lahendus hinna ja võimaluste suhte koha pealt. Monofunktsionaalne, ainult E-passi funktsionaalsusega ID-kaart jääks oma E-pass+RFID osas kasutatavaks sisuliselt vaid EU lennujaamades - see on küsitava väärtusega investeering.
- ID kaardile RFID mooduli kui identse kasutajavastutusega sekundaarse suhtluskanali lisamine integreerituna ID kaardi oma kiviga (digiallkirja võimaldamine RFID tehnoloogia kaudu) oleks tõsiselt kahjulik kogu ID kaardiga seonduvale infrastruktuurile, kuna kogu senise infrastruktuuri turvalisust ja kasutuskeerukust tuleks hakata tõstma. See tähendab ootamatuid kulutusi kolmandatele osapooltele(teenuspakkujatele). Kombinatsioon piiramatust kasutaja vastutusest, digitaalallkirjast ja RFID kaardist on üsna unikaalne ja omas tehnoloogiasektoris levinud laiatarbelahendustega hetkel vastuolus.
- RFID laiatarberakendused on mõeldud mini ja mikrotehinguteks. Sellesse sektorisse võiks esialgu suunduda ka Eesti riiklikud RFID alased arengud. Pilootprojektina võiks väljastada mini-ID kaardi, see võiks olla ldap.sk.ee'ga seotud ja transpordi/uksekaartide sektorisse suunatult. Näiteks siis ID kaardiga analoogne, vähemate füüsiliste turvaelementidega(odavam) kaart, mida saaks kasutada multifunktsionaalselt (väikemaksed, uksed, transport, sissepääs üritustele). Mõeldav oleks näiteks täiendava RFID kleebise paigaldamine ID-(sõidu)kaardile piletituvastuse kiirendamiseks.
- Universaalse, ID-kaardiga ekvivalentse, RFID kanaliga isikutuvastusvahendi otsingutel võib osutuda arukamaks oodata veidi mobiilinduses levivate RFID tehnoloogiate arengusuundade täpsustumist. Võib juhtuda, et multifunktsionaalne kaart on mõne aasta möödudes pea igas müüdavas mobiilis. Multifunktsionaalseid kaardilahendusi ei saa olla riigis lõpmatul hulgal, seega "mainstream" lahenduse valimine on valik aastakümneks.

6.2 Soovitused RFID tagi lisamiseks Eesti ID kaardile

- Üldpõhimõttena peame RFID tagi lisamist Eesti ID kaardile võimalikuks ja kasulikuks. Eelduseks on siin vähemalt ühe nõude täitmine:
  - Konkreetne Euroliidu nõue E-Passi süsteemi kohutuslikkusest Euroliidu sisestes reisidokumentides (kasvõi ainult lennusõidu puhul).
  - Tagi täiendamine laiatarbekasutust võimaldavate funktsioonidega.

  Teoreetiliselt mõeldav on ka tagi lisamine, mis ei sisalda E-passi funktsionaalsust, vaid ainult laiatarbefunktsionaalsust analoogiliselt RFID-ga ISIC kaardile, kuid me peame seda võimalust organisatoorsest aspektist vähetõenäoliseks.

  Seejuures tuleb siin töös toodud turvariske ja lahendusvõimalusi detailsemalt edasi uurida, soovitavalt eraldi uurimis-projekteerimisprojektis.
- Kui laiatarbe-funktsionaalsust RFID tagile mitte lisada, siis ainult E-passi funktsionaalsuse lisamine ID-kaardile on hetkeseisus vähe põhjendatud.
- RFID peab igal juhul olema realiseeritud ISO 14443 standardi järgi (seda nõuab nii E-pass kui enamus muid smartcard tüüpi lahendusi).
- RFID peaks olema elektriliselt täiesti eraldatud digiallkirja võimaldavast ID-kaardi mikroprotsessorist. Praegune digiallkirja jõud on liiga tugev tekkida võivate turvariskide taustal.
- Laiatarbe funktsionaalsus võiks olla integreeritud samasse RFID tagi, kus on realiseeritud E-passi funktsionaalsus, kuid tarkvaraliselt/kaitstuse mõttes oleks E-passi funktsionaalsusest eraldatud. Uuemad komplekssed RFID tagid võimaldavad taolist lähenemist juba praegu.
- Laiatarbe-funktsionaalsus peaks olema realiseeritud analoogiliselt näiteks ISIC kaartidesse paigutatud RFID kividele, kasutades samu standardeid: liiga keeruliste krüptosüsteemide nõudmine muudab praktikas keeruliseks või võimatuks nende kasutamise pääslasüsteemides ja transpordis. Krüpto lisamine andmeareaalidesse peab olema võimalik, kuid kõigi areaalide jaoks mitte tingimata hädatarvilik.
- Laiatarbe-andmeareaalide osas tuleb tingimata arvestada riski, et süsteemide haldajad/piirivalve jne võivad hakata moodustama andmebaase, kus on vabalt või suhteliselt kergesti kopeeritavate võtmetega kaitstud laiatarbe-info seostatud konkreetsete isikutega. Niisugused andmebaasid võimaldaksid teoreetiliselt teha isikute massilist jälgimist, nagu seda on töö varasemates osades ühe olulise ohustsenaariumina kirjeldatud.
- Laiatarbe-areaalid peavad olema vastavate rakenduste (pääslad, piletisüsteemid) haldajate/müüjate poolt üle kirjutatava/muudetava sisuga. Kindlasti tuleb tekitada punkte/kohti/tuge selleks, et kaartide omanikud saaksid soovi korral ise kontrollida, mis on nende kaardi laiatarbe-osasse kirjutatud, samuti saaksid nad neid areaale üle kirjutada. Taoline lähenemine raskendab oluliselt laiatarbe info kindlat seostamist isikuga ja eelmises punktis mainitud ohustsenaariumi realiseerumist.
- RFID tagiga varustatud ID kaarti tuleks inimestele anda komplektis koos raadio teel lugemist välistava ümbrikuga. Taolisi ümbrikke toodavad mitmed firmad, neid ümbrikke kontrollitakse ja sertifitseeritakse. Nagu varem mainitud, nõuab USA justiitsministeerium RFID-ga varustatud töötõendite puhul (mis on samas ka krüptograafiliselt kaitstud) taolise varjestava ümbriku kasutamist.

6.3 Edasised uuringud teema raames

- Kuna teema on väga detailidest sõltuv, siis tuleks saavutada detailküsimuste süstematiseeritud ja sõltumatu hindamine hankel ja auditeerimine hanke järel ning hiljem. Küllalti raske saab olema organiseerida auditeerimist, mis läheks sügavamale suusõnalistest kinnitustest kõigis detailides. Näiteks detailküsimuses: kas kaardil on olemas voolumõõtmisrünnakute vastased segajad; selles küsimuses oleks vaja üsna keerulist aparatuuri sõltumatu hinnangu andmiseks.

  See on järelvalveorganisatsioonide pädevuse küsimus: täna ei ole tehniliste lahenduste kontroll pädev. Eeldatakse, et teenus vastab nõuetele. Eesti pisikeses vastava ala kitsas spetsialistide valdkonnas on raske saavutada sõltumatut järelvalveorganisatsiooni. Seega tuleb otsustada, kas tegutseda edasi "sõlmime head lepingud ja reageerime siis kui midagi juhtub" viisil või hankida järelvalve rahvusvaheliselt turult.

- Mitmikkasutusega kaartide kasutusjuhtumite kaardistamine. ID-kaardile RFIDi otsesel lisamisel tekib palju uusi erineva nõutud turvatasemega rakendusvõimalusi. See omakorda loob väga tõsise riski turvalisuse "ristlekkeks". S.t. olukorraks, kus ühe teenuse operaator suhtub oma süsteemi turvalisusse palju väiksema tähelepanuga kui teise teenuse operaator ja see pole kasutajale ilmne. Tulemuseks on näiteks uksekaardi lugeja edastamas andmeid uksekaardiga samas rahakotis asuvast ID-kaardist teise riigi otsa, teostamaks suure mahuga tehingut turvalises terminalis, kasutades varem kasutaja tööarvutist trooja hobusega näpatud PIN koodi.

- Tänaste kaarte väljastavate organisatsioonide süstemaatiline ja kõikehõlmav küsitlus universaalse riikliku keskse isikuandmebaasiga seotud mini ja mikrotehingute kaardi väljastamiseks.

- Mobiilinduse trendide prognoos RFID standardite küsimuses.

- Remote replay jms seadmete hinnaprognoosid erinevate arengustsenaariumite puhul ja seejärel turvarünnakuseadmete hinnast lähtuvalt tehingute maksimaalse mõistliku määra ja limiidi hindamine.

- Juhtivate kaarditootjate küsitlemine kompaktse PIN koodi sõrmistikuga kaardi (v.t. 2.8) laiatarbesse jõudmise ajaprognooside osas.

7. LISA: Mifare SmartMX perekond

Mifare SmartMX on juhtiv mikroprotsessoriga kaartide perekond. Olulist Mifare SmartMX spetsifikatsioonist:

7.1 Product Specific Features

- **12 Kbytes** EEPROM (including 192 bytes reserved manufacturer/security area)
- **96 Kbytes** User ROM
- **4608 bytes** RAM
  - 256 bytes + 3 Kbytes CXRAM
  - 1280 bytes FXRAM usable for FameXE
- **Memory Management and Protection Unit** (MMU)
  - for more details see Section 2.2 “Security Features”
- **Contactless Interface Unit (CIU)** fully compatible with ISO/IEC14443A
  - fully supports the T=CL protocol acc. ISO/IEC14443-4
  - Data Transfer rates supported (106/212/424/848 kbit/s)
- **MIFARE® RF contactless interface** acc. ISO/IEC14443-2
  - 13.56 MHz operating frequency
  - Reliable communication due to 100% ASK
  - High speed (106/212/424/848 kbit/s, efficient frame support)
  - True anticollision
  - High speed CRC co-processor according to CCITT
- **MIFARE® reader infrastructure compatibility**
- **High speed DES-3 co-processor** (64 bit parallel processing DES engine)
- **PKI Co-processor** FameXE
  - The major Public Key Cryptosystems like RSA, El’Gamal, DSS, Diffie-Hellmann,
- Guillou-Quisquater, Fiat-Shamir and Elliptic Curve are supported
  - 4096 bits maximum key length for RSA with randomly chosen modulus
  - 32-bit interface
  - Boolean operations for acceleration of standard, symmetric cipher algorithms
  - Performance example: RSA Modular Exponentation (Straight forward) < 35 ms
- (2048 bit key length and 17 bit exponent)
- **Optional free of charge MIFARE® 1K and MIFARE® 4K functionality**

7.2 Security Features

- **Enhanced Security Sensors**
  - Low / high clock frequency sensor
  - Low / high temperature sensor
  - Single Fault Injection (SFI) attack detection
  - Light sensors
- **Electronic fuses** for safeguarded mode control
- **Unique ID for each die**
- **Clock Input Filter for protection against spikes**
- **Power-up / Power-down reset**
- **Optional programmable “Card Disable” feature**
- **Memory Security** (encryption and physical measures) for RAM, EEPROM and ROM
- **Memory Management and Protection Unit (MMU)**

    - Secure multi application operating systems via two different operation modes
        - System Mode and Application Mode
    - OS controlled access restriction mechanism to pheripherals in Application Mode
    - Memory mapping up to 8 Mbytes Code memory
    - Memory mapping up to 8 Mbytes (-64K) Data memory
- **Optional disabling of ROM read instructions by code executed in EEPROM**
- **Optional disabling of any code execution out of RAM**
- **EEPROM** programming:
    - No external clock
    - Hardware sequencer controlled
    - On-chip high voltage generation
    - Enhanced error correction mechanism
- **64 or 128 EEPROM bytes for customer-defined Security FabKey.** Featuring batch-, wafer- or die-individual security data, incl. encrypted diversification features on request
- **14 bytes User Write Protected Security area in EEPROM** (byte access, inhibit functionality per byte)
- **32 bytes Write Once Security area in EEPROM** (bit access)
- **32 bytes User Read Only area in EEPROM** (byte access)
- **Customer specific EEPROM initialization** optional

7.3 Family Standard Features

- Dedicated Secure_MX51 Smart Card CPU (Memory eXtended / enhanced 80C51)
    - 0.18 µ 5 metal layer CMOS technology
    - operating in contact and contactless mode (dependent on family type option)
    - featuring a 24 bit universal memory space, 24 bit program counter
    - combined universal program/data linear address range up to 16 Mbyte
    - additional instructions to improve
        - pointer operations
        - performance
        - code density of both C and Java source code
- Low power / low voltage design using Philips handshaking technology
- Development and portation support of existing P8WE / P8RF family masks
- Multiple source vectorized interrupt system with four priority levels
- Watch exceptioprovides for software debugging facility
- Multiple source RESET system
- Two 16-bit timers
- High reliable EEPROM for both data storage and program execution
    - Bytewise EEPROM programming and read access
    - EEPROM endurance: up to 500 k programming cycles per byte
    - EEPROM data retention time: 20 years minimum
- Versatile EEPROM programming of 1 to 64 byte at a time
- Typical EEPROM page erasing time: 2.5 ms
- Typical EEPROM page programming time: 1.5 ms
- Power-saving IDLE Mode
    - Wake-up from IDLE Mode by RESET or any activated interrupt
- Power-saving SLEEP (power down) Mode or CLOCKSTOP Mode
    - Wake-up from SLEEP or CLOCKSTOP Mode by RESET or External Interrupt
- Contact configuration and serial interface according to ISO/IEC 7816: GND, VCC,
- CLK, RST, IO1
- ISO/IEC 7816 UART supporting standard protocols T=0 and T=1 as well as high speed personalization at 1Mbit/s
- External or internally generated configurable CPU clock
- 1 MHz to 10 MHz operating external clock frequency range
- Internal CPU clock up to 31 MHz with synchronous operation
    - Internal clocking independent of externally applied frequency

- High speed Triple-DES co-processor (two or three keys loadable)
- DES3 performance < 50 μs
- High speed 16 bit CRC Engine according to CCITT polynom definition
- Low power Random Number Generator (RNG) in hardware, FIPS140-2 compliant
- 1.62 V to 5.5 V extended operating voltage range for class C, B and A
- -25 to +85 °C operating ambient temperature range