

ID-kaart

Lähteuringu aruanne

Sisukord

Sisukord	2
Sissejuhatus.....	4
Kaardistus	5
Kaardistatud asutused.....	5
Põhilised seisukohad.....	6
Kodakondsus- ja Migratsiooniamet	6
Autoregistrikeskus.....	6
Maksuamet.....	6
Piirivalveamet	7
Politseiamet.....	7
Kaitsepolitseiamet.....	7
Kaitseministeerium	8
Siseministeerium.....	8
Teede- ja Sideministeerium	8
Keskhaigekassa	8
Sotsiaalkindlustusamet.....	8
Riigikantselei	9
Digitaalsignatuuri seaduse komisjon	9
Hansapank.....	10
Ühispank.....	10
Pankade Kaardikeskus.....	10
Eesti Energia	10
Eesti Telefon	11
Neste	11
Tallinna Kaubamaja.....	11
Andmete koondtabel.....	12
Teenuste koondtabel.....	13
Olemasolevad autentimisskeemid.....	14
Pank	14
Haigekassa	18
Tankla	19
Pääsla	20
Taksofon	21
Digitaalsignatuur	22
ID-kaardile esitatavad nõuded.....	23
Nõuded visuaalsele komponendile	23
Nõuded elektroonilisele komponendile.....	23
Esmase väljaandja andmed.....	23
Kaasväljaandjate andmed.....	24
Nõuded protseduuridele	24
Nõuded väljaandmise protseduurile	24
Nõuded kasutamise protseduuridele	25
Nõuded tühistamise protseduurile	25
ID-kaardi foorum ja ankeet.....	26
ID-kaardi foorum.....	26
ID-kaardi ankeet.....	27
Plussid-miinused eraisiku jaoks	27
Plussid-miinused asutuse, organisatsiooni jaoks	27
Plussid-miinused riigi jaoks.....	28
Lahendusvariandid.....	29
Kaardi väljastamine.....	29
Hajutatud väljastamine.....	29
Tsentraalne andmebaas.....	30

Hajutatud andmebaas.....	31
Osaliselt hajutatud väljastamine.....	32
Kokkuvõte.....	33
Kaardi kasutamine	34
Autentimine kaardi staatiliste andmete alusel	34
Autentimine kaardi privaatvõtme alusel.....	34
Autentimine kaardi ja terminaali privaatvõtmete alusel.....	35
PINi kontrollimine terminaali poolt.....	36
PINi kontrollimine kaardi poolt.....	36
Nihkega PINi kontrollimine kaardi poolt.....	37
Signeeritava tehingu kontrollimine kaardiomaniku poolt.....	38
Signeeritava tehingu fikseerimine kaardiomaniku poolt.....	38
Kokkuvõte.....	39
Kaardi blokeerimine	42
Hajutatud blokeerimine.....	42
Tsentraalne andmebaas.....	42
Hajutatud andmebaas.....	43
Kokkuvõte.....	44
Kokkuvõte.....	46

Sissejuhatus

Vastavalt Informaatikakeskuse ja AS Aprote vahel sõlmitud lepingule viis AS Aprote aja-vaheajal 27. juulist kuni 18. septembrini 1998 läbi lähteuringu ID-kaardi potentsiaalsete kasutajate poolt kaardile esitatavate nõudmistele väljaselgitamiseks ja võimalike lahendusvariantide väljatöötamiseks.

Lähteuring koosnes kolmest osast:

- kaardistus – kaardistati ID-kaarti oma klientide identifitseerimiseks kasutada võivate asutuste olemasolevad teenused ja käesoleval ajal kasutatavad klientide autentimise meetodid, nende asutuste poolt esitatavad nõuded kaardile kantavate andmete ja nende turvalisuse osas ning uued teenused, mis võiks ID-kaardi kasutuselevõtuga võimalikuks saada;
- ID-kaardi foorum ja ankeet – aadressil <http://www.id.ee> avati WWW-server, milles on projekti lühike tutvustus, foorum serveri kasutajate omavaheliseks arvamustevahetuseks ID-kaardi teemadel ja ankeet;
- lahendusvariantide väljatöötamine – kaardistuse ja ankeedi kaudu saadud arvamuste ja nõudmistele põhjal töötati välja võimalikud lahendusvariandid kaardi väljastamise, kasutamise ja blokeerimise haldamiseks.

Kaardistus

Kaardistus toimus intervjuudena AS Aprote küsitlejate ja kaardistatavate asutuste esindajate vahel. Allpool on ära toodud intervjuude põhjal koostatud koondid. Kaardistusintervjuude täielikud protokollid on käesoleva aruande Lisas 1.

Kuna protokollid koostati pärast intervjuud ainult küsitletud isikutega, ei tarvitse protokollides toodud seisukohad olla vastavate asutuste ametlikud seisukohad. Küsitletud isikute positsioonid lubavad siiski arvata, et võimalikud erinevused ei tohiks olla suured.

Kaardistatud asutused

Asutus	Nimi	Ametikoht
Kodakondsus- ja Migratsiooniamet	Kalev Pihl	infoosakonna juhataja asetäitja
Autoregistrikeskus	Juhan Kaarpalu	direktori asetäitja
Maksuamet	Aare Lapõnin	peadirektori asetäitja
Piirivalveamet	Alar Jõeeste	arvutiosakonna ülem
Politsei	Andrus Voolaine Raul Savimaa Toomas Adson	infosüsteemide talituse vanemohvitser info- ja sideosakonna politseidirektor andmeside projekti juht
Kaitsepolitsei	Arnold Sinisalu	
Kaitseministeerium	Avo Elme	side ja infotehnoloogia osakonna juhataja
Siseministeerium	Hillar Aareleid	andmekaitse järelevalveasutuse juhataja
Teede- ja Sideministeerium	Neeme Mozolev	
Keskaigekassa	Kaljo Tinn	infotehnoloogia osakonna juhataja
Sotsiaalkindlustusamet	Indrek Kressa	infotehnoloogia osakonna juhataja
Riigikantselei	Rein Kauber Uno Vallner	nõunik nõunik
Digitaalsignatuuri seaduse komisjon	Ahto Buldas	
Hansapank	Heiki Kübbar	infotehnoloogia asedirektor jaotuskanalite alal
Ühispank	Eero Tohver	jaotuskanalite arendusosakonna juhataja
Pankade Kaardikeskus	Margus Aun	tegevdirektor
Eesti Energia	Tarmo Soodla	
Eesti Telefon	Avo-Rein Tereping	teenuste turunduse osakonna juhataja
Neste	Heikki Vuorinen	jaemüügijuht
Tallinna Kaubamaja	Tiit Tammiste	
ID Süsteemide AS	Enn Lakspere	juhatuse esimees

Põhilised seisukohad

Järgnevas on ära toodud kaardistuste käigus selgunud põhilised seisukohad asutuste lõikes.

Kodakondsus- ja Migratsiooniamet

- Positiivne suhtumine ei tähenda tingimata seda, et kõik andmed ja funktsioonid tuleks panna just sellele kaardile. Riigi poolt väljastatava kaardi põhiline funktsioon peaks olema isiku identifitseerimine. Muude andmete (kontonumbri vms) kirjutamine otse riigi poolt väljastatavale kaardile oleks pigem isegi ebasoovitav, need andmed peaks saama vastava teenuse pakkuja andmebaasist, kui teenuse saaja isik on kaardi abil kindlaks tehtud, või väljastab teenuse pakkuja oma kaardi, mis on valmistatud sama profiili järgi ja seega sama infrastruktuuriga kasutatav. Ainult isikut tõendavaks dokumendiks pole ID-kaarti siiski ka mõtet teha, see oleks liiga kulukas.
- Omaette probleemi tekitavad ajas muutuvad andmed: neid saab kaardil hoida ainult elektroonilisel kujul, kuid mõnda neist peaks saama kasutada ka visuaalselt.
- Kaardi *offline* kasutamise võimalus on pigem ebasoovitav, sest see suurendab riske kaardi kaotuse korral. Pigem võiks kaardil olevat protsessorit kasutada kaardi abil tehtavate tehingute krüptimise ja signeerimise jaoks, et tagada piisav turvalisus *online*-tehingutes.
- Kaotatud kaardi asemele uue väljastamise protseduur peab olema piisavalt tülikas, et inimesel ei tekiks huvi oma kaarti müüa (praegu passidega on see probleem). Samuti peaks tekitama motivatsiooni leitud kaardi tagastamiseks (omanikule või KMAle). Vaja oleks ka suhteliselt raskeid sanktsioone kaardi või signatuuri "laenamise" eest nii laenajale kui ka laenutajale.
- Rahvusvahelise reisidokumendina kasutatava ID-kaardi jaoks on ICAO töögrupp välja pakkunud nimetuse PASSPORT CARD ja on töötanud välja omapoolsed nõuded kaardile.
- Digitaalse signeerimise funktsiooni lisamine ID-kaardile on oluline ennekõike sellepärast, et see annaks riigile tegeliku vahendi digitaalsignatuuri kasutamiseks.
- Oluline on ka inimeste valmisolek, näiteks Taiwanis tehti ID-kaart mis seoti panga-funktsioonidega, aga inimesed lihtsalt ei võtnud seda endale.

Autoregistrikeskus

- Rahvusvahelistele juhilubadele kehtestatud tingimused on küllalt ranged ning Euroopa Ühenduse direktiivide kohaselt tuleks vältida mingi oma infotehnoloogia sisseviimist tuginedes EÜ juhiloa näidisele. Samas on eraldi siseriikliku ning rahvusvahelise juhiloa sisseviimine (ka juhul, kui siseriiklik juhiluba on ühitatud ID-kaardiga) suhteliselt mõttetu.
- Sõidukite ümberregistreerimisel (auto müügil) tuleb hetkel kehtivate seaduste kohaselt kontrollida ka seda, kas sõiduk pole abikaasade ühisomand. Seega on vaja teada ka vähemalt isiku perekonnaseisu.

Maksuamet

- Plaanid on rohkem Interneti poole suunatud. Plaanis on pakkuda võimalust kontokaardi vaatamiseks. See võimaldaks, analoogiliselt pankade poolt pakutava Internetipangaga, vaadata oma jooksvat maksude laekumise seis.

- Hetkel on pass ainuke täielikult aktsepteeritav isikut tõendav dokument, kuna praegustele autojuhilubadele on allkirjanäidis trükitud, mitte aga isiku oma käega kirjutatud.
- Maksuametil pole probleeme sellega, et deklaratsioon oleks võltsitud, seega pole erilist vajadust deklaratsiooni autentsust kontrollida. Kui siiski hakatakse kasutama digitaalset signeerimist ID-kaardi baasil, ei näe ka Maksuamet põhjust seda mitte teha.

Piirivalveamet

- Teised riigid saavad ID-kaarti tunnustada piiriületusel vaid vastavate kokkulepete alusel. Seni on vastavate kokkulepete sõlmimine välisministeeriumi kompetentsis. Otstarbekas on kaarti rakendada eeskätt lähinaabritega (Läti, Soome, ehk ka Rootsi) piiri ületamisel, kuna nende riikidega on Eestil viisavabadus ning piiriületusi ka kõige rohkem.
- Piiri ületamiseks lihtsustatud korras peab inimene omama kas passis vastavat templit või tõendit omavalitsuselt. Samuti on mõnel pool koostatud nimekirjad lihtsustatud piiriületust kasutada tohtivatest isikutest. ID-kaardi rakendamisel võib vastavaid andmeid hoida kas kaardil (kaardil vastav aplikatsioon, mille kirjutab Piirivalveamet omavalitsusest saadud andmete põhjal) või piirivalve andmebaasis.

Politseiamet

- Kaart peaks olema ka suhteliselt halva valgusega hästi loetav. Politsei seisukohalt on seda parem, mida rohkem informatsiooni kaardil on. On asju, mida politseinik peab saama kohapeal kontrollida ning oleks väga positiivne, kui need paikneksid otse kaardil, näiteks relvaloa ja autojuhiloa andmed. Viited peaksid olema nii passi-, rahvastiku-, autojuhilubade-, autode-, hoone-, relva-, karistus-, kui ka kriminaalhooldusregistrisse – see vähendab eelkõige vajadust erinevate dokumentide kaasaskandmiseks isikute poolt.
- Relvaloal vajalikud andmed: loa nr, omaniku andmed (ees- ja perekonnanimi, isikukood, elukoht), omaniku foto, omaniku allkiri, loa kehtivusaeg, loa väljaandnud (politsei)asutus, relva(de) hoiukoha aadress, relva(de) otstarve, liik, mark, kaliiber, number, optilis(t)e või lasersihiku(te) number.
- Probleeme võib tekkida erinevate registrite ühitamisel, aga paratamatult tuleb see töö kunagi ära teha ning kaardiprojekt oleks selleks küllalt hea.

Kaitsepolitseiamet

- Kaardil peaks olema võimalikult vähe andmeid, kõik mistahes teenuse spetsiifilised andmed peaksid asuma vastavat teenust osutava ametkonna andmebaasis ja ainult selle teenuse kasutamisel kaardi ID alusel sealt andmebaasist kättesaadavad olema. See võimaldaks tõhusamalt reguleerida, kes milliseid andmeid isiku kohta kätte saab.
- ID-kaardil ei peaks olema isikukoodi, ei visuaalselt ega elektrooniliselt loetaval kujul. Isikukood ei muutu inimese elu jooksul ja see muudab erinevatest allikatest ja erinevatest aegadest pärit andmete koondamise liiga kergeks. Kaardil peaks olema kaardi ID, mis kaardi vahetumisel muutuks ja seega takistaks erinevatel aegadel ja erinevatest allikatest pärinevate andmete ühendamist.
- Sõrmejälje kaardile kandmisele oleks alternatiiviks sõrmejälgede võtmine ja nende kandmine andmebaasi kaardi väljastamisel. See andmebaas oleks ühtlasi ka aluseks uue ID-kaardi väljastamisel selle kadumise või rikkumise korral.

- Kui ID-kaart saab üleüldiseks ja universaalseks dokumendiks, tuleb teha ka põhimõtteline poliitiline otsus, kas selle pidev kaasaskandmine on kohustuslik.

Kaitseministeerium

- Arendatakse pääslakaarte. Plaanis on välja töötada kutsealustele antav tunnistus kaardi kujul. Lisaks on plaanis välja töötada ühtne süsteem arvutitele ligipääsu piiramiseks.

Siseministeerium

- Kaardil peaks olema üks (esmane) väljaandja. Tema õigused ning kohustused peaksid olema samad, mis passide väljaandjal.
- Kaardi planeerimise algstaadiumis tuleks läbi mõelda nii kaardi toimimine tavaolukorras (kui kaart on juurutatud), kui ka kaardi juurutamise etapis (üleminekustaadiumis).
- Tuleb tagada, et inimene mitte mingil juhul ei annaks kaarti kellelegi teisele. Ideaalis võiks PINi millegi paremini isikuga samastatava vastu vahetada (sõrmejalg, silma sarvkest vms) Samas tuleks seaduslikult sätestada, et kui inimene annab oma PINi kellelegi teisele, siis vastutajaks jääb ikkagi tema.
- Kaaluda tasuks ka varianti, et distantsilt tehtavatele tehingutele panna piirang, millest suuremaid tehinguid võib küll teha, aga pole seaduslikku alust nende tunnistamiseks (vastava limiidi kehtestamist praegu digitaalsignatuuri seaduse komisjonis arutatakse).

Teede- ja Sideministeerium

- TSM võiks ID-kaarti kasutada autojuhiloana, kuid selle välistavad ühelt poolt vajadus kasutada juhiluba ka väljaspool Eestit ja teiselt poolt Euroopa Ühenduse direktiiviga kehtestatud nõuded juhiloa väljanägemisele ning tungiv soovitus mitte lisada juhiloale oma infotehnoloogiat.

Keskhaigekassa

- Kuna magnetkaartide projekt sai alles äsja hoo sisse, siis esialgu midagi uut ei planeerita. Samas kehtivad olemasolevad kaardid 3 aastat (magnetkaardi füüsilise kulumise piir) ja järgmine ring kaarte võib olla vabalt mõnel muul alusel (ka näiteks ID-kaart).

Sotsiaalkindlustusamet

- Peamine huvi oleks arvatavasti ID-kaardi rakendamisel pensionikindlustuse registri liikme-kaardina. Kuna isikute identifitseerimine pensionikindlustuse registri seisukohalt toimub isikukoodi või selle komponentide alusel, on kaardi kasutamine suhteliselt lihtne.
- ID-kaart võiks asendada ka pensionitunnistust. Probleemiks võib saada see, kui isikule määratakse mingi muu pension, mitte vanaduspension, kuna pensionäridele osutatakse mitmeid soodustusi pensionitõendi ettenäitamisel. Vanaduspensioni puhul on võimalik pensionilolek üheselt sünniaastast tuletada, aga teistele pensionäridele oleks hea teha ID-kaardile mingi visuaalselt nähtav märk. Samas on probleemiks, et muud pensionid võidakse määrata lühemaks ajaks kui ID-kaardi kehtivusaeg (1-5 aastat).

Riigikantselei

- Kaardi väljastamisel peaks kogu riiklike asutuste poolt sinna kantav info juba olema olemas. Inimest ei tohiks info kaardile kandmiseks mööda erinevaid asutusi jooksutada. Kommertsasutuste poolt kaardile kantava info suhtes pole kindlat suhtumist. Nad võivad kas info ise kaardile kirjutada või tellida selle teenuse kaardi väljaandjalt.
- ID-kaardi kasutuselevõtmine on paratamatus. Kõigis arenenud riikides on see nii läinud, meie pole ilmselt mingi erand. Küsimus on ainult selles, kui palju sellele kaardile funktsioone anda. Üldiselt pole hea panna liiga palju funktsionaalsust ühte kaarti – mida rohkem funktsionaalsust, seda suurem on kahju selle kadumise või rikkumise korral. Kui kõik inimese õigused on ühe kaardi peal, jääb ta selle kadumisel korraga ilma kõigist oma õigustest.
- Kui ID-kaart saab siiski olema digitaalsignatuuri hoidjaks, tuleks kindlasti ette näha võimalus mitme erineva signatuuri hoidmiseks samal kaardil, sest esiteks ei tarvitse kommertsstruktuurid Passiameti väljastatud võtmeid aktsepteerida, teiseks sätestab tulevane digitaalsignatuuri seadus tõenäoliselt mitme erineva tasemega signatuure ja on üsna loomulik eeldada, et inimene võib endale tahta mitut erinevat erineva tasemega signatuuri, ja kolmandaks, on üsna loomulik eeldada, et näiteks Jaapanis töötav Eesti diplomaat tahab endale nii Eesti kui Jaapani autoriteetide sertifitseeritud signatuure.

Digitaalsignatuuri seaduse komisjon

- Omaette probleem on KMA võtmete sertifitseerimine. Kui KMA ise on sertifitseerimise hierarhia tipp (tema sertifitseerib kõiki teisi sertifitseerijaid), siis ei saa tema võtmeid süsteemiselt sertifitseerida. Ainus võimalus on kasutada mingeid süsteemiväliseid vahendeid, näiteks avaldada võtmed ajalehtedes (ilmselt võib eeldada, et keegi ei suuda võltsida ega hävitada kõigi ajalehete täistiraape).
- Kaardi omaniku ja selle esitaja isikusamasuse tuvastamiseks peaks olema mingi biomeetriline atribuut (allkiri koos kirjutamise dünaamikaga, foto infrapunases valguses vms). Kui kaarti hakatakse kasutama ainult *online*, siis ei pea biomeetriline element kaardil olema, selle võib kaardi ID alusel lugeda kesksest serverist.
- ID-kaardi ja elektronrahakoti funktsioonid peaks jääma eraldatuks – raha peaks olema anonüümne, kuid ükski ID-kaardil olev funktsioon ei saa seda olla, juba kasvõi sellepärast, et kaardile on isikuandmed ka trükitud ja nende lugemise üle pole kaardil mitte mingit kontrolli.
- Digitaalsignatuuri sertifitseerimisel tuleks sertifitseeritavale võtmele kindlasti kehtestada vastutuse ülempiir; see ülempiir peaks ilmutatud kujul kajastuma ka võtme sertifikaadis, et signatuuri vastuvõtja saaks kontrollida signatuuri pädevust antud tehingu või dokumendi kinnitamiseks. (Esiialgu võikski digitaalsignatuuri kasutada ainult rahaliselt määratava vastutusega tehingutes, muud tehingud (mille puhul ka vastutuse piiri määramine on raskem) võiksid jääda hiljemaks, kui süsteem on juba sisse töötatud ja oma turvalisust ka praktikas tõestanud.) Digitaalsignatuuri seadus võiks kehtestada mingi kanoonilise tehingute nimekirja, millest sertifikaadi taotleja valib need, mille tegemiseks ta oma võtmele sertifikaati soovib.

Hansapank

- Arvatavasti oleks parem teha eraldi kaardid riiklike ja kommertsfunktsioonide jaoks. Ühine kaart tekitab mitmeid põhimõttelisi probleeme:
 - Eesti riik võib ID-kaarte väljastada ainult Eesti kodanikele (ja äärmisel juhul ka siin alaliselt elavatele isikutele), aga kommertsstruktuuride kliendid võivad olla ka välismaalased;
 - ilmselt tahaks pangakaart tulevikus olla ühilduv kas VISA või MasterCardi elektronraha standarditega, aga selle funktsiooni ühendamine ID-kaardiga tähendaks seda, et Eesti riik peaks oma riikliku isikut tõendava dokumendi väljaandmiseks taotlema sertifikaati välismaiselt kommertsorganisatsioonilt;
 - riiklikul ID-kaardil olevad andmed peaksid olema märksa pikaealisemad pangakaardil (või muudel kommertskaartidel) olevatest;
 - nõutavad turvatasemed on erinevad, riikliku ID-kaardi kui passi turvatase peaks olema suurusjärg üle pangakaardi turvataseme (mis on kõrgeimate nõuetega kommertsrakenduste hulgas);
 - riiklik ID-kaart kui pass ei ole see asi, mida inimene peaks toppima igasse bussi-kompostrisse või telefoni- ja parkimisautomaati.
- Digitaalse signeerimise funktsioonil pole panga jaoks mingit väärtust, kui sellel pole riigi garantiid, et digitaalselt allkirjastatud dokument on kõikjal (sealhulgas kohtus) samaväärne paberdokumendiga.

Ühispank

- Igal juhul on pank kohustatud ID-kaarti aktsepteerima, kui see on riiklikult kehtestatud isikut tõendav dokument.
- Kaardi (kui riikliku isikut tõendava dokumendi) esmane väljaandja peaks kindlasti olema selleks volitatud riigiasutus. Muu haldusega (salvestusruumi haldamine, teenusmodulite salvestamine kaardile, kaardilugejate- ja kirjutajate taatlemine jne) võib tegeleda ka mingi muu (võimalik, et spetsiaalselt selleks loodud) organ.
- Selline kaart parandab tõenäoliselt ka passikasutuse distsipliini – kui palju eluks vajalikke toiminguid toimub ID-kaardi alusel, käivad inimesed seda õigeaegselt pikendamas jmt.

Pankade Kaardikeskus

- Idee on põhimõtteliselt hea ja seni, kuni kaardil pole maksefunktsiooni, võib EV sellega tegeleda. Kui aga kaardiga seotakse rahalised funktsioonid, siis, vaadates andmeturbe olukorda riigiasutustes, ei usu, et mõni erafirma (eriti aga pank) usaldaks oma andmed kaardile, mille turvet haldab riigiasutus.

Eesti Energia

- Üldine suhtumine ID-kaardi ideesse on positiivne, kuid Eesti Energia ei taha olla kaardi katsetamisel või juurutamisel pioneeriks. Kui kaart käibima hakkab ning piisava turvalisusega on, hakkab ka Eesti Energia seda kasutama.

- Kuna Eesti Energial on hetkel suhteliselt väike kokkupuude oma eraisikust klientidega (tasumine toimub reeglina panga vahendusel ja muud polegi vaja), siis pole otsest vajadust ka mingi kliendikaardi järele. Tulevikus, kui energiaturg vabaks lastakse, võib ka Eesti Energial tekkida vajadus kliendikaardi järele ja siis võiks ta olla kliendikaardi funktsiooni kasutaja.

Eesti Telefon

- Plaanis on luua klienti identifitseeriv kaart, mille alusel klient saaks kasutada mitmeid teenuseid ning lisateenuseid tellida (kliendikaart). Loodava ID-kaardiga oleks väga lihtne kliendikaardi funktsioone katta. Eesti Telefoni jaoks muutub määravaks see, kas ta saab kaardi järgi üheselt identifitseerida inimese, kes seda kaarti kasutab.

Neste

- Positiivne, ehkki esialgu jäädakse äraootavale seisukohale. Esmane rakendus tuleb arvatavasti maksevahendina (kui pangad hakkavad ID-kaarti kasutama, ei jää Nestel ka muud üle kui seda aktsepteerida).

Tallinna Kaubamaja

- Kaubamaja kliendikaardi funktsioon ei ole ID-kaardiga ühendatav, sest kliendikaart peab teenindajal võimaldama kliendi visuaalselt ära tunda (st kaubamaja kliendi kaart peab visuaalselt erineva kõigist muudest kaartidest, mis ID-kaardi korral pole ilmselt võimalik).

Andmete koondtabel

Allolev tabel võtab kokku põhilised nõudmised ID-kaardil olevatele andmetele, funktsionaalsusele ja turvaele

Asutus	Inimloetavalt													M:				
	Nimi	Sünniaeg	Sünnikoht	Isikukood	Sugu	Foto	Allkiri	Sõrmejalg	Veregrupp	Kaardi ID	Kehtivus	Väljaandja	Muud	Nimi	Sünniaeg	Sünnikoht	Isikukood	Sugu
Kodakondsus- ja Mirgatsiooniamet	+	+		+	+	+	+			+	+	+		+	+		+	+
Autoregistrikeskus	+	+		+		+	+				+			+	+		+	
Maksuamet	+	+		+		+	+				+			+	+		+	
Piirivalveamet	+	+		+		+	+			+	+	+		+	+		+	
Politseiamet	+			+		+	+	+			+			+			+	
Kaitsepolitseiamet	+	+	+	-			+	+	+	+				+	+	+	-	
Kaitseministeerium	+	+		+		+	+										+	
Siseministeerium	+			+		+	+						+ ⁵	+			+	
Teede- ja sideministeerium																		
Keskhaigekassa	+	+		+		+	+				+			+	+		+	
Sotsiaalkindlustusamet	+	+		+		+	+				+			+	+		+	
Riigikantselei	+/+	/+		+/+		+/+	+/+							+/+	/+		+/+	+
Digitaalsignatuuri seaduse komisjon	+			+		+	+			+				+			+	
Hansapank	+			+		+	+				+			+			+	
Ühispank	+			+		+	+			+	+			+			+	
Pankade Kaardikeskus	+			+		+	+							+			+	
Eesti Energia																		+
Eesti Telefon	+	+		+		+	+											+
Neste																		+
Tallinna Kaubamaja																		

- 1 Mingid lisaandmed, mida kaardi vastuvõtja saab vajadusel kasutada kaardi
- 2 Perekonnaseis, kodakondsus
- 3 Viiteid erinevatesse registritesse; lisaks juhiloa ja relvaloa andmed ka otse
- 4 KAPO ei kasutaks ID-kaarti oma töötõendi või uksekaardina, sest KAPO is
- 5 Kõik riigi poolt antavad õigused: juhiluba, relvaluba jne
- 6 Juhilubasid ei saa ID-kaardiga ühendada, sest juhilubadele on EL kehtestar
- 7 Muutuvaid andmeid (aadress, telefon jne) ei tohiks kaardile kanda, need pe
- 8 Kaardil peaks elektrooniliselt loetavalt olema mingi biomeetriline atribuut: all
- 9 Isikut tõendava dokumendi kohustuslikud andmed
- 10 Kliendikaart peab võimaldama visuaalselt klienti eristada

Teenuste koondtabel

Teenuste koondtabel annab ülevaate küsitluste käigus selgunud (nii olemasolevatest kui potentsiaalsetest) teenustest.

Asutus	Arv ¹	Teenus	Olemas ²	Kliente	Tehinguid	Punkte	Andmeid ³	Aeg ⁴
Kodakondsus- ja Migratsiooniamet	1 / 0 / 0	isikut tõendavate dokumentide väljaandmine	J / E / E	1000000				
Autoregistrikeskus	2 / 0 / ?	autojuhulibade väljaandmine autode registreerimine	J / E / E J / E / ?	360000	? ⁵			
Maksuamet	3 / 2 / 3	maksude kogumine maksude laekumise arvestamine kontokaardi väljastamine	J / J / J J / J / J J / E / J	20000	1000		10 / 0 / ?	
Piirivalveamet	2 / 0 / 1	passikontroll piiriületamisel passikontroll lihtsustatud piiriületamisel	J / E / E J / E / J	50000	50000	20		10 sek / 10 sek
Politseiamet	2 / 0 / ?	relvalubade väljastamine dokumentide kontrollimine	J / E / ? J / E / ?	36000	200	17		1 min
Kaitsepolitseiamet								
Kaitseministeerium	4 / 3 / ?	kaitseväelaste ja kohuslaste arvestamine sissepääs kaitseväge territooriumidele sissepääs kaitseväge arvutivõrku sissepääs kaitseväge tanklasse	J / E / ? J / J / J J / J / J J / J / J	1000		500	10 / ? / ? 10 / 0 / ?	
Siseministeerium								2-5 min
Teede- ja sideministeerium								
Keskhaigekassa	3 / 0 / 3	ravikindlustusteenuse osutamine haigekassakaartide väljastamine ravikindlustuse registri pidamine	J / E / J J / E / J E / E / J	1400000 1400000		1000	100 / ? / ?	/ 1 min - 1 h
Sotsiaalkindlustusamet	3 / 0 / ?	pensionide määramine ja maksmine lastetoetuste määramine ja maksmine pensionikindlustuse registri pidamine	J / E / ? J / E / ? E / E / ?	370000 350000	15000 10000			
Riigikantselei	1 / 1 / 1	pääslakaart-töötöend	J / J / J	1000	4000	50		
Digitaalsignatuuri seaduse komisjon	1 / 0 / 1	dokumendi elektrooniline signeerimine	E / E / J				10K / ? / ?	
Hansapank	4 / 1 / 4	liitumislepingu sõlmimine konto kasutamine teenuse lepingu sõlmimine universaalse kliendikaardi kasutamine	J / E / J J / J / J J / E / J E / E / J	100000				2-3 sek
Ühispank	5 / 3 / 5	ATM või makseautomaadi kasutamine maksetermiinaali kasutamine telefonipanga/internetipanga kasutamine muu pangateenuse kasutamine elektronrahakott	J / J / J J / J / J J / J / J J / E / J E / E / J	100000 100000		500 1500	50 / 0 / ?	10 sek / 1-3 min 10 sek / 2-30 sek
Pankade Kaardikeskus	7 / ? / ?	maksetermiinaalide hooldus maksetermiinaalide riskasutus pangaautomaatide riskasutus krediitkaartide andmebaasi haldamine kaardimaksete tagasinõuete vahendamine Neste kliendikaartide haldamine elektronrahakott	J / E / E J / J / J J / J / J J / ? / ? J / E / ? J / J / J E / E / J	2000 ⁶ 2000 ⁶ 5 ⁷	25000 15000	2500 2500		
Eesti Energia	2 / 2 / ?	energia müük eraisikutele energia müük ettevõtetele	J / E / ? J / E / ?					
Eesti Telefon	4 / 2 / ?	abonenttelefoni kasutamine andmeside kasutamine taksofoni kasutamine täiendavate klienditeenuste kasutamine	J / J / J J / J / J J / J / J E / E / J	400000				
Neste	1 / 1 / 1	kütuse ja autotarvete müük	J / J / J	20000	3000	30		/ 5 min
Tallinna Kaubamaja								

1 Teenuste koguarv / praegu elektroonilise autentimisega / võiks olla elektroonilise autentimisega

2 Teenus olemas / elektrooniline autentimine olemas / elektrooniline autentimine võimalik

3 Andmeid kaardil / teeninduspunktis ühe kliendi kohta / keskuses ühe kliendi kohta (baitides)

4 Lubatav autentimise aeg / teenuse osutamise koguaeg

5 Kuna juhuluba on laialt kasutatav ka isikut tõendava dokumendina, siis väga raske anda hinnangut selle kasutamise kohta

6 PKK kliendid maksekaartide riskasutuses on pangad ja äriettevõtted

7 PKK kliendid automaatide riskasutuses on pangad

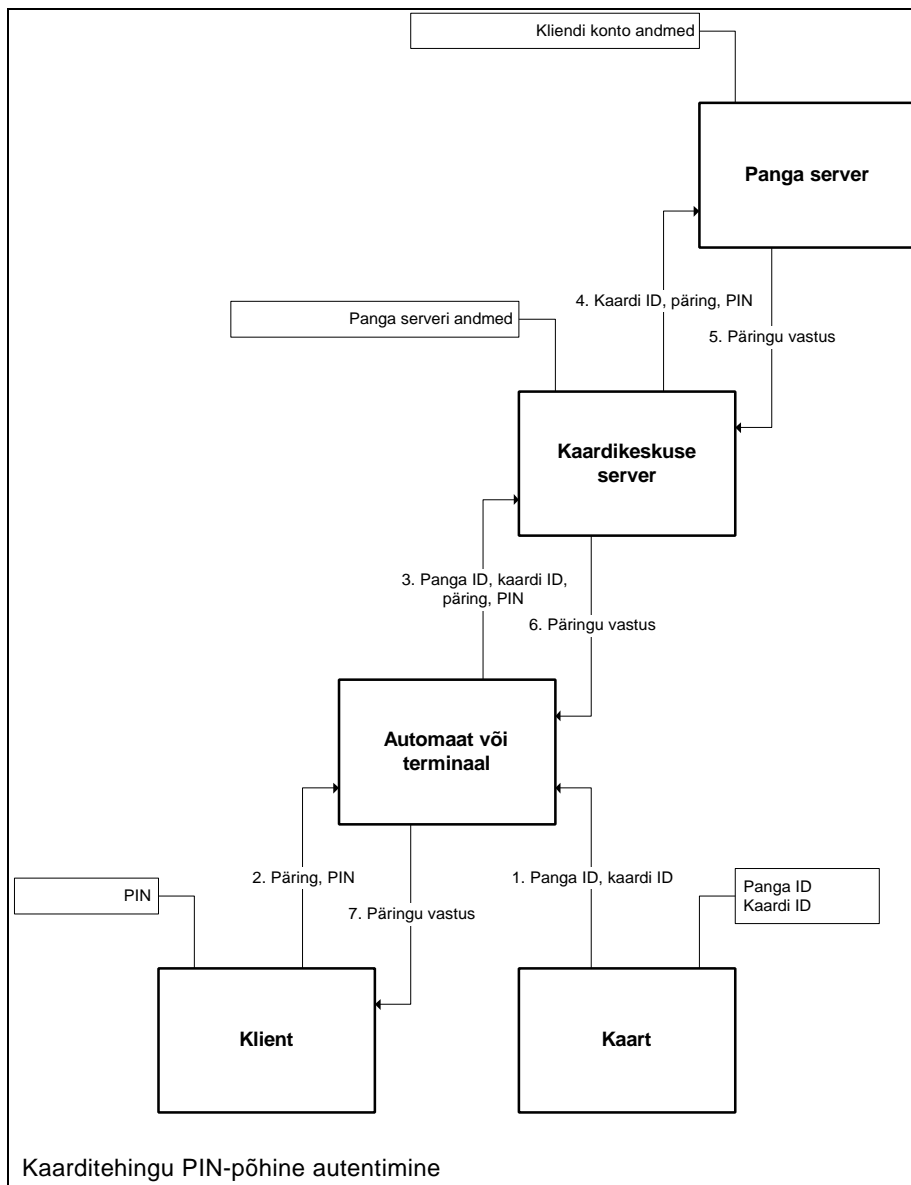
Olemasolevad autentimisskeemid

Allpool on toodud kaardistuse käigus selgunud olemasolevate elektrooniliste autentimisskeemide lühikirjeldused kasutusvalade lõikes.

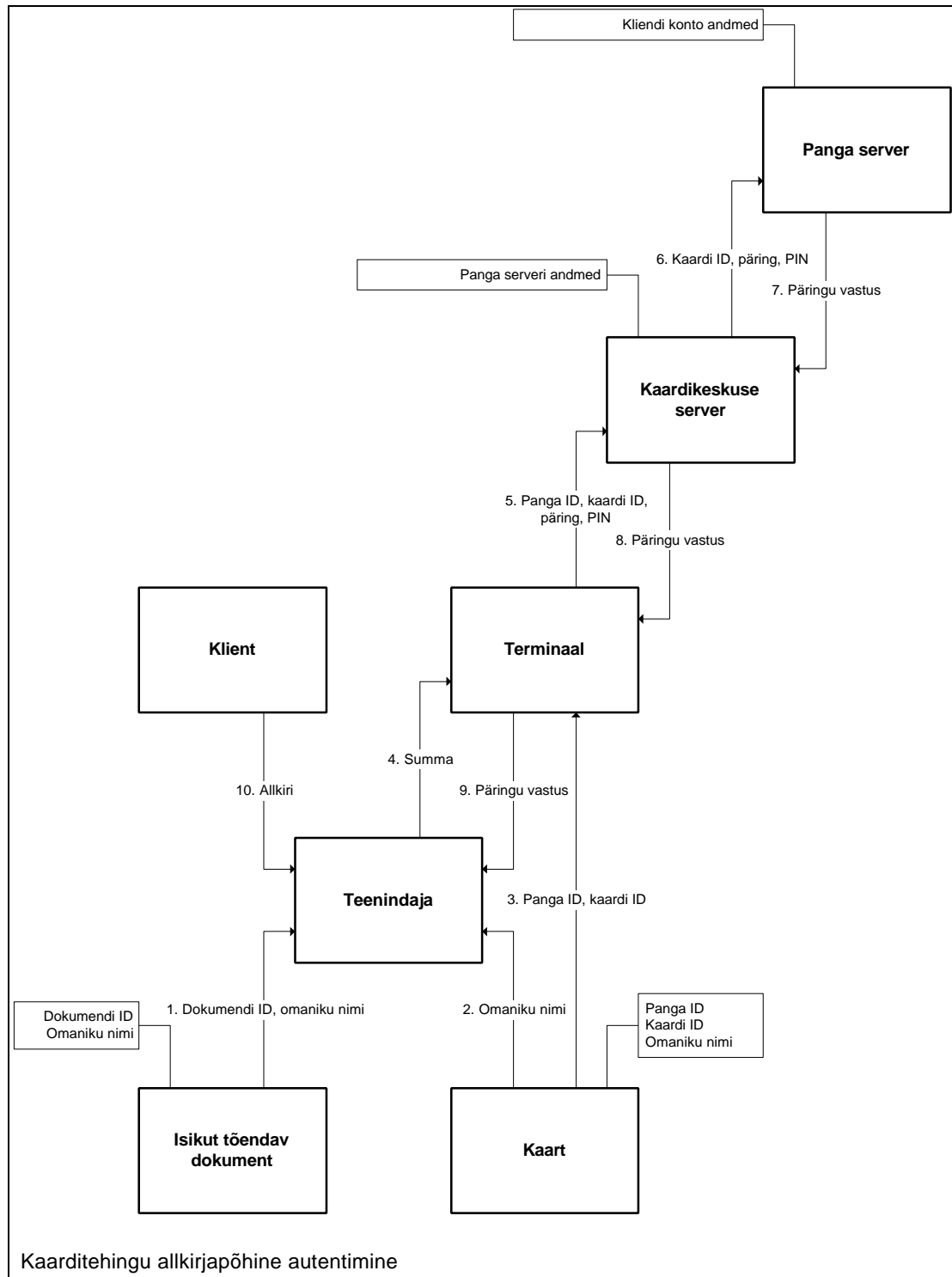
Pank

Eesti pangad toetavad kolme osaliselt või täielikult elektroonilist autentimisviisi: kaardi tehingu PIN-põhine autentimine, kaarditehingu allkirjapõhine autentimine, internetipanga või telefonipanga tehingu koodipõhine autentimine.

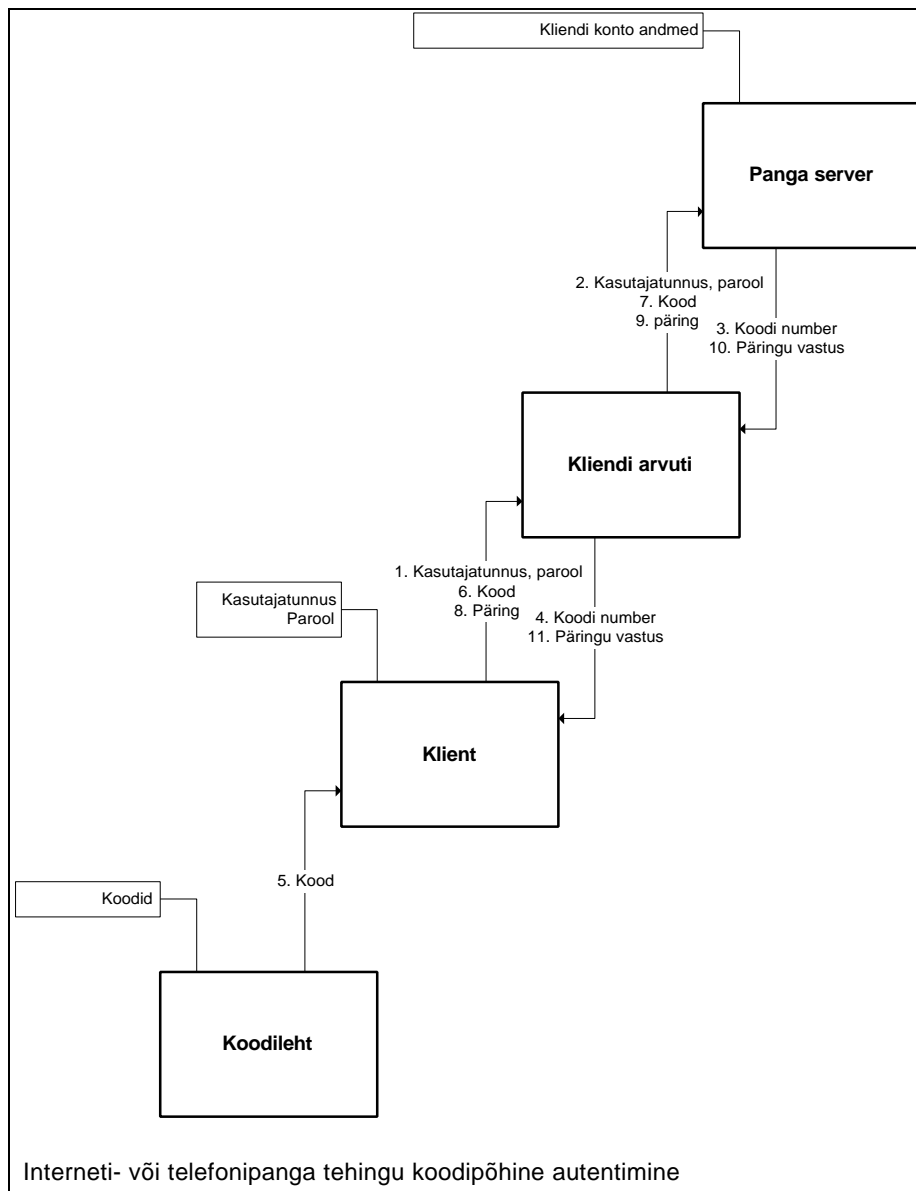
Kaarditehingu PIN-põhisel autentimisel kontrollib pangaautomaat või terminaal kaardil olevate andmete põhjal selle kehtivust ja kliendi sisestatud PINi põhjal tema õigust kaardiga seotud arvet käsutada. Kui automaat, kaart ja kaardiga seotud arve on kõik sama panga valduses, saadab automaat päringu otse pank, jättes kaardikeskuse vahele. Mõne panga automaadid sisaldavad oma panga kaartide PINide kontrollimiseks vajalikku infot kohapeal, siis toimub PINi kontrollimine automaadis ja päring edastatakse panga serverisse alles siis, kui klient on sisestanud korrektse PINi. Side automaadi ja serveri vahel on krüptitud.



Kaarditehingu allkirjapõhisel autentimisel teeb teenindaja kliendi poolt esitatud dokumendi alusel kindlaks kliendi isiku. Kui klient on kaardi seaduslik omanik, kontrollib terminaal kaardil olevate andmete põhjal selle kehtivust ja lõpuks kinnitab klient tehingu oma allkirjaga terminaalist väljastatud kviitungil.

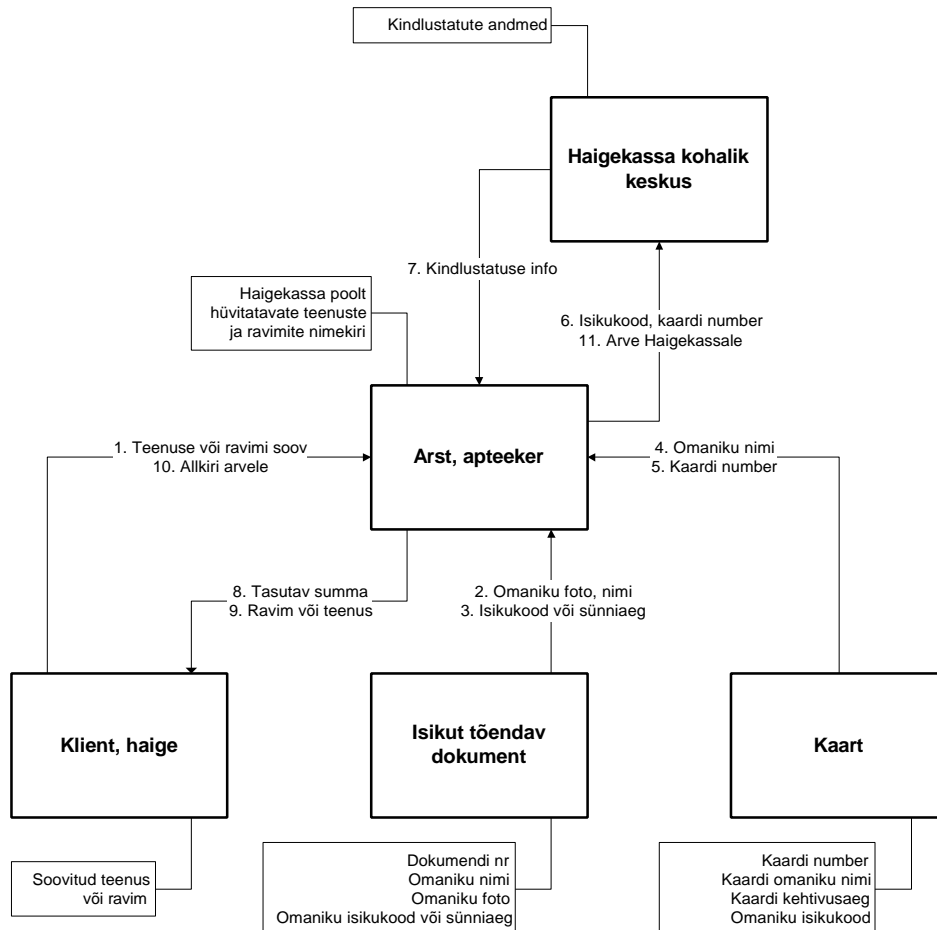


Interneti- ja telefonipanga kasutamisel raskendab kliendi autentimist asjaolu, et kliendi juures pole ühtegi seadet, mida pank võiks kliendi autentsuse kontrollijana usaldada, samuti pole garanteeritud kliendi ja panga vahelise sidekanali turvalisus. Seetõttu on lisaks staatilisele kasutajatunnusele ja paroolile kasutusel ka (mõne panga puhul ainult ühekordselt kasutatavad, mõne panga puhul korduvalt kasutatavad) muutuvad koodid. Klient saab lepingu sõlmimisel lehe nummerdatud koodidega ja peab pangateenuse igakordsel kasutamisel sisestama panga serveri poolt nõutud järjekorranumbriga koodi sellelt lehelt. Nii tagatakse, et ühe sideseansi salvestamine ei anna potentsiaalsele sissetungijale võimalust hiljem panga kliendina esineda.



Haigekassa

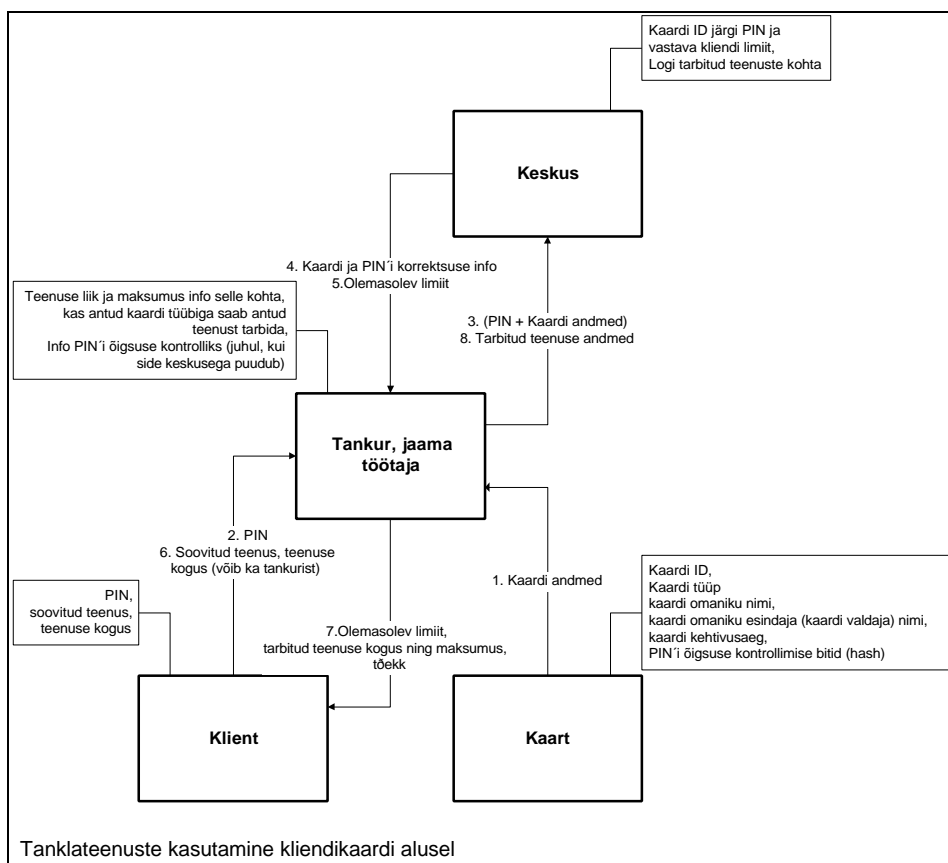
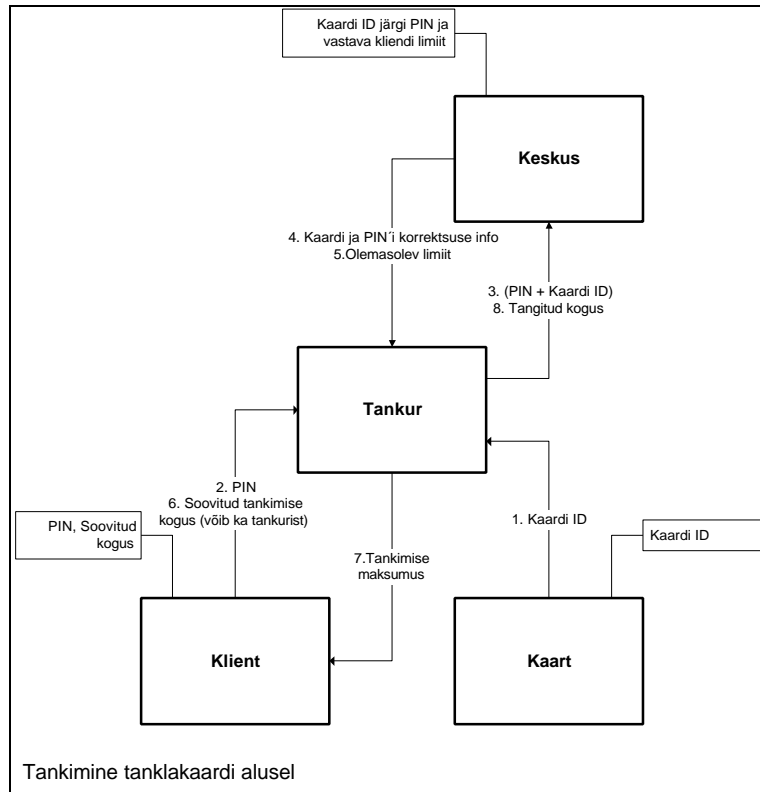
Täielikult või osaliselt tasuta arstiabi saamiseks esitab patsient haigekassa liikmekaardi koos isikut tõendava dokumendiga. Meditsiinitöötaja teeb esitatud dokumendi alusel kindlaks patsiendi isiku. Kui patsient on kaardi seaduslik omanik, kontrollib terminaal kaardil olevate andmete põhjal haigekassa andmebaasist kaardi kehtivust ja lõpuks kinnitab patsient tehingu õigsust oma allkirjaga arsti või apteekri esitatud arvel. Nendes meditsiinasutustes, millel pole pidevat ühendust haigekassa andmebaasiga, kontrollitakse patsientide kindlustatust haigekassa andmebaasi kohapeal oleva ja aeg-ajalt uuendatava koopia alusel.



Arstiabi saamine haigekassa liikmekaardi alusel

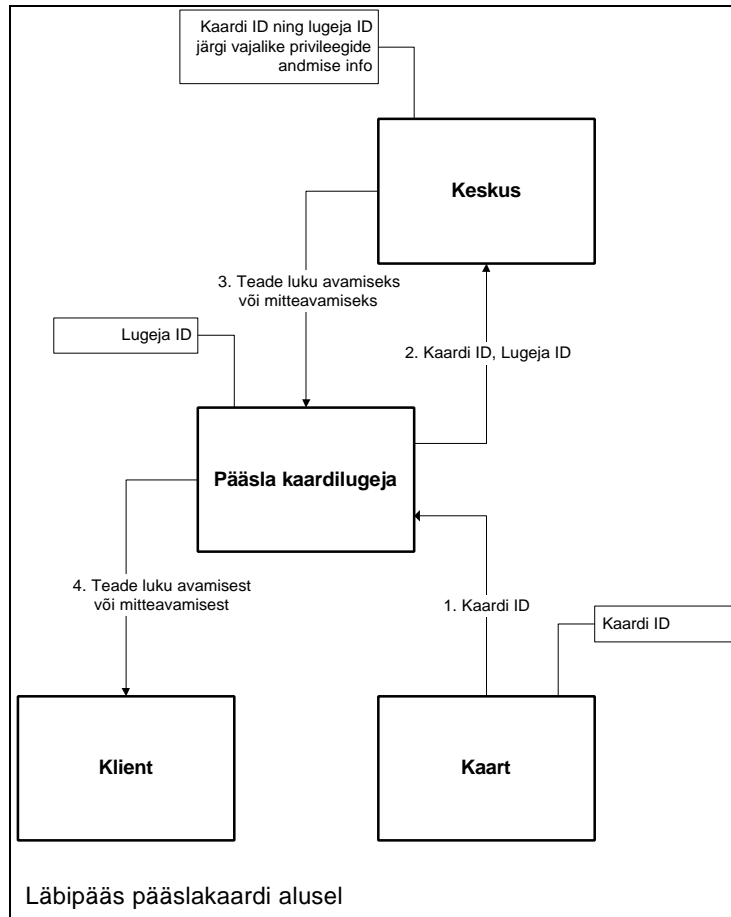
Tankla

Erinevate tanklakettide kliendikaardid annavad klientidele veidi erinevaid võimalusi kaardi alusel pakutavate teenuste osas, siiski on autentimise mehaanika väga sarnane.



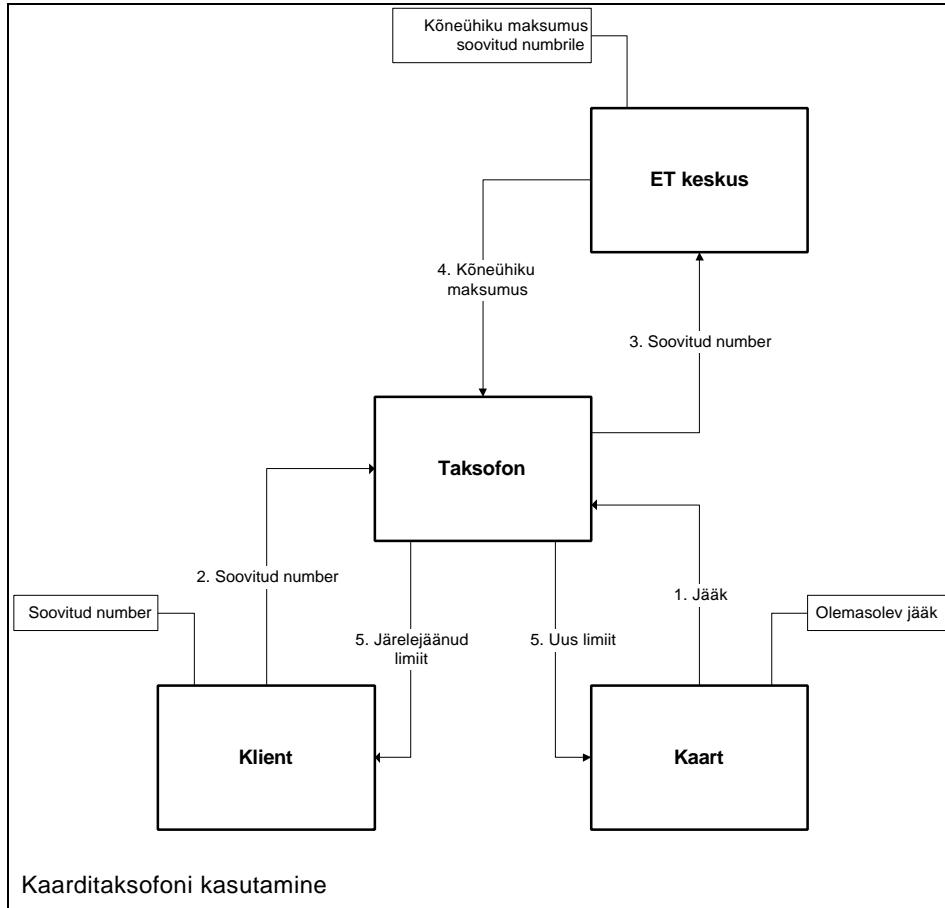
Pääsla

Pääslakaartidena on Eestis olemasolevates süsteemides kasutusel nii magnet- kui ka kiip kaarte. Kahjuks ei osanud (või ei tahtnud) ükski kiipkaarti kasutavatest küsitlevatest selgitada, kas nende süsteem kasutab kiipkaarti ainult kontaktivaba lugemise võimaluse pärast või on kiipkaardi kasutamise põhjuseks (ka) selle kõrgendatud võltsimiskindlus. Arvatavasti on kiipkaartide kasutamise peapõhjuseks siiski mugavus, mida kontaktivaba kaart pakub.



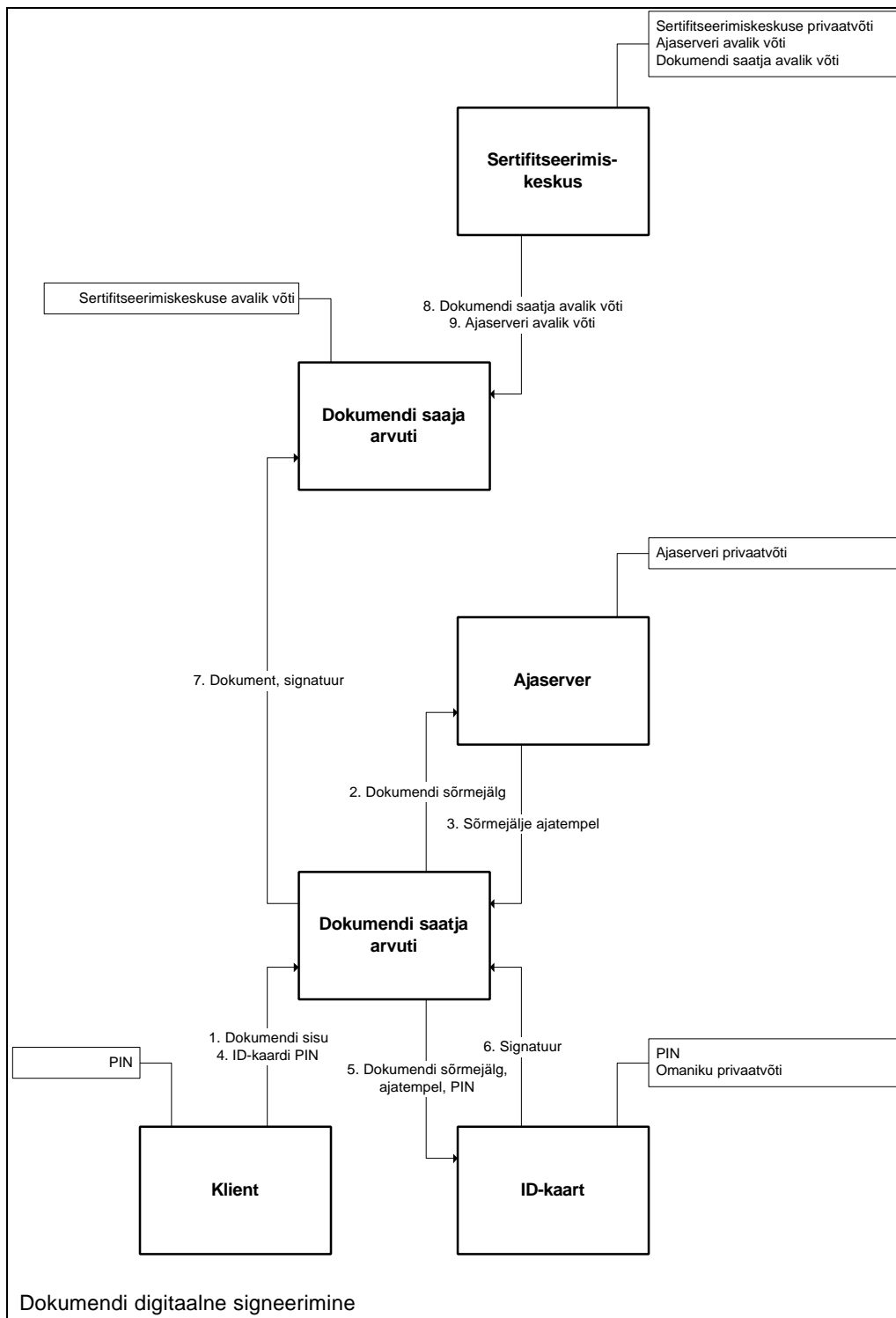
Taksofon

Kaarditaksofonide süsteemi turvalisus põhineb 100% kaardi turvalisusel, sest ettemaksu summa jääk on kirjas ainult kaardil ja krüptovahendite puudumise tõttu pole taksofonil mingit võimalust eristada autentset kaarti võltskaardist, kui viimane taksofoniga suhtlemise protokollist kinni peab.



Digitaalsignatuur

Kuigi digitaalsignatuur ametlikus asjaajamises mingit juriidilist kaalu ei oma, on elektron-dokumentide digitaalne signeerimine teatud ringkondades juba kasutusel. Vastavate kaartide puudumise tõttu hoitakse signeerimiseks vajalikke privaativõtmeid käesoleval ajal lihtsalt krüptitud failidena (kus privaativõtme hoidmiseks kasutatava faili krüptimisparool on kasutaja valitav ja seetõttu kergemini meeles peetav – ja kahjuks ka kergemini ära arvatav, kuigi samas ka kergemini ja seetõttu loodetavasti sagedamini muudetav – kui tema poolt kaitstav võti).



ID-kaardile esitatavad nõuded

Allpool on toodud kaardistuse käigus selgunud põhinõuded ID-kaardil olevatele andmetele ja nende kasutamisele.

Nõuded visuaalsele komponendile

Visuaalselt loetaval kujul peaks kaardil olema järgmised andmed:

- kaardi ID – kuigi selle vajalikkust mainis ilmutatult ainult 5 küsitletut, on selge, et igal dokumendil peab olema oma unikaalne identifikaator, mille alusel teda teistest sama liiki dokumentidest eraldada;
- kaardi kehtivuse aeg – kui see pole kaardi ID osa (nagu sünniaeg on isikukoodi osa);
- kaardi väljaandja – kuigi seda pidas vajalikuks ainult kaks asutust, on need kaks KMA ja Piirivalveamet;
- omaniku nimi;
- omaniku isikukood;
- omaniku sünniaeg – kuigi sünniaeg on ka isikukoodi osa, leidis üle poole küsitletutest eraldi sünniaja väljatoomise vajaliku olevat;
- omaniku foto;
- omaniku allkirjanäidis.

Veel nimetati vajalike andmete hulgas omaniku sünnikohta, sugu, veregruppi ja sõrmejälge ning juhiloa ja relvaloa andmeid.

Nõuded elektroonilisele komponendile

Esmase väljaandja andmed

Esmane väljaandja peaks kaardile kandma järgmised andmed:

- kaardi ID;
- kaardi kehtivuse aeg;
- omaniku nimi;
- omaniku isikukood;
- omaniku mingi biomeetriline info – foto, allkirjanäidis, sõrmejalg vms.

Veel nimetati vajalike andmete hulgas omaniku sünniaega, sünnikohta, sugu, veregruppi, kaardi väljaandja andmeid, omaniku perekonnaseisu ja kodakondsust ning juhiloa ja relvaloa andmeid.

Võltsimise vältimiseks peaks see kirje olema kaardi esmase väljaandja poolt signeeritud. Kui kaardil on oma identiteedi tõestamiseks oma võtmepaar, siis peaks ka selle võtmepaari avalik võti olema signeeritud andmete hulgas – see välistab isikuandmete kirje kopeerimise ühelt kaardilt teisele. Loomulikult peab mistahes võtmepaari privaatvõti olema kaardilt välja lugemise eest kaitstud.

Kaasväljaandjate andmed

Kaasväljaandjad võib nende andmevajaduste järgi jagada nelja rühma:

- 1) need, kes on huvitatud ainult kaardiomaniku mingit liiki kliendikoodi salvestamisest kaardile (sellise huvi tüüpiline näide on pangakaart, kus lisaks kliendi isikuandmete on vaja ainult arvenumbrit või uksekaardisüsteem, kus kaardiomaniku tegelik liikumisvabadus on kirjas keskses serveris); üldjuhul ei peaks selline kliendikood olema loetav kõrvalistele isikutele, seega peaks see olema lugemise eest kaitstud või enne kaardile kandmist vastava kaasväljaandja poolt krüptitud; vajalike andmete maht sellise rakenduse korral on suurusjärku 10-20 baiti kaasväljaandja kohta;
- 2) need, kes on huvitatud mingite kvalitatiivsete õiguste kandmisest otse kaardile (sellise huvi tüüpiline näid uksekaardisüsteem, kus kaardiomaniku tegelik liikumisvabadus on kirjas otse kaardil, tulevikus võib-olla ka juhiluba, relvaluba); sellise süsteemi korral on andmete kaitstud kaardil kriitiline – volitamata muutmise korral võib kaardile kanda õigusi, mida kaardiomanikul tegelikult pole, volitamata lugemise korral võib osutada võimalikuks õiguste ülekandmine teisele isikule; vajalike andmete maht sõltub oluliselt rakendusest, kuid on tüüpiliselt märksa suurem eelmist liiki rakenduse andmemahust; selle-eest saab niisugune süsteem toimida ka ilma püsiva side olemaoluta;
- 3) need, kes on huvitatud mingite kvantitatiivsete õiguste kandmisest otse kaardile (sellise huvi tüüpiline näide on telefonikaart, tulevikus võib-olla ka parklakaart, bussikaart); sellist liiki süsteemide puhul on vajalik mälu maht küllaltki väike, võtmeküsimuseks on jällegi andmete turvalisus, ennekõike nende volitamata kirjutamise vältimine – kui kellelgi õnnestub kaardi turvalisus murda, saab ta endale piiramatu krediidi teenusepakkuja arvelt;
- 4) need, kes on huvitatud mingit liiki sessioonivõtmete hoidmisest kaardil (a la telefoni- ja Internetipanga muutuvad turvakoodid); sellist liiki rakenduse puhul on valida kahe lahenduse vahel:
 - a) kanda sessioonivõtmete tabel otseselt kaardile – mis on oluline mälu kulu;
 - b) kanda kaardile mingi PIN-kalkulaatori tüüpi funktsioon – kui selle funktsiooni osas kokkuleppele jõuda, on võimalik kasutada ühte kalkulaatorit (erinevate võtmetega) mitme erineva kaasväljaandja poolt;

Kaasväljaandjate korral on oluline ka salvestusruumi jagamine nende vahel – teatava failisüsteemi loomine kaardi mälus. Loodav failisüsteem peaks kindlasti omama faili omaniku mõistet ja mingit vahendit erinevatele failidele juurdepääsu ja erinevate väljaandjate poolt kasutatavate mälu mahtude piiramiseks. Väga väikese mälu kulu rakenduste (liigid 1 ja 3) puhul võib failisüsteemi haldusinfo maht olla samas suurusjärgus failis hoitava info mahuga või seda isegi ületada.

Nõuded protseduuridele

Nõuded väljaandmise protseduurile

Kõik küsitatud olid ühel meelel selles, et ID-kaardi kui riikliku isikut tõendava dokumendi väljaandja peab olema selleks volitatud riigiasutus.

Mitmed küsitatud (nii riigiasutuste kui eraettevõtete esindajad) avaldasid arvamust, et riiklike ja kommertsfunktsioone ei tuleks panna ühele kaardile. Nende arvamuse kohaselt võiks riiklikule kaardile jääda isikut tõendava dokumendi, riigi poolt antud õiguste (haigekassa

liikmekaart, pensionitunnistus, relvaluba jmt) kandja ja digitaalsignatuuri hoidja funktsioonid, samal ajal kui kommertskaart (mille esmasteks väljaandjateks võiks erinevate arvamuste kohaselt olla pangad, Eesti Telefon või mingi selleks loodav organ *a la* Pankade Kaardikeskus) peaks katma pangakaardi ja mitmesuguste kliendikaartide funktsioonid.

Lisaks arvas enamuse küsitletutest, et kaardi väljaandmine peaks toimuma ühes kohas, et kaardiomanikul ei oleks vaja kaardi väljastamise järel sellele andmete kandmiseks läbi käia kõiki asutusi, mille klient ta on. Samas peab kadunud kaardi asendamine olema piisavalt tülikas, et mitte soodustada kaartide müümist (mis on praegu probleemiks passide ja vähemal määral ka juhilubadega).

Nõuded kasutamise protseduuridele

Kaardi kasutamisele esitatavad nõudmised on seotud peamiselt turvalisuse tagamisega:

- kaardi füüsiline võltsimiskindlus peab vastama vähemalt olemasoleva passi turvasemele;
- kaardi kasutamine elektrooniliseks autentimiseks peab võimaldama üheselt tuvastada kaardi valdaja ja selle omaniku isikusamasuse;
- varastatud kaardi kasutamise vältimiseks peaks kõik funktsioonid ja andmed (peale esmaste isikuandmete) olema kaitstud PINide süsteemiga (erinevate teenuste kasutamiseks erinevad PINid);
- elektroonilise autentimise laialdase kasutamise korral on vaja kaardiomanike teadlikkuse olulist tõstmist või tuleks kehtestada ranged sanktsioonid kaardi (ja eriti digitaalsignatuuri) "laenamise" eest.

Kaardi *offline* kasutamise võimaluse vajalikkuse ja soovitatavuse osas läksid arvamused lahku. Osa küsitletustest arvas, et *offline* kasutamise võimalus tekitab täiendavaid turvariske, osa aga leidis, et kui ID-kaart realiseerida kiipkaardina, siis saab seda ära kasutada selleks, et muuta mõned praegu tehnilistel põhjustel ainult *online* osutatavad teenused autonoomseteks.

Peaaegu kõik küsitletud arvasid, et digitaalse signeerimise funktsioon on kaardil vajalik, muu funktsionaalsuse, samuti füüsiliste turvaelementide vajaduste kohta nii üksmeelset arvamust ei olnud.

Nõuded tühistamise protseduurile

Kõik küsitletavad olid ühel meelel selles, et kaardi kadumise või varastamise korral peaks saama kõik kaardi funktsioonid blokeerida ühest kohast. Valeblokeerimiste vältimiseks peaks ka blokeerimisel olema mingisugune autentimine, mis võiks toimuda:

- mingi (kaardi väljaandmisel kokkulepitud) spetsiaalse koodi või parooli alusel;
- mingite kaardiomaniku väga spetsiifiliste isikuandmete alusel (mida kõrvalised isikud tõenäoliselt ei tea);
- kahefaasilisena, kus telefoni teel on võimalik kaardile panna ainult ajutine tõke ja lõplik tühistamine saab toimuda ainult kaardiomaniku füüsilise kohaloleku alusel.

Igal juhul peab samale isikule uue kaardi väljastamine automaatselt tühistama selle isiku kõik eelmised kaardid.

ID-kaardi foorum ja ankeet

Lähteuringu projekti raames koostas AS Halo ID-kaardi tutvustamiseks ja sellega seotud küsimuste avalikuks aruteluks WWW-lehe aadressil <http://www.id.ee>. WWW-leht sisaldas lisaks ID-kaarti tutvustavale tekstile foorumit kõigi külastajate vabaks arvamustevahetuseks ja ankeetküsitlust, mis oli aluseks SWOT-analüüsile.

ID-kaardi foorum

Foorum oli avatud kuu aega ja selle aja jooksul saabus sinna 40 kirja 30lt autorilt. Otseselt ID-kaarti ning vastavat projekti puudutas 30 kirja.

Peamised küsimused ning probleemid, mis välja toodi, olid järgnevad:

- Kas on mõtet luua passi dubleeriv dokument (kas sellega seoses tekkivad täiendavad kulutused on õigustatud)?
- Milline peaks olema kaardile kantav info (info olemus, väärtus, struktuur)? Kui palju infot mahub kaardile?
- Kas sellist asja on üldse vaja ja kui on, siis kas see peab just kaart olema?
- Kui kaardiga konkureerival lahendusel (näiteks "Java sõrmus") pole pilti, kuidas siis tagada selle esitaja visuaalne autentimine?
- Milline tehniline lahendus on hetkel võimalik välja pakkuda?
- Milline peaks olema prioriteetide järjekord asutuste lõikes, kelle info paigutatakse kaardile (milliseid asutusi eelistada ning milliste info kirjutamist takistada)? Milline peaks see järjekord olema riiklike ning eraõiguslike asutuste suhtes ning nende omavaheline vahekord?
- Mis saab, kui ID-kaart pangaautomaadis "alla neelatakse" st kuidas peaks toimuma kaardi kehtetuks tunnistamine ning kehtetu kaardi kõrvaldamine ringlusest?
- Kui kaarti hakatakse kasutama elektroonilise rahakotina, rakendab Eesti Pank sellele rangeid kontrollivaid nõudeid. Kas kaardi väljaandjad on selleks valmis?
- Millise turvalisusega oleks mõtet ühtset kaarti rakendada?
- Kui paljusid rahvusvaheliselt tunnustatud reegleid ning piiranguid antud kaardi rakendamisel peaks arvestama ning kui paljusid võiks ignoreerida?

Põhilised ettepanekud olid:

- Kasutada isikusamasuse tuvastamiseks kaardi asemel või kaardiga koos ka mingisuguseid biomeetrilisi andmeid.
- Rakendada kaardi juures tehnoloogiat, mille alusel kaardilt saadav info oleks sõltuv sellest, mismoodi kaardi poole pöördutakse.
- Kaaluda võiks 1...3 erineva turbetasemega protsessorkaardi kasutamist.

Samuti oli foorumi tekstide hulgas ID-kaardi projekti tutvustavaid kirjutisi.

Foorumil osalejatest ligikaudu pooled suhtusid ID-kaardi juurutamisse positiivselt ning ligikaudu pooled suhtusid sellesse skeptiliselt.

ID-kaardi ankeet

Ankeedi täitjatel paluti välja tuua uued võimalused ja uued ohud, mida nad näevad seoses ID-kaardi kasutuselevõttuga tekkivat endale kui eraisikule, oma asutuse või ettevõtte sisemises infrastruktuuris ja välises suhtlemises ning Eesti riigi sisemises infrastruktuuris ja välises suhtlemises.

Ankeet oli täitmiseks väljas kuu aega ja selle aja jooksul täitis ankeedi 46 inimest. Vastavalt ankeedi täitjatele antud lubadusele AS Aprote ankeete ei avalikusta. Koondtabelites on sisuliselt samaväärsed vastused ühtlustatud ja järjestatud iga grupi piires esinemiste arvu kahanemise järjekorras.

Plussid-miinused eraisiku jaoks

Plussid	Arv
Väheneb erinevate kaartide kasutamise vajadus (mugavus)	18
Saab mugavalt kaasas kanda palju rohem infot ning dokumente (mugavus)	9
Digitaalsignatuur võimaldab dokumente distantsilt allkirjastada (mugavus)	6
Võimalus mitmetes asutustes asjaajamist kiirendada	5
Passi asendamine mugavama dokumendiga	3
Sularaha kaasaskandmiseks pole vajadust (mugavus)	2
Miinused	Arv
Kaardi kaotamisel, varastamisel röövimisel, rikkumisel või võltsimisel kaob suur osa isiku andmetest ja tema tegutsemisvabadusest, samuti identiteedist, samas suureneb oht, et selle abil saab isikule suuremat kahju teha	22
Tekib oht, et kaardiomanikke saab paremini jälgida	5
Kaardi rahvusvaheline tunnustamatus	2
Lisadokumentide küsimise võimalus muutub väiksemaks ning kaardi puudumisel on raskem isiku tõestamine	2
Sideseansside pealtkuulatavus ning seeläbi andmete avalikukstulek	1
PINide meelespidamine muutub raskemaks	1
Suureneb sõltuvus tehnikast ja selle korralikust töötamisest	1
Seoses uue lähenemisega turvalisusele tuleb muuta käitumisharjumusi	1
Vead andmete kaardile kandmisel ning registrites	1

Plussid-miinused asutuse, organisatsiooni jaoks

Plussid sisemises kasutuses	Arv
Eraldi pääslakaartide vähenemine (mugavus)	5
Isiku või töötaja kiire tuvastamine	2
Signeerimisega muutub elu lihtsamaks	2
Miinused sisemises kasutuses	Arv
Võõraste ligipääsu lihtsustumine	1
Kaardi kadumine toob kaasa senisest suuremaid probleeme	1
Kaardi vähene seostatus konkreetse isikuga	1
Inimeste kehv valmisolek kaardi rakendamiseks	1
Kiipkaardi rakendamine pääslakaardina võib osutada liiga aeglaseks	1
Plussid välises suhtlemises	Arv
Parema klienditeenindamise võimalus	1
Andmete liikumise täpsus suureneb	1
Miinused välises suhtlemises	Arv
	0

Plussid-miinused riigi jaoks

Plussid sisemises kasutuses	Arv
Riik saavutab kontrolli kaardiomanike üle	10
Registrite korrastatus, mis kaardi juurutamisega kaasneb tagab palju vähem edaspidisi probleeme	7
Bürokraatia vähenemine	3
Võiks tekkida ühtne standard kaardi kasutamiseks	1
Digitaalsignatuur võimaldab residentidel mistahes paigast asju ajada	1
Miinused sisemises kasutuses	Arv
Kuritahtlik infole ligipääs võimaldab liiga suurt kontrolli, kaardil on liiga palju infot	15
Kõikvõimalikud kelmused lihtsustuvad	6
Vajalikeks muutusteks (seoses turvaprobleemidega) ei olda valmis	4
Bürokraatia kasvab	2
Plussid välises suhtlemises	Arv
Väljavaated riiklikult eesrindlikuks IT maaks tõusta	9
Isiku tuvastuse kiirenemine lihtsustab reisimist	6
Lihtsustuks piirikontroll	1
Miinused välises suhtlemises	Arv
Musta stsenaariumi juures kahjustub Eesti maine	4
Võõrriikide organid võivad saada kaardiinfo üle kontrolli	3
Süsteemi sõltuvus arvutitest ning programmidest (kus kindlasti on vigu)	1
Euroopas tekkida võiva ühtse standardi puhul pole meie kaart sellele vasta	1

Lahendusvariandid

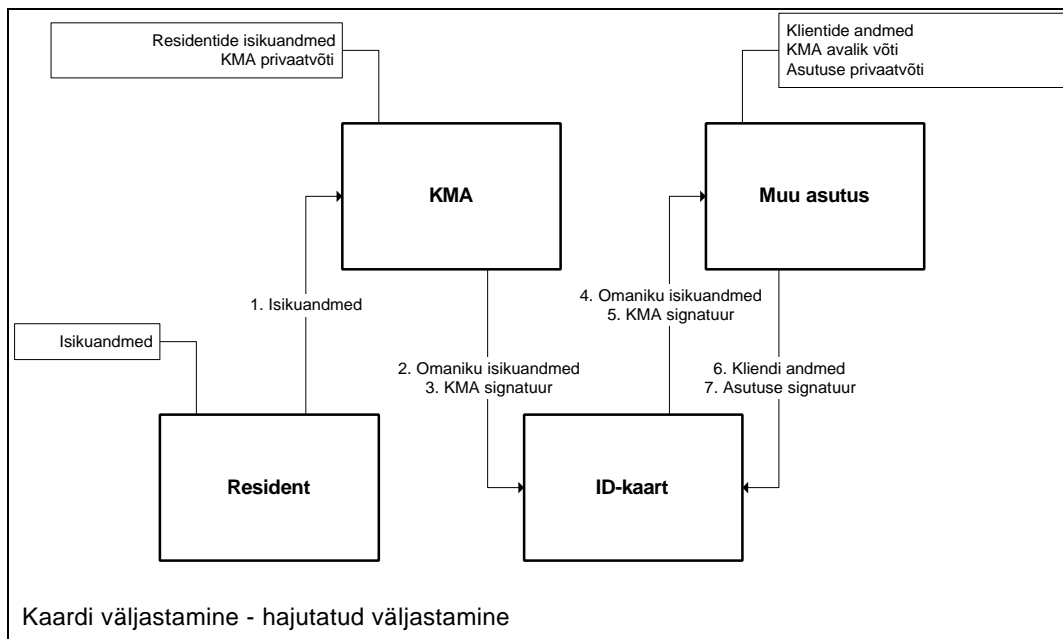
Allpool on kirjeldatud võimalikke lahendusvariante kaardi väljastamiseks, kaardi ja selle valdaja autentsuse ja õiguste tõestamiseks kaardi abil ning kaotatud või aegunud kaardi blokeerimiseks.

Kaardi väljastamine

Hajutatud väljastamine

Kaardi saamiseks pöördub resident KMA poole, kus pärast isikusamasuse tuvastamist ja isikuandmete kontrollimist väljastatakse talle ID-kaart, millele on kantud kaardiomaniku isikuandmed ja nende autentsust kinnitav KMA signatuur. Kui resident soovib ID-kaarti kasutada ainult isikut tõendava dokumendina, on protsess sellega lõppenud.

Kui resident soovib ID-kaarti kasutada ka mingites muudes funktsioonides, peab ta selleks võtma ühendust iga teenusepakkujaga, kus ta esitab ID-kaardi oma isiku tõendamiseks ja vajalike andmete kaardile kandmiseks.



Plussid:

- iga asutus haldab oma andmebaasi ise, miinimumini on viidud võimalused ühe asutuse andmebaasi kaudu teiste asutuste andmetele ligi pääseda ja puudub andmete tarbetu dubleerimine;
- klient saab oma kaardile garanteeritult kirjutamise hetkel kehtivad andmed.

Miinused:

- kaardiomanik peab igal kaardi väljastamisel (nii esmasel väljastamisel kui ka kaardi aegumisel või kadumisel) käima isiklikult läbi kõik asutused, mille klient ta on (digitaal-signatuuride kasutamise korral saab võrguühendust ja kaardilugejat omav isik seda teha ka füüsiliselt kohale minemata, kui ta saadab igale teenusepakkujale digitaalselt signeeritud

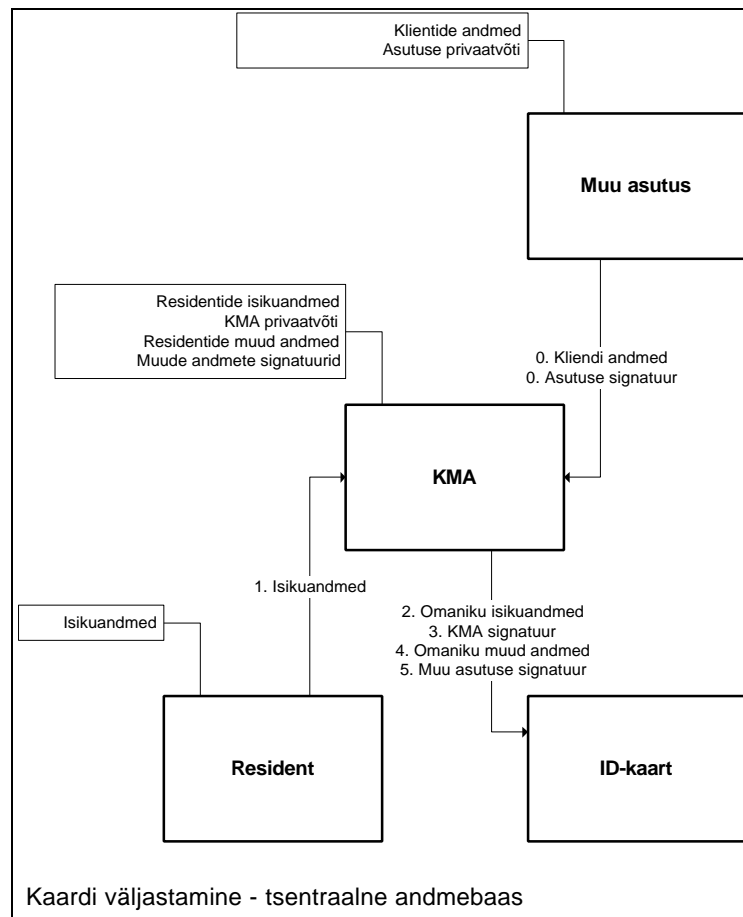
avalduse ja kannab selle avalduse alusel teenusepakkujalt saadud andmed ise oma kaardile; siiski jääb kaardiomanikule kohustus kõigi teenusepakkujatega ühendust võtta);

- kaardile oma andmeid kirjutavate asutuste paljususe tõttu tekib vajadus kaitsta kaarti võimalike vigade eest andmete kirjutamisel (lõviosa rakendustest vajab kaardile kirjutamist ainult kaardi väljastamisel, igapäevasel kasutamisel tahetakse kaardilt ainult lugeda).

Tsentraalne andmebaas

Kaardi saamiseks pöördub resident KMA poole, kus pärast isikusamasuse tuvastamist ja isikuandmete kontrollimist väljastatakse talle ID-kaart, millele on kantud kaardiomaniku isikuandmed ja nende autentsust kinnitav KMA signatuur. Kui resident soovib ID-kaarti kasutada ainult isikut tõendava dokumendina, on protsess sellega lõppenud.

Kui resident soovib ID-kaarti kasutada ka mingites muudes funktsioonides, peavad vastavate teenuste pakkujad olema eelnevalt saatnud KMAle info, mida nemad ID-kaardile kirjutada soovivad ja KMA kirjutab ka need andmed kaardile.



Plussid:

- kaardiomanik saab kõik vajalikud andmed kaardile ühes kohas;
- kuna kaardile kirjutab ainult KMA, lihtsustub tunduvalt kaardi kaitsmine kirjutusvigade eest (kui kaardilugeja viga rikub kaardi, saab selle kohapeal uuega asendada, kohe on võimalik kontrollida, et mitte mingid kaks asutust ei püüa kirjutada kaardile samasse piirkonda jne).

Miinused:

- kõik isikuandmed on koondatud ühte kohta, mistõttu KMA andmebaasi turvalisus on süsteemi turvalisuse seisukohalt äärmiselt kriitiline;
- isikuandmed on tarbetult dubleeritud (KMAI on paratamatult ainult koopiaid teenusepakkujate andmetest), mistõttu kaardile kirjutatavad andmed võivad kirjutamise hetkel olla juba vananenud.

Hajutatud andmebaas

Kaardi saamiseks pöördub resident KMA poole, kus pärast isikusamasuse tuvastamist ja isikuandmete kontrollimist väljastatakse talle ID-kaart, millele on kantud kaardiomaniku isikuandmed ja nende autentsust kinnitav KMA signatuur. Kui resident soovib ID-kaarti kasutada ainult isikut tõendava dokumendina, on protsess sellega lõppenud.

Kui resident soovib ID-kaarti kasutada ka mingites muudes funktsioonides, esitab KMA päringud kõigile temaga ID-kaardi kasutamise lepingu sõlminud teenusepakkujatele ja kirjutab ka neilt saadud andmed kaardile.



Plussid:

- iga asutus haldab oma andmebaasi ise, oluliselt on piiratud võimalusi ühe asutuse andmebaasi kaudu teiste asutuste andmetele ligi pääseda ja puudub andmete tarbetu dubleerimine;
- kaardiomanik saab kõik vajalikud andmed kaardile ühes kohas;

- klient saab oma kaardile garanteeritult kirjutamise hetkel kehtivad andmed;
- kuna kaardile kirjutab ainult KMA, lihtsustub tunduvalt kaardi kaitsmine kirjutusvigade eest.

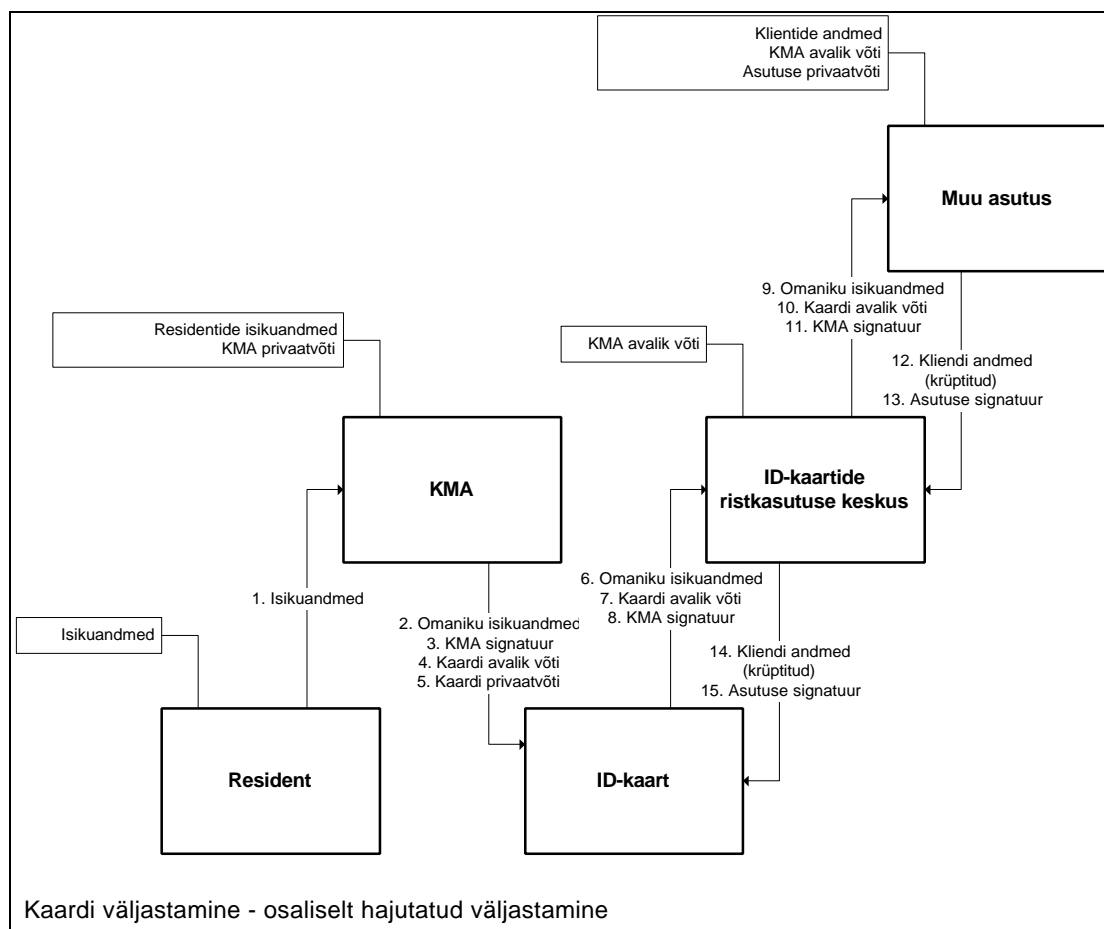
Miinused:

- kaardi väljaandmine on võimatu, kui KMA ei saa ühendust kasvõi ühe potentsiaalse kaardilekirjutajaga;
- süsteem toimib ainult juhul, kui kõik muud asutused usaldavad KMA-d piisavalt, et talle oma andmeid saata.

Osaliselt hajutatud väljastamine

Kaardi saamiseks pöördub resident KMA poole, kus pärast isikusamasuse tuvastamist ja isikuandmete kontrollimist väljastatakse talle ID-kaart, millele on kantud kaardiomaniku isikuandmed ja nende autentsust kinnitav KMA signatuur. Lisaks sellele genereerib KMA kohe ka kaardi võtmepaari ning sertifitseerib ja avalikustab selle avaliku võtme. Kui resident soovib ID-kaarti kasutada ainult isikut tõendava dokumendina, on protsess sellega lõppenud.

Kui resident soovib ID-kaarti kasutada ka mingites muudes funktsioonides, pöördub ta selleks loodud keskuse poole, kust esitatakse kaardi abil signeeritud päringud kõigile temaga ID-kaardi kasutamise lepingu sõlminud teenusepakkujatele ja kirjutab ka neilt saadud andmed kaardile.



Plussid:

- iga asutus haldab oma andmebaasi ise, oluliselt on piiratud võimalusi ühe asutuse andmebaasi kaudu teiste asutuste andmetele ligi pääseda ja puudub andmete tarbetu dubleerimine;
- kaardiomanik saab kõik vajalikud andmed kaardile ühes kohas;
- klient saab oma kaardile garanteeritult kirjutamise hetkel kehtivad andmed;
- kuna kaardile kirjutavad ainult KMA ja kaardikeskus, lihtsustub tunduvalt kaardi kaitsmine kirjutusvigade eest.

Miinused:

- kaardi väljaandmine on takistatud, kui kaardikeskus ei saa ühendust kasvõi ühe potentsiaalse kaardilekirjutajaga;
- süsteem toimib juhul, kui kõik muud asutused usuvad, et KMA ja kaardikeskus ei tee nendelt andmete väljapetmiseks koostööd.

Kokkuvõte

Esimene pakutud lahendusvariant (kaardiga seotud volituste hajutatud väljastamine) on sisuliselt samaväärne praegu kehtiva süsteemiga – kuna enamus inimesi kannab kõiki olemasolevaid kaarte rahakotis, tähendab rahakoti kadumine või varastamine kõigi nende kaotsiminekut ja vajadust käia uute kaartide saamiseks läbi kõik asutused.

Teine variant ei tule praktilise lahendusena kõne alla, sest keskne andmebaas oleks vastuolus nii isikuandmete kaitse seaduse kui ka selle aluseks olevate põhimõtetega. Selle variandi korral pole kasu ka krüptograafiast, sest kaardi väljaandmise ja sellega seotud võtmepaari kasutuselevõtmiseni pole mingit võimalust hoida muude asutuste andmeid KMA andmebaasis nii, et neid saaks lugeda ainult vastava kaardi abil.

Kolmas lahendusvariant oleks piisavalt stabiilse side olemasolul kaardiomanikule esimesest märksa mugavam. Selle kõige olulisem puudus on vajadus tagada, et kaardile kirjutatavatest andmetest (või kaardile kirjutamise ettekäändel saadud andmetest) ei tehtaks illegaalseid koopiaid. Kuigi ka selle variandi kasutamise korral pole võimalik KMAle saadetavaid andmeid KMA-poolse kuritarvituse eest krüptograafia vahenditega kaitsta, on andmete valdajatel siiski teatav kontroll neilt väljastatavate andmete üle.

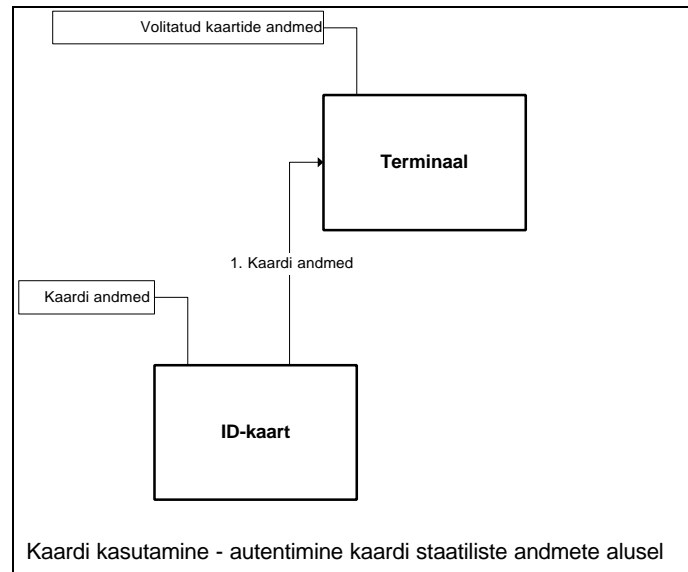
Neljas lahendusvariant ühendab endas esimese ja kolmanda lahenduse põhilised plussid, olles samal ajal vaba nende kõige olulisematest puudustest. Väärrib eraldi toonitamist, et KMA poolt kaardile genereeritud võtmepaar ei ole kaardiomaniku digitaalsignatuuri võtmepaar, seda kasutatakse ainult kaardi identifitseerimiseks. Selline võtmepaar oleks kasulik isegi siis, kui seda poleks vaja muude asutuste andmete kaardile edastamiseks, sest seda saaks kasutada kaardi ehtsuse tõestamiseks ka edaspidi (vt järgmine alajaotus). Selle lahendusvariandi kasutamise korral on oluline kaardi privaativõti kohe selle kaardile kandmise järel hävitada. Parim lahendus oleks kasutada kaarte, mis ise võtmeid genereerivad ja privaativõtit kunagi välja ei anna, kuid kahjuks on sellised kaardid tavalistest märksa kallimad.

Kaardi kasutamine

Autentimine kaardi staatiliste andmete alusel

Kaardi valdaja volitused määratakse kaardil olevate staatiliste andmete põhjal. Nendeks andmeteks võivad olla nii kaardi omaniku isikuandmed kui ka mingid teenusepakkuja poolt varem kaardile salvestatud andmed.

Selle autentimisviisi kasutamiseks peab kaart omama ainult tavalist mälu, terminaal tavalist mälu ja protsessorit (kaardil olevate andmete ja oma andmebaasi võrdlemiseks).



Plussid:

- autentimine eeldab nii kaardilt kui terminaalilt minimaalseid vahendeid.

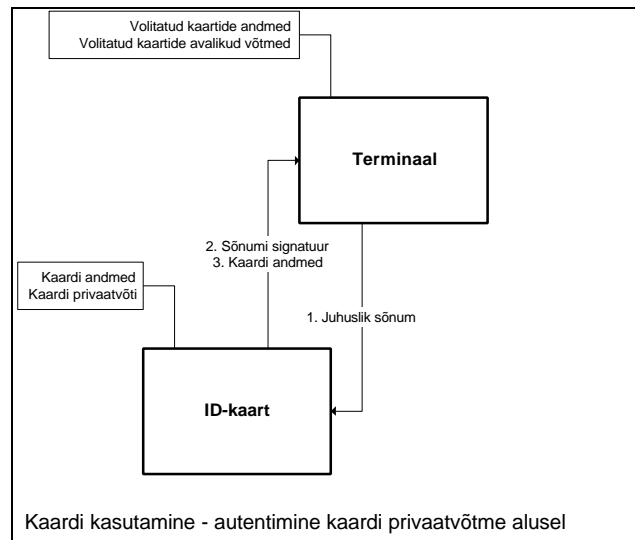
Miinused:

- kaarti on kerge võltsida;
- meetod ei välista varastatud kaardi kasutamist;
- terminaal ei saa kaardi esitamise fakti tõestada;
- kaart ei saa terminaali autentsust kontrollida;
- kaart ei saa esitamise fakti tõestada.

Autentimine kaardi privaatvõtme alusel

Kaardi valdaja volitused määratakse kaardi andmete põhjal, kuid enne seda peab kaart oma autentsust tõestama. Selleks võib kasutada näiteks terminaali poolt genereeritud juhusliku sõnumi signeerimist kaardi privaatvõtme abil.

Selle autentimisviisi kasutamine eeldab kaardilt nii kaitstud mälu (privaatvõtme hoidmiseks) kui ka protsessori (signeerimiseks) olemasolu. Terminaalilt eeldatakse tavalise mälu, protsessori (signatuuri verifitseerimiseks) ja juhuarvude generaatori (signeeritava sõnumi genereerimiseks) olemasolu.



Plussid:

- kaarti on raske võltsida;
- terminaal saab kaardi esitamise fakti tõestada.

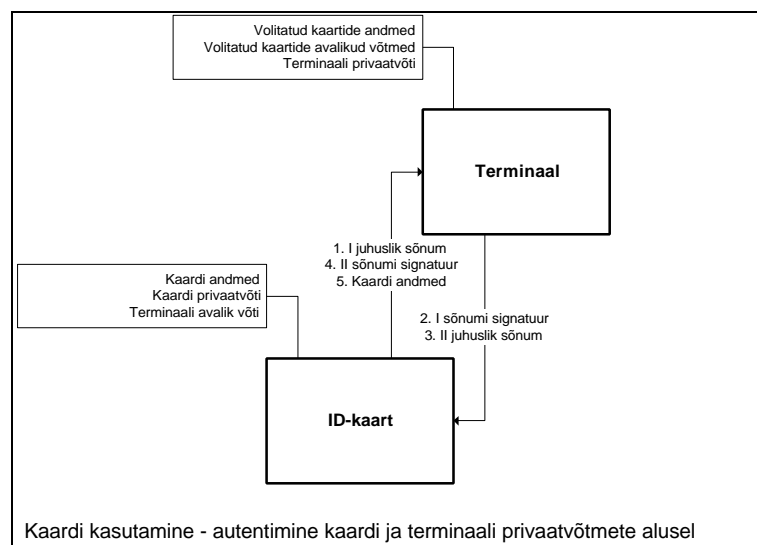
Miinused:

- meetod ei välista varastatud kaardi kasutamist;
- kaart ei saa terminaali autentsust kontrollida;
- kaart ei saa esitamise fakti tõestada.

Autentimine kaardi ja terminali privaatvõtmete alusel

Kaardi valdaja volitused määratakse kaardi andmete põhjal, kuid enne seda peavad kaart ja terminaal vastastikku oma autentsust tõestama. Selleks võib kasutada näiteks kaardi poolt genereeritud juhusliku sõnumi signeerimist terminali privaatvõtme abil ja terminali poolt genereeritud juhusliku sõnumi signeerimist kaardi privaatvõtme abil.

Selle autentimisviisi kasutamine eeldab nii kaardilt kui terminalilt kaitstud mälu, protsessori ja juhuarvude generaatori olemasolu.



Plussid:

- kaarti on raske võltsida;
- terminaal saab kaardi esitamise fakti tõestada;
- kaart saab terminaali autentsust kontrollida;
- kaart saab esitamise fakti tõestada.

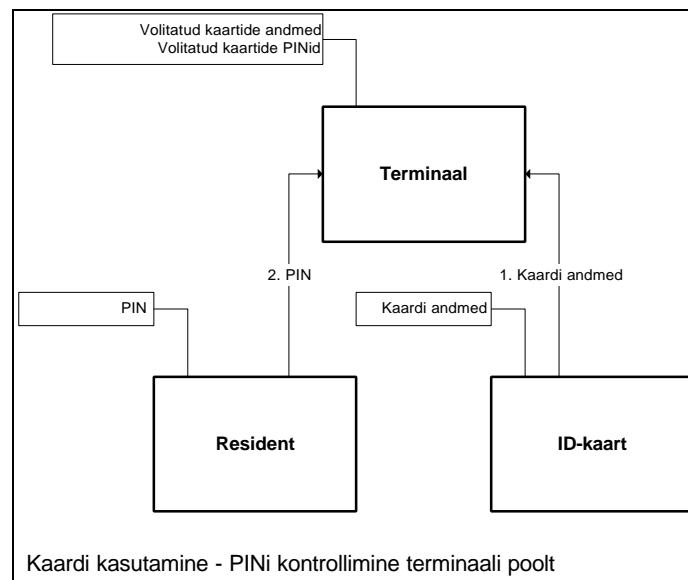
Miinused:

- meetod ei välista varastatud kaardi kasutamist.

PINi kontrollimine terminaali poolt

Varastatud kaardi kasutamise vältimiseks fikseerib teenusepakkuja igale kliendile isikliku koodi (PINi), mille alusel terminaal tuvastab, et kaarti kasutab selle legaalne omanik.

Selle meetodi kasutamine eeldab mälu olemasolu kaardil ja kaitstud mälu (PINide andmebaasi hoidmiseks) ning protsessori (sisestatud PINi ja kaardi andmete vastavuse kontrollimiseks oma andmebaasi põhjal) olemasolu terminaalil.



Plussid:

- tõkestab varastatud kaardi kasutamise.

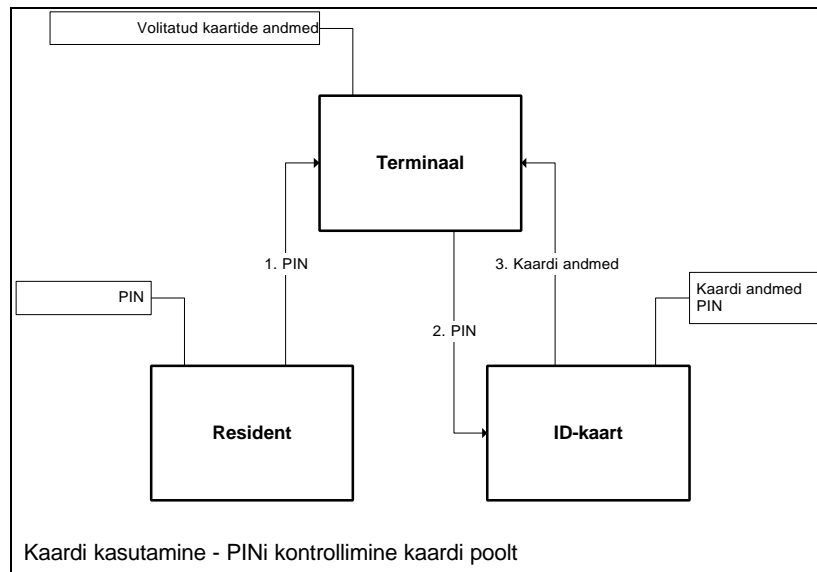
Miinused:

- eeldab kaardiomanikult PINi usaldamist terminaalile.

PINi kontrollimine kaardi poolt

Varastatud kaardi kasutamise vältimiseks fikseerib teenusepakkuja igale kliendile isikliku koodi (PINi), mille alusel kaart tuvastab, et teda kasutab selle legaalne omanik.

Selle meetodi kasutamine eeldab kaitstud mälu ja protsessori olemasolu kaardil.



Plussid:

- tõkestab varastatud kaardi kasutamise.

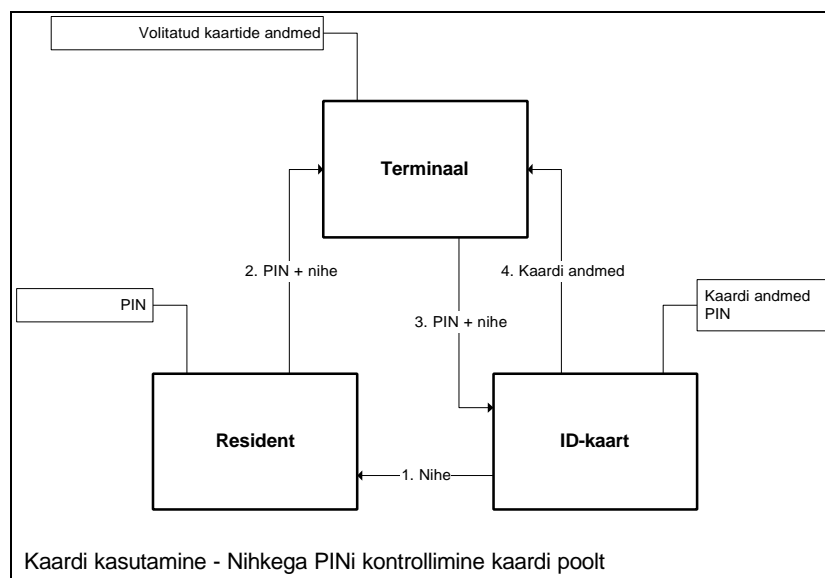
Miinused:

- eeldab kaardiomanikult PINi usaldamist terminaalile.

Nihkega PINi kontrollimine kaardi poolt

Varastatud kaardi kasutamise vältimiseks fikseerib teenusepakkuja igale kliendile isikliku koodi (PINi), mille alusel kaart tuvastab, et teda kasutab selle legaalne omanik. Selleks, et vältida PINi lekkimist terminaali kaudu, genereerib kaart juhusliku arvu (nn nihke) ja teatab selle (terminaalivälise kanali kaudu) kaardiomanikule. Kaardiomanik liidab nihke oma PINile ja sisestab terminaali saadud summa. Terminal edastab summa kaardile, mis lahutab sellest nihke ja saab esialgse PINi.

Selle meetodi kasutamine eeldab kaitstud mälu, protsessori, juhuarvude generaatori ja ekraani olemasolu kaardil, lisaks kalkulaatori (või peastarvutamise oskuse) olemasolu kaardi omanikul.



Plussid:

- tõkestab varastatud kaardi kasutamise;
- ei eelda kaardiomanikult PINi usaldamist terminaalile.

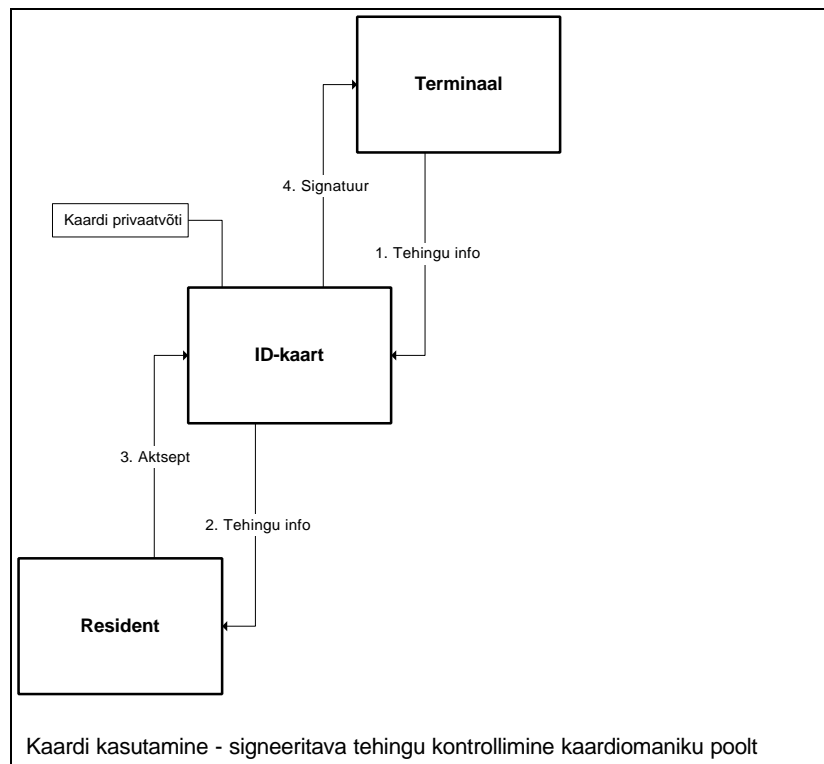
Miinused:

- eeldab ekraani olemasolu kaardil;
- eeldab kalkulaatori või peastarvutamise oskuse olemasolu kaardiomanikul.

Signeeritava tehingu kontrollimine kaardiomaniku poolt

Selleks, et vältida kaardiomaniku petmist terminaali poolt, mis võib ekraanil esitada ühe tehingu andmed, aga kaardile signeerimiseks saata hoopis teise tehingu, võib kaart enne tehingu signeerimist näidata oma ekraanil signeeritava tehingu andmeid ja nõuda tehingule kaardiomaniku aktsepti.

See autentimismeetod eeldab ekraani ja klaviatuuri olemasolu kaardil.



Plussid:

- ei eelda kaardiomanikult mingit usaldust terminaali suhtes.

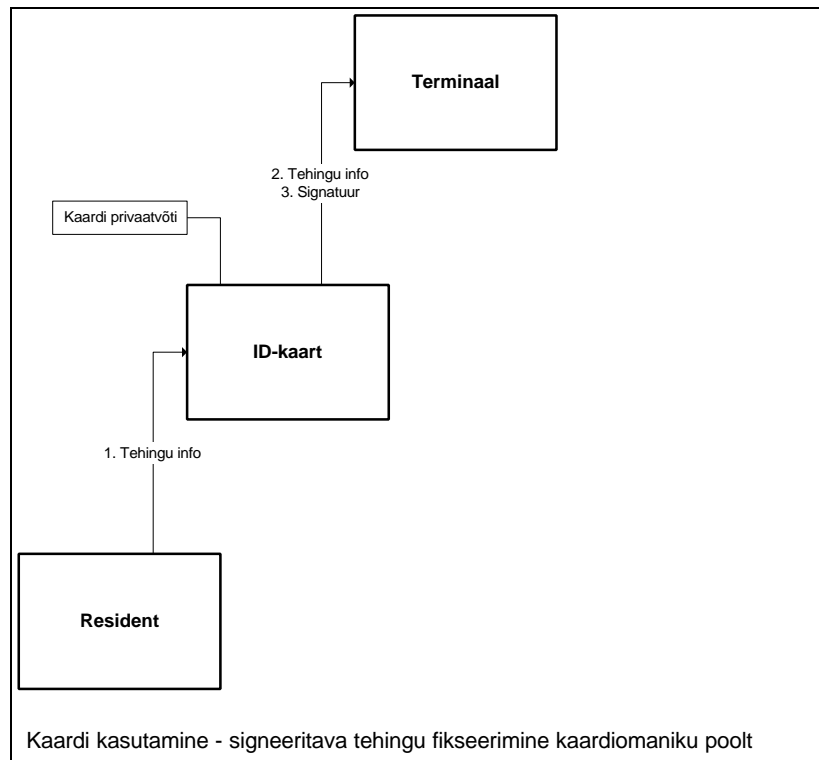
Miinused:

- eeldab ekraani ja klaviatuuri olemasolu kaardil.

Signeeritava tehingu fikseerimine kaardiomaniku poolt

Selleks, et vältida kaardiomaniku petmist terminaali poolt, mis võib ekraanil esitada ühe tehingu andmed, aga kaardile signeerimiseks saata hoopis teise tehingu, võib omanik enne tehingu signeerimist sisestada kaardile signeeritava tehingu andmed, et kaart saaks vale tehingu signeerimisest keelduda.

See autentimismeetod eeldab klaviatuuri olemasolu kaardil.



Plussid:

- ei eelda kaardiomanikult mingit usaldust terminaali suhtes.

Miinused:

- eeldab klaviatuuri olemasolu kaardil.

Kokkuvõte

Esimesed kolm kirjeldatud autentimisviisidest pakuvad erineva turvatasemega võimalusi kaardi ja terminaali omavahelise identifitseerimise lahendamiseks.

Esimene autentimisviis (autentimine kaardi staatiliste andmete alusel) on kasutusel enamikus olemasolevates kaardisüsteemides (mis on põhinevad magnetkaartidel). Kaardi võltsimise raskendamiseks võib kaardiomaniku andmete asemel kasutada mingit teenusepakkuja poolt signeeritud kirjet. Kui kaardiomaniku andmed on võimalik ära arvata või muudest allikatest teada saada ja nende põhjal valmistada võltskaart ka ilma originaali oma valdusse saamata, siis teenusepakkuja signatuuriga kirjet on võimalik saada ainult originaalkaardilt (või teenusepakkujalt). Siiski on originaalkaardi olemasolul sellest koopia tegemine triviaalne.

Teine autentimisviis (kaardi privaatvõtme alusel) välistab kaardist koopia tegemise ka juhul, kui originaalkaart satub volitamata isikute kätte (seda muidugi ainult eeldusel, et kaardi privaatvõtit pole võimalik hankida). Ainult kaitstud mälu olemasolu pole kaardi kopeerimise välistamiseks piisav – kui kaart peab oma autentsuse tõestamiseks oma kaitstud mälus olevad andmed terminalile esitama, saab terminalina esinev kolmas isik need andmed teada.

Terminali jääv sõnum ja selle signatuur võimaldavad terminalil hiljem kaardi esitamise fakti tõestada. Kui kaardile signeerimiseks esitatav sõnum on ajaserverist saadud ajatempel ja kaardi antud signatuur kohe ajaserveris uue ajatempliga varustada, võimaldab see tõestada ka kaardi esitamise aega.

Kolmas autentimisviis (kaardi ja terminaali privaatvõtmete alusel) välistab ka kaardi andmete eksliku väljastamise valesse terminaali. Ka saab kaart terminaali poolt signeeritud sõnumite logi abil hiljem esitamise fakte tõestada. Analoogiliselt eelmise meetodiga võimaldab ka see autentimisviis ajaserveri olemasolu korral lisaks kaardi esitamise faktile tõestada ka esitamise aega.

Selle autentimisviisi puuduseks on vajadus hoida kaardil terminaali (ja terminaali esitatud ajatempli kontrollimiseks ajaserveri) avalikku võtit. Sellest vajadusest saab hoiduda, kui tuua süsteemi sisse terminaalist eraldiseisev server, mida kaart (kaardi omanik) usaldab. Sel juhul võib kaart hoida ainult selle usaldusväärse serveri avalikku võtit ja lasta kõik (nii terminaalide signatuuride kui ka ajatemplite) verifitseerimised teha sellel serveril. Kui eeldada selle serveri privaatvõtme puutumatus, on kaudne verifitseerimine sama turvaline kui otsene. Teine võimalus on kasutada kõigi protsessis osalevate avalike võtmete sertifitseerimist kaardi väljaandja poolt. Sel juhul peab kaart omama ainult oma väljaandja avalikku võtit talle esitatud terminaalide ja ajaserverite avalike võtmete sertifikaatide kontrollimiseks.

Järgmised kolm autentimisviisi pakuvad erineva turvatasemega võimalusi kaardikasutaja ja kaardiomaniku isikusamasuse kontrollimiseks.

Esimene autentimisviis (PINi kontrollimine terminaali poolt) eeldab PINide terminaalise hoidmise võimalust. Reaalselt pole kõigi klientide PINide hoidmine igas terminaalises ei tehniliselt ega turvalisuse seisukohast vastuvõetav, sellepärast on praktikas kasutusel kaks modifikatsiooni kirjeldatud baasmeetodist:

- PINe ei omistata klientidele suvaliselt, vaid need arvutatakse teatud salajase algoritmi järgi mingitest muudest kaardil olevatest andmetest (selliselt töötavad mõnede pankade automaadid oma panga poolt väljastatud kaartide PINide kontrollimisel);
- PINe ei kontrollita terminaalises kohapeal, vaid need saadetakse (koos muude kaardilt loetud andmetega) krüptitult teenusepakkuja serverisse kontrollimiseks (selliselt töötab enamus PIN-põhised kontrollid olemasolevates süsteemides).

Ka kirjeldatud modifikatsioonid eeldavad kaitstud mälu olemasolu terminaalises (esimesel juhul kaardi andmetest PINi arvutamise algoritmi, teisel juhul serveriga suhtlemiseks kasutatava võtme hoidmiseks) ja kaardiomanikult oma PINi avatekstina terminaalile usaldamist.

Teine autentimisviis (PINi kontrollimine kaardi poolt) eeldab samuti PINi terminaalile usaldamist kaardiomaniku poolt ja lisaks annab vargale vabamad käed varastatud kaardiga eksperimenteerimisel. Siiski on sellel meetodil eelmisega võrreldes ka üks eelis – kuna andmete kaardilt väljumist kontrollib täielikult kaart, ei saa ilma õiget PINi teadmata andmeid kaardilt kätte.

Kolmas autentimisviis (nihkega PINi kontrollimine kaardi poolt) on eelmise meetodi edasiarendus, mis ei eelda kaardiomanikult oma PINi usaldamist terminaalile, kuid selle realiseerimiseks on vaja omada terminaalist sõltumatut kanalit kaardilt selle kasutajale info edastamiseks. Kui terminaal saaks teada kasutatava nihke, saaks selle abil kasutaja sisestatud summast PINi välja arvutada.

Kahe esimese meetodi puhul on võimalik PINi asemel kasutada ka mingit biomeetrilist informatsiooni (kaardikasutaja sõrmejälge, häält vms parameetreid), mis on raskemini võltsitavad ja mille korral pole unustamise ohtu, kuid need eeldavad vastavate lisaseadmete olemasolu terminaalises või kaardil ja pole seetõttu paljudeks rakendusteks sobivad.

Viimased kaks autentimisviisi pakuvad võimaluse tagada, et terminaal ei kasuta sisestatud kaarti selleks, et signeerida kaardiomaniku nimel lubamatuid tehinguid. Kuna need meetodid eeldavad kaardilt võrdlemisi arenenud suhtlusvahendeid, siis pole nad tegelikult ID-kaardi projekti raames realiseeritavad. Pigem oleks reaalne loobuda teatud piirist olulisemate tehingute signeerimisest mitteusaldusväärsetes terminaalides.

Eeltoodud autentimismeetodid pole sugugi üksteist välistatavad. Pigem tuleks mistahes teenuse autentimisel kasutada kõigi kolme (või vähemalt kahe esimese) grupi meetodeid kombineeritult. Seejuures ei pea kõigi teenuste autentimiseks kasutama samasuguseid meetodeid. Näiteks on täiesti võimalik, et inimene kasutab oma kodumaja trepikotta sissepääsemiseks oma kaardi identifitseerimisfunktsiooni ilma PIN-kontrollita, kuid oma korterisse pääsemiseks lisaks ka PINi. Kui keegi peaks tema kaardi varastama, pääseb varas küll trepikotta (mis pole oluline kahju), kuid mitte korterisse (mis oleks oluline kahju).

Kaardistusintervjuude põhjal tehtud järeldused erinevate autentimismeetodite vastuvõetavuse erinevate asutuste jaoks võib kokku võtta järgmise tabelina:

Kasutussituatsioon	KMA	Pank	Piirivalve- amet	Maksu- amet	ARK	Kaitse- minis- teerium	Kesk-haige- kassa	Spetsiaal- kindlustus- amet	Eesti Telefon	Neste Eesti	Digitaal- signatuur
Kaardi autentsuse kontrollimine											
Autentimine kaardi staatiliste andmete alusel	+	+ ¹	+ ¹	+	+ ¹	+ ¹	+	+	+ ¹	+ ¹	-
Autentimine kaardi privaatvõtme alusel	v	v	v	v	-	v	-	-	v	-	-
Autentimine terminali ja kaardi privaativõtmete alusel	v	v	v	v	-	v	-	-	v	-	+
Kasutaja autentsuse kontrollimine											
PINi kontrollimine terminali poolt	v	-	v	v	-	v	-	-	v	-	v
PINi kontrollimine kaardi poolt	v	-	v	v	-	v	-	-	v	-	+
Nihkega PINi kontrollimine kaardi poolt	v	+	v	v	-	v	-	-	v	+	v
Tehingute signeerimise kontrollimine											
Signeeritava tehingu kontrollimine kaardiomaniku poolt	v	+ ²	-	-	-	v	-	-	v	v	+
Signeeritava tehingu fikseerimine kaardi- omaniku poolt	v	+ ²	-	-	-	v	-	-	v	v	+

+ on kasutatav

- pole kasutatav

1 kasutatav teatavas osas (näiteks isikut tõendava dokumendi funktsioonides)

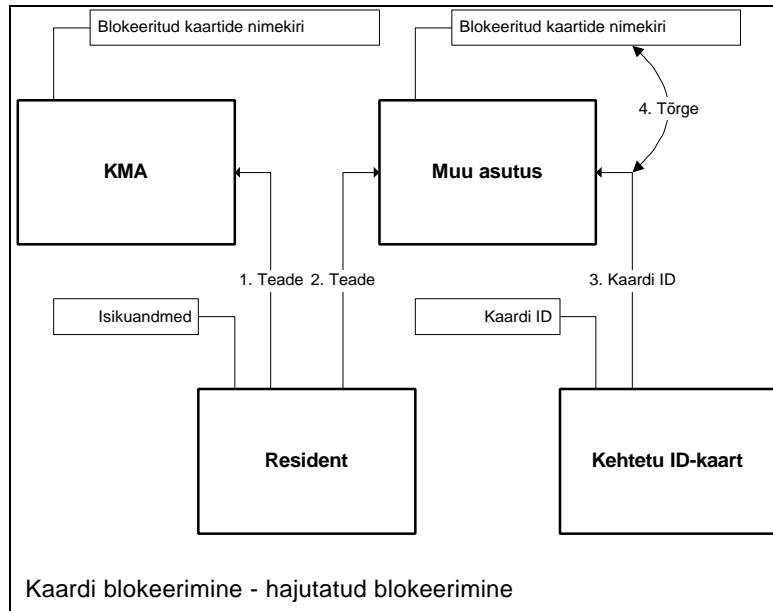
2 vaid juhul, kui signatuuril on riigi garantii

v pole kindlat otsust, sooviks sellist võimalust

Kaardi blokeerimine

Hajutatud blokeerimine

Kaardi kadumise korral teatab kaardiomanik sellest ise kõigile teenusepakkujatele. Kõik teenusepakkujad on kohustatud enne kaardi aktsepteerimist oma andmebaasi alusel selle kehtivust kontrollima.



Plussid:

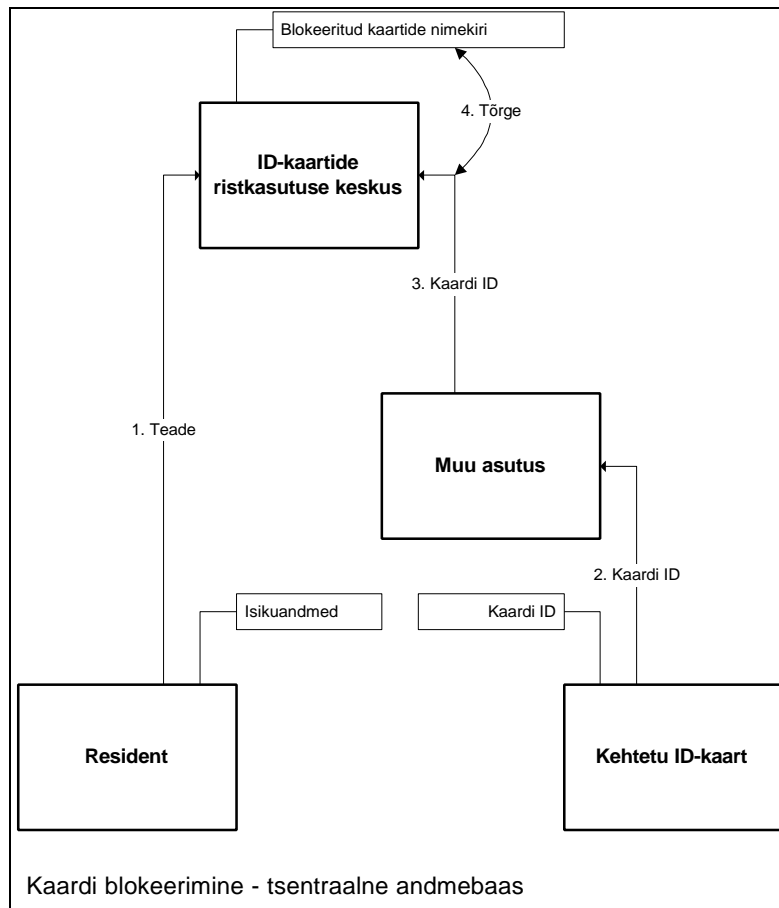
- iga teenusepakkuja saab kaardi kehtivust kontrollida lokaalselt ja ei sõltu sideoludest.

Miinused:

- kaardiomanik peab kaardi blokeerimiseks võtma ühendust kõigi asutustega, seejuures on võimalik, et ta unustab mõne asutuse või jõuab kaardi omastaja seda mõnes asutuses kasutada enne kui teade kaardi kadumisest sellesse asutusse jõuab;
- kui kaart ühes süsteemis blokeeritakse (näiteks korduva vale PIN sisestamise tõttu vms), jääb ta teistes süsteemides avatuks.

Tsentraalne andmebaas

Blokeeritud kaartide kohta peetakse ühtset kesket andmebaasi. Kaardi kadumise korral teatab kaardiomanik sellest keskse andmebaasi haldajale, kes kaardi oma andmebaasi kannab. Kõik teenusepakkujad on kohustatud enne kaardi aktsepteerimist keskbaasi alusel selle kehtivust kontrollima.



Plussid:

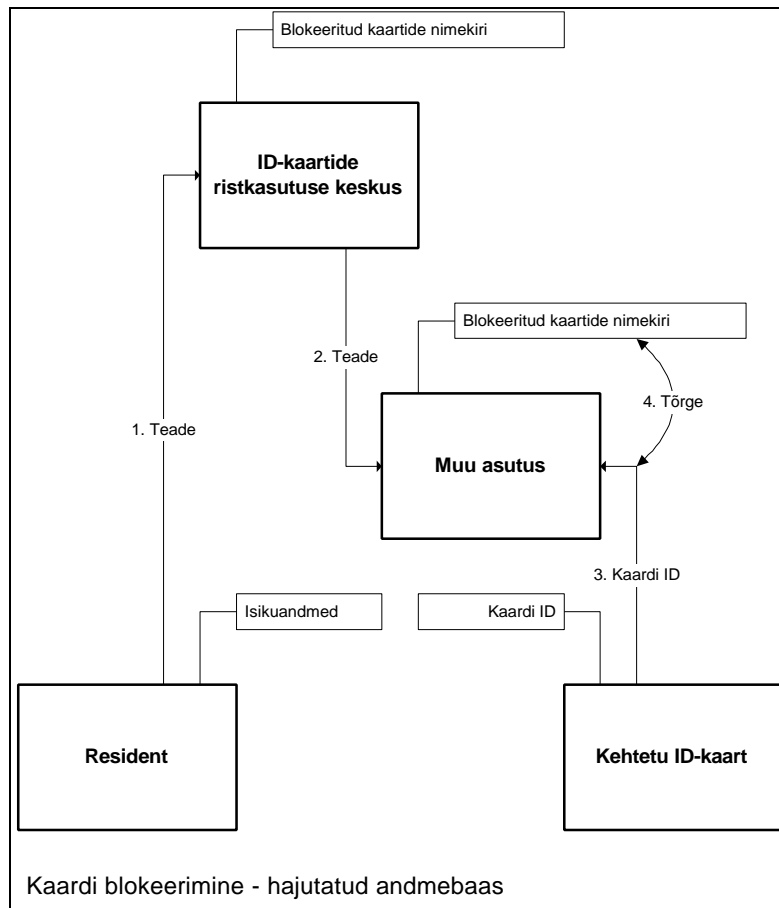
- kaardiomanik saab kaardi ühekorruga täielikult blokeerida;
- kui kaart ühes süsteemis blokeeritakse (näiteks korduva vale PIN sisestamise tõttu vms), on võimalik seda ka teistele süsteemidele laiendada (kui kesksbaasi ja teenusepakkuja vahelise lepinguga antakse teenusepakkujale volitused blokeeritud kaartide nimekirja täiendada miseks).

Miinused:

- sidekatkestuse korral teenusepakkuja ja kesksserveri vahel pole üldse võimalik teenust osutada.

Hajutatud andmebaas

Blokeeritud kaartide kohta peetakse kesksset andmebaasi ja igal teenusepakkujal on sellest oma koopia. Kaardi kadumise korral teatab kaardiomanik sellest kesksbaasi haldajale, kes kaardi oma andmebaasis blokeerib. Kõik teenusepakkujad on kohustatud teatud sagedusega oma andmebaasi kesksse andmebaasi alusel uuendama ja enne kaardi aktsepteerimist oma andmebaasi alusel selle kehtivust kontrollima.



Plussid:

- kaardiomaniik saab kaardi ühekorraga täielikult blokeerida;
- iga teenusepakkuja saab kaardi kehtivust kontrollida lokaalselt ja ei sõltu sideoludest;
- kui kaart ühes süsteemis blokeeritakse, on võimalik seda ka teistele süsteemidele laiendada.

Miinused:

- kui teenusepakkujate andmebaaside uuendamise sagedus pole piisavalt suur, on võimalik, et kaardi omanik jõuab kaarti mõnes asutuses kasutada enne kui teade kaardi kadumisest sellesse asutusse jõuab (eriti juhul, kui sidekatkestuse tõttu baasi uuendamine viibib).

Kokkuvõte

Esimene pakutud lahendusvariant (hajutatud blokeerimine) on sisuliselt samaväärne praegu kehtiva süsteemiga – kuna enamus inimesi kannab kõiki olemasolevaid kaarte rahakotis, tähendab rahakoti kadumine või varastamine kõigi nende kaotsimineku ja vajadust helistada kaartide blokeerimiseks läbi kõik asutused.

Kõige tõenäolisemalt rakendatakse praktikas teise ja kolmanda variandi segastrateegiat:

- mõned asutused peavad oma lokaalset koopiat blokeeritud kaartide andmebaasist ja täiendavad seda pidevalt vastavalt uute andmete kesksaasi laekumisele;
- mõned asutused kontrollivad kõiki neile esitatavaid kaarte kesksaasi põhjal;
- mõned asutused peavad oma lokaalset koopiat blokeeritud kaartide andmebaasist ja täiendavad seda kindlate ajavahemike järel.

Selleks, et vähendada kahju kaartide eksikombel või kuritahtlikest valeblokeerimistest, võiks kaaluda järgmisi variante:

- kaardi väljastamisel kinnitatakse sellele spetsiaalne salasõna; kaarti blokeerida saab ainult selle alusel;
- kaardi blokeerimisel peab blokeeriija teadma mingit väga spetsiifilist informatsiooni kaardiomaniku isikuandmetest;
- telefoni teel, nõ "kiirabi korras" saab kaardile panna ainult ajutise tõkke, mida tuleb hiljem isiklikult kohale minnes kinnitada; kui kinnitust mingi fikseeritud aja jooksul ei laeku, tühistatakse ajutine tõke automaatselt.

Esimese võimaluse puudus on see, et tõenäoliselt unustavad paljud inimesed selle salasõna ära, kuna seda ei lähe pidevalt vaja. Teise võimaluse puudus on see, et ID-kaart võib saada perekonnatülide lahendamise vahendiks (abikaasad teavad tüüpiliselt väga paljusid üksteise isikuandmeid). Kolmas võimalus (mida võib kasutada ka esimese või teisega kombineeritult) tundub olevat kõige töökindlam.

Kokkuvõte

Kaardistuse tulemusena selgus, et ID-kaardilt kui visuaalselt kasutatavalt isikut tõendavalt dokumendilt oodatakse ligikaudu olemasoleva passi mahus isikuandmete kandmist, lisaks peaks samad andmed olema loetavad ka elektrooniliselt (foto ja allkirjanäidise asemel võib olla ka mingi muu vahend kaardi esitaja ja selle tegeliku omaniku isikusamasuse kontrolliks).

Eriti oluliseks peeti kaardi nii trükitehnilist kui infotehnoloogilist võltsimiskindlust, kusjuures eraldi probleemina toodi seda välja rohkem elektrooniliselt salvestatavate andmete ja nendega seotud infrastruktuuri kontekstis. Oluliseks peeti ka seda, et ID-kaardi jaoks loodav infrastruktuur ei saaks isikuandmete lekkimise kanaliks.

Elektrooniliste dokumentide digitaalset signeerimist olid valmis aktsepteerima peaaegu kõik küsitletud asutused, kuid ainult juhul, kui digitaalsignatuurile antakse seadusandlikult traditsioonilise allkirjaga võrdne jõud. Elektroonilise autentimise, eriti aga digitaalsignatuuri kasutamise eeltingimuseks pidasid mõned küsitletud ka kaardiomanike teadlikkuse tõstmist.

Mitmed küsitletud avaldasid arvamust, et riiklikke ja kommertsfunktsioone ei tuleks panna ühele kaardile. Kaartide lahususe korral võiks riiklikule kaardile jääda isikut tõendava dokumendi, riigi poolt antud õiguste (haigekassa liikmekaart, pensionitunnistus, relvaluba jmt) kandja ja digitaalsignatuuri võtme hoidja funktsioonid, samal ajal kui kommertskaart (mille esmasteks väljaandjateks võiks erinevate arvamuste kohaselt olla pangad, Eesti Telefon või mingi spetsiaalselt selleks loodav organ *a la* Pankade Kaardikeskus) peaks katma panga kaardi ja mitmesuguste kliendikaartide funktsioonid.

Lisaks selgus, et autojuhilubade ja mõnede ettevõtete kliendikaardi funktsioonid esitavad kaardile (ennekõike selle visuaalsele küljele) ID-kaardi põhimõtetega vastuolulisi nõudeid ja seega ei ole need funktsioonid ID-kaardiga ühendatavad.

Lähteuring näitas, et erinevate asutuste (nii riigiametite kui ka erafirmade) põhimõtteline huvi ühtse kaardi vastu on küllaltki suur, kuid konkreetseid plaane on tehtud vähe. Arvatavasti on selle üheks olulisemaks põhjuseks asjaolu, et avalikkust teavitati ID-kaardi loomise plaanist alles väga hiljuti ja asutused pole lihtsalt jõudnud seda teematikat enda jaoks läbi mõelda. Sellega seoses tekib ka küsimus kaardistustulemuste usaldusväärsusest, mille hindamise meetrikatena võib kasutada ankeetide täituvust ja tagasiside aktiivsust.

Tagasiside aktiivsust iseloomustab järgmine tabel:

24	kaardistuseks valitud asutuses
1	kadus enne kaardistuse tegelikku algust
2	tõid põhjuseks ajapuuduse ja keeldusid intervjuust
2	teatasid, et ID-kaart on nende nõuetega mitteühilduv ja keeldusid intervjuust
12	ei tagastanud kooskõlastamiseks saadetud protokoll
3	tagastasid kooskõlastamiseks saadetud protokoll ühegi paranduse või märkuseta
5	tagastasid kooskõlastamiseks saadetud protokoll paranduste või märkusteg;

Ankeetide täituvust iseloomustavad järgmised tabelid:

- üldosa:

20	intervjueeritud isikust
10	kirjeldasid plaane kaarditehnoloogia arendamiseks
20	spetsifitseerisid nõuded inimloetavatele andmetele
20	spetsifitseerisid nõuded masinloetavatele andmetele
19	spetsifitseerisid nõuded kaardil olevatele algoritmidele
14	spetsifitseerisid nõuded kaardi turvalisusele
18	loetlesid asutuse poolt osutatavaid teenuseid
15	kirjeldasid asutuse poolt osutatavaid teenuseid

- teenused:

51	nimetatud teenusest
23	kirjeldatud teenusest
44	on olemasolevad teenused
7	on potentsiaalsed teenused
19	kohta loetleti reguleerivad normatiivaktid
23	kohta kirjeldati kaardil vajalikke andmeid
15	kohta kirjeldati teeninduspunktis vajalikke andmeid
16	kohta kirjeldati keskbaasis vajalikke andmeid
16	kohta teatati klientide arv
9	kohta teatati tehingute arv
11	kohta teatati teeninduspunktide arv
10	kohta teatati lubatav autentimise aeg
10	kohta teatati teenuse osutamise aeg
16	kohta kirjeldati kaardi väljastamisega seotud riske
21	kohta kirjeldati kaardi kasutamise seotud riske
20	kohta kirjeldati kaardi kaotamisega kaasnevat kahjusid

- autentimismeetodid:

22	nimetatud autentimismeetodist
17	kirjeldatud autentimismeetodist
15	kohta kirjeldati kaardil vajalikke andmeid
10	kohta kirjeldati teeninduspunktis vajalikke andmeid
10	kohta kirjeldati keskbaasis vajalikke andmeid
6	kohta teatati turvaelemendi maksumus
8	kohta kirjeldati saavutatav turvatase

Ankeetide suhteliselt kõrge täituvus on siiski petlik, sest üldiselt oli küsitluste käigus näha, et mitmed ID-kaardi ja elektroonilise autentimisega seotud probleemid (andmekaitse, kehtivatest normatiivaktidest tulenevad kitsendused, kulud ja tulud) on paljudes asutustes läbi mõtlemata – vastuseid ankeedis olevatele küsimustele mõeldi välja kohapeal *ad hoc*, need polnud varem paika pandud poliitika järeldused. Erandid on kahjuks ainult pangad ja mingil määral ka asutused, kus on juba kaardikasutamise kogemus.

Täpsema ja usaldusväärsema kaardistustulemuse saamiseks näeme kahte võimalust:

- kaarditehnoloogia ja sellega seonduvate probleemide alast koolitust koos järelemõtlemisajaga ning seejärel uue kaardistuse läbiviimist;
- kaardistatavate asutuste detailsemat analüüsi, mille käigus turvaprobleemidega kursis olev analüütik jõuaks süveneda konkreetsete asutuste spetsiifikasse (sellise analüüsi korral tuleks iga asutuse kaardistamiseks planeerida ca 10-20 korda rohkem aega, seega vähemalt 2-3 inimnädalat asutuse kohta).