CYBERNETICA

Euroopa Liit
Euroopa
Regionaalarengu Fond

Eesti
tuleviku heaks

CDOC 2.0 analüüs

Tehniline dokument

Versioon 1.0

26. märts 2020. a.

31 lk

Dok T-184-4

Sisukord

1 Sissejuhatus

Pärast ROCA kaasust 2017. aastal [11] sai selgeks, et kolmest ID-kaardi kasutusmallist (signeerimine, autentimine, krüpteerimine) osutus mitmeski mõttes kõige haavatavamaks just krüpteerimine [3]. Ühest küljest pakkus ID-kaart mugavat platvormi, tänu millele olid valdavale osale Eesti elanikest asümmeetrilised krüptovõtmed juba mugavalt laiali jagatud. Teisalt aga kasutati krüpteerimisstsenaariumis ID-kaarti sisuliselt pikaajalise staatilise dekrüpteerimisvõtme hoidlana, mistõttu tähendas selle võtme murdumine automaatselt kõigi talle krüpteeritud dokumentide kompromiteerumist.

Praegune aruanne analüüsib Eestis reaalselt kasutatavaid krüpteerimisstsenaariume ning pakub välja arhitektuursed ideed neile vastava krüpteerimistaristu loomiseks, mis ei oleks nii haavatav ROCA-laadse probleemi kordumisel.

Juhime seejuures tähelepanu kahele aspektile.

Esiteks erinevad krüpteerimisstsenaariumid oma nõuetelt märkimisväärselt, mistõttu pole võimalik luua ühte kõigile universaalselt sobivat lahendust. Uus taristu (koodnimetusega CDOC 2.0) hakkab pakkuma mitut alamprotokolli, mille hulgast tuleb kasutajal valida sobiv tema enda vajadustest lähtudes. Erinevad protokollid esitavad ka juurutusele erinevaid nõudeid ja nii ei saa öelda, et üks alamprotokoll on parem või turvalisem kui teine – neil lihtsalt ongi erinevad omadused.

Teiseks hakkab uus lahendus tegema rangemat vahet transpordi- ja säilituskrüptograafia vahel. Vajadus selle vahe järele tuleneb eeskätt asjaolust, et transpordikrüptograafia on probleem, mille jaoks on erisustest hoolimata võimalik sõnastada tehniline probleemipüstitus (näiteks kasutusmallide kujul) sellisel viisil, et see kirjeldab kõigi huvitatud osapoolte vajadusi ning seetõttu on võimalik seda probleemi ka tehniliste vahenditega lahendada. Säilituskrüptograafia korral aga ei ole see suure hulga kasutajate jaoks võimalik, sest nende vajadused ja võimalused on liiga erinevad - me võime küll defineerida üksikuid kasutusmalle, aga see pole kasulik, sest ei moodustu terviklikku süsteemi. Praegune aruanne keskendub peamiselt dokumentide krüpteerimisele transpordi jaoks. Aruandes käsitletakse ka dokumentide pikaajalist krüpteerimist, kuid tehniliselt madalama detailsusega, sest üksikute kasutajate vajadused on vaja iga realisatsiooni korral eraldi välja selgitada[1] ning see toob tõenäoliselt kaasa ka suuri erisusi lõplikus tehnilises lahenduses.

Uue lahenduse nõuete tuvastamiseks viisid autorid läbi rea intervjuusid; intevjuude küsimustik on toodus lisas A. Autorid avaldavad tänu järgmistele asutustele, mille esindajad intervjuudes osalesid:

[1] Ka käesoleva analüüsi käigus tehtud intervjuud ei andnud väga selget sisendit säilitudkrüptograafiaga tegelemiseks.

- Kaitseministeerium,
- Kaitsepolitseiamet,
- Küberkaitseliit,
- SK ID Solutions AS,
- Sotsiaalministeerium,
- Swedbank,
- Tervise ja Heaolu Infosüsteemide Keskus,
- Välisluureamet.

2 Krüpteerimislahenduse kasutusstsenaariumid

2.1 Intervjuude põhjal leitud stsenaariumid

Intervjuude käigus selgus, et krüpteeritud failide vahetamist kasutatakse Eesti asutustes väga erinevates stsenaariumites.

2.1.1 Asutusesisene suhtlus

- Süsteemiadministraatorite vahel paroolide edastamine.
- Isikutega seotud intsidentide lahendamiseks vajaliku info edastamine asutuse sees.
- *Ad hoc* info edastamine.

2.1.2 Asutustevaheline suhtlus

- Info edastamine ministeeriumite ja õiguskaitseorganite vahel.
- AK-märkega info edastamine.
- Riigisaladuse märkega info edastamine (oli varem rohkem kasutuses, nüüd pigem piiratud).
- Välisvõrgust kohtunikele aegkriitilise info edastamine.
- Kriminaamlenetluse jaoks vajaliku info edastamine.
- Lepingud, ametlikud päringud.

2.1.3 Eraisikute ja asutuste vaheline suhtlus

- Terviseandmed, mida ei taheta edastada üle Digiloo (nt eralaboris tehtud analüüside tulemused).
- Kodanikult riigiametile konfidentsiaalse info edastamine.
- Lepingud, ametlikud päringud.
- Trahviteadete edastamine.
- Kodaniku ja panga vaheline suhtlus (nt pangaväljavõtete edastamine eluasemelaenu taotlemisel).

2.1.4 Eraisikutevaheline suhtlus

Kuna eraisikutevaheline suhtlus polnud otseselt intervjuude fookuses, siis vastavaid stsenaariume intervjuudes ei mainitud. Puudub ka selge viis teada saada, kui palju eraisikud omavahelises suhtluses ID-kaardi krüpteerimisfunktsionaalsust kasutavad, kui arvata võib, et seda tehakse.

2.1.5 Suhtlus välispartneritega

Ka seda teemat intervjuud otseselt ei katnud, kuid mitmel korral ilmnes, et kui CDOC 2.0 võimaldaks mugavat suhtluse turvamist piiritaguste partneritega, siis see oleks teretulnud lisandväärtus.

2.1.6 Säilituskrüptograafia

See alapunkt on siia toodud ainult dokumendi terviklikkuse huvides. Tänuväärsel moel ei tuvastanud intervjuud, et keegi intervjueeritavatest kasutaks ID-kaardi võtmetega kaitstud CDOC konteinereid pikaajalise krüpteerimise vahendina.

2.2 Stsenaariumite jaotus nõuete klassidesse

Järgnevalt esitame peamised krüpteerimislahenduse kasutusstsenaariumite klassid rühmitatuna sarnaste nõuete alusel.

2.2.1 *Ad hoc* infoedastus, madal konfidentsiaalsusvajadus

Sellesse klassi kuuluvad stsenaariumid, mille korral

- sõnumi saatja ja saaja ei lepi sõnumi edastamises eelnevalt kokku,
- sõnumi saatja ja saaja ei oma motivatsiooni sõnumi edastamiseks lisaoperatsioone ette võtta,
- sõnumi konfidenstiaalsusvajadus on väike, ulatudes ajaliselt ca aasta või paarini; kahju info avalikukstulekul on piiratud.

Selle klassi teabel võib olla lühike eluiga (näiteks kui edastatakse perioodiliselt uuendatavat olukorrainfot). Selle eluea möödumisel võib olla koguni soovitav, et info muutuks dekrüpteerimatuks.

2.2.2 Sünkroonses režiimis toimuv infoedastus

Sellesse klassi kuuluvad stsenaariumid, mille korral

- sõnumi saatja ja saaja on üheaegselt liinil (nt samal kiirsuhtlusplatvormil või muul moel üle Interneti ühendatult).

2.2.3 Kaitstud perimeetris toimuv infoedastus

Sellesse klassi kuuluvad stsenaariumid, mille korral

- sõnumi saatja ja saaja kuuluvad samasse organisatsiooni, millel on lisaks CDOC-i poolt pakutavale kaitsele olemas veel omaette turvakiht (VPN, ainult sisevõrgus toimiv dokumendihaldussüsteem vms),
- info on oluline asutuse sees,
- siseründajal on välise ründaja ees teatav eelis,
- kahju info avalikukstulekul on piiratud asutuse enda operatsioonide ja vastutusalaga.

2.2.4 Kõrge konfidentsiaalsusvajadusega info edastamine asutuste vahel üle välisvõrgu

Sellesse klassi kuuluvad stsenaariumid, mille korral

- sõnumi saatjal ja saajal on reeglina eelnev kokkulepe info edastamiseks,
- sõnumi saatjal ja/või saajal on motivatsioon vajaliku konfidentsiaalsustaseme saavutamiseks eraldi pingutada,
- salastustähtaeg on reeglina pikk (mõnikümmend aastat kuni tähtajatu),
- info avalikukstulekul enne salastustähtaja möödumist võivad olla tõsised tagajärjed,
- kasutatav lahendus peaks ideaalis olema akrediteeritud/sertifitseeritud.

2.2.5 Kõrge konfidentsiaalsusvajadusega info edastamine isikute ja asutuste vahel üle välisvõrgu

Sellesse klassi kuuluvad stsenaariumid, mille korral

- isikul ja asutusel ei pruugi olla eelnevat kokkulepet info edastamiseks,
- asutusel on motivatsioon ja võimekus vajaliku konfidentsiaalsustaseme saavutamiseks eraldi pingutada,
- konfidentsiaalsusvajaduse ajaline horisont on keskpikk (mõni kuni mõnikümmend aastat).

3 Transpordikrüptograafia

Suurim sisuline probleem, mille tõttu ROCA kaasus senisele ID-kaardi krüpteerimisfunktsionalsusele nii suurt mõju avaldas, on võtmehaldus, mille korral ID-kaarti kasutatakse pikaajalise staatilise asümmeetrilise dekrüpteerimisvõtme hoidlana. Kui see võti murdub, kompromiteeruvad kõik võtme kasutusajal talle krüpteeritud dokumendid.

Selle probleemi lahendus on mitte kasutada ID-kaardil asuvat võtit ainsa dekrüpteerimisfaktorina ja luua olukord, kus iga dokumendi dekrüpteerimiseks on vaja (vähemalt osaliselt) unikaalset võtit. Niisugune lähenemine toob aga endaga kaasa dekrüpteerimisvõtmete levitamise probleemi. Kuidas seda probleemi kõige paremini lahendada, sõltub konkreetse stsenaariumi nõuetest ning keskkonna poolt pakutavatest võimalustest.

3.1 Sünkroonses režiimis toimuv infoedastus

Krüptograafiliselt on see mingis mõttes kõige lihtsam olukord, sest suhtluspartnerite vahel saab kokku leppida värske ühekordse võtme (näiteks Diffie-Hellmani võtmevahetusprotokolliga). Praktikas kasutatakse suurt hulka kiirsuhtlusplatvorme ja intervjuudest tuli välja, et võimalus liidestada mõni levinum neist Eesti (või ka näiteks mõne teise EU riigi) eID lahendustega identiteedi tugevaks tuvastamiseks oleks paljudele asutustele huvitav. Samas tuleb arvestada, et platvormi arendaja ei puugi olla huvitatud sellise liidestuse integreerimisest oma koodibaasi.

Teine võimalus on kasutada DigiDoc klienti krüptovõtmete vahetamiseks ning mõnda kiirsuhtlusplatvormi ainult ühise aja kokkuleppimiseks suhtluspartnerite vahel.

Kolmandaks on võimalik, et korraga ei pea liinil olema füüsilised inimesed, piisab ka nende digitaalsetest agentidest.

3.2 Ühekordsete avalike võtmete kasutamine

Ühekordsete (piiratud kasutusaja ja -otstarbega) avalike võtmete kasutamine on tulevikuturvalisuse saavutamise jaoks levinud võte, alates efemeersest Diffie-Hellmani võtmevahetusest [6] ja lõpetades Signali kiirsuhtlusprotokoliga [5].

Niisuguse lahenduse juurutamise praktiline probleem seisneb selles, et ükski Eestis kasutuses olev tugev digitaalne isikutuvastuse vahend ei toeta otse ühekordsete võtmete kasutamist. Alates 2017. aastast toetab ID-kaart küll ühepoolset Diffie-Hellmani võtmevahetust elliptkõveratel (v.t. [2]), kuid see mehhanism ei paku tulevikuturvalisust, sest ühekordseid võtmeid kasutatakse ainult saatja pool ning seega sõltub krüpteeritud andmete turvalisus ikkagi vastuvõtja pikaajalise privaatvõtme turvalisusest.

Esmane võimalik lahendus on lasta vastuvõtjal genereerida endale ajutised võtmepaarid, kuid sellega kaasneb mitmeid probleeme.

1. Kuidas tagada ajutiste avalike võtmete autentsus, s.h. nende operatiivne tühistamine pikaajalise salajase võtme kompromiteerumise, aegumise või hävimise korral?
2. Vastuvõtja ei pruugi olla motiveeritud võtmeid genereerima või on see tema jaoks liiga keeruline.
3. Vastuvõtja poolt genereeritud võtmepaaride salajasi pooli peab kuidagi kaitsma ning nende lihtviisiline hoidmine vastuvõtja arvuti/nutiseadme salvestusseadmes avatekstina ei ole üldjuhul piisavalt turvaline.
4. Kuidas tagada, et võtmepaare tegelikult ka ainult ühe korra kasutatakse või kuidas veenduda, et piiratud mitmekordne kasutamine ei kujuta endast turvaprobleemi?
5. Kuidas ajutisi avalikke võtmeid pikaajalise võtmega signeerida? Siin on kaalukausil signeerimise kiirus (ID-kaardiga 1000 võtme ühekaupa signeerimine ei ole praktiline) v.s. võtmehalduse praktilised aspektid (kui on vaja tühistada üks võti 1000-st, mis on ühe signatuuriga kaitstud, siis kas tuleb tühistada kõik?).

Ühekordsete avalike võtmete kasutamist võib kaaluda olukordades, kus edastatava info salajasus on kriitiline ning vastuvõtjal on olemas piisav võtmehalduse kompetents.

3.3 Võtmeedastusserveri ja võtmeosakute kasutamine

Alternatiivina ühekordsete avalike võtmete (asümmeetriliste võtmepaaride) kasutamisele pakume välja ühekordsete sümmeetriliste võtmete kasutamise.

Kui seda lähenemist rakendada nii, et vastuvõtja ei genereeri omale piiratud kasutusega asümmeetrilisi võtmepaare, siis ei panusta ka sümmeetriliste võtmete kasutamine midagi krüptograafilisse tulevikuturvalisusesse, kuid seda skeemi saab täiendada kahe erineva meetmega, mis aitavad süsteemi kindlustada pikaajalise asümmeetrilise võtme kompromiteerumise vastu. Nendeks meetmeteks on

- usaldusväärse (v.t. jaotis 3.3.1) võtmeedastusserveri kasutamine ja
- sümmeetrilise võtme ühissalastamine (vt [12]) mitme edastuskanali vahel ning iga osaku eraldi kaitsmine.

Skeem näeb lühidalt välja järgmine.

1. Saatja genereerib sümmeetrilise võtme ning ühissalastab selle kahe või enama osapoole vahel (v.t. allpool).
2. Saatja kasutab terviklikku sümmeetrilist võtit sõnumi krüpteerimiseks, lisades seejuures CDOC konteineri metainfosse kogu vajaliku info kasutatud ühissalastuse kohta.
3. Saatja edastab CDOC konteineri vastuvõtjale.

Sõltuvalt ühissalastuse meetodist võib olla vaja osakuid veel eraldi kaitsta, näiteks järgmistel viisidel:

1. krüpteerimine vastuvõtja pikaajalise avaliku võtmega,
2. krüpteerimine vastuvõtja ajutise avaliku võtmega,

3. krüpteerimine võtmeedastusserveri avaliku võtmega (mis võib kuuluda näiteks mõnda postkvant-turvalisse krüptoskeemi).

Hästivalitud ühissalastuse meetodi korral võib üldiselt ühe osaku edastada avatekstina, kuna üksik osak ei anna salastatud võtme kohta mingit informatsiooni.

Osakuid saab edastada

1. lisatuna CDOC konteinerisse või
2. edastatuna läbi võtmeedastusserveri, kusjuures võtmeedastusserver nõuab vastuvõtja autentimist pikaajalise salajase võtme abil.

Erinevaid osakute kaitsmise ja edastamise meetodeid saab omavahel kombineerida, mis loob aluse paindlikule võtmeedastusraamistikule.

Saadaval raamistikul on potentsiaalselt mitu kasulikku omadust.

- Kui kasutatakse võtmeedastuserverit, siis ei ole võimalik CDOC konteinerit dekrüpteerida ilma võtmeedastusserveri vähemalt ühekordse osaluseta.
- Täielikku sümmeetrilist võtit ei hoita korrektselt käituva klienditarkvara puhul CDOC konteineri juures isegi mitte krüpteeritud kujul.
- Lisaks pikaajalisele sümmeetrilisele võtmele, mille krüptosüsteemi muutmine on potentsiaalselt väga keeruline, saab osakute kaitsmiseks kasutada ka täiendavaid, näiteks post-kvant avaliku võtme krüptosüsteeme. See panustab otseselt hüpoteetilise „ROCA2" intsidendi mõju vähendamisesse.

Kokkuvõtteks saame väita, et kuhugi „vedelema jäänud" CDOC konteinerid ei ole dekrüpteeritavad isegi siis, kui vastuvõtja pikaajaline privaatvõti kompromiteerub. Samal ajal tuleb tähele panna, et vajadus suhelda võtmeedastusserveriga võib põhjustada käideldavusprobleeme.

Lisaks saab võtmeedastusserverit juurutada nii, et saavutatakse järgmised täiendavad omadused.

- Võimalus määrata serveris hoitud osakutele aegumistähtaega, s.t. dekrüpteerimine osutub pärast mingit tähtaega võimatuks.
- Saatja võib võtmeosakud tagasi kutsuda, näiteks selleks, et sõnumis olev info dekrüpteerimatuks muuta.

Mõlema omaduse vastu ilmutati intervjuude käigus huvi.

Juhime tähelepanu, et samal ajal peab klienditarkvara kasutajakogemus olema disainitud nii, et sõnumi vastuvõtjal ei tekiks kiusatust kasutada (sõnumi transpordiks kasutatud) CDOC konteinerit pikaajalise säilituskrüptograafia vahendina.

3.3.1 Võtmeedastusserveri usaldusväärsus

Kuigi ideaalsel juhul tahaks me esitada võtmeedastusserverit mingis tugevas turvamudelis, mis võimaldaks nõuda serveri võimalikult vähest usaldusväärsust, ei ole see praktikas hästi võimalik[2].

[2] Põhiliselt algseks eelduseks oleva tulevikuturvaliste protokollide toe puudumise tõttu eID vahendites.

Seetõttu on vaja nõuda, et võtmeedastusserver oleks usaldusväärne vähemalt järgmistest aspektides.

- Juhul, kui mingit osakut krüpteeritakse võtmeeedastusserveri privaatvõtmele, siis ei tohi server seda osakut lekitada (s.h. läbi oma privaatvõme lekitamise).
- Juhul, kui kasutatakse osaku aegumist, tagasikutsumist vms. funktsioone, peab server neid funktsioone tõesti korrektselt täitma.
- Juhul, kui server hoiab tõesti mõnd osakut, siis peab ta selle õigustatud päringu peale ka väljastama[3].

Nõuded võtmeedastusserveri usaldusväärsusele ning sellest tulenevad kulud on paratamatult midagi, mida tuleb kogu CDOC 2.0 ökosüsteemi planeerimisel arvesse võtta.

3.4 Kahesuunaline turvatud kanal

Kahesuunaline turvaline kanal on edasiarendus punktis 3.1 kirjeldatud lahendusest.

Saadav süsteem erineks oluliselt praegusest konteineri-põhisest lahendusest ning keskenduks rohkem turvalisele universaalsele sidekanalile, mille sees võib edastada mitmesuguseid infovooge.

Niisuguse arhitektuuri põhilised ehituskivid on järgmised.

1. Mõne valmisprotokolli (näiteks Signal [5]) baasil ehitatud klientrakendus[4].
2. Protokollile lisatud Eesti tugevate isikutuvastusvahendite tugi.
3. Võtmevahetusserver lühiajaliste avalike võtmete vahetamiseks (see on tüüpiliselt niisuguste protokollide osa).
4. Sideserver, mis lubab krüpteeritud sõnumeid asünkroonse side võimaldamiseks puhverdada (nii seda kui eelmist serverit võib olla mitu).
5. Mehhanism võtmete turvaliseks säilitamiseks klientrakenduses. Sõltuvalt vajalikust turvatasemest ning kasutatavast riistvarast on siin mitmesuguseid variante (süsteemne *keychain*, TPM jms).

Selliselt konstrueeritud kanali sisse on võimalik omakorda multipleksida mitmesuguseid protokolle: sõnumirakendust, failivahetust jms.

3.5 Integratsioon asutusesisese dokumendihaldussüsteemiga

Paljudes asutustes ja organisatsioonides on kasutusel mingi dokumendihaldussüsteem. Intervjuude käigus tuli välja, et nii transpordikrüptosüsteemi dekrüpteerimine kui pikaajalise säilitamise jaoks krüpteerimine võiks olla sellise süsteemi funktsionaalsus. Ideaalis saaks krüpteerimis-dekrüpteerimisfunktsionaalsus olla lõppkasutajale praktiliselt läbipaistev.

[3] Tegu on küll rohkem nõudega käideldavusele, kuid see mahub üldisesse konfidentsiaalsus-terviklikkus-kättesaadavus turvamudelisse.

[4] Täpsustus: tegu ei oleks oleks mõne olemasoleva teenuse laiendusega, vaid ainult protokolli ja selle realisatsiooni taaskasutamisega.

Ühest küljest võimaldaks selline lähenemine lahendada mugavalt asutuse sees delikaatse info edastamise probleemi, aga teisalt käib ka infovahetus väliste osapooltega nagunii läbi dokumendihaldussüsteemi.

On teada, et näiteks Microsofti Sharepointil on olemas API-d, mille kaudu saab dokumendihalduse alla kuuluvaid faile CDOC kliendirakendusest hallata, kuid vähemlevinud dokumendihaldussüsteemide kohta tuleb läbi viia täiendav analüüs.

4 Pikaajaline säilituskrüptograafia

Pikaajalise turvalisuse (nii konfidentsiaalsuse, autentsuse kui tervikluse) tagamine on oma olemuselt andmete transpordi turvamisest väga erinev. Kui transpordikrüptosüsteemidele esitatavad nõuded oli võimalik jagada paari suuremasse rühma, siis pikaajalise säilitamise puhul see nii ei ole. Küsimus, milline pikaajaline andmete turvalise säilitamise lahendus on antud organisatsioonile parim, on väga konkreetse organisatsiooni spetsiifiline. See sõltub juba kasutusel olevast dokumendihalduskeskkonnast, kaitsvatate dokumentide salastusvajadusest, rollide jaotusest organisatsioonis, andmemahtudest jpm.

Samuti paneme tähele, et pikaajaline säilituskrüptograafia ei pea olema nii tugevalt seotud Eesti spetsiifiliste oludega (eID vahendid) kui transpordikrüptograafia.

Küll on aga oluline juba analüüsi sissejuhatuses püstitatud „negatiivne´´ eesmärk: vältida olukordi, kus inimesed kasutavad tänast CDOC krüpteerimist pikaajalise salastamise vahendina.

Saksamaa Liitvabariigi infoturbeagentuur BSI on välja pakkunud omapoolse lahenduse pikaajalise säilitamise probleemile [1], kuid see keskendub ennekõike tõendusväärtusega dokumentide kättesaadavusele ning terviklusele, mitte niivõrd konfidentsiaalsusele.

Pikaajalise konfidentsiaalse säilitamise jaoks on turul hulk valmislahendusi, millest mõni sobib suure tõenäosusega enamiku konkreetsete juhtude jaoks. Universaalset eeskirja sobiva lahenduse valikuks on siinkohal raske anda, seesõltub tugevalt iga organisatsiooni vajadustest, võimalustest ja võimekusest. Lahenduse valik peaks algama vastuste leidmisest muuhulgas järgmistele küsimustele.

- Kas ligipääs andmetele on isiku- või rollipõhine?
- Milline on asutuse võtmehaldusvõimekus?
- Kas koos töötajate arvutisüsteemi ligipääsude tühistamisega (näiteks töölt lahkumise korral) koos tuleb lisaks tühistada/vahetada ka krüptovõtmeid?
- Kas on vaja krüpteerida tööjaamades asuvaid andmeid?
- Kas on vaja krüpteerida lihtsalt failiserverit või mõnd keerukamat struktuuri (näiteks maili- või dokumendiserver)?
- Kas on vaja krüpteerida transaktsionaalset andmebaasi?
- Kas andmebaasis on vaja krüpteerida üksikuid välju või kirjeid?
- Kas andmete dekrüpteerimine on normaalse IT-töövoo osa (arvutisse sisse logides avatakse krüpteeritud salvestusseade) või on tegu eraldi tseremooniaga, mis võib nõuda ka rohkem kui ühe inimese osavõttu?
- Millised on andmemahud?

- Milline on säilitatavate andmete konfidentsiaalsusvajadus? Mis juhtub, kui andmetes talletatud teave avalikuks saab? Kui pikka aega andmete konfidentsiaalsust säilitada tuleb?
- Kuidas krüpteeritud andmeid varundatakse?

Siinses aruandes saame ilma konkreetsete organisatsioonide spetsiifilistesse nõuetesse süüvimata võimalikke kasutusstsenaariume jagada vaid paari suuremasse klassi. Võtmeküsimuseks on siinjuures ülaltoodud loetelust esimene – millisel põhimõttel korraldatakse ligipääs pikaajaliselt säilitatavatele andmetele?

Kõigepealt panemegi tähele, et andmeid ei säilitata mitte säilitamise enda pärast, vaid neile tuleb vajadusel tagada ka ligipääs kogu säilitusperioodiks (vastasel juhul võiks andmed pärast transpordikrüptogrammide dekrüpteerimist kustutada). Lähtuvalt sellest, kes ja millistel tingimustel andmetele ligi peab pääsema, tuleb korraldada võtmehaldus, mille jaoks saame anda kaks suuremat stsenaariumikategooriat. Järgnevalt kirjeldame neid lähemalt. Seejärel kirjeldame jaotises 7 arendustegevusi, transpordikrüptograafia riskide vähendamiseks ning säilituskrüptograafia rakendamiseks.

4.1 Ligipääs krüpteerijale endale

Sellesse kategooriasse kuuluvad kõigepealt loomulikult kõik need juhud, kus eraisik säilitab omaenda andmeid isiklikuks tarbeks ning võimalikud andmelekked on pigem juhuslikku laadi (vedelema ununenud irdmeedia, uudishimulik noor sugulane vms). Samuti võib isikupõhisest ligipääsust piisata väiksemate ettevõtete puhul, kus ühe isiku lahkumine tähendaks nagunii ettevõtte tegevuse lõppu.

Enamasti pole sellistel juhtudel vaja keerukaid lahendusi, piisab juba operatsioonisüsteemide poolt pakutavatest vahenditest (nt BitLocker Windowsis, FileVault macOSis, LUKS Linuxis). Samuti on olemas hulk suhteliselt lihtsalt kasutatavaid ketta- või partitsiooni taseme krüptolahendusi (nt VeraCrypt).

Nagu iga krüpteerimismeetodiga, avaldub ka nende lahenduste puhul tõeline keerukus võtmehalduses. Enamasti pakuvad need lahendused paroolipõhist võtmetuletamist. Niisugue lähenemise eelised ja puudused on nagu paroolisüsteemidel ikka – neid on lihtne üles seada, aga korraliku parooli meeldejätmine on keeruline. Siinkohal võib tulu tõusta personaalsetest paroolihalduritest, mis võimaldavad peaparooliga kaitstud paroole hoida näiteks USB-pulgal.

4.2 Ligipääs isikute grupile

Juba veidigi suuremas organisatsioonis tekib olukord, kus organisatsioonilisi rolle võivad täita erinevad inimesed. See tähendab, et ka andmetele ligipääs ei saa enam olla isikupõhine. Samas peavad andmed ikkagi konfidentsiaalsuse tagamiseks olema krüpteeritud mingi võtmega, millele tuleb vajadusel ligipääs tagada. Seega taandub probleem jälle võtmehaldusele.

Vastavalt erinevatele nõuetele ning organisatsiooni võimekusele võivad ka vastavad lahendused erineda.

- Krüptovõti võib olla talletatud riistvaralisele kandjale (USB-pulk, kiipkaart vms), mida antakse käest kätte vastavalt rolli täitmisele.

- Krüptovõtmeid haldab asutusesisene server, võtme kasutamiseks peab rolli täitja ennast autentima ja tema õigusi kontrollitakse pääsuloendi alusel.
- Krüptovõtmed on ühissalastatud, erinevad osakud antakse erinevatele inimestele, võibolla koos riistvaralise kandjaga. Ükski osak eraldi võetuna ei sisalda mingit infot võtme kohta. Ühissalastusskeemi saab ehtiada ka nii, et n osakust on võtme rekonstrueerimiseks vaja ainult osa (nt $m < n$).

Andmete pikaajalise säilitamise juures tuleb kindlasti hinnata võimalikust lekkest tulenevaid riske. Üks aspekt, mille poolest pikaajaline säilitamine tavalisest andmehaldusest erineb, ongi lai ajaaken, mille jooksul ka väikese tõenäosusega riskide esinemise ohtu ei saa enam pikemas perspektiivis kaduvväikeseks pidada.

Andmete endi (kuritahtliku) lekitamise vastu pole võimalik võidelda krüptograafiliste meetoditega. Küll aga on võimalik kavandada taastemeetmeid juhuks, kui on alust kahtlustada krüptovõtmete kompromiteerumist.

Vastavad meetmed erinevad vastavalt sellele, millist võtmehaldusmehhanismi kasutatakse. Kui võti tehakse kasutajale kättesaadavaks näiteks riistvaralisel kandjal, millelt pahatahtlik kasutaja võib võtme endale kopeerida, on ainsaks võimaluseks pärast lekke avastamist kõik andmed uue võtmega krüpteerida.

Kui aga kasutatakse ühissalastatud võtit ja kui mõni osak kompromiteerub (nt töötaja kaotab usalduse või lahkub töölt), saab allesjäänud osakute pealt võtme uuesti n osaks ümber jagada.

Igal juhul tuleb krüpteeritud materjalile ligipääsu meetmed läbi mõtelda juba süsteemi planeerimise faasis, kuna krüptovõtmete pikajaline säilimine ning salajasus on probleemid, mida on raske samaaegselt lahendada (v.t. jaotis 5.2).

5 Võtmehaldus

Krüpteerimine ei lahenda automaatselt andmete konfidentsiaalsuse probleemi, ta kõigest taandab konfidentsiaalsuse saavutamise võtmehaldusele. Teisisõnu, ükskõik kui tugev krüptograafiline salastusalgoritm muutub mõttetuks, kui võtmetega lohakalt ümber käia.

Teisalt on krüptograafilised võtmed piisavalt pikad (tänapäevastes süsteemides vähemalt 128 bitti) ning juhuslikud, et nende päheõppimine või meeldejätmine pole realistlik. Seega on oluline pöörata tähelepanu kasutajatele efektiivsete võtmehaldusvahendite pakkumisele.

5.1 Transpordikrüptograafia võtmete haldus

ID-kaart on mugavalt kättesaadava võtmehoidlana juba pikemalt kasutusel olnud, kuid tuginemine ID-kaardile kui ainsale staatilise asümmeetrilise võtme hoidlale on probleemne (vt jaotis 1). Küll tuleb ID-kaardi kasutamine dekrüpteerimisvõtme hoidlana kõne alla stsenaariumis, kus osa võtit laadidakse nt võtmeedastusserverist (vt jaotis 3.3).

Teine võimalus on ID-kaardi võtmeid üldse mitte kasutada dekrüpteerimiseks, vaid autentimiseks. Üks võimalus on autentimine võtmeedastusserverisse võtmeosaku laadimiseks (vt jaotis 3.3), teine võimalus aga kahesuunalise turvatud kanali loomiseks (vt jaotis 3.4). Paneme tähele, et nende rakenduste jaoks polegi vaja just ID-kaarti, kasutada saab ka teisi eID vahendeid, näiteks mobiili-ID-d ja Smart-ID-d.

Põhimõtteliselt on võimalik võtmeedastusserveri lahenduse juures kasutada ühe osaku dekrüpteerimist ID-kaardiga ning teise laadimist serverist läbi autenditud TLS-kanali, kuid TLS-kanali loomine mõne teise vahendiga tähendaks kasutaja jaoks täiendavat ebamugavust.

Potentsiaalselt täiesti omaette võtmehalduslahendust vajab ühekordsete avalike võtmete süsteem, vt jaotis 3.2. Pärast avalike ja salajaste võtmete paaride loomist ning avalike võtmete publitseerimist tuleb salajasi võtmeid hoida kuni vastavate krüptogrammide saabumise ning dekrüpteerimiseni. Vastavalt edastatava info kriitilisusele tulevad siinkohal kõne alla kas tavaline PC või eraldi riistvara. Vastavalt organisatsiooni vajadusele ja võimekusele saab viimase rolli kaaluda näiteks riistvaralist turvamoodulit (HSMi) või mõnda eriotstarbelist USB-pulka[5].

Eriti kriitilistes rakendustes on võimalik ka salajastele dekrüpteerimisvõtmetele ligipääs hajutada ühissalastuse vahenditega. Seda lahendust saab vajadusel täiendada erinevate lisafunktsioonidega, näiteks mõne osaku tühistamise ning ülejäänud osakute pealt pääsuõigust tagava ühissalastusjaotuse taastamisega.

[5] Vt nt `https://www.crowdsupply.com/f-secure/usb-armory-mk-ii`

5.2 Pikaajalise säilitamise võtmete haldus

Kui transpordikrüptograafia võtmed on uues arhitektuuris olemuslikult lühiajalised ja need võib (ning tegelikult lausa tuleb) pärast dekrüpteerimist kustutada, siis pikaajalise krüpteerimise võtmed peavad olema kättesaadavad kauem (potentsiaalselt aastaid ja aastakümneid).

Samal ajal on selge, et mida pikem on aeg, mille jooksul on vaja andmeid krüpteeritult säilitada, seda suurem on tõenäosus, et

- võtmed võivad avalikuks saada või
- võtmed võivad hävida.

Olukorra teeb raskemaks asjaolu, et võtme konfidentsiaalsust vähegi tugevamal tasemel tagavad vahendid on valdavalt mõne erafirma tooted, mis paratamatult tähendab, et ühel päeval lõppeb nende tehniline tugi[6] või avastatakse neis parandamatuid turvavigu ning sel hetkel peab võtme omanik olema valmis võtmeid migreerima (kui see on üldse võimalik) või krüptogramme rekrüpteerima.

Võimalikud võtmehaldusstrateegiad olenevad kasutaja vajadustest ja võimekusest. Eraisikul on mõistlik kasutada ketta- või failitaseme krüpteerimislahendusi koos võtme/parooli turvalise valiku ja varundamisega füüsiliselt kaitsud meediale (nt vastava otstarbega USB pulk).

Organisatsioonidel on siinkohal aga lisanõuded, kuivõrd ligipääs kaitstud infole pole reeglina mitte isiku-, vaid rollipõhine. Isikule saab anda krüptograafilise pääsutõendi (kiipkaart, USB-pulk), mis sisaldab näiteks privaatvõtit, millega kasutaja saab majasisesest võtmeserverist pärineva krüpteeritud säilitusvõtme oma terminali laadida. Pärast kasutamist tuleks võti terminalist kustutada (mis omakorda eeldab muidugi korrektselt käituvat terminali).

Majasisese võtmeserveri uuendamine peab olema eraldi protseduur, mille käigus näiteks õhkeraldatud keskkonnas säilitatavaid pikaajalise krüpteerimise võtmeid krüpteeritakse uute töötajate avalikele võtmetele.

Ühtlasi pakume siin dokumendis praktilise meetmena välja krüptovõtmete ühissalastuse, mis võimaldab võtme osakute kaitsmiseks mõlema ohu eest kasutada avalikult dokumenteeritud matemaatilisi meetodeid ning üldlevinud IT-turvameetmeid (tavalised kõvakettad mitmes tulekindlas kapis), mitte kellegi konkreetset toodet.

[6] Selles valdkonnas on suur probleem ka plaaniline vananemine (*planned obsolence*).

6 CDOC 2.0 konteineri struktuur

Asünkroonses režiimis toimiva transpordikrüpteerimise (v.t. jaotised 3.2 ja 3.3) jaoks on vaja kasutada mingit konteinerformaati sarnaselt praegu kasutusel oleva CDOCi versiooniga 1.0, mis baseerub *XML Encryption* standardi versioonil 1.1 [9].

Kuna *XML Encryption* ei paku otseselt häid võimalusi ühissalastatud võtmete kirjeldamiseks, tuleb vastavat XML skeemi sobivate elementidega laiendada. Õnneks on sobivad laienduskohad standardskeemis olemas.

6.1 Loogiline andmemudel

Konteineri strukuuri läbitöötamiseks tuleb esmalt moodustada loogiline andmestruktuur, mis võimaldaks lahendada nii tänaseid CDOC 1.0 kasutusjuhte kui CDOC 2.0 ühissalastusega skeeme.

Nii hetkel eksisteerivate kasutusjuhtude kui praeguse dokumendi eelnevate osade (ennekõike jaotised 3.3 ja 5) põhjal saame anda alljärgneva loendi toetamist vajavatest stsenaariumitest. Kõigis neis stsenaariumites kirjeldame *hübriidskeeme*, kus dokument krüpteeritakse (ühekordse) sümmetrilise (näiteks AES-GCM) võtmega ning seda võtit omakorda kaitstakse tesite krüptograafiliste meetmetega (asümmeetriline krüptograafia või ühissalastatud sümmeetriline võti).

- Krüpteerimine otse avaliku RSA võtmega, kasutades vastuvõtja usaldusväärset sertifikaati.
- Krüpteerimine kombineeritud ECDH-ES protokolli abil ECC võtmetega ID-kaartidele vms. vahendile, kasutades vastuvõtja usaldusväärset sertifikaati. V.t. [2].
- Krüpteerimine ühekordsele avalikult võtmele (RSA või ECDH-E), kasutades võtme autentsuse kinnitamiseks võtme genereerija poolt loodud võtme identifikaatorit ning signatuuri.[7]
- Krüpteerimine (mähkimine) sümmeetrilise võtmega, mis on ühissalastatud $m < n$ läviskeemiga.
- Krüpteerimine (mähkimine) sümmeetrilise võtmega, mis on ühissalastatud erinevate kanalite vahel, millest kõigist peab vastuvõtja unikaalse võtmekomponendi kätte saama, et transpordivõti dekrüpteerida. Sisuliselt on tegu ühissalastusega läviskeemi erijuhuga $m = n$.

[7] Puhttehniliselt oleks võimalik luua ajutise võtme autentsuse kinnitamiseks ka sertifikaat, aga kuna lõppkasutaja sertifikaat ei näe sellist kasutust ette, oleks tegu mittestandardse lahendusega.

Nimekiri ei ole lõplik ning konteineri tehniline lahendus peab võimaldama uute skeemide kasutuselevõttu, eriti pidades silmas postkvantturvaliste algoritmide teket ja standardimist.

Joonised 1 ja 2 kirjeldavad loogilisel tasemel erinevaid andmekomplekte, mida on vaja CDOC 2.0 konteineris edastada.

Joonistel 1 ja 2 on esitatud järgmised olemid:

TransportKeyEnc Krüpteeritud ühekordne transpordivõti oma kõigis võimalikes variantides.

IDCard RSA/ECDH-ES ID-kaardi poolt otse toetatud asümmeetrilise krüptoprimitiivi abil krüpteeritud ühekordne transpordivõti.

Onetime RSA/ECDH Ühekordse avaliku võtme abil krüpteeritud ühekordne transpordivõti.

SharedSecret Ühissalastatud võti.

Share Ühissalastatud võtme üks osak.

Plain share Avatekstina edastatud osak.

Encrypted share Krüpteerituna edastatud osak. Siin tekib rekursiivne seos krüpteeritud transpordivõtmega: osakut saab kaitsta täpselt samadel viisidel kui terviklikku võtit.

Keyserver enc share Võtmeserveri avalikule võtmele krüpteeritud osak.

6.2 Konteineri tehnoloogia valiku põhjendused

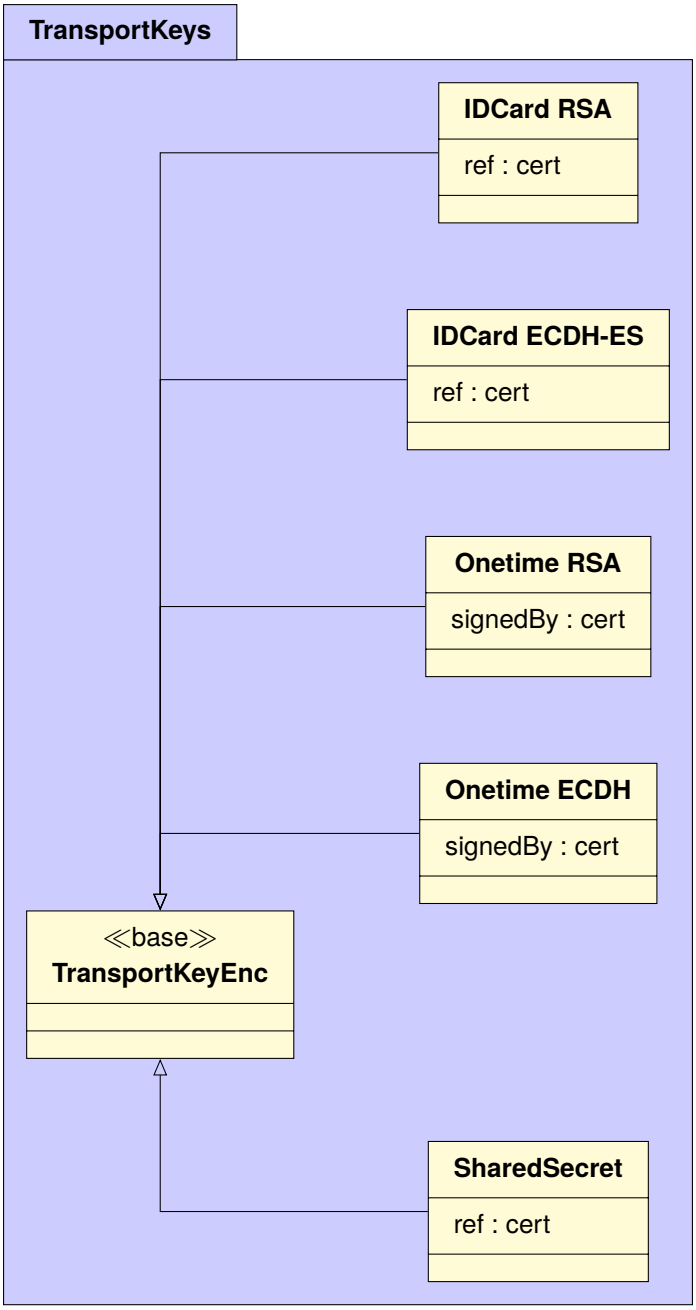
CDOC 2.0 konteiner on kombinatsioon kahest olemasolevast tehnoloogiast:

- *XML Encryption* koos viidetega välistele krüptogrammidele ning
- ASiC-E konteinerformaat *XML Encryption* dokumendi ning krüptogrammide sidumiseks.

Alternatiividena võib veel vaadelda mõningaid levinumaid tehnoloogiaid, kuid neil on kõikil suuremad või väiksemad puudused võrreldes *XML Encryption*'iga.

- **PGP** – PGP (standarditud kui OpenPGP [7]) on paremate valikute puudumisel endiselt suhteliselt populaarne, kuid nagu prominentsed krüptoloogid ja infoturbeekspedid on[8] korduvalt[9] tähelepanu juhtinud, on tema „parim enne" tähtaeg kaugelt möödas. Ennekõik on probleemideks ülearu komplitseeritud ning *ad hoc* meetodil arendatud konteinerformaat ning väga halva kvaliteediga etalonteostus (GnuPG) - need kaks elementi koos tekitavad probleeme nii vormingu käideldavusega kui krüpteeritud dokumentide salajasusega.
- **CMS** – *Cryptographic Message Syntax* [8], ASN.1 ja PKCS#7 põhine formaat, mida kasutakse ka standardsete CAdES signatuuride alusena. Probleemiks on vähene tuntus ning ASN.1 kodeeringu keerukus koos sellest omakorda tulenevate turvaprobleemidega. XML põhine XAdES on täna oluliselt levinum, oluliselt inimsõbralikum tulenevalt oma inimloetavast süntaksist ning seetõttu ka eelistatum. Funktsionaalselt võib XML krüpteeringu ja CMS-i lugeda võrdväärseteks, kuid kohaliku oskusteabe olemasolu annab XML-ile eelise.
- **JSON JWE** – *JSON Web Encryption* [10], JSON-i põhine formaat. Kuigi moodne ja lihtsasti kasutatav, on tema suureks puuduseks (JSON-ist pärinev) skeemikirjeldusvahendite

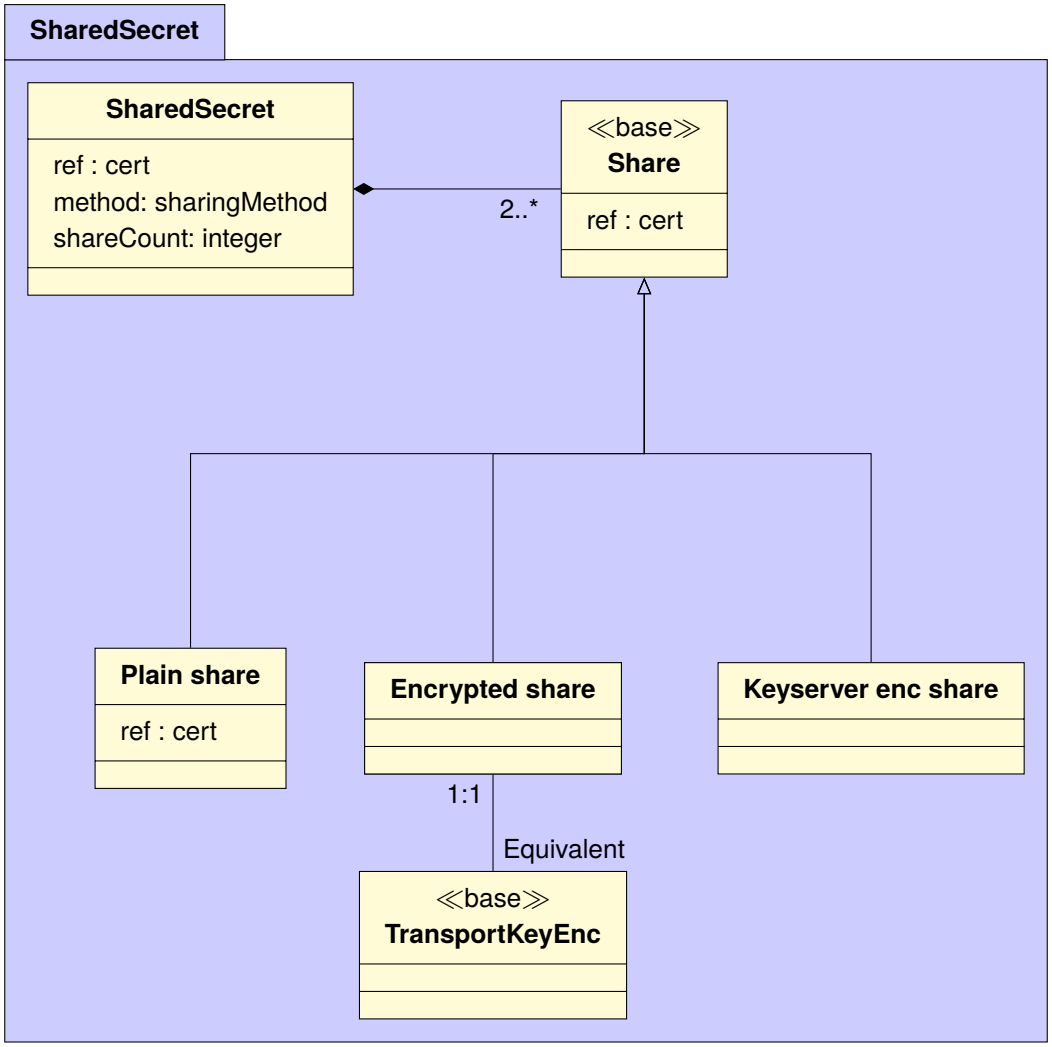
[8] https://blog.cryptographyengineering.com/2014/08/13/whats-matter-with-pgp/
[9] https://latacora.micro.blog/2019/07/16/the-pgp-problem.html



Joonis 1. Transpordivõtme krüpteeringuviiside seosed

puudumine, mis sunnib igal platvormil programmeerijat väga hoolikalt läbi mõtlema, kuidas JWE struktuuri turvaliselt parsida ning töödelda, samuti tekib probleeme ühilduvusega. On teada, et olemasolevad teegid ei taga kõiki vajalikke turvakontrolle. Teiseks puuduseks on JWE aluseks oleva JOSE [4] suletud algoritmide nimekiri, mis ei võimalda JWE-d kasutada standardis määramata algoritmidega.

Ülejäänud alternatiive võib lugeda pigem eksootilisteks, vaid üksikutel platvormidel toetatud katsetusteks.



Joonis 2. Ühissalastuseks vajalik andmestruktuur konteineris

6.3 CDOC 2.0 XML skeem

Dokumendile on lisatud ASiC-E konteineris signatuuri metainfo kirjeldamiseks kasutatava XML skeemi mustand (`cdoc20-schema.xsd`), mis võimaldab kodeerida eelpool toodud loogilisele mudelile vastavaid andmestruktuure.

Enamikku struktuuri variante on võimalik kodeerida standardse *XML Encryption 1.1* skeemi alusel, kuid näiteks ühissalastust see skeem ei toeta, mistõttu on vaja `ds:KeyInfo` elemendile lisada CDOC 2.0 spetsiifiline alamelement. Õnneks jätab standard sobivasse kohta laiendusvõimaluse.

Lisatud näitefail (`cdoc20-secretsharing-sample.xml`) illustreerib ühissalastuse kasutamist.

NB! Nimetatud XML skeem ei ole lõplik ega mõeldud realiseerimiseks! Realiseerimiskõlbuliku skeemi saamiseks on vaja täiendavalt läbi mõtelda skeemis kasutatavad identifikaatorid ja nimeruumid, kuna sellest tekib seotud osapooltele pikaajaline vastutus. V.t. alapeatükk 7.2.

7 Arendustegevuste esialgne plaan

Selles peatükis visandame tegevusplaani, mida saab kasutada järgnevate arendusprojektide alusena.

Tulemusena moodustuvat kõrge taseme arhitektuuri illustreerime punktis 7.5 andmevooskeemide abil (komponentarhitektuuri väljapakkumine oleks praeguses faasis ennatlik).

Ülevaatlikuse huvides on säilitus- ja transpordikrüptograafia tegevused jagatud eri alampeatükkidesse, kuid praktilise arendustegevuse käigus tuleb kaaluda nende tegelikku teostamise järjekorda, sest tehnilised ülekatted on suured.

7.1 Arendustegevuste ülesandepüstitus

Arendatav krüpteerimistarkvara peab lahendama kodukasutajate ning vähemalt osade asutuste probleemid materjalide pikaajalise krüpteeritud säilitamisega. On tõenäoline, et lahendus sobib väiksemate või lihtsamate nõuetega asutuste vajaduste rahuldamiseks, kuid kindlasti on neid, mille puhul tuleb valida mõni turul saada olev sobiv lahendus.

Arendataval tarkvaral peavad olema allpool loetletud omadused.

- Interaktiivne klient levinumatele operatsioonisüsteemidele, tänase DigiDoc kliendi edasiarendus.
- Toetab transpordikrüptograafia konteinerina tänast CDOC-i formaati.
- Toetab nii transpordi- kui säilituskrüptograafia konteinerina käesolevas dokumendis visioneeritud ning edaspidi arendatavat CDOC 2.0 formaati.
- Võimaldab dokumente krüpteerida nii transpordiks (ID-kaardi avalikule võtmele, võtmeserverit kasutades) kui pikajaaliseks säilitamiseks (parooliga, krüptopulga avalikule võtmele).
- Võimaldab dokumente dekrüpteerida, kui on olemas ligipääs vastavale võtmematerjalile.
- Võimaldab dokumente rekrüpteerida ühe võtme alt teise alla (s.h. tähendab see teisendamist transpordikrüptograafia kaitse alt säilituskrüptograafia kaitse alla).
- Võimaldab vähemalt ühel viisil lahendada pikaajalise võtmesäilitamise probleemid, arvestades, et salastatuse ajahorisont on kümnetes aastates.
  - Pikaajalise võtmesäilitamise lahendusena näeme ette ühissalastuse kasutamise. Lisaks tavalisele avaliku võtme krüptograafiale kasutataks paralleelselt ka krüpteerimist ühissalastatud võtmele. Kuna ühe komponendina hoitava salajase võtme üheaegne salajasuse ning tervikluse tagamine on väga keeruline

ülesanne[10], siis on otstarbekas hoida tagavaravõtit ühissalastatuna, mis võimaldab protseduuriliste ja füüsiliste meetmega tagada salajasuse ning seejuures ka mõne osaku hävimisel tagada võtme tervikluse.

- Võimaldab asutustel rakendada keskseid profiile, mille abil dokumentide krüpteerimist juurutada. See on hädavajalik, et üldse oleks võimalik lahendada pikaajalise dekrüpteeritavuse probleemi.
  - Eraldi kaasneva rakendusena tuleb luua vahend profiilide haldamiseks.
- Võimaldab leida saaja avalikku võtit erinevatel viisidel (LDAP-ist, võtmevahetusserveri käest, lokaalsest võtmehoidlast, asutuse profiilist).

7.2 Säilituskrüptograafia arendustegevused

Allpool on loetletud arendused, mis on vajalikud elementaarse säilituskrüptograafia lahenduse pakkumiseks DigiDoc kliendi ning CDOC 2.0 konteinerformaadi põhjal.

1. Peatükis 6 visandatud konteinerstrukuuri lõplik disain ja realiseerimine (protsess nõuab iteratiivset lähenemist koos prototüüpimisega, et mitte langeda „komitees disainitud" konteinerformaadi lõksu).
2. Peatükis 6 visandatud profiilisüsteemi lõplik disain ja realisatsioon. Sisaldab võtmehaldusskeemide esimese komplekti valikut.
3. Dokumendi transpordikrüpteeringu alt muu kaitsemeetme alla teisendamise funktsionaalsus. See peab olema realiseeritud nii, et lõppkasutajal oleks võimalik aru saada, milliste riskidega on seotud dokumentide vaid transpordikrüpteeringuga kaitstuks jätmine, ning nii, et kaitsemeetme vahetamine oleks võimalikult lihtne.
   - Rekrüpteerimine mingi pikaajaliseks säilitamiseks sobiva krüptoskeemiga. Tööriist peab olema kasutatav ka säilituskrüptograafia eri viiside vahel rekrüpteerimiseks.
   - Ülekandmine mingisse välisesse süsteemi, mis juba ise pakub vajalikul tasemel kaitset[11]. Ülekandemehhanism võiks olla laiendatav, sest ei ole mõeldav, et DigiDoc kliendi arenduse eest vastutav asutus kõiki võimalikke integratsioone suudaks hallata.
4. Võimalus valida krüpteerimisvõtit või -skeemi. Täna on sisuliselt ainuke valik kasutada krüpteerimisel saaja avalikku sertifikaati, mis annab saajale võimaluse dekrüpteerida dokumenti oma salajase võtmega. See võimalus tuleb modulariseerida sellisel moel, et oleks võimalik valida tänase variandi, praeguses dokumendis kirjeldatud krüptoskeemide ning ka hüpoteetiliste tulevikus toetatud skeemide vahel.
5. Järgnevad elementaarsed krüpteerimisviisid (korraga võib kasutada mitut, sellisel juhul on täiendavad meetmed kaitseks ühe meetme võtmematerjali riknemise eest).
   - Parooliga kaitsmine (paroolist tuletatakse turvalise võtmepärimisalgoritmiga sümmeetriline krüpteerimisvõti).

[10] V.t. näiteks probleeme krüptoraha „rahakottide" privaatvõtmetega, nii säilivuse kui salajasuse vaatest:
`https://www.secureworks.com/research/cryptocurrency-stealing-malware-landscape`
`https://cointelegraph.com/news/infamous-discarded-hard-drive-holding-7500-bitcoins-would-be-worth-80-million-today`

[11] Kõige lihtsamal juhul on selliseks vahendiks riistvaralise krüpteerimisega kaitstud USB mäluseade, näiteks `https://www.kingston.com/en/usb-flash-drives/datatraveler-2000-encrypted-usb-flash-drive`. Valikud sõltuvad kasutaja vajadustest, tarkvara peaks jätma selleks võimalused.

- Krüptopulgal või muus riistvaralises turvamoodulis oleva pikaajalise asümmeetrilise võtmega kaitsmine (pikaajalise võtmega krüpteeritakse sümmeetriline ühekordne krüpteerimisvõti).
- Krüptopulgal või muus riistvaralises turvamoodulis oleva pikaajalise sümmeetrilise võtmega kaitsmine.

6. Peatükis visandatud ühissalastatud krüpteerimisskeemi lõplik disain ja realisatsioon. Dekrüpteerimiseks on vaja kas kõigi või osade ühissalastatud võtme osakute hoidjate osavõtt ($n-n$ või $n-m$ skeemid). Levinumad ühissalastusskeemid on Shamiri skeem [12] ning aditiivne skeem.
7. Krüpteerimiseks vajalike avalike võtme levitusmehhanismide mitmekesisuse formaliseerimine ning vähemalt ühe täiendava levitusmehhanismi valik ja realiseerimine. Täna on sisuliselt ainsaks formaalseks võtmelevitusmehhanismiks LDAP ning pikas perspektiivis ei saa eeldada, et see on alati kättesaadav või et kõik avalikud võtmed on seal esindatud.

7.3 Transpordikrüptograafia arendustegevused

Kuigi transpordikrüptograafiat on võimalik arendada väga erinevates suundades ja erinevate kasutusjuhtude jaoks, keskendume siinkohale põhiliselt arendustegevustele, mis aitaks vähendada „järgmise ROCA" mõju ning toetada jaotises 7.2 toodud säilituskrüptograafia vahendite arendust ja kasutuselevõttu.

Juhul, kui transpordikrüptograafia vallas mitte midagi muuta, võib juhtuda, et ka kõige hoolikamalt läbi mõeldud säilituskrüptograafia lahendus ei täida oma rolli, sest süsteemi nõrgimaks lüliks on tulevikuturvalisust mittepakkuv CDOC vorming.

Allpool on loetletud arendused, mis on vajalikud säilituskrüptograafia toetamiseks transpordikrüptograafia vaatest.

1. Vähemalt üks CDOC krüpteerimisviis, mis toetab võtmeserveri kasutust.
    - See on vajalik, et elimineerida olukord, kus CDOC konteineri ainuke kaitsemeede on saaja pikaajaline salajane võti.
    - Ühtlasi võimaldab see piirata aega, mille jooksul on CDOC konteinerit võimalik avada, võimaldades luua kasutajakogemuse, mis loomulikul moel sunnib kasutajat dokumente dekrüpteerima ning eraldi hoidma (sõltumata sellest, kas neid on vaja krüpteerida või mitte).
2. DigiDoc tarkvara kasutajakogemuse täiendused, mis suunavad kasutajat vastuvõetud faili või faile säilitama misiganes muul viisil peale transpordiks kasutatud CDOC konteineri. Siia alla ei kuulu ainult liidestus säilituskrüptograafiaga, vaid ka faili salvestamine avatekstina.

7.4 Õiguslike nõuete analüüs

Riigi ja kohaliku omavalitsuse andmekogudes sisalduvate andmekoosseisude töötlemiseks kasutatavate infosüsteemide ning nendega seotud infovarade turvameetmete süsteem on kehtestatud Vabariigi Valitsuse 25.01.2009 a jõustunud määrusega „Infosüsteemide turvameetmete süsteem". Turvameetmete süsteem koosneb turvanõuete spetsifitseerimise korrast ning andmete organisatsiooniliste, füüsiliste ja infotehniliste turvameetmete kirjeldustest ning selle rakendamine seisneb infoturbe eesmärkidele vastavate turvaklasside määramises

ja nendele vastavate turvameetmete valimises vastavalt infosüsteemide kolmeastmelise etalonturbe süsteemi (ISKE) rakendamisjuhendile ja nende rakendamises ning rakendamise auditeerimises. Kehtiv ISKE ei piira kirjeldatud tehnilise lahenduse teostatavust.

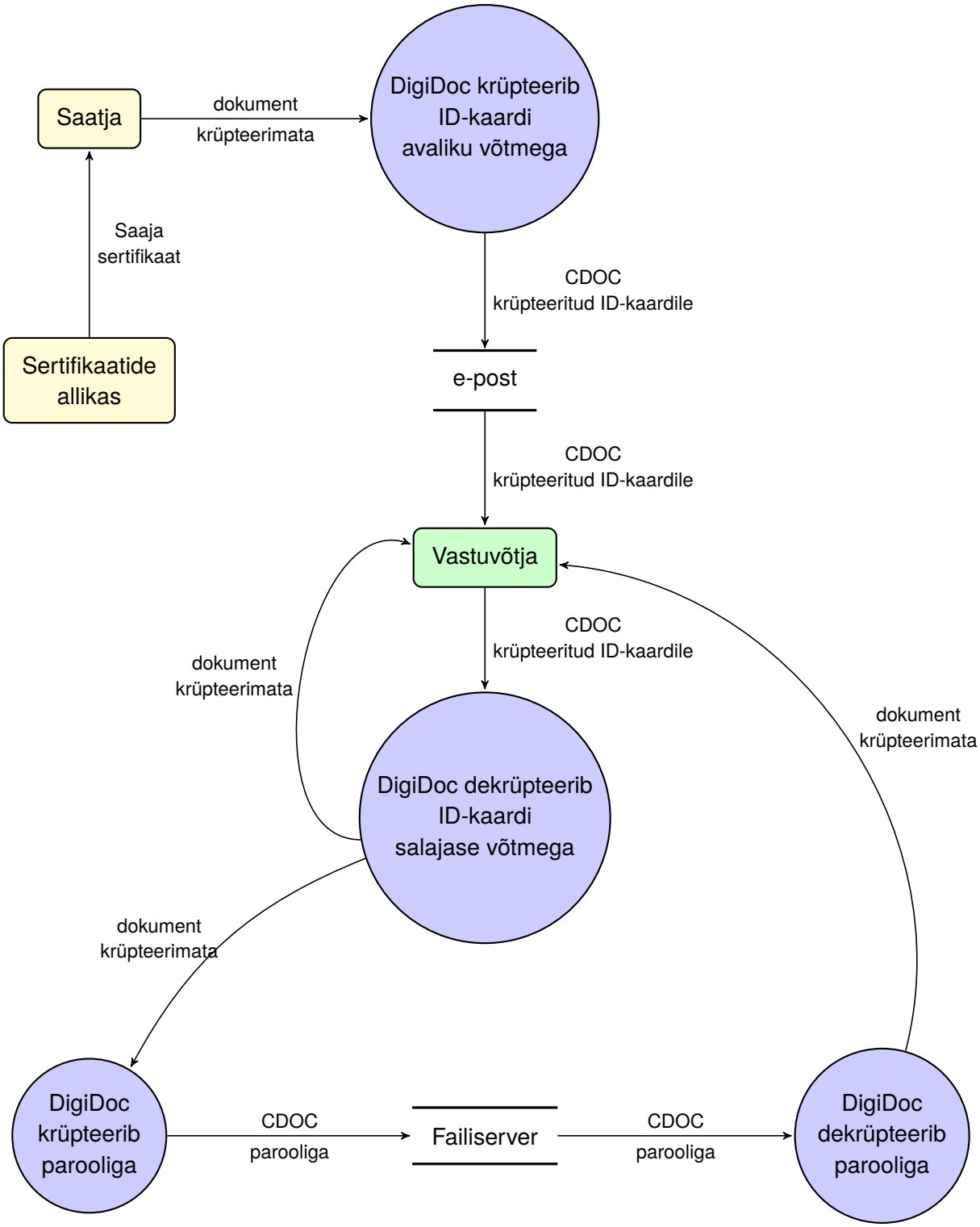
23.05.2018 jõustunud küberturvalisuse seaduse kohaselt peab teenuse osutaja rakendama alaliselt organisatsioonilisi, füüsilisi ja infotehnilisi turvameetmeid küberintsidendi ennetamiseks, küberintsidendi lahendamiseks, küberintsidendi tõttu teenuse toimepidevusele või süsteemi turvalisusele avalduva mõju ennetamiseks ja leevendamiseks või teise sõltuva teenuse toimepidevusele või süsteemi turvalisusele avalduda võiva mõju ennetamiseks ja leevendamiseks (KüTS § 7 lg 1 p 1-3). Konkreetsete organisatsioonide igapäevast majandustegevust ja tegevusega kaasnevaid turvalisuse küsimusi reguleerivad valdkondlikud eriseadused, mis ei sea teadaolevalt konkreetseid kitsendusi tehnilistele lahendustele.

Vastavalt isikuandmete kaitse seadusele, täpsustades ja täiendades sätteid, mis sisalduvad Euroopa Parlamendi ja nõukogu määruses (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus), tuleb isikuandmeid töödelda viisil, mis tagab nende turvalisuse, sealhulgas kaitseb loata või ebaseadusliku töötlemise eest ning juhusliku kadumise, hävimise või kahjustumise eest, rakendades asjakohaseid tehnilisi või korralduslikke meetmeid (IKS §14 p 6), neid meetmeid konkreetselt täpsustamata, jättes turvalisuse (nii konfidentsiaalsuse, autentsuse kui tervikluse) tagamise lahenduse valiku konkreetse organisatsiooni kanda vastavalt selle spetsiifikale. Paratamatult eeldab krüpteeritud dokumentide edastamine konkreetsele isikule selle isiku andmete teadmist ja töötlemist, kuid selline töötlemine tehnilist lahendust kasutades saab toimuda kooskõlas eeltoodud seaduse ja määrusega ning ei eelda õigusliku raamistiku osas muutusi.

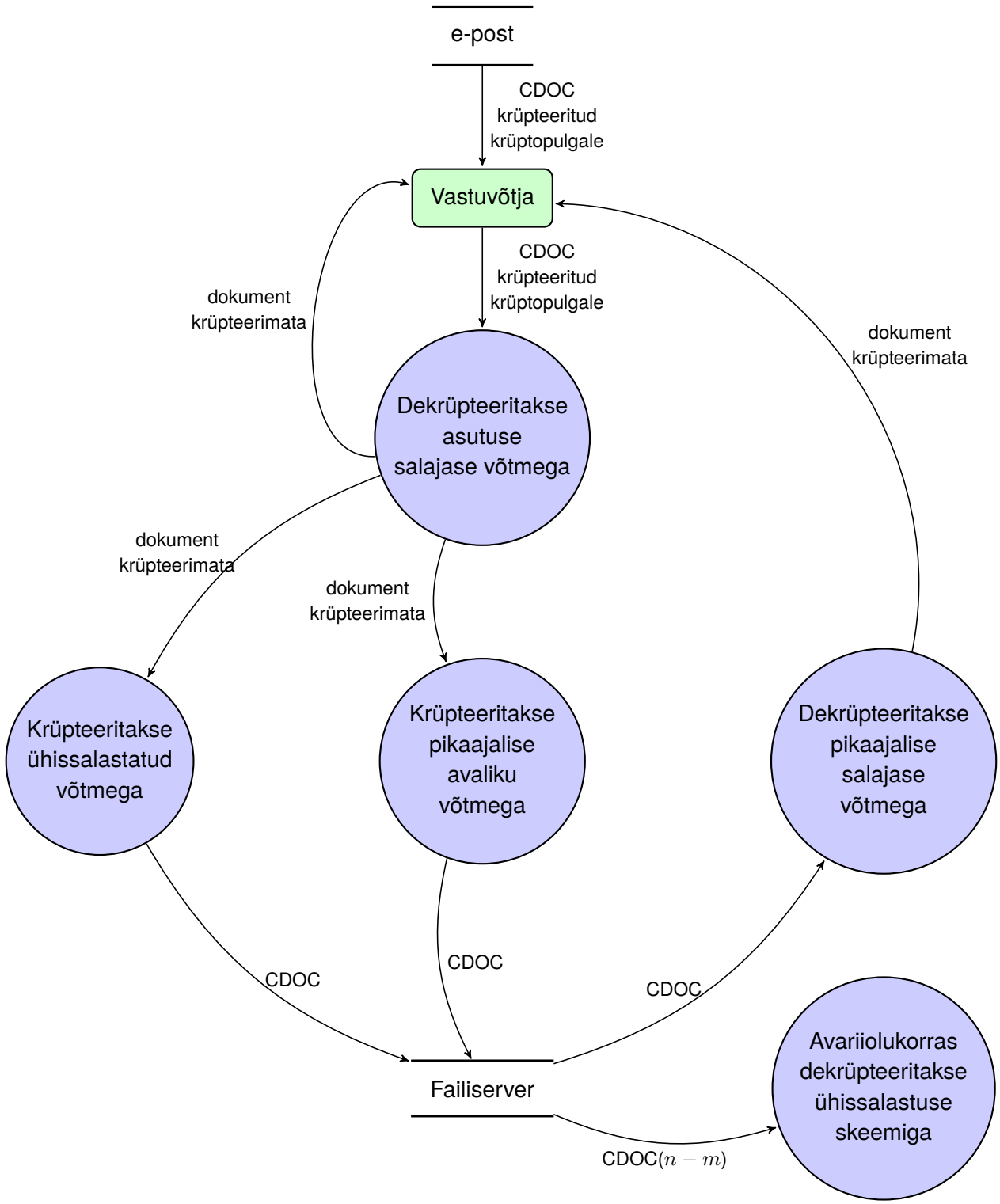
Kokkuvõtvalt, pakutav lahendus on reguleeritav olemasoleva õiguse raames.

7.5 Illustreeritud andmevood

- Joonis 3 illustreerib olukorda, kus saatja saadab dokumendi ID-kaardi avaliku võtme abil krüpteeritult, vastuvõtja rekrüpteerib selle kasutades parooli ning salvestab tulemuse failiserverisse, kust aeg-ajalt dekrüpteerib seda lugemiseks.
- Joonis 4 illustreerib olukorda, kus saatja saadab dokumendi asutuse krüptopulga avaliku võtme abil krüpteerituna (krüpteerimise ahel on sarnane joonisega 3 ning kompaktsuse huvides välja jäetud). Dokument kaitstakse asutuse privaatvõtmega ning samal ajal asutuse ühissalastusskeemiga. Joonis illustreerib ka võimalikku avariiolukorda (s.t. primaarselt dekrüpteerimiseks kasutatav krüptopulk on riknenud), kui on vaja dokumenti ühissalastuse skeemi abil dekrüpteerida.



Joonis 3. Dokumendi liikumine kasutades ID-kaardi krüpteerimist ning parooli



Joonis 4. Dokumendi liikumine asutuses kasutades asutuse võtmeid ning ühissalastust, millega tagatakse ligipääs krüpteeritud materjalile.

A Küsimustik

1. Millised on kirjeldatavas töövoos tüüpilised dokumendid, nende saajad ja saatjad?
2. Millise konfidentsiaalsusvajadusega need dokumendid on?
    - Mis juhtub, kui dokument saab avalikuks kolmandatele osapooltele?
    - Kui pikk on dokumendis kajastatud informatsiooni tüüpiline salastustähtaeg?
3. Kas teie asutuses on olemas vajadus turvalise kiirsuhtlusplatvormi järele?
    - Milliseid kiirsuhtlusplatvorme te hetkel kasutate ja millised on nende poolt pakutavad turvamehhanismid?
    - Milliseid võimalusi oleks nelie lisaks vaja (nt Eesti digitaalse identiteediga autentimine)?
4. Kas te olete oma asutuses teadvustanud vajaduse eraldada (CDOC vormingus) transpordikrüpto pikaajalise säilitamise krüptost?
    - Kas teie asutuses on olemas mingi pikaajalise turvalise säilitamise mehhanism (nt krüpteeritud varukoopiad koos võtmete varundamisega)?
    - Mis juhtub, kui mingil põhjusel (nt ID-kaardi füüsiline hävimine) pole enam vanu CDOC'e võimalik avada?
5. Kas teie rakenduses on oluline tulevikuturvalisus (st et pikaajalise asümmeetrilise võtmepaari kompromiteerumisel ei kompromiteeruks edastatud informatsioon)?
6. Kas teie rakenduses on oluline postkvant-turvalisus?
7. Kas teie asutusele on oluline, et krüpteeritud andmevahetusega tegelev riist- ja/või tarkvara oleks formaalselt sertifitseeritud? Kui jah, siis millise sertifitseerimisskeemi järgi ja millisel tasemel?
8. Kas krüpteeritud sõnumi saaja on ise motiveeritud sõnumi avamise nimel eraldi pingutama? Kas sõnumi saajalt võib eeldada mittetriviaalset ettevalmistust (nt ühekordsete võtmete moodustamist)?
9. Kas sõnumi saatjal peaks olema osaline kontroll sõnumi dekrüpteerimise üle (nt piirates ajaliselt seda perioodi, mil dekrüpteerimine võimalik on)?
10. Kas võib olla vajalik kasutada mingisugust mittesidusat režiimi? S.t. osapooled on kas eri aegadel mingi kesksüsteemiga ühendatud või on mõnel osapoolel vajalik kasutada õhuvahega võrku.
11. Milline on teie asutuse stsenaariumis vajadus CDOCi allika autentimise järele?
    - Kas võib juhtuda, et allikas peakski jääma anonüümseks?
    - Või on mingitel juhtudel allika tugev tuvastamine kindlasti vajalik?

Kirjandus

[1] TR 03125 TR-ESOR: Preservation of Evidence of Cryptographically Signed Document. BSI, fetched 05.03.2020, https://www.bsi.bund.de/EN/Publications/TechnicalGuidelines/TR03125/BSITR03125.html.

[2] Required modifications to CDOC for elliptic curve support, September 2017. Cybernetica AS, Report number A-101-7, https://www.ria.ee/sites/default/files/content-editors/EID/cdoc.pdf.

[3] Arne Ansper, Ahto Buldas, and Jan Willemson. Krüptograafiliste algoritmide elutsükkel. Technical Report A-101-7, Cybernetica, 2017. https://www.ria.ee/sites/default/files/content-editors/publikatsioonid/kruptograafiliste_algoritmide_elutsukli_uuring_2017.pdf.

[4] Richard Barnes. Use Cases and Requirements for JSON Object Signing and Encryption (JOSE). RFC 7165, April 2014.

[5] Katriel Cohn-Gordon, Cas Cremers, Benjamin Dowling, Luke Garratt, and Douglas Stebila. A Formal Security Analysis of the Signal Messaging Protocol, Extended Version. Cryptology ePrint Archive, Report 2016/1013, 2016. https://eprint.iacr.org/2016/1013.

[6] Whitfield Diffie and Martin E. Hellman. New directions in cryptography. *IEEE Trans. Information Theory*, 22(6):644–654, 1976.

[7] Hal Finney, Lutz Donnerhacke, Jon Callas, Rodney L. Thayer, and David Shaw. OpenPGP Message Format. RFC 4880, November 2007.

[8] Russ Housley. Cryptographic Message Syntax (CMS). RFC 5652, September 2009.

[9] Takeshi Imamura, Blair Dillaway, Ed Simon, Kelvin Yiu, and Magnus Nyström. XML Encryption Syntax and Processing Version 1.1, April 2013. https://www.w3.org/TR/2013/REC-xmlenc-core1-20130411/.

[10] Michael Jones and Joe Hildebrand. JSON Web Encryption (JWE). RFC 7516, May 2015.

[11] Matús Nemec, Marek Sýs, Petr Svenda, Dusan Klinec, and Vashek Matyas. The Return of Coppersmith's Attack: Practical Factorization of Widely Used RSA Moduli. In Bhavani M. Thuraisingham, David Evans, Tal Malkin, and Dongyan Xu, editors, *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, CCS 2017, Dallas, TX, USA, October 30 - November 03, 2017*, pages 1631–1648. ACM, 2017.

[12] Adi Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, 1979.