Kontaktivabadel andmekandjatel põhinev Eesti ühtne õpilaspilet: analüüs ja soovitused

Versioon 2, 18. juuli 2011

OÜ ELIKO
Tanel Tammet, Alar Kuusik

Sisukord

1. Analüüsi eesmärgid

Käesoleva töö põhieesmärgiks on kontaktivabadel andmekandjatel põhineva Eesti ühtse õpilaspileti tehnoloogiliste nõuete analüüs, vastava raamistiku kaardistamine ja valdkonna standardite ning erinevate süsteemide liideste analüüs Eesti üldharidus- ja kutsekoolide vajadustest lähtuvalt.

Samuti annab töö soovitusi kontaktivabadel andmekandjatel põhineva õpilaspileti rakendamiseks Eestis. Soovitused on mõeldud juhindumiseks üldharidus- ja kutsekoolides kasutusele võetavate õpilaspiletite hankimisel ja rakendussüsteemide arendamisel või nendega liitumisel.

Konkreetsemalt käsitleb töö järgmisi küsimusi:

- Eestis tarvitatavate ja arendatavate õpilaspiletite kasutusvajadused
- Olemasolevate standardite ja lahenduste analüüs
- Soovitused õpilaspiletite standarditud numereerimiseks erinevate koolide õpilaspiletite süsteemide ühildamise saavutamiseks.
- Õpilaspiletitel salvestatavate andmete mahud, võrgulahendused ning komponentide/tarkvara põhimõtted.
- Soovitused enamlevinud kaarditüüpide kasutusele võtmiseks Eesti õpilaspiletina.
- Soovitused nõuete määratlemiseks privaatsusele ja infoturbele.
- Üldised soovitused tehniliste tingimuste sätestamiseks õpilaspiletite hangete läbiviimisel. Nimetatud tehniliste soovituste eesmärgiks on tagada valmisolek hangitavate süsteemide ühildamiseks ning erinevate koolide kontaktivabade õpilaspiletite ristkasutamiseks, tagades liidesed huvitatud osapooltega.

2. Sissejuhatus ja ülevaade kontaktivabadest kaartidest

Tüüpiline kontaktivabadel kaartidel põhinev süsteem koosneb kaartidest endist, nende lugemise seadmetest ning süsteemi kesktarkvarast. Keerukamad süsteemid võivad sisaldada ka kaartide kirjuajamise seadmeid. Kesktarkvara tegeleb süsteemi põhifunktsioonidega ja kaartide haldusega, lugejad ning nendega seotud kontrollerid vahendavad nende lugemiskaugusesse jäänud kaartide infot kesktarkvarale. Harilik lihtsamat sorti kaart ise oskab saata kaardilugejale oma identifitseerimisnumbri ning muid funktsioone tal tehnilises mõttes ei olegi.

Kontaktivabadel kaartidel on küll palju tüüpe ja kolm peamist töösageduspiirkonda (125-134kHz madalsageduslik; 13,56MHz kõrgsageduslik; 0,86-2,45GHz ülikõrgsageduslik), kuid mõistlike valikute ja ühispõhimõtete järgimise korral võib olla võimalik kasutada sama sidestandardiga süsteemi kaarte mitmes teiseski süsteemis. Näitena võiks ühe kooli süsteem registreerida/avada uksi ka teise kooli õpilaskaardiga õpilastele, kelle info on kesktarkvarasse kantud, samuti võiks olla võimalik kaarti kasutada RFID lugejaga transpordivahendis.

Kontaktivabad kaardid (*tag*id) sisaldavad RFID (Radio Frequency Identification) energiasäästlikke mikroelektroonikalülitusi, millega peetakse ühendust raadiosagedusel, st juhtmeta, kasutades elektri- või magnetväljasidestust. RFID tag koosneb niisiis digitaalelektroonika ja toitelülitusest ning sellega seotud antennist.

RFID tagide Eestis levinuimad rakendused on:

- vargusvastased riputid/kleepsud kauplustes müüdavatel toodetel
- kontaktivabad ukseavamis-kaardid (pääslasüsteemid). Käesoleva töö kontekstis rõhutame, et nende hulgas on ka MinuKool (www.minukool.ee) poolt väljastatavate ISIC/ITIC jms kaartidega kasutatavad, samuti In Deal poolt mitmetes üldhariduskoolides väljastavaid kaarte tarvitavad süsteemid.
- Eestis esialgu peamiselt hangete ja juurutusfaasis: piletisüsteemid

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

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

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 madalsageduslikke tage kasutatakse kauplustes vargusvastaste vahenditena. Töökorras tagiga väravast läbiminek käivitab alarmi muutes väravaantenni magnetvälja.
- Tag, mis on suuteline lugejale vastama talle peale salvestatud *unikaalse ID-numbri* ehk UIDi. Sellised numbrid on reeglina suhteliselt pikad (64 või 96 bitti). Niisuguseid tage kasutatakse toodete identifitseerimiseks ribakoodi asemel (näiteks EPC – Electronic Product Code), samuti pääslakaartidena. mõnedes ühistranspordisüsteemides sõiduõiguse kinnitamiseks. Need UIDi kannab kaardile tootja ning neid ei ole hiljem võimalik muuta. UID vastamine on igas tehnoloogias tagide põhifunktsionaalsus: see on nende kiireim ja suurima töökindlusega kasutusviis.
- Tag, mis sisaldab *ühekordselt või korduvalt ülekirjutatavat mälu*, mida saab kasutada ID või (suure mälumahuga tagi korral isegi kilobaitide) andmete hoidmiseks. Tüüpiliselt kasutatakse

selliseid tage logistikas, ravimite märgistamisel, transpordis. Mälumaht on 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 mitmetes transpordisüsteemides piletina.

- Tag, mille erinevad mälupiirkonnad on *kaitstud salajase võtmega/võtmetega*: lugeda või kirjutada saab ainult võtit (parooli) teades.. Enamus niisugust tüüpi (samuti keerukamad, vt järgmist lõiku) RFID tage järgib ISO 14443 standardit ja töötavad 13.56MHz sidesagedusel.
- Tag, mis sisaldab *mikroprotsessorit*, 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.

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.

Pääslasüsteemides on levinuimad vanemad, 125kHz ja 134kHz madalsageduslikud RFID kaardid. Mittekirjutatavas (read only) kaardis sisaldub unikaalne kood, tüüpiliselt 40 bitti. Kontrollerisse edastatakse kood, mida võrreldakse kontrollerisse salvestatud andmebaasi kirjetega. Areng toimub kõrgsageduslike 13,56MHz kasutuselevõtu suunas.

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 tehnoloogiliselt keerukas ja nõuab spetsiaalriistvara.

Õpilas- ja üliõpilaskaartidena on Eestis kasutusel aga uuemad, kõrgsageduslikud 13.56 MHz RFID kaardid, neist järgmistes peatükkides.

3. Eestis tarvitatavate ja arendatavate õpilaspiletite kasutusvajadused

Õpilaspiletitel on Eestis mitu traditsioonilist rolli nii kooli sees (isikutunnistus, RFID puhul pääsla, registreerimine ja mitmed lisateenused) kui koolist väljas (eeskätt õpilase staatuse tõestamiseks, samuti isiku või tema vanuse tuvastamiseks olukordades, kus viga ei ole kriitiline, näiteks kinos).

Õpilaspilet peab tingimata olema mugav kaasas kanda, vastupidav ja kergesti loetav. Kõige levinum õpilaspileti - ja mistahes kaardi - formaat on plastist nn pangakaardi-formaat.

RFID lisamine õpilaspiletile võimaldab piletil lisaks traditsioonilistele täita tervet kogumit uusi rolle (edaspidistes paragrahvides analüüsitakse neid detailsemalt). Toome kõigepealt põhirakenduse, kooli sissepääsu ja -registreerimise:

- Kaart on kooli sissepääsusüsteemis võtmeks. Uks avaneb - nii seest kui väljast avades - kui kaart asetatakse ukse kõrval oleva kaardilugeja vastu.
- Kaart on sisenemise/väljumise registreerimisvahendiks. See on loomulik ja tüüpiline täiendus sissepääsusüsteemile: eeskätt on vaja lihtsalt salvestada sisenejad ja väljujad koos kellaaegadega. Seda infot on võimalik aga mitmel moel täiendada.

Lisaks neile põhirollidele kasutatakse RFID õpilaspileteid tihti veel järgmistes funktsioonides, mh on kõik järgmised realiseeritud mõnes/mitmes Eestis olemasolevas RFID-koolisüsteemis, põhinäitena Gustav Adolfi gümnaasiumis:

- Identifitseerimisvahend kooli raamatukogus. Taoline lahendus on realiseeritud mitmes eesti koolis ning kõrgkoolidest näiteks IT Kolledžis.
- Kasutamiste registreerimise / kasutusõiguse tuvastamise vahend koopiamasinale.
- Koolisööklas söögi/lisasöögi saamise õigus/registreerimine.
- Õpilase isikliku garderoobikapi avamine.
- Sissepääs kooli tõkkepuuga varustatud parklasse (eeskätt töötajad ja lapsevanemad).

Lisaks eelmistele võimaldaks RFID-ga õpilaspilet täita järgmisi täiendavaid rolle, mida on realiseeritud mitmetes koolides maailmas, kuid seni mitte Eestis:

- Õpilaste registreerimine tunnis puudujaks. Nõuab kaardilugejate lisamist klassiuste juurde ja saab olla täiendavaks abivahendiks õpetaja visuaalsele kontrollile.
- Sissepääs koolibussi. Populaarne rakendus välismaa koolides, mis kasutavad aktiivselt koolibusse.
- Kasutamine tava-ühistranspordi elektroonilise pileti kandjana: pilet seotakse õpilaspiletiga, täiendavat piletikandjat/kaarti vaja ei ole. Võimalik mugav rakendus lähitulevikus, mil Eestis hakatakse laiemalt juurutama RFID-põhiseid bussipiletisüsteeme. Nõuab RFID elementaarset ühilduvust ühistranspordi RFID-piletistandardiga.

Esitame järgnevas olulisi detaile keerukamatest alamsüsteemidest.

Kaartide liigid, väljastamine, tühistamine

Mistahes RFID-õpilaskaartide süsteemi hädavajalik osa on kaartide väljastamise ja tühistamise süsteem, mis koosneb nii organisatsioonist, lepingutest kaarditarnijatega kui süsteemi kesktarkvara funktsionaalsusest.

Kesktarkvara peab võimaldama uute kaartide mugavat registreerimist ja kategoriseerimist, samuti tühistatud/kaotatud kaartide õiguste kaotamist.

Kaartide haldamisel on mõistlik lähtuda kooli infosüsteemist, kus hallatakse reaalset õpilaste liikumist, vahetus/ajutisi jne õpilasi, vanemaid, personali. Üleriiklikes hariduse infosüsteemides hallatakse ainult osa vajaminevast isikute andmestikust.

Üldjuhul on koolil vaja mitut sorti RFID "õpilaskaarte", millest ainult osa on reaalsed õpilaskaardid, osa on lühiajalised ja asenduskaardid ning ülejäänud on eeskätt ligipääsu/registreerimiskaardid töötajatele ja vanematele:

- Õpilaspilet – väljastatakse õpilasele kehtivusega üks õppeaasta. Kaarti saab füüsiliselt kasutada rohkem. Võimalik stsenaarium on iga uue kooliaasta alguse sama kaardi ees- või tagaküljele uue kehtivuse lõpu kuupäeva trükkimine või vastava kleebise kandmine.
- Vahetusõpilaspilet – analoogne eelmisega, kuid väljastatakse koolis viibivale vahetusõpilasele. Isikukoodi asemel - kui tegu ei ole eesti elanikuga ja kui kaardile kantakse isikukoode - on kaardile kantud õpilase sünniaeg.
- Õpetajakaart – väljastatakse kooli õppepersonalile.
- Personalikaart – väljastatakse kooli tugipersonalile.
- Lapsevanemakaart – väljastatakse sooviavalduse alusel õpilase lapsevanematele kehtivusega üks õppeaasta. Kaarti saab füüsiliselt kasutada pikemat aega.
- Asenduskaart – personaliseerimata tähtajatu kaart. Antakse õpilasele üheks õppepäevaks juhuks, kui ta on enda õpilaspileti kas koju unustanud või ära kaotanud. Väljaandmise hetkel seotakse kaart infosüsteemis antud õpilasega ning õpilane saab sellega koolis samad õigused, nagu oma õpilaspiletiga.
- Külalise kaart – personaliseerimata tähtajatu kaart. Antakse kooli külastavatele isikutele nende koolis viibimise ajaks.

Sissepääsu- ja sisenemiste/väljumiste registreerimissüsteem: detailid

Anname ülevaate eeskätt Gustav Adolfi gümnaasiumi näitel.

Maja sissepääsud varustatakse kaardilugejatega ning neist pääsevad läbi isikud, kellele on omistatud vastavad õigused (õigusi saab piirata nädalapäeva ja kellaaja täpsusega). Peauksest sissepääs on

koolipäeviti etteantud ajavahemikus vaba, kuid õpilastel lasub kohustus peale koolimajja sisenemist oma kohalolek registreerida (selleks paigutatakse käepärastesse kohtadesse kaardilugejad). Samuti peavad õpilased registreerima ka oma koolimajast lahkumise. Õpilaste kohaloleku registreerimise motiveerimine saab toimuda puudujate registreerimise protsessi kaudu – kui õpetaja avastab puudujaid märkides, et keegi õpilastest on jätnud oma saabumise fikseerimata, peab ta talle seda alati meelde tuletama (vajadusel korduva rikkumise korral märkuse tegema vms).

Vajadusel on võimalik rakendada ka nn. *turnikee* seadmete paigaldamisega möödapääsmatut kohaloleku registreerimist, kuid seda ei peeta koolides otstarbekaks tema liigse keerukuse ja aegluse tõttu.

Gustav Adolfi gümnaasiumis on sissepääsukontrolli täpsemaks ja turvalisemaks realiseerimiseks täiendatud videosalvestussüsteemiga.

Peasissepääsu juurde on paigaldatud videokaameraga inimeste loendamise lahendus. See lahendus edastab uksest sisenenud inimeste info (inimeste arv, kellaaeg) reaalajas ligipääsuhalduse serverisse. Infosüsteemi kasutajaliidesest on reaalajas jälgitav koolis viibivate isikute info: kokku koolimajas viibivate inimeste arv, kaardiga ennast tuvastanud isikute arv, tundmatute isikute arv. Süsteemis on võimalik jälgida tundmatute isikute arvu muutumist ajas.

Sisse- ja väljapääsusüsteemid peavad olema täiendavalt integreeritud tuletõrjekeskuse ja üldise häiresignaaliga. Kui tuletõrjekeskus või muu häire andja aktiveerib häire, signaliseeritakse seda kontrollerisse. Kontrolleri tarkvara saadab kõigile süsteemi ühendatud uksekontrolleritele signaali ukse avamiseks, samuti saadetakse signaal kesksüsteemi.

Võimalik uus funktsionaalsus: õpilaste registreerimine puudujateks

Järgnev süsteem ei ole sellisena realiseeritud üheski eesti koolis, kuid tema realisatsioon oleks võimalik ja pilootrakenduste loomine oleks selgelt mõttekas.

Süsteem peab arvestust majas ruumidesse sisenemiste ja väljumiste kohta, eeldusel, et ruumide jaoks on paigaldatud kaardilugejad. Süsteemis peab olema kirjeldatud kogu klassi koosseis, seega on võimalik aruandega välja võtta soovitud klassi kohaloleku info suvalisel kellaajal.

Õpilaste tundi hilinemise/puudumise märkimine peab üldjuhul toimuma õppeinfosüsteemis. Loodav RFID-süsteemi kesktarkvara peab sisaldama liideseid, mille abil saab õppeinfosüsteem küsida RFID-süsteemi kesktarkvaralt kas konkreetses ruumis või majas viibivate õpilaste nimekirja. Kuna konkreetses õppetunnis osalevate õpilaste nimekiri ei pruugi paljudel juhtudel kokku langeda klassi nimekirjaga, on kesktarkvara liides võimeline vastama kohaloleku infot ka nimekirja alusel – õppeinfosüsteem annab päringuga ette õpilaste nimekirja, kelle kohalolekut vajatakse, ning kesktarkvara tagastab kõigi küsitud õpilaste kohaloleku info kas siis - üldjuhul - koolis või - klassiuksele paigaldatud lugeja korral - antud ruumis.

Tuleb arvestada, et vaatamata sellele, et enamikes koolides ja klassides saab õpetaja tundide läbiviimisel kasutada arvutit, sisestatakse siiski arvestatav osa puudumiste infost õpetajate poolt oma pabermärkmikusse ning õppeinfosüsteemi viiakse sisse alles hiljem. Sellise käitumise peamiseks põhjuseks on kiirus – märkmikusse info märkimine on oluliselt kiirem, kui arvutisse sisselogimine, õppeinfosüsteemi avamine, vajaliku tunni valimine ning seal info reakaupa sisestamine. Lisaks on takistuseks ka õppeinfosüsteemi kasutajaliidesei kasutusmugavusega seotud küsimused – veebikeskkond paneb paratamatult omad piirangud.

Puudujate märkimise protsess RFID süsteemi toega võiks käia järgmise stsenaariumi kohaselt.

1. Õpetaja siseneb õppeinfosüsteemi ning avab hetkel alanud tunni andmete sisestamise lehe
2. Õppeinfosüsteemis on tunniplaanis fikseeritud ruumid, kus üldjuhul mingit tundi läbi viiakse. Õpetaja saab seda iga konkreetse läbiviidava tunni korral muuta.
3. Peale õpetaja poolt ruumi muutmist või siis vaikimisi kasutatava ruumi kinnitamist teostab õppeinfosüsteem kohaloleku info lugemise RFID kesktarkvara keskkonnast.
4. Õpetajale kuvatakse tunni õpilaste nimekiri kujul, kus kas spetsiaalsete tähiste või värvide kasutamise abil on ära märgitud õpilased, keda infosüsteem kohaloleku registreerimise info baasilt peab puudujaks. Need tunnused peaksid olema erinevad õpetaja poolt puudujaks või hilinejaks märkimise staatusest, et hiljem oleks võimalik tuvastada nii õpetaja poolt käsitsi märgitud puudumis/kohaloleku infot kui ka süsteemi poolt pakutud infot.
5. Õpetaja kontrollib kohaloleku ja puudumise info üle ning teeb vajadusel parandused – kas märgib kedagi täiendavalt puudujaks või siis märgib süsteemi poolt puudujaks pakutud õpilase kohal olevaks. Viimasel juhul on soovitatav, et õpetaja juhiks ka õpilase tähelepanu sellele, et ta pole ennast kooli sisenedes registreerinud.
6. Õppeinfosüsteem peab sisaldama tunni kohaloleku info kinnitamise tegevust – sellega annab õpetaja märku, et antud tunni kohaloleku info on tema poolt üle vaadatud ning see on viidud vastavusse tegelikkusega. Selle tegevuse puudumise korral on hiljem raske aru saada, et kas tunni kohaloleku info on ikka korrektselt täidetud või mitte.

Juhul, kui kool ei kasuta vajaliku funktsionaalsusega õppeinfosüsteemi, oleks võimalik kohaloleku info märkimine realiseerida ka otse RFID süsteemi kesktarkvara keskkonnas, eeldusel, et selline funktsionaalsus kesktarkvaras realiseeritakse. Sellisel juhul avab õpetaja kesktarkvaras kohaloleku info lehe, valib sealt välja klassi, kelle kohaloleku infot soovib vaadata/muuta, ning teeb vajadusel sobivad täiendused.

4. Olemasolevad standardid ja lahendused

Kõigepealt märgime, et RFID valdkond on sedavõrd lai ja kiiresti arenev, ning ootused RFID-i kasutava infosüsteemi kasutajatel on sedavõrd erinevad, et enamuses rakendusetüüpides ei ole kujunenud välja konkreetseid riiklikke või rahvusvahelisi standardeid. Sama kehtib ka koolide kohta.

Erinevalt infosüsteemidest ja liidestest on standardid - suuresti küll mingi tootja loodud de facto standardid - olemas RFID kaardiperekondadel endil, mida käsitleme edaspidistes peatükkides. Siin anname ülevaate eesti RFID-õpilaskaartide süsteemidest ja toome olulisemaid näiteid välismaalt.

Eesti põhikoolides, kutsekoolides ja gümnaasiumides kasutatavad RFID süsteemid jaotame kaheks:

- Standardsed sissepääsusüsteemid. Nende süsteemide kaardid ei ole ühildatud õpilaspiletiga ning nad ei paku koolides erifunktsionaalsusi. Kuivõrd sellised süsteemid ei erine sisuliselt harilike asutuste RFID-põhisest sissepääsusüsteemidest, siis me neid edaspidises ei vaata.

- Spetsiaalselt koolidele loodud RFID-põhised infosüsteemid, kus RFID-kaart on õpilaspiletisse integreeritud ning on realiseeritud erinevat kooli jaoks vajalikku funktsionaalsust. Järgnevas vaatleme ainult selliseid süsteeme.

Eesti koolides RFID-süsteemid kasutavad kõik ühtsama lihtsat mäluga kaarditüüpi - Mifare Classic (vt http://en.wikipedia.org/wiki/MIFARE#MIFARE_Classic) ning hoiavad kaardil

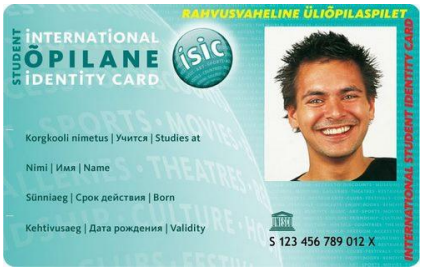
- Kaardi unikaalset UID-d. Juhime tähelepanu, et sellist UID-d hoitakse pea kõiki tüüpi RFID-kaartidel, mitte ainult Mifare Classicul. Tegu on RFID-kaartide põhilise infoobjektiga, mida süsteemi lugejad kaardilt loevad. UID-dei saa kaardile tavavahenditega ise kirjutada, see ei ole algselt mingilgi viisil seotud kaardi omanikuga ning ta kantakse kaardile tootmise käigus, mis teeb kaardi raskelt kloonitavaks ja raskelt võltsitavaks. Lisainfot järgmistes peatükkides.

- Osadel kaartidel - konkreetselt inDeal süsteemi Gustav Adolfi gümnaasiumis kasutusel olevatel - on kaardile kantud UID lisaks loetavalt kaardile trükitud, osadel kaartidel - konkreetselt MinuKool süsteemi ISIC kaartidel - UID kaardile trükitud ei ole. Viimasel juhul on kaardile trükitud rahvusvaheliselt unikaalsed ISIC seerianumbrid ning seost UID ja kaardile trükitud numbriga hoitakse MinuKool andmebaasis. Selline pealetrükitud info võimaldab kaardi haldamist ka ilma kaardilugejata. See võimalus ei ole koolis kasutamiseks hädavajalik, küll aga võimaldab ta perspektiivis täiendava funktsionaalsuse kasutamist, näiteks võimalikku kaardi kasutamist RFID-ühistranspordisüsteemis. Edaspidises soovitame kaardile kirjutada mitte kogu UID, vaid eesti ühilduvussüsteemi järgset mugavamalt kasutavat lühinumbrit PAN-i, mis on analoogiline põhimõte MinuKool süsteemiga.

- Kaardimällu kirjutatud isikukoodi. Enamus kaardirakendusi seda isikukoodi ei tarvita - erandiks raamatukogude infosüsteemid, kus see võimaldab keremini realiseerida universaalsemaid infosüsteeme, mis võimaldavad töötajal isikut kiiremini registreerida.

Nimetatud info kodeerimise viisid on töötatud välja eesti ettevõtte In Deal OÜ ja SEB panga ühistöös. Lisaks annab SEB välja sama standardi põhist pangakaardi/ISIC kaardi kombineeritud kaarti. Eraldi annab sama standardi põhiseid kaarte välja Gustav Adolfi gümnaasium.

Kaardinäide: kirjeldatud standardi kohane ISIC kaart:



Kaardinäide: kirjeldatud standardi kohane Gustav Adolfi gümnaasiumi kaart:

Täiendava info kaardile kandmine on turvakaalutlustel mittesoovitav ning sellisel infol ei oleks RFID-le kantuna ka sisulist rakendust: üldjuhul piisab kaardi UID kasutamisest.

Nimetatud kaartidel on Mifare Classicule vastav tehnoloogia, kaardid:

- Väljastavad lugejale 4-baidise seerianumbri (3 sisubaiti + 1 kontrollbait) (mitte isiku ID) ja täiendavat informatsiooni RFID mälust (kokku kaardil üks kilobait mälu).

  Juhime tähelepanu, et neljabaidiste UID aladega kaartide tootmine on lõpetatud, uuematel kaartidel on seitsmebaidised alad, st UID on oluliselt pikem, kui senistel kaartidel. See muudaks UID terviknumbri visuaalse esitamise kaardil senisest olulisemalt raskemaks ja on üks põhjusi PAN lühinumbri soovitamiseks visuaalse esituse jaoks.

- Võimaldavad osade andmeareaalide krüpteerimist.

  Juhime tähelepanu, et kui kaardi RFID-le ei kanta täiendavat infot, ei ole see funktsionaalsus vajalik.

- Võimaldavad krüpteeritud sidet kaardilugejaga.

Taolist tüüpi kaartide trükituna ja partiina tarnimisel on ühe kaardi ootuspärane hind praegu vahemikus umbmääraselt 3.2 kuni 6.4 eurot. Võrdluseks: ilma pealetrükita Mifare Ultralight UID kaarte saab partiina osta hinnada suurusjärgus 0.5 eurot.

Kaardile lisatud RFID tagid ei ole seotud kaardi muude võimalustega, muuhulgas ei ole SEB pangakaart+ISIC+RFID kaartidel olevate RFID tagide abil mitte kuidagi võimalik läbi viia pangaoperatsioone.

Järgnevates peatükkides selgitame, et eeltoodud kaartidel kasutatud UID täispikk visuaalne esitus kaardil ei ole mitmel põhjusel sobiv kaartide ühtlustamiseks ning esitame ühilduvusstandardi järgse visuaalse esituse numeratsiooni koolide jaoks, mis vastab Eestis hiljuti väljatöötatud RFID UID ühilduvusstandardi nõuetele, võimaldamaks sama kaarti kasutada eri infosüsteemides (teises koolis, ühistranspordis jne).

Samuti ei pea me üldjuhul otstarbekaks isikukoodi elektroonilist kandmist kaardile: põhjuseks turvaküsimused, mida käsitleme eraldi peatükis. Muus osas on eeltoodud kaartide parameetrid ja põhimõtted täpselt sobivad eesti koolide vajadustele ning me soovitame nende põhimõtetega jätkata ka uutes süsteemides.

Eestis on enamlevinud RFID-i kandev õpilas/üliõpilaspilet ISIC kaart, millest enamust aga elektrooniliselt - eeskätt kooli läbipääsusüsteemis - ei kasutata.

Rõhuv enamus koole, kus RFID-põhist kooli poolt hallatavat läbipääsu-infosüsteemi kasutatakse, tarvitab selle peatüki alguses eelmainitud kaarte ja eesti ettevõtte In Deal OÜ loodud süsteemi, rakendades selle süsteemi funktsionaalsuse võimaluste endale sobivat komplekti. Esimesi süsteeme hakati ehitama 2006 aastal. Nimekiri koolidest, kus süsteem on rakendatud (funktsionaalsused on kirjeldatud eelmises peatükis):

- Gustav Adolfi gümnaasium
- Tabasalu ühisgümnaasium
- Keila kool
- Pärnu kutsehariduskool
- Tallinna tervishoiukeskkool

Lisaks kasutatakse mitmes koolis Hotronicu / Multilink'i sissepääsusüsteemi ja Hardmeieri süsteemi, täpsemat infot nende rakenduskohtade osas ei ole autoritel teada.

Anname järgnevas väikese loetelu tuntumatest RFID-koolisüsteemidest välismaal:

- InClass RFID süsteem, tootja inCom (http://www.incomcorporation.com/) kasutusel Brittani koolis Californias (esimene juurutus aastal 2005) ja veel mitmetes USA koolides. Esimene juurutus tekitas probleeme ja vastuseisu seoses privaatsusküsimustega.
- Mitmetes Osaka koolides Jaapanis (esimene juurutus 2004).
- Plaanis juurutada Connecticuti koolides USA-s, tootja SecureRF (http://www.securerf.com/)

- Hungerhilli kool Doncasteris Suurbritannias, tootja Darnbro (http://websites.uk-plc.net/Darnbro_Limited/), RFID-tagid paigutatud kooli vormirõivaste sisse
- Cambridge ülikool (ja mitmed muud Suurbritannia ülikoolid), vt detailset ülevaadet http://www.admin.cam.ac.uk/offices/misd/univcard/contactless/

5. Soovitused õpilaspiletite standarditud numereerimiseks

2010 ja 2011 aasta jooksul on mitme eesti IT-ettevõtte, uurimisasutuse, pankade ja telekommunikatsioonifirmade koostöös loodud RFID kaartide ühildumisstandard. Ühildumisstandard on orienteeritud RFID-kaardisüsteemide jaoks, kus kaartide infot ei hoita otse RFID-l, ehk siis *online* süsteemidele, mis on kindlasti kõige sobilikum variant koolide RFID-süsteemide jaoks. Standard on lihtne ning valdavale enamikule RFID kaartide tüüpidele sobiv.

Standardis kasutatakse ära fakti, et ISO/IEC 14443 ühilduv RFID kaart omab unikaalset identifikaatorit UID, mis on tootja poolt juba kaardile salvestatud. Standard arvestab turvalisuse poolelt asjaoluga, et kaardi unikaalse identifikaatori muutmine on väga raske, kaarti emuleeriva spetsiaalseadme valmistamine on keerukas ning enamuse rakenduste valdkonnas, sh koolis, ei tasu selline tegevus ennast ka rahaliselt ära. Tuleb märkida, et erikaardid nagu pangakaardid ja RFID passid vastavad privaatsuse eesmärgil UID päringule muutuva numbrikombinatsiooniga.

Standardi üks põhiideid on kaardile kantava visuaalse numbri (või selle numbri piisavalt mahukas osa) määramine lisaks kaardi RFID tagi tootja poolt salvestatud mittemuudetavale UID-le.

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-standarditega (pangakaardid, kliendikaardid jne), mis muudakse nende kasutamise ühises süsteemis väga vaevarikkaks.

Eeldame järgnevas, et RFID kaart on füüsiliselt ISO/IEC 7810 standardi ID-1 formaadis kaart (kõik tavalised krediitkaardi-mõõdus kaardid vastavad sellele standardile).

Kaart peab sisaldama ISO/IEC 14443 Type A (nn. firma NXP MIFARE standard, kõige levinum), väga paljud standardid toetavad seda – ITSO, VDV) nõuetele vastavat RFID-kiipi. Sellist kiipi sisaldavad ka ülalkirjeldatud eesti koolide RFID-süsteemide kaardid.

Pikk ja lühike tunnusnumber

Mõisted:

- PAN – identifikaatorkaardi täispikk tunnusnumber, omistatud kaardile vastavuses ISO/IEC 7812 standardiga. PAN on rahvusvaheliselt unikaalne.
- Identifikaatorkaardi lühinumber – identifikaatorkaardile visuaalselt loetaval kujul prinditud number, mis moodustab alamosa PAN-ist. Lühinumber tuletatakse PAN-ist selle algusosast teatud arvu numbripositsioonide ärajätmise teel.

Identifikaatorkaartide numereerimise põhimõtted on reguleeritud rahvusvahelise standardiga ISO/IEC 7812. Selle standardi põhiselt peab iga identifikaatorkaart omama kuni 19-kohalist numbrit, nn. PAN-i. PAN-i esimesed 6 kohta on väljaandja kood (IIN), sellele järgneb kuni 12-kohaline antud väljaandja korral unikaalne number ning viimane koht on Luhn modulus 10 algoritmiga arvutatud kontrolljärk.

Antud põhimõtetel koostatud kaardi number on suhteliselt pikk. Võimaldamaks kaardinumbrite mugavamat kasutamist, on alljärgnevas soovituses toodud põhimõtted, kuidas tuleks Eestis identifikaatorkaardile omistada PAN ning selle baasilt koostada kaardile visuaalselt kantav lühinumber. Meetodi eeliseks on kaardile kantava numbri kompaktsus (kasutatakse 11 numbrikohta) ning lisaks on numbri alguse järgi võimalik otsustada kaardi otstarbe üle. Samas on meetod ühilduv ka rahvusvahelise standardiga – lühinumbrist on võimalik lihtsa meetodiga arvutada kaardile vastav täispikk PAN.

Alltoodus järgime OÜ Eliko poolt 15.12.2010 koostatud analüüsi “Kontaktivabade piletisüsteemide ühilduvus: ülevaade ja soovitused hangeteks ning arendusteks” ettepanekuid.

Identifikaatorkaardi PAN-i koostamise põhimõtted

Tagamaks identifikaatorkaardi PAN-i esitust lühinumbrina, peab see olema koostatud ühel järgmistest kujudest:

$$i_1 \dots i_8 7vvvn_1 \dots n_6 c$$

$$i_1 \dots i_8 8mmkkn_1 \dots n_5 c$$

$$i_1 \dots i_8 9mmn_1 \dots n_7 c$$

Siin:

- $i_1 \dots i_8$ – väljaandja kood, mis on kas Eesti-sisene IIN (8 kohta) või siis rahvusvaheline IIN (6 kohta) koos kahekohalise suffiksiga (väljaandja poolt vabalt määratav).
- Liigi tähis määrab identifikaatorkaari kasutusotstarbe:
  - 7 – kliendikaart
  - 8 – kooli õpilaskaart
  - 9 – ühistranspordi sõidukaart
- mm – piirkonna kood (2 kohta)
- vvv – väljaandja kood (3 kohta)
- kk – haridusasutuse kood antud piirkonnas (2 kohta)
- n – kaardi seerianumber (pikkus on sõltuvalt kaardi liigist kas 7, 6 või 5 kohta)
- c – PAN-i kontrolljärk arvutatuna Luhn modulus 10 algoritmiga täispikast PAN-ist (ilma kontrolljärguta)

Identifikaatorkaardi lühinumbri esitamine

Identifikaatorkaardi lühinumber on esitatud 11-kohalisena, millest viimane koht on PAN-i kontrolljärk. Lühinumber saadakse PAN-ist selle esimese 8 numbrikoha ärajätmise teel.

Identifikaatorkaardi lühinumbri esimene koht määrab kaardi liigi ning see võib olla üks järgmistest:

- 7 – kliendikaardid
- 8 – haridusasutuste õpilaskaardid
- 9 – ühistranspordi sõidukaardid

Muud numbrid on reserveeritud ning neid kasutada ei tohi. Sõltuvalt kaardi liigist formeeritakse lühinumber ühel allpool toodud kujudest.

Haridusasutuste õpilaskaardid

Haridusasutuste õpilaskaardid esitatakse kujul:

8mmkknnnnnc

Kus:

- 8 – tähistab haridusasutuse õpilaskaarti
- mm – kahekohaline haridusasutuse asukoha piirkonna tähis ning see võib olla üks järgmistest:
  - 00 – Tallinn
  - 95 – Tartu

    - 11 – Narva
    - 22 – Kohtla-Järve
    - 25 – Pärnu
    - Kõik muud koodid -maakonna määrang, kus on esitatud maakonna EHAK koodi kaks viimast kohta (vt http://metaweb.stat.ee/view_xml.htm?id=2733999&siteLanguage=ee)
- kk – kahekohaline haridusasutuse kood, unikaalne antud piirkonnas
- nnnnn – 5-kohaline unikaalne seerianumber antud haridusasutuses

Lühinumbrite väljaandmine

Tagamaks lühinumbrite unikaalsust peetakse lühinumbrite prefiksite kohta üldist registrit, kus on kirjas iga konkreetse prefiksi korral väljaandja, kes sellise prefiksiga lühinumbreid väljastab. Teistel väljaandjatel pole sellise prefiksiga lühinumbrite väljastamine lubatud.

Lühinumbrite prefiksite registrit peavad ühiselt Maanteeamet (Ingmar Roos, ingmar.roos@mnt.ee) ja Ühendatud Piletite AS (Ivo Mehide, ivo@unitedtickets.ee). Väljaandja, kes soovib kasutada oma identifikaatorkaartidel antud soovitusega kooskõlalisi lühinumbreid, peab prefiksi saamiseks pöörduma ühe eelpool toodud kontakti poole.

Lühinumbrite kasutamine infosüsteemides

Infosüsteemides teisendatakse lühinumber alati täispikaks PAN-iks ning elektroonilises infovahetuses, andmete töötlemisel ja säilitamisel kasutatakse alati PAN-i. Lühinumbri teisendamisel PAN-iks tuleb kontrollida kontrolljärgu vastavust. Teisendamine teostatakse vastavalt järgmises punktis kirjeldatud metoodikale.

Lühinumbri teisendamine PAN-iks

Lühinumbri PAN-iks teisendamiseks tuleb lühinumbri prefiksi baasilt leida antud prefiksile vastava väljastaja IIN ning liita see lühinumbri ette. Peale seda tuleb kontrollida PAN-i korrektsust kontrolljärgu abil.

Lühinumbri prefiksi leidmine:

- Kui lühinumber algab ‘7’-ga, on prefiksiks lühinumbri neli esimest kohta
- Kui lühinumber algab ‘8’-ga, on prefiksiks lühinumbri viis esimest kohta
- Kui lühinumber algab ‘9’-ga, on prefiksiks lühinumbri kolm esimest kohta

Lühinumbri prefiksi baasilt leitakse väljaandja tabelist väljaandja.

Leitud väljaandja koodile lisatakse lühinumber ning kontrollitakse kontrolljärgu vastavust.

Lühinumbri baasilt PAN-i leidmise näide

Olgu meil antud identifikaatorkaart lühinumbriga “80001123450”.

Teisendame selle PAN-iks:

- Lühinumbri prefiks on “80001” (8-ga algava lühinumbri korral on prefiksiks 5 esimest kohta).
- Prefiksile vastab väljaandja “30864900” (vt eelmises punktis toodud tabel).
- PAN on seega: “8086490070001123455” (ühendame kokku väljaandja + lühinumber).
- Kontrollime kontrolljärku. Arvutame numbrist “808649007000112345” kontrolljärgu Luhni mod 10 algoritmi põhjal, selleks on “5”. See klapib PAN-i viimase kohaga, seega on esitatud lühinumber korrektne.

6. Õpilaspiletitel salvestatavate andmete mahud, võrgulahendused ja liideste/komponentide tarkvara põhimõtted

Nagu varasemas öeldud, soovitame õpilaspileti RFID-le üldse mitte mingeid andmeid kanda ning kasutada ainult kaardile tootja poolt kantavat unikaalset UID-d.

Soovi korral on võimalik lisada RFID-le kasutaja isikukood: selle info võimaliku rakendusena näeme eeskätt erinevaid raamatukogusid. Otsest vajadust isikukoodi järele ei ole ka raamatukogudel.

Peamiseks põhjuseks kaardi RFID-le isikuinfo kirjutamise vältimiseks on turvakaalutlused: rakendused, mis otsest isikuinfot kasutavad, muutuvad kergeks saagiks piletivõltsingutele, samuti muutub väga keeruliseks piletite tühistamine, näiteks kadumise korral.

Kaardil oleva unikaalse UID kasutamise põhimõtete osas juhime tähelepanu, et RFID-d kasutavaid tarkvarasüsteeme võib jaotada kahte äärmusvarianti, kusjuures koolisüsteemide jaoks soovitame kindlasti online süsteeme:

- Offline süsteemid. Sellistes süsteemides on kaardi liik, info ja selle kehtivus elektrooniliselt salvestatud otse füüsilisele kaardile sisenemisel või kontrollimisel kasutatav seade ei vaja ühendust kesktarkvaraga. Offline süsteemi eeliseks on sõltumatus võrguühendusest, miinuseks aga vajadus rakendada kaardile info kirjutamisel (ja sealt lugemisel) keerukat krüptosüsteemi, mis, nagu praktika näitab, võib osutuda suhteliselt kergesti murtavaks. Ilma krüptosüsteemita muutuks kaartide võltsimine väga lihtsaks. Krüpteeritud andmete vahetus ja töötlus kaardil võib võtta sekundeid.

- Online süsteemid. Online süsteemi korral ei ole kaardile enamasti salvestatud liiki, infot ja selle kehtivus, selle asemel on kaardi mikroskeemi tootja poolt RFID-i salvestatud unikaalne kood (UID), mis võib olla kas kaardiomanikust sõltumatu (anonüümne) või seotud

tarkvaraliselt, andmebaasi kaudu kaardiomanikuga. UID unikaalsuse tagavad kaartides sisalduvate mikroskeemide tootjad, kaardi kloonimine nõuab eritehnikat. Kaardi liigi ja kehtivuse kontroll tehakse üle võrgu tsentraalse kaartide andmebaasi vastu, kasutades kaardi mikroskeemis olevat UID-d. Plussiks asjaolu, et mingit krüptosüsteemi ei ole kaardi kontrollimisel vaja rakendada ja kaarte ei tule "eeltäita", seega on süsteem fundamentaalselt turvalisem, kui offline süsteem. Lisaväärtuseks on kiirem andmevahetus kaardiga (0,1-0,5 sekundit) ja odavam kaarditooriku hind. Miinuseks vajadus kaardi lugemissüsteemidel regulaarselt võrguühendust võtta, kuigi üldjuhul piisab sagedasest võrguühendusest, võrguühendust igal kontrollikorral vaja ei ole.

Näiteid online süsteemidest (mitte ainult RFID süsteemid):

- Eelnevas kirjeldatud eesti koolide RFID-põhised infosüsteemid
- Tallinna/Tartu ID-pileti süsteem
- Tallinna turistikaardi süsteem on online süsteemid
- Kontserdi/kinopiletisüsteemid, mis võimaldavad veebi kaudu pileti ostu (sebrapilet, Coca Cola plaza piletid jms vöötkoodi lugemisel baseeruvad piletid).
- MinuKool kaardihaldussüsteem

Online süsteemi on - suhteliselt väiksemate kaardihulkade korral - enamasti ratsionaalne realiseerida selliselt, et kogu kehtivate kaartide andmebaas talletatakse regulaarselt kõigisse kontrollseadmetesse ning lugemisel talletatakse loetav info lugeja (kontrolleri) mällu. Selle tulemusena ei ole kaartide lugemisseadmel vaja kesksüsteemiga pidevas võrguühenduses olla.

Koolisüsteemi realiseerimisel tähendab see arhitektuuri, kus lugeja/kontroller on küll võrguühenduses (eeldatavalt Etherneti kaabli kaudu) ühendused kesksserveriga, kuid:

- Sissepääsu- või toitlussüsteem laeb kesksüsteemist regulaarselt info kõigist kehtivatest/loaga kaartidest oma sisemällu.
- Registreerimissüsteem talletab kesksüsteemiga võrguühenduse puudumise korral loetud kaardid oma sisemällu ja saadab need kesksserverisse võrguühenduse taastumise korral.

Eesti koolides realiseeritud süsteemid, mida varem kirjeldasime/loetlesime, on ehitatud nimelt sellist arhitektuuri järgides.

Toome järgnevas süsteemi paljude võimalike komponentide kontrollerite ja tarkvara soovitavad põhimõtted, osad neist on realiseeritud Gustav Adolfi gümnaasiumis.

- Sisenemiste loendur. Sisaldab videokaamerat ja kontrollerit tarkvaraga. Paigaldatakse kooli peasissepääsu juurde selliselt, et videokaamera jäädvustaks kõik peauksest sisenejad ja väljujad. Kaamera videopilt salvestatakse kesksserveris. Kontrolleri tarkvara tuvastab

videopildilt kõik uksest sisenejad ja väljujad ühikuliselt ning edastab isikute arvulise info koos kellaajaga keskserverisse. Tulemusena omatakse selget ülevaadet majja sisenevate ja väljuvate inimeste arvust. Inimeste loendamise täpsus on 95% - 99%.

- Ukse kontroller. Sisaldab Mifare RFID-kaardilugejat, ukseluku juhtimise releed (mis on ühendatud olemasoleva elektrilise ukselukuga), kontrollerit tarkvaraga. Kontroller fikseerib kaardikasutuse ning vastavalt kaardi omaniku juurdepääsuõigustele kas annab või ei anna signaali ukseluku avamise releele. Kõik kaardikasutused logitakse ning edastatakse keskserverisse. Ligipääsuhalduse serveri kasutajaliidese abil saab ukse kontrollerit ka käsitsi juhtida (st – anda signaali ukseluku avamiseks), samuti jookseb online info kontrolleri tööst ka kasutaja ekraanile (valvuril on võimalik pidevalt näha, kes kaarti kasutas ning kas uks avati).
- Lifti kontroller. Töötab analoogselt uksekontrollerile, kuid ukseluku juhtimise relee asemel on relee, mille abil aktiveeritakse lifti kasutamise nupud. St – ilma vajalike õigusteta pole võimalik lifti nuppe kasutada.
- Tulekahju hoiatussüsteemi kontroller. Kui tulekahju keskseade aktiveerib tulekahju hoiatussignaali, edastatakse ka juhtsignaal kõigile süsteemi ühendatud uksekontrolleritele ukse avamiseks, samuti saadetakse signaal ka pääsla kesksüsteemi.
- Loendur. Sisaldab RFID-kaardilugejat ning kontrollerit tarkvaraga. Kontroller fikseerib kaardikasutusi ning edastab info keskserverisse. Loendureid kasutatakse koolimajas sobilikes kohtades õpilaste majja sisenemiste ja väljumiste fikseerimiseks, samuti ka klassiruumis õpilaste klassi sisenemiste fikseerimiseks. Saadud infot kasutatakse õpilaste kohaloleku staatuse määratlemiseks.
- Paljundusmasina kontroller. Sisaldab RFID-kaardilugejat ja kontrollerit tarkvaraga. Kaardi kasutamisel saadab kontrolleri tarkvara kaardi omaniku isikukoodi paljundusmasina juhttarkvarasse. Juhttarkvara ülesanne on seejärel aktiveerida paljundusmasin ning vastavalt kaardi omaniku paljundamisele seatud õigustele lubada teostada paljundamist ning pidada arvestust teenuse kasutamise mahtude osas.
- Raamatukogu kontroller. Sisaldab RFID-kaardilugejat ja kontrollerit tarkvaraga. Kaardi kasutamisel saadab kontrolleri tarkvara kaardi omaniku isikukoodi raamatukogu tarkvarale RIKS. Raamatukogu töötaja teostab seejärel RIKS tarkvara abil õpilasele raamatute laenutamise või tagasivõtmise. Alternatiivina on võimalik RFID-kaardilugeja ühendada otse RIKS tarkvara sisaldava arvutiga – siis tuleb kirjeldada kasutatavad kaardid ära RIKS tarkvaras. Sama tehnilist lahendust saab tulevikus rakendada ka muu inventari laenutamiseks.
- Söökla kontroller. Sisaldab RFID- kaardilugejat, sööklatöötajale kasutamiseks mõeldud nuppu, LCD-ekraani ja kontrollerit tarkvaraga. Kaardikasutuse peale teostab kontrolleri tarkvara kontrolli, kas antud isik peab koolitoitu saama ning kas ta on seda juba täna saanud või mitte. Tulemusest antakse söökla töötajale teada helisignaaliga ning vastava infoga ekraanil. Ekraanile kuvatakse ka õpilase info (pilt, nimi). Söökla töötajal on võimalik nupuvajutusega märkida, et kaarti näidanud õpilasele väljastatakse lisatoit.
- Süsteemi haldaja arvuti. Infosüsteemi kasutajad saavad veebiliidese abil juhtida süsteemi, genereerida erinevaid aruandeid, hallata andmeid jms.
- Õpitarkvara. Väline iseseisva tarkvarana realiseeritud õpitarkvara saab liideste abil vahetada infot õpilaste kohta, nende kohaloleku infot jms.
- Ligipääsuhalduse server. Keskne server, mille funktsioonideks on isikute ja nende juurdepääsuõiguste haldamine (nii infosüsteemi juurdepääsud kui ka ruumidele juurdepääsud), keskne sündmuste logi haldamine, e-kaartide haldamine, aruandlus. Toitlustamise aruandlus, sööjate haldamine, väliste sööjate (näiteks Reaalkoolis Muusikakooli õpilaste) haldamine. Server loeb suhtlusserveri kaudu sisse õpilaste, kooli töötajate ja teiste isikute infot, keda on vaja süsteemis kirjeldada. Server edastab suhtlusserverisse isikute kohalolekuinfot.

- Mobiilne RFID-kontrolleriga ajavõtuseade spordipäevade jms läbiviimiseks. Õpilased näitavad kontrollerile stardis oma kaarti ning samuti näitavad oma kaarti finišis. Kontroller edastab kaardikasutamiste info koos ajainfoga liigpääsuhalduse serverisse, kust hiljem saab koostada aruande õpilaste tulemuste kohta.
- RIKS raamatukogu tarkvara. Kui raamatukogu töötaja sooritab RIKS tarkvaras raamatute laenutamise või tagastamise tegevust, teostab RIKS tarkvara päringu raamatukogu kontrollerile. See tagastab tarkvarale hetkel kaarti kasutanud isiku isikukoodi.
- Paljundusmasina juhttarkvara. Kaardi kasutamisel paljundusmasina kaardilugejas teostab kontrolleri tarkvara kaardi omaniku isikukoodi edastamise paljundusmasina juhttarkvarasse. Viimane aktiveerib selle peale paljundusmasina, võimaldab masinat kasutada isikul selles ulatuses, nagu paljundustarkvaras selle isiku jaoks on määratud, ning teostab ka isiku teenuste kasutuse mahu arvestuse.

7. Soovitused enamlevinud kaarditüüpide kasutusele võtmiseks

Kaardid peaksid olema ISO/IEC 7810 standardi ID-1 formaadis ning sisaldavad ISO/IEC 14443 Type A standardile vastavat RFID-kiipi.

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

Teisisõnu, kaardid peaksid olema krediitkaardi formaadis ning sisaldama Mifare Classic andmevahetusstandardiga ühilduvaid (näiteks ka Mifare Ultralight) kiipe. Kaardilugeja ja infosüsteem peaks toetama nii 4 ja 7 baidiseid UID-e (Mifare Plus).

Alternatiivselt võib kaaluda keerukamate/kallimate RFID kiipide kasutamist, eeskätt siis Mifare DESFire, kuid me ei pea seda otstarbekaks: tegemist on Mifare Classicust ca kaks korda kallima kaardiga ning me ei näe tema täiendavatel võimalustel kooli infosüsteemi kontekstis mõtet.

Ka teiste RFID-süsteemidega võimaliku ühilduvuse aspektist on ratsionaalne kasutada lihtsamat ja väga massiliselt levinud Mifare Classic-ut.

7. Soovitused nõuete määratlemiseks privaatsusele ja infoturbele.

RFID kaartidega seotud infoturbe küsimused jagunevad kahte põhikategooriasse:

- Tagide sisu kopeerimine või muutmine, mis on kasutatav pettusteks (näiteks võimaldamaks õigustamata isikutel läbipääsu pääslast, võõra kapi avamist, kellegi teise toidu söömist 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 kandvat tagi saab niisiis kasutada esialgsest ettenähtud rakendusest sõltumatult mitmekesiseks jälitustegevuseks ja informatsiooni korjamiseks nii esemete kui neid kasutavate inimeste kohta.

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.

Varjatud jälitustegevuse vastu on võimalikud järgmised kaitsed:

- Elektroonilise isikuinfo kaardile mittekandmine (meie soovitus antud töös).
- 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 tagid 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 varjestavas (metalliseeritud) ümbrikus.

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

Siin tuleb eristada kahte võimalust:

- RFID UID massiline kandmine teistele kaartidele. Nagu eelnevalt 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 pääslalahendust ainult kaartidele, mitte aga telefonidele või eriseadmetele. Kuritarvituse alternatiivse vältimise viis oleks keerukate ja kallite PKI-põhiste kaartide kasutamine, näiteks Mifare SmartMX, mis antud rakenduse jaoks ei ole meie arust ratsionaalne. Kriitilistes pääslapunktides soovitame takistada näiteks NFC RFID kaardiemulaatori kasutamist kaardilugeja konstruktsiooniga, mis arvestaks kaardi mõõtmetega.

- 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 lahti paari sekundiga. Nimelt sellist kaarti kasutab näiteks Londoni Oyster offline süsteem. Samuti väidetakse, et kaardi "pealtkuulamise" järel on võimalik kaarti kloonida alla minutise ajakuluga. Kaardi pealtkuulamine eritehnikaga on võimalik 2-5 meetri kauguselt.

Siintoodud asjaolud on ka põhjuseks, miks elektroonilise isikuinfo kaardile kandmine on riskantne, kui ei kasutata samut tehnoloogiaid, mida näiteks RFID-ga Eesti passis (kus elektrooniline info üksi ei ole ilma visuaalse osa lugemiseta väljaloetav):

- Võimaldab massilise varjatud jälitustegevuse läbiviimist ehk suurendab selle läbiviimise riski.

- Tekitab motivatsiooni ehitada kaardilugemissüsteeme, mis autendivad isikut kaardile kantud isikuandmete (eeskätt isikukoodi) põhjal, mis on aga - erinevalt kaardi UID-st - väga lihtsalt kopeeritav ja kuritarvitatav, kui ei kasutata keerukaid krüptosüsteeme, ning ka krüptosüsteemide korral ei ole turvalisus garanteeritud.

8. Üldised soovitused tehniliste tingimuste sätestamiseks õpilaspiletite hangete läbiviimisel

Anname siinkohas kokkuvõtlikud soovitused nõuete ja tingimuste sätestamiseks RFID tehnoloogiat kasutavata õpilaspiletite hankeks.

Kaardid

Õpilaspilet on RFID-ga varustatud kaart, füüsiliselt ISO/IEC 7810 standardi ID-1 formaadis kaart (kõik tavalised krediitkaardi-mõõdus kaardid vastavad sellele standardile).

Nimetatud kaart peab sisaldama ISO/IEC 14443 Type A (nn. MIFARE Classic ühilduv standard) RFID kiipi.

Elektrooniliselt ei kanta kaardile midagi: rakendustes kasutatakse ainult tootja poolt kaardile kirjutatud UID-d.

Kaardile peaks olem visuaalselt kantud (siintoodud konkreetsed andmeliigid ja nende asukohad on soovituslikud ja vastavad MinuKool ISIC kaartide ja inDeal süsteemi kaartide visuaalsele paigutusele):

- Ülal või vasakul kooli logo/nimi
- Paremal kasutaja näopilt
- Vasakul kasutaja info: nimi, sünniaeg, töötaja/vanema korral amet või lapsevanem
- Paremal all RFID UID-le vastav visuaalselt loetav lühem PAN number (vt lõpus)

Infosüsteem, arhitektuur ja selle komponendid

RFID tagidega õpilaskaardid iseenesest ei anna koolile midagi, kuid nad võivad olla kasutajale abiks teistes RFID-toetavates koolides ja perspektiivis ka RFID-põhistes transpordisüsteemides.

Selleks, et koolil oleks RFID tagidest abi, on vaja planeerida infosüsteem, mida tellida. Infosüsteemi soovitame võtta valiku varasemas kirjeldatud komponentidest ja võimaluse korral järgida komponendi all kirjeldatud põhimõtteid:

- Sisenemiste loendur. Sisaldab videokaamerat ja kontrollerit tarkvaraga. Paigaldatakse kooli peasissepääsu juurde selliselt, et videokaamera jäädvustaks kõik peauksest sisenejad ja väljujad. Kaamera videopilt salvestatakse keskserveris. Kontrolleri tarkvara tuvastab videopildilt kõik uksest sisenejad ja väljujad ühikuliselt ning edastab isikute arvulise info koos kellaajaga keskserverisse. Tulemusena omatakse selget ülevaadet majja sisenevate ja väljuvate inimeste arvust. Inimeste loendamise täpsus on 95% - 99%.
- Ukse kontroller. Sisaldab RFID-kaardilugejat, ukseluku juhtimise releed (mis on ühendatud olemasoleva elektrilise ukselukuga), kontrollerit tarkvaraga. Kontroller fikseerib kaardikasutuse ning vastavalt kaardi omaniku juurdepääsuõigustele kas annab või ei anna signaali ukseluku avamise releele. Kõik kaardikasutused logitakse ning edastatakse keskserverisse. Ligipääsuhalduse serveri kasutajaliidesei abil saab ukse kontrollerit ka käsitsi juhtida (st – anda signaali ukseluku avamiseks), samuti jookseb online info kontrolleri tööst ka kasutaja ekraanile (valvuril on võimalik pidevalt näha, kes kaarti kasutas ning kas uks avati).
- Lifti kontroller. Töötab analoogselt uksekontrollerile, kuid ukseluku juhtimise relee asemel on relee, mille abil aktiveeritakse lifti kasutamise nupud. St – ilma vajalike õigusteta pole võimalik lifti nuppe kasutada.
- Tuletõrje kontroller Kui tuletõrjekeskus aktiveerib tulekahjusignaali, saadetakse kõigile süsteemi ühendatud uksekontrolleritele signaal ukse avamiseks.
- Loendur. Sisaldab RFID-kaardilugejat ning kontrollerit tarkvaraga. Kontroller fikseerib kaardikasutusi ning edastab info keskserverisse. Loendureid kasutatakse koolimajas sobilikes kohtades õpilaste majja sisenemiste ja väljumiste fikseerimiseks, samuti ka klassiruumis õpilaste klassi sisenemiste fikseerimiseks. Saadud infot kasutatakse õpilaste kohaloleku staatuse määratlemiseks.
- Paljundusmasina kontroller. Sisaldab RFID-kaardilugejat ja kontrollerit tarkvaraga. Kaardi kasutamisel saadab kontrolleri tarkvara kaardi omaniku isikukoodi paljundusmasina juhttarkvarasse. Juhttarkvara ülesanne on seejärel aktiveerida paljundusmasin ning vastavalt kaardi omaniku paljundamisele seatud õigustele lubada teostada paljundamist ning pidada arvestust teenuse kasutamise mahtude osas.
- Raamatukogu kontroller. Sisaldab RFID-kaardilugejat ja kontrollerit tarkvaraga. Kaardi kasutamisel saadab kontrolleri tarkvara kaardi omaniku isikukoodi raamatukogu tarkvarale RIKS. Raamatukogu töötaja teostab seejärel RIKS tarkvara abil õpilasele raamatute laenutamise või tagasivõtmise. Alternatiivina on võimalik RFID-kaardilugeja ühendada otse RIKS tarkvara sisaldava arvutiga – siis tuleb kirjeldada kasutatavad kaardid ära RIKS tarkvaras. Sama tehnilist lahendust saab tulevikus rakendada ka muu inventari laenutamiseks.
- Söökla kontroller. Sisaldab RFID- kaardilugejat, sööklatöötajale kasutamiseks mõteldud nuppu, LCD-ekraani ja kontrollerit tarkvaraga. Kaardikasutuse peale teostab kontrolleri tarkvara kontrolli, kas antud isik peab koolitoitu saama ning kas ta on seda juba täna saanud või mitte. Tulemusest antakse söökla töötajale teada helisignaaliga ning vastava infoga LCD-ekraanil. Ekraanil kuvatakse ka õpilase info (pilt, nimi). Söökla töötajal on võimalik nupuvajutusega märkida, et kaarti näidanud õpilasele väljastatakse lisatoit.
- Kasutaja arvuti. Infosüsteemi kasutajad saavad veebiliidese abil juhtida süsteemi, genereerida erinevaid aruandeid, hallata andmeid jms.
- Õpitarkvara. Väline iseseisva tarkvarana realiseeritud õpitarkvara saab liideste abil vahetada infot õpilaste kohta, nende kohaloleku infot jms.
- Ligipääsuhalduse server. Keskne server, mille funktsioonideks on isikute ja nende juurdepääsuõiguste haldamine (nii infosüsteemi juurdepääsud kui ka ruumidele juurdepääsud), keskne sündmuste logi haldamine, e-kaartide haldamine, aruandlus. Toitlustamise aruandlus, sööjate haldamine, väliste sööjate (näiteks Reaalkoolis Muusikakooli õpilaste) haldamine. Server loeb suhtlusserveri kaudu sisse õpilaste, kooli töötajate ja teiste

isikute infot, keda on vaja süsteemis kirjeldada. Server edastab suhtlusserverisse isikute kohalolekuinfot.

- Mobiilne RFID-kontrolleriga ajavõtuseade spordipäevade jms läbiviimiseks. Õpilased näitavad kontrollerile stardis oma kaarti ning samuti näitavad oma kaarti finišis. Kontroller edastab kaardikasutamiste info koos ajainfoga liigpääsuhalduse serverisse, kust hiljem saab koostada aruande õpilaste tulemuste kohta.
- RIKS raamatukogu tarkvara. Kui raamatukogu töötaja sooritab RIKS tarkvaras raamatute laenutamise või tagastamise tegevust, teostab RIKS tarkvara päringu raamatukogu kontrollerile. See tagastab tarkvarale hetkel kaarti kasutanud isiku isikukoodi.
- Paljundusmasina juhttarkvara. Kaardi kasutamisel paljundusmasina kaardilugejas teostab kontrolleri tarkvara kaardi omaniku isikukoodi edastamise paljundusmasina juhttarkvarasse. Viimane aktiveerib selle peale paljundusmasina, võimaldab masinat kasutada isikul selles ulatuses, nagu paljundustarkvaras selle isiku jaoks on määratud, ning teostab ka isiku teenuste kasutuse mahu arvestuse.

Infosüsteemi arhitektuurina kasutatakse online süsteemi järgmises tähenduses. Online süsteemi korral ei ole kaardile enamasti salvestatud liiki, infot ja selle kehtivus, selle asemel on kaardi mikroskeemi tootja poolt RFID-i salvestatud unikaalne kood (UID), mis võib olla kas kaardiomanikust sõltumatu (anonüümne) või seotud tarkvaraliselt, andmebaasi kaudu kaardiomanikuga. UID unikaalsuse tagavad kaartides sisalduvate mikroskeemide tootjad, kaardi kloonimine nõuab eritehnikat. Kaardi liigi ja kehtivuse kontroll tehakse üle võrgu tsentraalse kaartide andmebaasi vastu, kasutades kaardi RFID-l olevat UID-d.

Kaardi lühinumbri - PAN - leidmine

Mõisted:

- PAN – identifikaatorkaardi täispikk tunnusnumber, omistatud kaardile vastavuses ISO/IEC 7812 standardiga. PAN on rahvusvaheliselt unikaalne.
- Identifikaatorkaardi lühinumber – identifikaatorkaardile visuaalselt loetaval kujul prinditud number, mis moodustab alamosa PAN-ist. Lühinumber tuletatakse PAN-ist selle algusosast teatud arvu numbripositsioonide ärajätmise teel.

Identifikaatorkaartide numereerimise põhimõtted on reguleeritud rahvusvahelise standardiga ISO/IEC 7812. Selle standardi põhiselt peab iga identifikaatorkaart omama kuni 19-kohalist numbrit, nn. PAN-i. PAN-i esimesed 6 kohta on väljaandja kood (IIN), sellele järgneb kuni 12-kohaline antud väljaandja korral unikaalne number ning viimane koht on Luhn modulus 10 algoritmiga arvutatud kontrolljärk.

Antud põhimõtetel koostatud kaardi number on suhteliselt pikk. Võimaldamaks kaardinumbrite mugavamat kasutamist, on alljärgnevas soovituses toodud põhimõtted, kuidas tuleks Eestis identifikaatorkaardile omistada PAN ning selle baasilt koostada kaardile visuaalselt kantav lühinumber. Meetodi eeliseks on kaardile kantava numbri kompaktsus (kasutatakse 11 numbrikohta) ning lisaks on numbri alguse järgi võimalik otsustada kaardi otstarbe üle. Samas on meetod ühilduv

ka rahvusvahelise standardiga – lühinumbrist on võimalik lihtsa meetodiga arvutada kaardile vastav täispikk PAN.

Alltoodus järgime OÜ Eliko poolt 15.12.2010 koostatud analüüsi “Kontaktivabade piletisüsteemide ühilduvus: ülevaade ja soovitused hangeteks ning arendusteks” ettepanekuid.

Identifikaatorkaardi PAN-i koostamise põhimõtted

Tagamaks identifikaatorkaardi PAN-i esitust lühinumbrina, peab see olema koostatud ühel järgmistest kujudest:

$$i_1 \dots i_8 7vvvn_1 \dots n_6 c$$

$$i_1 \dots i_8 8mmkkn_1 \dots n_5 c$$

$$i_1 \dots i_8 9mmn_1 \dots n_7 c$$

Siin:

- $i_1 \dots i_8$ – väljaandja kood, mis on kas Eesti-sisene IIN (8 kohta) või siis rahvusvaheline IIN (6 kohta) koos kahekohalise suffiksiga (väljaandja poolt vabalt määratav).
- Liigi tähis määrab identifikaatorkaari kasutusotstarbe:
  - 7 – kliendikaart
  - 8 – kooli õpilaskaart
  - 9 – ühistranspordi sõidukaart
- mm – piirkonna kood (2 kohta)
- vvv – väljaandja kood (3 kohta)
- kk – haridusasutuse kood antud piirkonnas (2 kohta)
- n – kaardi seerianumber (pikkus on sõltuvalt kaardi liigist kas 7, 6 või 5 kohta)
- c – PAN-i kontrolljärk arvutatuna Luhn modulus 10 algoritmiga täispikast PAN-ist (ilma kontrolljärguta)

Identifikaatorkaardi lühinumbri esitamine

Identifikaatorkaardi lühinumber on esitatud 11-kohalisena, millest viimane koht on PAN-i kontrolljärk. Lühinumber saadakse PAN-ist selle esimese 8 numbrikoha ärajätmise teel.

Identifikaatorkaardi lühinumbri esimene koht määrab kaardi liigi ning see võib olla üks järgmistest:

- 7 – kliendikaardid
- 8 – haridusasutuste õpilaskaardid
- 9 – ühistranspordi sõidukaardid

Muud numbrid on reserveeritud ning neid kasutada ei tohi. Sõltuvalt kaardi liigist formeeritakse lühinumber ühel allpool toodud kujudest.

Haridusasutuste õpilaskaardid

Haridusasutuste õpilaskaardid esitatakse kujul:

8mmkknnnnnc

Kus:

- 8 – tähistab haridusasutuse õpilaskaarti
- mm – kahekohaline haridusasutuse asukoha piirkonna tähis ning see võib olla üks järgmistest:
  - 00 – Tallinn
  - 95 – Tartu
  - 11 – Narva
  - 22 – Kohtla-Järve
  - 25 – Pärnu
  - Kõik muud koodid -maakonna määrang, kus on esitatud maakonna EHAK koodi kaks viimast kohta (vt http://metaweb.stat.ee/view_xml.htm?id=2733999&siteLanguage=ee)
- kk – kahekohaline haridusasutuse kood, unikaalne antud piirkonnas
- nnnnn – 5-kohaline unikaalne seerianumber antud haridusasutuses

Lühinumbrite väljaandmine

Tagamaks lühinumbrite unikaalsust peetakse lühinumbrite prefiksite kohta üldist registrit, kus on kirjas iga konkreetse prefiksi korral väljaandja, kes sellise prefiksiga lühinumbreid väljastab. Teistel väljaandjatel pole sellise prefiksiga lühinumbrite väljastamine lubatud.

Lühinumbrite prefiksite registrit peavad ühiselt Maanteeamet (Ingmar Roos, ingmar.roos@mnt.ee) ja Ühendatud Piletite AS (Ivo Mehide, ivo@unitedtickets.ee). Väljaandja, kes soovib kasutada oma identifikaatorkaartidel antud soovitusega kooskõlalisi lühinumbreid, peab prefiksi saamiseks pöörduma ühe eelpool toodud kontakti poole.