CYBERNETICA

Euroopa Liit
Euroopa
Regionaalarengu Fond

Eesti
tuleviku heaks

SPOF2.1 – autentimisprotokollistikud

Eelanalüüs
Versioon: 1.1
19. juuli 2022. a.
91 lehekülge
Dokumendi nr: D-26-11

Projektijuhid: Tõnis Reimo (Riigi Infosüsteemi Amet)
Kaija Kirch ja Liis Peets (Cybernetica)

Autorid: Aivo Kalu (Cybernetica)
Aleksander Kamenik (Cybernetica)
Triin Siil (Cybernetica)

Riigi Infosüsteemi Amet, Pärnu maantee 139a, 15169 Tallinn, Eesti.
Email: ria@ria.ee, Web: https://www.ria.ee, Telefon: +372 663 0200.

Cybernetica AS, Mäealuse 2/1, 12618 Tallinn, Eesti.
E-mail: info@cyber.ee, Web: https://www.cyber.ee, Telefon: +372 639 7991.

Sisukord

Joonised

Tabelid

1 Sissejuhatus

1.1 Taust

2019-2020 teostatud projekti „eID infrastruktuuri tõrkekindluse analüüs (SPoF analüüs, 1.etapp)“ tulemused [10] tõid välja Eesti eID ökosüsteemis olevad nõrgad lülid, millega seotud probleemid võivad mõjutada väga paljusid kasutajaid. Muude nõrkade lülide seast paistis välja ka see, et Eestis on kasutusel rohkelt erinevaid autentimisvahendeid ning autentimisteenuseid. Nende erinevate tüüpide paljusus võib olla positiivne omadus, näiteks juhul, kui ühes autentimisvahendis või -teenuses tekib käideldavusprobleem või avastatakse turvanõrkus, siis võib loota, et mõnda teist autentimisvahendit saab edukalt edasi kasutada. Samas tähendab vahendite ja eriti teenuste paljusus praeguses olukorras ka seda, et neid kasutavad infosüsteemid peavad kandma mitmekordseid kulusid, et kõiki alternatiivseid vahendeid ja teenuseid kasutada. Seda eelkõige seepärast, et erinevate vahendite liidestus on erinev.

Projekti SPOF2.1 eesmärkideks ongi uurida Eestis kasutusel olevaid autentimisvahendeid ja -teenuseid selle pilguga, kas nende API-t on võimalik ühildada ning kuidas nende juures vältida vahemeheründeid.

1.2 Lühendid

AKIT

Andmekaitse ja infoturbe leksikon (`https://akit.cyber.ee`)

API

Application Programming Interface, rakendusliides. Reeglid ja vahendid tarkvarakomponentide ja -teenuste omavaheliseks suhtluseks ning teenuste ja funktsioonide kutseteks

AvTS

Avaliku teabe seadus [2]

BLE

Bluetooth Low Energy. Bluetooth seadmed, mis kasutavad andmesideks BLE traadita andmesidet

CA

Certificate Authority. PKI süsteemi osapool, mis kinnitab võtmepaari seost kasutaja identiteediga.

CTAP

Client to Authenticator Protocol. Brauseri ning autentimisseadme vaheline sideprotokoll, mis kasutab transpordikihis USB, NFC või Bluetooth ühendusi.

eIDAS

***e**lectronic **ID**entification, **A**uthentication and trust **S**ervices*. E-identimise (sh autentimise) ja usaldusteenuste korraldamise raamistik ja EU regulatsioon [11] (vt ka `https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation`).

eIDAS-1501

„*Komisjoni rakendusmäärus (EL) 2015/1501, 8. september 2015, koostalitlusvõime raamistiku kohta vastavalt Euroopa Parlamendi ja nõukogu määruse (EL) nr 910/2014 (e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul) artikli 12 lõikele 8*“ [17]

eIDAS-1502

„*Komisjoni rakendusmäärus (EL) 2015/1502, 8. september 2015, millega kehtestatakse e-identimise vahendite usaldusväärsuse tasemete minimaalsed tehnilised kirjeldused ja menetlused vastavalt Euroopa Parlamendi ja nõukogu määruse (EL) nr 910/2014 (e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul) artikli 8 lõikele 3*“ [18]

EL

Euroopa Liit

EUTS

E-identimise ja e-tehingute usaldusteenuste seadus [7]

GOVSSO

GOV Single-Sign On. Ühekordse sisselogimisega seotud funktsioonid teenuses TARA. Tehniliselt võib SSO funktsioone pakkuv rakendus paikneda ka teenuse TARA ees.

HoS

Hädaolukorra seadus [15]

ITDS

Isikut tõendavate dokumentide seadus [16]

JSON

JavaScript Object Notation. Andmete vahetamise vorming, defineeritud RFC8259.

JWT

JSON Web Token. JSON-kodeeringut kasutav tõend, millega esitatakse autentimisprotsessi tulemusena selgunud väited kasutaja identiteedi ja isikuandmete kohta. JWT tõend vastab RFC7519 standardile.

KorS

Korrakaitseseadus [19]

KüTS

Küberturvalisuse seadus [20]

NDEF

NFC Data Exchange Format. NFC andmesides kasutatav andmevorming

OIDC

OpenID Connect. OAuth2.0 protokolli peale ehitatud autentimisprotokoll, mis võimaldab RP-l edastada autentimispäringuid ning OP-l tagastada isikuandmete tõendeid. (`https://openid.net/connect/`, [24])

OP

OIDC Provider. Autentimisteenuse pakkuja. Teenusepakkuja, kes käitab autentimisteenust ning pakub RP-dele võimalust tellida kasutaja autentimist või suunata kasutaja brauser OP autentimisportaali või suunata kasutaja OP autentimisrakendusse. Tihti kasutatakse RP ja OP vaheliseks suhtluseks protokolli OIDC. Eestis tegutsevate OP-de näideteks on SK ID Solutions (teenused Mobiil-ID ja Smart-ID), RIA (teenus TARA), või Haridus- ja Teadusministeerium (teenus HarID).

PEM

Privacy-Enhanced Mail format. X.509 sertifikaatide esitamise formaat, mis kasutab Base64 kodeeringut. RFC7468

PKCE

Proof Key for Code Exchange. RFC7636 ja standardi OAuth2.1 mustandis defineeritud pretensioonil ja vastusel põhinev turvamehhanism, millega saab turvata protokolli OAuth2 täitmist teatud rünnete eest.

PKI

Public Key Infrastructure. Avaliku võtme taristu (vt ka `https://akit.cyber.ee/term/609-avaliku-votme-taristu-pki`)

PPA

Politsei- ja Piirivalveamet

QR-kood

QR code. Masinloetav visuaalne maatrikskood, kasutatakse märgistamiseks, identifitseerimiseks ja andmete edastamiseks.

RIA

Riigi Infosüsteemi Amet

RP

Tuginev osapool (*Relying Party*). Autentimisteenust kasutav osapool või autentimisprotokollis osaleja, kes usaldab teenusepakkuja väiteid (AKIT: *sõltlane*).

Füüsiline või juriidiline isik, kes tugineb e-identimisele või usaldusteenusele (eIDAS art 3 p 6, *Relying Party*)

SIOP

Self-Issued OpenID Provider. Protokolli OIDC laiendus, mille kohaselt saab RP tellida autentimist otse (ilma OP osavõtuta) kasutaja valduses olevalt autentimisvahendilt ning autentimisvahend saab väljastada RP-le iseseisvalt (ilma OP osavõtuta) autentimise toimumise kohta tõendeid. Tõenditele saab lisada kolmandate teenusepakkujate poolt väljastatud isikuandmete atribuute (`https://openid.net/specs/openid-connect-core-1_0.html#SelfIssued`, `https://openid.net/specs/openid-connect-self-issued-v2-1_0.html`)

SPA

Single Page Application. Veebirakendus, mille kasutajaliides töötab brauseris kuvatud üheainsa veebilehe dünaamilise ümberkirjutamise abil, samal ajal kui tavapäraste

veebirakenduste puhul toimub kasutaja suunamine järgmistele veebilehtedele. SPA-rakendused töötavad brauseris käivitatava JavaScript tehnoloogia abil ning laadivad serverist vajalikud andmed ja failid käigu pealt.

TLS

Transport Layer Security. Protokollistikus TCP/IP kasutatav transpordikihi turvaprotokoll, mis vastab RFC8446 standardile.

TLS-CCA

Transport Layer Security - Client Certificate Authentication. Protokolli TLS osa, mis võimaldab kliendil ja serveril vastastikku üksteist autentida (AKIT *TLS*, RFC8446 jaotis 4.4.2)

TsÜS

Tsiviilseadustiku üldosa seadus [27]

Web eID

Web eID. Järgmise põlvkonna lahendus, mis võimaldab veebirakendustel kasutada brauserist ID-kaardiga autentimise ja allkirjastamise funktsioone. `https://web-eid.eu`

VVS

Vabariigi Valitsuse seadus [29]

X.509

Tänapäevases digiühiskonnas kasutatavate avaliku võtme sertifikaatide de-facto standard. RFC5280

1.3 Terminid

autentimine

Identiteediväite kontrollimise protsess: kasutaja, süsteem või muu olem kontrollib teise olemi väidetava identiteedi tõesust. Autentimise aluseks on tavaliselt mõni autentimistegur või nende kombinatsioon (AKIT: *authentication*, ITDS: *digitaalne isikutuvastamine*).

Elektrooniline protsess, mis võimaldab füüsilise või juriidilise isiku e-identimist[1] või elektrooniliste andmete päritolu ja tervikluse kinnitamist (eIDAS art 3 p 5).

autentimisandmed

Andmed, mis võimaldavad autentimisprotokolli vahendusel tõendada teisele osapoolele isiku identiteeti. Näiteks parool või salajane võti (AKIT authentication data). ITDS defineerib ka mõiste *digitaalset tuvastamist võimaldavad andmed*. Võrdle ka isikutuvastusandmed, mis võimaldavad ainult identifitseerimist (eristamist) ning mitte autentimist.

autentimismehhanism

eIDAS mõiste, mis tähistab süsteemi või meetodit, kuidas RP (tuginev osapool – *Relying Party*) saab kasutada autentimisvahendit, et läbi viia autentimis-protsessi. Praeguses analüüsis oleme selle mõiste samastanud autentimisprotokolli mõistega. (eIDAS: *authentication mechanism*)

[1] eIDAS originaaltekstis (art 3 p 5) kasutatakse sõna *e-identimine*, mille asemel oleks õigem kasutada Eesti legaalterminit *isikusamasuse kontroll*.

autentimisprotokoll

Infoturbes kasutatav reeglistik (näiteks krüptograafiline protokoll), mis määrab sõnumivahetuse enda identiteeti väitva poole ja seda väidet kontrolliva teise osapoole vahel. Autentimisprotokoll võimaldab läbi viia autentimist ning temalt oodatakse ühtlasi kaitset teatud üldlevinud rünnete eest. (AKIT: *authentication protocol*, eIDAS: *authentication mechanism*)

autentimissignatuur

Autentimisprotsessi käigus autentimisvahendiga loodud krüptograafiline signatuur, mille ülesandeks on kinnitada autentimisvahendi osalust autentimisprotokollis ning kasutaja ainukontrolli.

autentimisteenus

Klient-server mudelis olev teenus, mida teenuse klient (RP) kasutab, et autentida RP teenuskanalis (nt veeb, äpid, arvutirakendused, telefonikõne, vms) RP poole pöörduvat füüsilist isikut. Autentimisteenuste näideteks on Mobiil-ID ja Smart-ID (pakub SK ID Solutions) või TARA (pakub RIA). Autentimisteenus võib füüsilise isiku tuvastamiseks kasutada kas ühte konkreetset autentimisvahendit (näiteks autentimisteenus Mobiil-ID tarvitab kasutajate autentimiseks ainult Mobiil-ID autentimisvahendit) või sõltuvalt isiku eelistustest lubada kasutada erinevaid autentimisvahendeid või -teenuseid (näiteks autentimisteenus TARA võimaldab kasutada autentimisvahendit ID-kaart, autentimisteenuseid Mobiil-ID ja Smart-ID ning läbi eIDAS-sõlmede võrgustiku ka paljusid EU liikmesriikide rahvuslikke autentimisvahendeid ja -teenuseid). Autentimisteenuse kasutamiseks on vajalik RP poolel realiseerida konkreetse liidestusprotokolli tugi.

autentimistegur

Teabekogum (ja/või protsess) olemi autentimiseks selle põhjal, mida olem teab (teadmisel põhinev autentimistegur, näiteks parool), mis olemil on (omandusel põhinev esemeline autentimistegur, näiteks kiipkaart või muu turvatõend), või milline olem on (eristatav püsitunnus, biomeetrik). (AKIT: *authentication factor*)

autentimisvahend

Füüsilisele isikule väljastatud füüsiline või digitaalne vahend, mis sisaldab autentimisandmeid ja võimaldab kasutajal digitaalselt tõendada oma isikusamasust ja/või isikutuvastusandmeid teisele osapoolele (autentimine). Autentimisvahenditeks on näiteks Eesti riigi poolt väljastatav ID-kaart koos isikusertifikaadiga või SK ID Solutions poolt väljastatav Smart-ID autentimisvahend koos isikusertifikaadiga. (NIST SP800-30: *authenticator*)

eIDAS kasutab autentimisvahendi asemel mõistet *e-identimise vahend – electronic identification means* (eIDAS art 3 p 2).

Eesti digiidentiteedi raamistik

Üldnimetus e-identimise, autentimisteenuste, digiallkirjastamise jms süsteemide komplektile ja reeglitele, millega Eestis tervikuna korraldatakse identiteedihaldust, autentimist ja digiallkirjastamist.

eIDAS-sõlm

eIDAS raamistiku kohaselt isikute piiriüleses autentimises osalev ühenduspunkt, mis pakub ühe liikmesriigi riigisisese e-identimise taristule liidest andmevahetuseks teiste liikmesriikide riigisiseste e-identimise taristutega (eIDAS-1501 art 2 p 1))

eIDAS-sõlme operaator

Üksus, kes vastutab selle eest, et eIDAS-sõlm täidab ühenduspunkti funktsioone korrektselt ja usaldusväärselt (eIDAS-1501 art 2 p 2)).

e-identimine

Protsess, mille käigus toimub füüsiliste või juriidiliste isikute elektroonilist tuvastamist võimaldavate andmete kasutamine, mis tähistavad üheselt vastavat isikut. Protsess hõlmab nii isikusamasuse tuvastamist, registreerimist, autentimisvahendi väljastamist, jms. Vt ka autentimine, mis on osa e-identimise protsessist. (eIDAS art 1 p 1: *electronic identification*)

e-identimise süsteem

Süsteem ja protsessid, millega korraldatakse füüsiliste või juriidiliste isikute identiteedihaldust (sealhulgas registreerimist, isikutuvastust ja isikusamasuse kontrolli), autentimiseks kasutatavate autentimisvahendite väljaandmist, autentimismehhanisme ja muude turvanõuete täitmist. E-identimise süsteem on laiem kui autentimisteenus, kuna hõlmab ka identiteedihaldust.

E-identimise süsteeme on palju ning igas riigis võidakse kasutada väga erisuguseid süsteeme. eIDASe määrus reguleerib neid süsteeme, mida liikmesriigid soovivad vastastikku tunnustada (eIDAS art 3 p 4: *electronic identification scheme*).

Vt ka Eesti digiidentiteedi raamistik.

isikuandmete tõend

Autentimisprotsessi tulemusena koostatud väidete komplekt kasutaja identiteedi kohta ja/või kasutaja isikuandmetega. Väidete komplekti saab esitada näiteks JWT andmestruktuurina vastavalt OIDC standardi jaotisele 2 (OIDC, *ID token*) või näiteks X.509 sertifikaadina.

(TARA dokumentatsioonis kasutatakse selle mõiste tähistamiseks terminit „identsustõend“, mille võib segamini ajada pääsmiku või autentimisvahendiga.)

isikusertifikaat

X.509 sertifikaat, mis seob autentimisvahendil oleva autentimiseks mõeldud võtmepaari ja dokumendi omaniku isikuandmed.

isikutuvastusandmed

Andmed, mis identifitseerivad ja eristavad unikaalselt füüsilise või juriidilise isiku. Eestis on sellisteks andmeteks isikukood või registrikood. Võrdle ka autentimisandmetega, mis võimaldavad identiteeti tõendada.

Andmed, mis võimaldavad teha kindlaks[2] füüsilise või juriidilise isiku või juriidilist isikut esindava füüsilise isiku (eIDAS art 3 p 3: *person identification data.*)

last

Krüptograafilistes sõnumites edastavad kasulikud andmed, ilma sõnumipäiste ja muude protokolli-põhiste lisadega. (AKIT: *payload*)

[2]eIDAS originaalteksti eestikeelses tõlkes (art 3 p 3) kasutatakse fraasi *võimaldavad teha kindlaks*, mida tõlgendatakse selles analüüsis ITDS § 15^5 lg 2 tähenduses *isiku tuvastamise* menetlusena ning mitte autentimisena.

liidestusprotokoll

RP teenuskanalis autentimisvahendi või autentimisteenuse kasutamiseks pakutav API, mida RP peab oma infosüsteemis kasutusele võtma. Liidestusprotokollide näideteks on standardis defineeritud OpenID Connect või firmapärased lahendused, näiteks Smart-ID RP-API.

naasmis-URI

URI (tavaliselt veebirakenduse URL), kuhu pöördutakse pärast konkreetse toimingu lõpetamist. Tihti toimub sellele URI-le pöördumine koos kasutaja brauseri ümbersuunamisega. (AKIT: *callback URL*)

pretensioon

Autentimisprotokollides kasutatav küsimussõnum, mis genereeritakse ühe suhtluspoole poolt ning millest teine osapool genereerib krüptograafilise algoritmiga vastuse. (AKIT: challenge, challenge and response)

ründepotentsiaal

Hindamisobjekti ründeks vajaliku pingutuse mõõt, ründaja oskuste, ressursside ja motivatsioonina (AKIT: *attack potential*.)

teenuskanal

E-teenuse osutamiseks ja kasutamiseks vajalik sidekanal. Näiteks võidakse teenust osutada veebibrauseri, mobiilirakenduse või telefonikõne vahendusel. Iga teenuskanal ei võimalda kasutada kõiki autentimisvahendite tüüpe. Teenuskanalis tuleb rünnete takistamiseks rakendada konkreetseid turvameetmeid.

usaldusteenus

Elektrooniline teenus, mida tavaliselt osutatakse tasu eest ning mis võib seisneda e-allkirjade, e-templite või e-ajatemplite jms teenustega seotud sertifikaatide loomises, säilitamises, kontrollimises ja valideerimises. (eIDAS art 3 p 16: *trust service*)

1.4 Viited

[1] *Analysis of planned architectural changes in Open-eID*. RIA, 2020. URL: https://web-eid.github.io/web-eid-cybernetica-analysis/webextensions-main.pdf.

[2] *Avaliku teabe seadus*. RT I, 15.11.2000, 92, 597 . . . RT I, 30.11.2021, 3. 15. november 2000. URL: https://www.riigiteataja.ee/akt/110032022004?leiaKehtiv.

[3] S.M. Bellovin ja M. Merritt. „An attack on the Interlock Protocol when used for authentication“. *IEEE Transactions on Information Theory* 40.1 (1994), lk. 273–275. DOI: 10.1109/18.272497.

[4] Agnès Brelurut, David Gerault ja Pascal Lafourcade. „Survey of Distance Bounding Protocols and Threats“. Teoses: veebruar 2016, lk. 29–49. ISBN: 978-3-319-30302-4. DOI: 10.1007/978-3-319-30303-1_3.

[5] *Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on the interoperability framework pursuant to Article 12(8) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market*. September 2015. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AJOL_2015_235_R_0002.

[6] *Digital Identity Guidelines: Authentication and Lifecycle Management*. NIST, juuni 2017. URL: https://pages.nist.gov/800-63-3/.

[7] *E-identimise ja e-tehingute usaldusteenuste seadus*. RT I, 25.10.2016, 1 ... RT I, 15.10.2021, 1. 12. oktoober 2016. URL: https://www.riigiteataja.ee/akt/EUTS.

[8] *Eesti Vabariigi infosüsteemis autentimislahendustele kehtivad nõuded*. RIA, 2017. URL: https://www.ria.ee/sites/default/files/content-editors/EID/autentimislahendustele-kehtivad-nouded.pdf.

[9] *Eesti Vabariigi infosüsteemis autentimislahendustele kehtivad nõuded (autentimisnormatiiv)*. 2017. URL: https://www.ria.ee/sites/default/files/content-editors/EID/autentimislahendustele-kehtivad-nouded.pdf.

[10] *eID infrastruktuuri tõrkekindluse analüüs: uuringu aruanne*. RIA, 2020.

[11] *Euroopa Parlamendi ja Nõukogu määrus e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul*. EU määrus 910/2014. 28. august 2014. URL: https://eur-lex.europa.eu/eli/reg/2014/910/oj.

[12] *Guidance for the application of levels of assurance which support the eIDAS Regulation*. EU Commission, eIDAS Cooperation Network, veebruar 2017. URL: https://ec.europa.eu/cefdigital/wiki/download/attachments/40044784/Guidance+on+Levels+of+Assurance.docx.

[13] Dick Hardt. *The OAuth 2.0 Authorization Framework*. RFC 6749. Oktoober 2012. DOI: 10.17487/RFC6749. URL: https://www.rfc-editor.org/info/rfc6749.

[14] Dick Hardt. *The OAuth 2.1 Authorization Framework*. Märts 2022. URL: https://datatracker.ietf.org/doc/html/draft-ietf-oauth-v2-1-05.

[15] *Hädaolukorra seadus*. RT I, 03.03.2017, 1 ... RT I, 17.11.2021, 1. 8. veebruar 2017. URL: https://www.riigiteataja.ee/akt/HOS.

[16] *Isikut tõendavate dokumentide seadus*. RT I, 03.03.2017, 1 ... RT I, 15.10.2021, 1. 15. veebruar 1999. URL: https://www.riigiteataja.ee/akt/ITDS.

[17] *Komisjoni rakendusmäärus (EL) 2015/1501, 8. september 2015, koostalitlusvõime raamistiku kohta vastavalt Euroopa Parlamendi ja nõukogu määruse (EL) nr 910/2014 (e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul) artikli 12 lõikele 8*. September 2015. URL: https://eur-lex.europa.eu/eli/reg_impl/2015/1501/oj.

[18] *Komisjoni rakendusmäärus (EL) 2015/1502, 8. september 2015, millega kehtestatakse e-identimise vahendite usaldusväärsuse tasemete minimaalsed tehnilised kirjeldused ja menetlused vastavalt Euroopa Parlamendi ja nõukogu määruse (EL) nr 910/2014 (e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul) artikli 8 lõikele 3*. September 2015. URL: https://eur-lex.europa.eu/eli/reg_impl/2015/1502/oj.

[19] *Korrakaitseseadus*. RT I, 22.03.2011, 4 ... RT I, 03.03.2021, 1. 23. veebruar 2011. URL: https://www.riigiteataja.ee/akt/kors.

[20] *Küberturvalisuse seadus*. RT I, 22.05.2018, 1. 9. mai 2018. URL: https://www.riigiteataja.ee/akt/122052018001.

[21] Kristiina Laanest ja Laura Kask. „ID-kaardi turvarisk, õiguslikud probleemid“ (2017). URL: https://www.ria.ee/sites/default/files/content-editors/publikatsioonid/id-kaardi-turvarisk-oiguslikud-probleemid.pdf.

[22] R. L. Rivest, A. Shamir ja D. A. Wagner. *Time-Lock Puzzles and Timed-Release Crypto*. Tehniline raport. USA, 1996.

[23] Ronald L. Rivest ja Adi Shamir. „How to Expose an Eavesdropper“. *Commun. ACM* 27.4 (aprill 1984), lk. 393–394. ISSN: 0001-0782. DOI: 10.1145/358027.358053. URL: https://doi.org/10.1145/358027.358053.

[24] Nat Sakimura *et al. OpenID Connect*. 2014. URL: https://openid.net/specs/openid-connect-core-1_0.html.

[25] Alan T. Sherman *et al.* „Chaum's protocol for detecting man-in-the-middle: Explanation, demonstration, and timing studies for a text-messaging scenario". *Cryptologia* 41.1 (2017), lk. 29–54. DOI: 10.1080/01611194.2015.1135487. eprint: https://doi.org/10.1080/01611194.2015.1135487. URL: https://doi.org/10.1080/01611194.2015.1135487.

[26] *Technical Guideline TR-03159 Mobile Identities. Part 1: Security Requirements for eIDAS LoA substantial*. BSI, august 2019. URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03159/TR-03159-1.pdf.

[27] *Tsiviilseadustiku üldosa seadus*. RT I 2002, 35, 216 ... RT I, 22.03.2021, 1. 27. märts 2002. URL: https://www.riigiteataja.ee/akt/Ts%C3%BCS.

[28] Enis Ulqinaku, Daniele Lain ja Srdjan Capkun. „2FA-PP: 2nd Factor Phishing Prevention". Teoses: *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*. WiSec '19. Miami, Florida: Association for Computing Machinery, 2019, lk. 60–70. ISBN: 9781450367264. DOI: 10.1145/3317549.3323404. URL: https://doi.org/10.1145/3317549.3323404.

[29] *Vabariigi Valitsuse seadus*. RT I 1995, 94, 1628 ... RT I, 18.06.2021, 1. 13. detsember 1995. URL: https://www.riigiteataja.ee/akt/vvs.

[30] *Web Authentication: An API for accessing Public Key Credentials Level 2*. W3C, 2020. URL: https://www.w3.org/TR/webauthn-2/.

2 Uuringu eesmärgid

Uuringu eesmärgiks on lähemalt vaadelda Eestis kasutusel olevaid autentimisvahendeid ja autentimisteenuseid ning pakkuda välja võimalusi, mis teeksid teenusepakkujatele (RP-d) lihtsamaks nende autentimisvahendite ja -teenustega liidestumise, ühe autentimisteenuse asemel teise kasutusele võtmine ning soodustada uute autentimisvahendite ja -teenuste tekkimist.

Uuringu teine eesmärk on luua Eesti autentimisprotokollistiku kavand, mis võimaldab taaskasutada RP liidestust erinevate autentimisteenuste pakkujate juures. Autentimisprotokollistiku laiendused nagu näiteks kasutajate seansside haldus, SSO teenused, vms ei ole käsitlusalas, kuid samas tuleb kavandi koostamisel arvestada, et selliste laienduste kasutamiseks ei seataks piiranguid. See on esmane kavand, mis on praktikas testimata ning mis kindlasti täieneb ja muutub vastavalt kogukonna tagasisidele, mis on väga oodatud. Tehniline kavandi kirjeldus on peatükis 5.

2.1 Ühilduvus

Eestis kasutusel olevad peamised autentimisvahendid (ID-kaart, Mobiil-ID, Smart-ID) on loodud erinevatel aegadel, põhinevad erisugustel tehnoloogiatel ning pakuvad autentimise läbiviimiseks erisuguseid tehnilisi võimalusi. Ka kasutajate hulgas ei ole need autentimisvahendid võrdselt levinud. See tähendab, et kui teenusepakkuja soovib pakkuda igale kasutajale talle kõige mugavamat ning kättesaadavamat autentimislahendust, siis peaks ta ideaalis liidestuma kõigi autentimisvahendite ning -teenustega. Liidestumist tuleks teha igale autentimisvahendile ja -teenusele sobival moel ning kokkuvõttes kolm korda. See on märkimisväärne kulu.

Veelgi enam - Kui teenusepakkuja soovib ühel hetkel oma senist liidestust muuta ning soovib oma senist autentimisteenuse pakkujat vahetada (näiteks kuna autentimisteenuse pakkuja ei soovi enam senistel ärilistel alustel teenust pakkuda, liidestusprotokollis või autentimisvahendis on avastatud oluline turvanõrkus või mingitel muudel põhjustel), siis peab ta jällegi tegema uue liidestuse arendamiseks täiendavaid kulutusi.

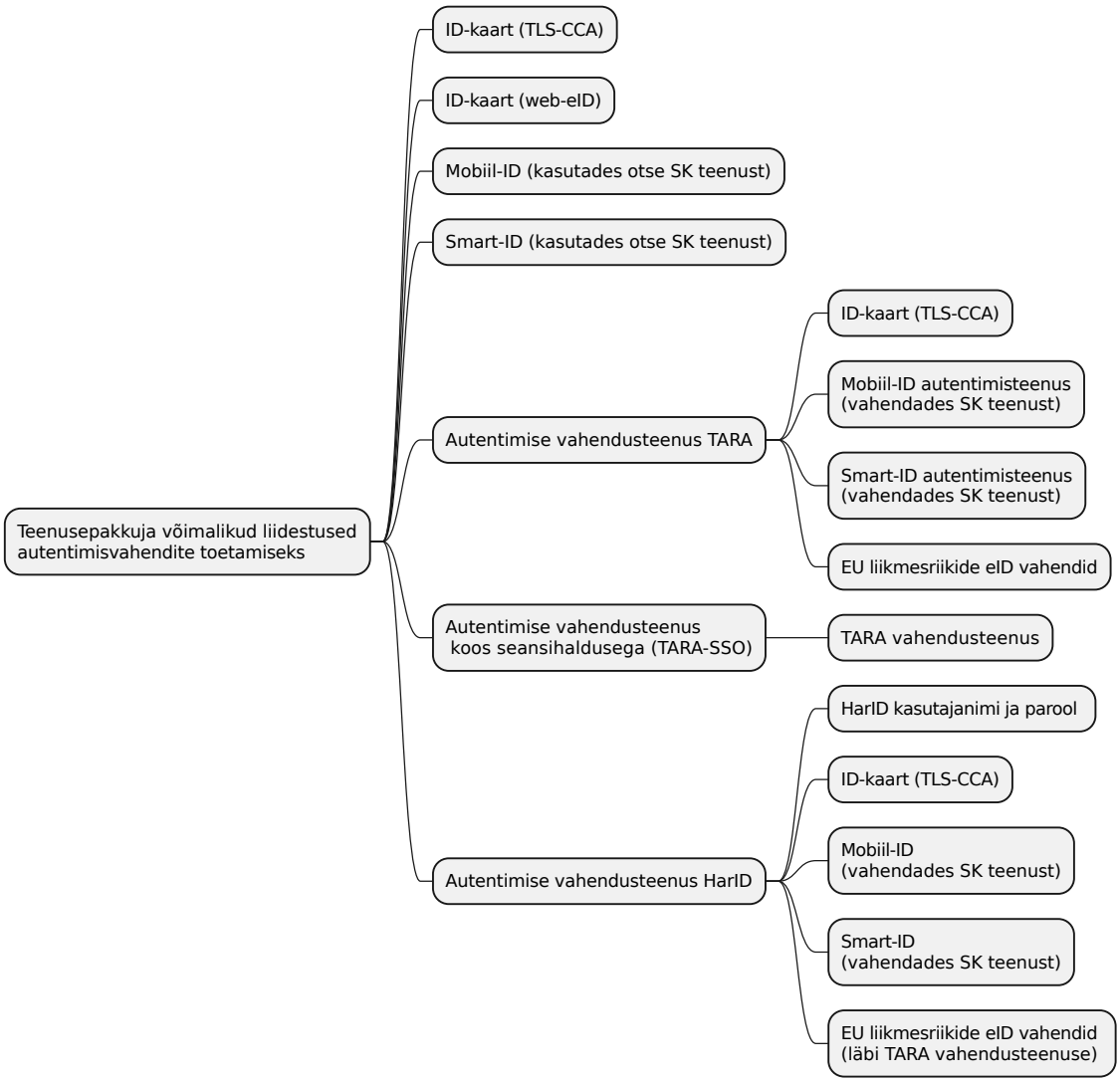
Olukorra illustreerimiseks on praegune olukord kujutatud joonisel 1. Kui teenusepakkujate ning erinevate autentimisvahendite ning vahendusteenuste vahel oleks universaalne ning standardne liidestusprotokoll, siis oleks uute integratsioonide tegemine ning uute teenuste kasutuselevõtmine lihtsam ning odavam. Uuring otsib selliseid võimalusi.

2.2 Piiriülene koosvõime

Uuringus kaardistatakse õiguslikud nõuded, mida tuleks autentimisprotokollistiku puhul täita, et tagada piiriülene koosvõime Eesti poolt teavitatud riikliku e-identimise süsteemi ja teiste Euroopa Liidu liikmesriikide poolt teavitatud riiklike e-identimise süsteemide vahel vastavalt eIDASele.

2.3 Ründekindlus

Lisaks sellele, et liidestusprotokoll võiks olla universaalne, peab liidestusprotokolli järgimine tagama kaitse enamlevinud rünnete eest. Töö käigus uuritakse nõudeid autentimisprotokollidele ning autentimisega seotud ründeid ja riske. Uuritakse milliseid turvameetmeid tuleks rakendada autentimisvahendite juures või liidestusprotokollides, et neid riske vähendada.



Joonis 1: Ristautentimise viisid ja autentimisteenuste pakkujad Eestis

2.4 Õigusliku kehtestamise võimalused

Uuringu üheks osaks on õiguslik analüüs, kus antakse hinnang autentimisprotokollistiku õigusliku reguleerimise võimalustele. Analüüsitakse, kas Riigi Infosüsteemi Ametil (RIA-l) on kehtiva õiguse järgi pädevus kehtestada reegleid autentimisprotokollistiku kohta ning millist õiguslikku tähendust need reeglid kannaksid.

2.5 Käsitlusala

Uuring keskendub riigiasutuste poolt pakutavatele avalikele teenustele ning suurema kasutusega lahendustele. Käsitlusalas on järgmised autentimisprotokollid:

1. ID-kaardi autentimisprotokoll, kasutades lahendust TLS-CCA.
2. ID-kaardi autentimisprotokoll, kasutades lahendust Web eID.

3. Autentimise vahendusteenuse TARA liidestusprotokoll[3] (ühilduvuse tagamiseks ka GOVSSO liidestusprotokolli[4] mõned osad)

4. SK Mobiil-ID ja Smart-ID teenuste liidestusprotokollid.

5. Autentimise vahendusteenuse HarID[5] liidestusprotokoll.

Kuna HarID liidestusprotokoll on väga sarnane TARA liidestusprotokollile, siis on neid edaspidi käsitletud koos ning analüüsis on ainult TARA-ga seotud aspektid.

Käsitlusalas ei ole „pangalingi“ liidestusprotokoll (`https://www.pangaliit.ee/arveldused/pangalingi-spetsifikatsioon`), kuna selle kasutusest on avalik sektor loobumas.

Käsitletud ei ole ka *Open Banking* maksevahendusprotokollid. Need on finantssektori-põhised ning kuigi nende täitmise käigus toimub ka kasutaja autentimine, siis oma olemuselt on need pääsuhaldus- või delegeerimisprotokollid. Sisemiselt võivad maksevahendusprotokollid kasutada siin uuringus käsitletud autentimislahendusi, mistõttu ei ole neid eraldi vajalik vaadelda.

2.6 Teenuskanalid

Praktikas kasutatav liidestusprotokoll ei saa olla universaalne ning peab arvestama konkreetses seansis kasutatavate seadmete ja transpordiprotokollidega. Näiteks lauaarvuti, veebibrauseri ja RP veebisaidi puhul saab ära kasutada TLS-CCA liidestust ning ID-kaarti, aga olukorras, kus kasutaja helistab panga infotelefonile, sama liidestust enam kasutada ei saa. Seetõttu kasutame siin analüüsis edaspidi mõistet teenuskanal, mis tähistab just nimelt kasutaja seadme, teenusepakkuja infosüsteemi ja sidekanali kombinatsiooni. Selle kombinatsiooni poolt pakutavate võimaluste ja nõrkustega peab autentimisteenuse liidestusprotokoll kohanema.

Analüüsis kasutame järgmiseid teenuskanaleid:

1. Veebirakenduse kasutaja autentimine veebibrauseri ja veebiserveri vahelises sidekanalis.

2. Mobiilirakenduse kasutaja autentimine mobiilirakenduse ja teenusepakkuja tagasüsteemi vahelises sidekanalis.

3. Kasutaja autentimine muudes sidekanalites või olukordades, näiteks telefonikõnes või pakiautomaadi kasutajaliideses.

Veebirakenduste puhul eristame veel järgmiseid võimalusi:

1. Traditsioonilised veebirakendused, kus toimub kasutaja brauseri ümbersuunamine autentimisteenusele protokolli HTTP või HTML/Javascript vahenditega, peamiselt HTTP teenuskoodiga 302.

2. SPA-veebirakendused, mis on ehitatud JavaScript tehnoloogial ning kus brauseri suunamist järgmistele lehtedele või teenustele ei toimu.

[3] `https://e-gov.github.io/TARA-Doku/TehnilineKirjeldus`
[4] `https://e-gov.github.io/TARA-Doku/Riigi%20SSO%20tehniline%20analüüs`
[5] `https://harid.ee/et/pages/dev-info`

3 Olemasolevad autentimislahendused

Selles peatükis kirjeldame lühidalt ja ülevaatlikult, millised autentimislahendused on Eestis kasutusel ning kuidas nad tehniliselt töötavad.

3.1 Abstraktne skeem

Uurime esmalt autentimist abstraktsemalt ja vaatame kuidas RP poolt kasutaja autentimine toimub ilma konkreetse autentimisvahendi või konkreetse autentimisteenuse tehnoloogiasse minemata.

Autentimine (isikutuvastus) toimub siis järgmiste osapooltega:

1. Kasutaja – füüsiline isik, kes soovib tõendada oma isikut RP-le, mingisuguses teenuskanalis
2. Teenusepakkuja (RP) infosüsteem – näiteks veebiserver või mobiilirakenduse tagateenus, mis pakub kasutajale isikustatud teenust
3. Autentimise alamsüsteem – RP infosüsteemi alamsüsteem (näiteks TLS-CCA realiseeriv komponent või siis lahenduse Web eID teegid programmeerimiskeelele Java) või väline autentimisteenus (näiteks Smart-ID teenus), mis pakub RP infosüsteemile kasutajate autentimise funktsiooni
4. Autentimisvahend – tehniline seade või vahend, mis võimaldab kasutajalt küsida isiku tuvastamise luba. Tihti on tegemist vahendiga, millel on nii autentimise kui ka signeerimise funktsioon, kusjuures mõlemad on väga sarnased. Autentimisfunktsiooni jaoks on sellisel juhul lihtsalt eraldi võtmepaar, eraldi isikusertifikaat, eraldi PIN-kood ning tehniliselt toimub autentimise kinnitamine selle võtmepaariga unikaalse räsi signeerimise teel.

Osapoolte vaheline suhtlus on kujutatud joonisel 2 oleval järgnevusskeemil.

Väga oluline küsimus on see, kus täpselt asuvad joonisel 2 usalduspiirid ning millistele komponentidele kehtivad konkreetselt millised nõuded. Siin analüüsis püütakse neid küsimusi mitme nurga alt uurida ning vastuseid pakkuda.

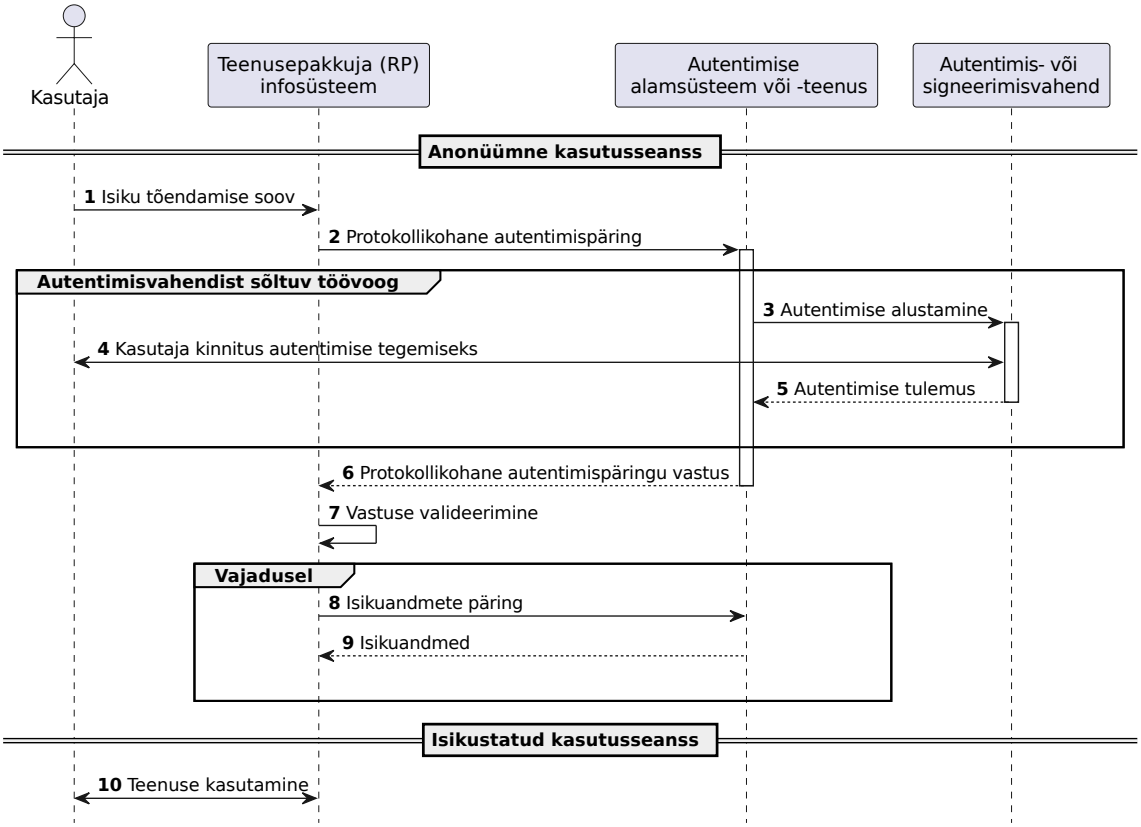
Järgnevalt vaatame konkreetseid Eestis kasutusel olevaid autentimisvahendeid ja autentimisteenuseid ning näitame, kuidas nad sobivad antud üldise mudeliga.

3.2 ID-kaardiga autentimine kasutades protokolli TLS-CCA

Kirjeldame ID-kaardiga autentimise lahenduse, mille puhul kasutatakse ära protokolli TLS (transpordikihi turvaprotokoll – *Transport Layer Security*) ning veebiserverite ja veebibrauserite sisse-ehitatud tuge sellele protokollile.

3.2.1 Komponendid

1. Teenusepakkuja rakendus on veebirakendus, mis kasutab veebiserveri või TLS-kiirendi pakutavat meetodit, et nõuda TLS-protokollis kasutaja brauserilt isikusertifikaadi kasutamist.
2. Autentimise alamsüsteem on TLS-CCA puhul komplekt veebiserveri ja brauseri komponentidest, mis realiseerivad TLS protokolli ning võimaldavad läbi TLS-CCA laienduse kasutada brauseri autentimiseks autentimisvahendil olevat krüptograafilist võtmepaari.
3. Autentimisvahend on komplekt ID-kaardist ja kasutaja arvutisse paigaldatud tarkvara komponentidest (PKCS#11 API, kiipkaardi draiver, jms), mis kuvavad kasutajale PIN1 sisestusakna ning signeerivad edastatud räsi kasutaja autentimisvõtmega.



Joonis 2: Autentimisteenuse kasutamise üldine skeem

3.2.2 Autentimispäring

1. RP veebirakendus alustab autentimist vastavalt veebiserveri konfiguratsioonile. Kasutaja autentimine on nõutud kas siis kogu veebisaidis (kogu veebisaidi URLi `https://www.example.org/*` kataloogide ruumis) või konkreetses alamkataloogis.

2. Autentimispäringuks võib pidada protokolli TLS1.3 sõnumit „Certificate Request“ (RFC8446 jaotis 4.3.2)

3.2.3 Autentimispäringu vastus

1. Autentimise alamsüsteem teeb veebirakenduse eest ära kõik TLS protokolli vajalikud kontrollid ning tavaliselt ei pea ning ei saa RP veebirakendus neid kontrolle ise teha.

2. Autentimispäringu vastusena tagastatakse alamsüsteemist kasutaja isikusertifikaat.

3. Isikusertifikaadi valideerimine tähendab kindlaks tegemist, et sertifikaat on väljastatud usaldusväärse CA poolt ning et sertifikaat ei ole aegunud ega tühistatud. Pikema loetelu tehnilistest kontrollidest leiab näiteks SK ID Solutions poolt välja töötatud autentimise realiseerimise juhendist.[6] Kõik need kontrollid võib veebirakendus delegeerida veebiserverile ning kasutada ainult usaldusväärsest isikusertifikaadist saadud isikuandmete väljasid.

TLS-CCA tüüpi autentimine on enamasti väga turvaline ning kaitseb paljude kalastus- ja MITM-rünnete eest, mida ei saa kahjuks öelda näiteks Mobiil-ID või Smart-ID autentimise

[6] `https://github.com/SK-EID/smart-id-documentation/wiki/Secure-Implementation-Guide#defence-implement-id-card-authentication-securely`

kohta. Samas tuleb tähele panna, et RP rakendusele kättesaadav autentimispäringu vastus ei ole kuidagi seotud RP veebirakenduse olekuga või seansiga. Selle tõttu on võimalik rünne, kus ründaja võtab TLS protokollis loodud sõnumid ja nonsid, transpordib need kasutajani ning meelitab kasutajat neid oma autentimisvahendiga signeerima. Signatuuri transpordib ründaja tagasi RP rakendusele. Juhul kui kasutaja autentimisvahendi isikusertifikaat on sama PKI osa (näiteks osad ID-kaardi ja Mobiil-ID isikusertifikaadid on ajalooliselt väljastatud sama CA poolt) või kui RP ei kontrolli detailselt, milline CA on talle esitatud signatuuriga seotud isikusertifikaadi väljastanud, siis on ka TLS-CCA tüüpi autentimine rünnatav MITM rünnetega. Selle ründe vältimiseks on vajalik hoolikalt järgida sama autentimise realiseerimise juhendit.

3.3 ID-kaardiga autentimine kasutades lahendust Web eID

Web eID (`https://web-eid.eu`) on RIA arendatud järgmise põlvkonna ID-kaardi kasutamise lahendus, mis võimaldab veebirakendustel pöörduda kasutaja arvutis oleva ID-kaardi poole töökindlamalt ja mugavamalt võrreldes senise TLS CCA API-ga.

3.3.1 Komponendid

1. Teenusepakkuja rakendus on veebirakendus, mis on integreeritud lahenduse Web eID teekidega programmeerimiskeeltele Java ning JS.
2. Autentimise alamsüsteemi moodustab lahendus Web eID, mis koosneb serveri-poolsetest teekidest ja komponentidest ning kasutaja brauseris ja kasutaja arvutis olevatest komponentidest. Web eID komponendid teevad kogu ID-kaardiga suhtlemise RP eest ära.
3. Autentimisvahend on komplekt ID-kaardist ja kasutaja arvutisse paigaldatud tarkvara komponentidest (brauseri laiendus, iga operatsioonisüsteemi jaoks loodud Web eID omarakendus ja tootjapõhised kiipkaardi draiverid), mis kuvavad kasutajale PIN1 sisestusakna ning signeerivad kasutaja autentimisvõtmega edastatud räsi.

3.3.2 Autentimispäring

1. RP veebirakendus genereerib nonsi `challengeNonce` ning salvestab selle seansiandmete hoidlasse.
2. RP veebirakendus saadab Web eID komponendile autentimispäringuna JS-funktsiooni `webeid.authenticate(challengeNonce)` kutse.

Detailsem Web eID kasutamise kirjeldus on toodud jaotistes 5.3.3 ja 5.3.4.

3.3.3 Autentimispäringu vastus

Web eID dokumentatsiooni järgi[7] antakse autentimispäringu vastuseks tõend (vaata 3.1), kus väli `signature` on autentimisvahendi poolt loodud signatuur üle andmete `hash(origin)+ hash(challengeNonce)`.

[7] `https://web-eid.github.io/web-eid-system-architecture-doc/web-eid-auth-token-v2-format-spec.pdf`

Näide 3.1: Web eID autentimispäringu tõend.

```
{
    "unverifiedCertificate": "MIIFozCCA4ugAwIBAgIQHFpdK-zCQsFW4...",
    "algorithm": "RS256",
    "signature": "HBjNXIaUskXbfhzYQHvwjKDUWfNu4yxXZha...",
    "format": "web-eid:1.0",
    "appVersion": "https://web-eid.eu/web-eid-app/releases/v2.0.0"
}
```

3.3.4 Vastuse valideerimine

RP peab kontrollima saadud vastuse sisu. Selleks otstarbeks on RIA välja töötatud teegid (näiteks `https://github.com/web-eid/web-eid-authtoken-validation-java`). RP veebiserver peab kasutama kutset 'tokenValidator.validate(authToken, challengeNonce)', mis tagastab RP-le seansi käigus autenditud isiku X.509 autentimissertifikaadi.

3.4 Veebiserveris autentimine teenustega Mobiil-ID või Smart-ID

Selles jaotises käsitleme koos nii Mobiil-ID kui ka Smart-ID teenust, kuna nende kasutamise API on suhteliselt sarnane.

3.4.1 Komponendid

1. Teenusepakkuja rakendus on veebirakendus, mis kasutab Mobiil-ID või Smart-ID teenust
2. Autentimise alamsüsteem on Mobiil-ID või Smart-ID teenusepakkuja, kes pakub võimalust tellida kasutaja autentimist Mobiil-ID või Smart-ID autentimisvahendiga. Veebirakendus ise ei saa otse autentimisvahenditega ühenduda.
3. Autentimisvahend on Mobiil-ID autentimisvahend (kasutaja telefoni SIM-kaardil olev rakendus, millel on kasutaja privaatvõti ning mis kontrollib kasutaja sisestatud PIN-koodi ning loob signatuure) või Smart-ID autentimisvahend (komplekt kasutaja nutiseadmes olevast rakendusest ja võtmematerjalist ning teenusepakkuja serveris olevast rakendusest ja võtmematerjalist, mis kontrollib kasutaja sisestatud PIN-koodi ning loob signatuure).

3.4.2 Autentimispäring

Teenusepakkuja peab genereerima juhusliku signeeritava räsi ning saatma Mobiil-ID või Smart-ID API-le päringu `/authentication(hash, ...)`.

Lisaks peab teenusepakkuja arvutama kontrollkoodi, mida kuvada brauseris kasutajale. Sama kontrollkoodi arvutab ka Mobiil-ID või Smart-ID rakendus, ning kuvab selle telefonis kasutajale.

3.4.3 Autentimispäringu vastus

Mobiil-ID või Smart-ID tagastab peale edukat autentimist vastuse, milles on kasutaja isikusertifikaat ning autentimissignatuur.

3.4.4 Vastuse valideerimine

RP peab kontrollima, et vastuses olev isikusertifikaat on väljastatud usaldusväärse CA poolt, et sertifikaat ei ole aegunud ega tühistatud ning kas vastuses olev autentimissignatuur on moodustatud RP loodud räsile ning sama võtmepaariga, millega on seotud esitatud isikusertifikaat.

3.5 Veebirakenduses autentimine teenusega TARA

3.5.1 Komponendid

1. Teenusepakkuja rakendus on veebirakendus, mis suunab kasutaja brauseri TARA veebisaiti koos autentimispäringuga.
2. Autentimise alamsüsteem on TARA veebisait koos RP-le pakutavate API teenustega. TARA kasutab kasutaja autentimiseks toetatud autentimisvahendeid ja -teenuseid.
3. Autentimisvahenditeks on ID-kaart, või autentimisteenused Mobiil-ID või Smart-ID.
4. Täiendavaks TARA komponendiks on veel eIDAS-sõlm, mille kaudu saab kasutada ka EU liikmesriikide teavitatud e-identimise süsteemides olevaid autentimisvahendeid.

3.5.2 Autentimispäring

Autentimise tellimiseks peab RP koostama TARA dokumentatsiooni jaotises 4.1 kirjeldatud autentimispäringu, ning suunama kasutaja brauseri sellele URL-ile. Koodinäide on kuval 3.2.

Näide 3.2: TARA-le saadetud autentimispäringu näide

```
GET https://tara.ria.ee/oidc/authorize?
    redirect_uri=https%3A%2F%2Feteenindus.asutus.ee%2FCallback&
    scope=openid&
    state=hkMVY7vjuN7xyLl5&
    response_type=code&
    client_id=58e7ba35aab5b4f1671a HTTP/1.1
```

Autentimispäringu unikaalsuse tagamiseks nõuab TARA parameetrit `state` ning kui RP soovib, siis lubab kasutada ka parameetrit `nonce`.

3.5.3 Autentimispäringu vastus

Peale edukat autentimist suunab TARA kasutaja brauseri päringus näidatud RP naasmis-URI-le ning annab kaasa volituskoodi.

3.5.4 Isikuandmete tõendi päring

RP peab volituskoodi kasutades tegema isikuandmete tõendi päringu, vastavalt TARA dokumentatsiooni jaotisele 4.3. Koodinäide on kuval 3.3.

Lisaks toetab TARA ka võimalust, et isikuandmete tõendit päritakse kasutajainfo päringuga, kasutades volituskoodi vastu saadud juurdepääsutalongi (`access_token`), vastavalt TARA dokumentatsiooni jaotisele 4.4.

Näide 3.3: TARA-le saadetud isikuandmete tõendi päringu näide

```
POST /oidc/token HTTP/1.1
Host: tara.ria.ee
Content-Type: application/x-www-form-urlencoded
Authorization: Basic czZCaGRSa3F0MzpnWDFmQmF0M2JW

grant_type=authorization_code&
code=SplxlOBeZQQYbYS6WxSbIA&
redirect_uri=https%3A%2F%2eteenus.asutus.ee%2Ftagasi
```

3.5.5 Isikuandmete tõendi sisu ja valideerimine

TARA väljastab signeeritud isikuandmete tõendi, mille näide on kuval 3.4.

Näide 3.4: TARA poolt signeeritud isikuandmete tõendi näide


```
{
  "jti": "0c597356-3771-4315-a129-c7bc1f02a1b2",
  "iss": "https://tara-test.ria.ee",
  "aud": "TARA-Demo",
  "exp": 1530295852,
  "iat": 1530267052,
  "nbf": 1530266752,
  "sub": "EE60001019906",
  "profile_attributes": {
    "date_of_birth": "2000-01-01",
    "family_name": "O'CONNE-USLIK TESTNUMBER",
    "given_name": "MARY ÄNN"
  },
  "amr": [
    "mID"
  ],
  "state": "1OnH3qwltWy81fKqcmjYTqnco9yVQ2gGZXws/DBLNvQ=",
  "nonce": "",
  "at_hash": "X0MVjwrmMQs/IBzfU2osvw=="
}
```

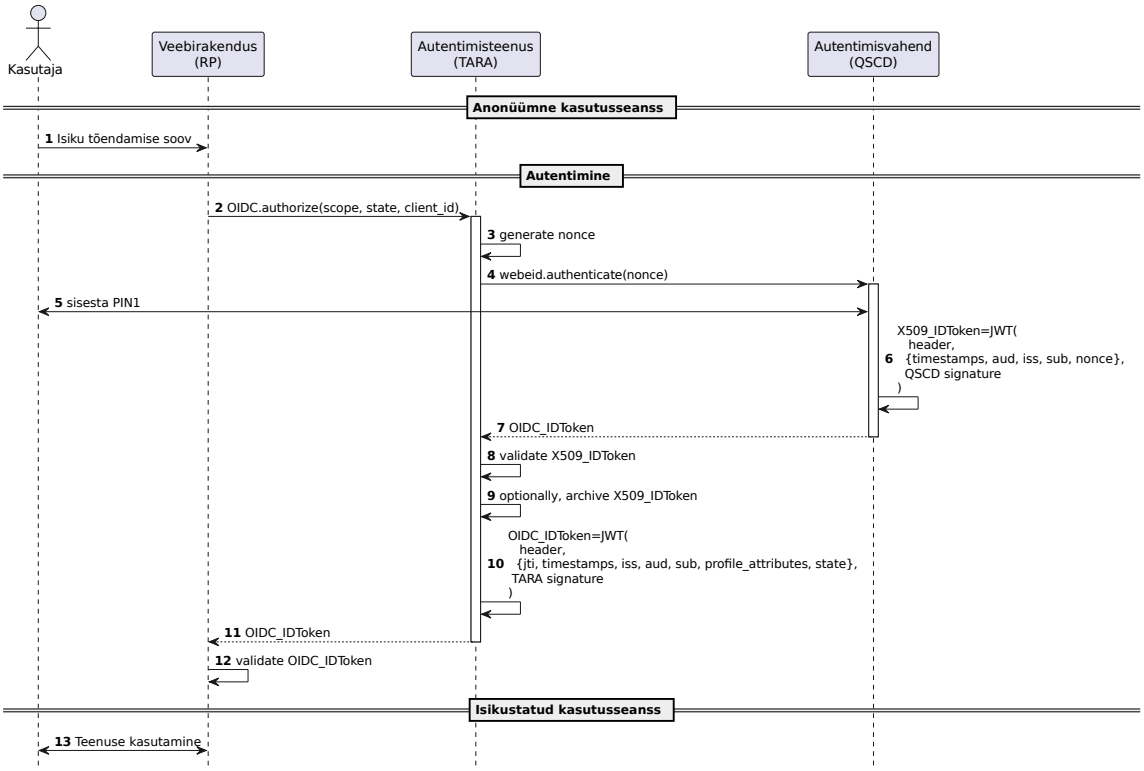

Isikuandmete tõendi valideerimiseks peab RP kontrollima, et tõend on väljastatud TARA poolt, et tõend ei ole aegunud, et tõend on väljastatud õigele RP-le ning et tõend on väljastatud õigele autentimisseansile. Viimase kontrolli jaoks peab RP kasutama parameetrit `state` või lisama autentimispäringule parameetri `nonce`. Täelik loetelu turvakontrollidest on TARA dokumentatsiooni jaotistes 5.1 ja 5.2.

Autenditud isiku identifikaator on tõendi väljas `sub`.

Tuleb tähele panna, et isikuandmete tõendis ei ole autentimissignatuuri ega isikusertifikaati. Ehk siis RP ei saa kontrollida, kas isiku autentimisvahend osales autentimisprotsessis ning kas isikusertifikaat kehtib või on tühistatud. ID-kaardi sertifikaadi kehtivusekontrolli teeb TARA ise (`https://e-gov.github.io/TARA-Doku/Toimivus`).

3.5.6 Läbiva turvalisuse ja usaldusankru küsimus

Juhime lühidalt tähelepanu sellele, et praegu saab RP autentimisteenus TARA poolt autentimisvastuse koos lõppkasutaja identiteediga ning RP ei saa mitte kuidagi kontrollida, kas autentimisprotosessis kasutati lõppkasutaja autentimisvahendit. Põhimõtteliselt on TARA muutunud iseseisvaks autentimisvahendiks. Seda situatsiooni kirjeldab joonis 3. Joonisel kujutatud „autentimisvahend“ võib olla nii isikut tõendav dokument (ID-kaart) kui ka autentimisteenus.



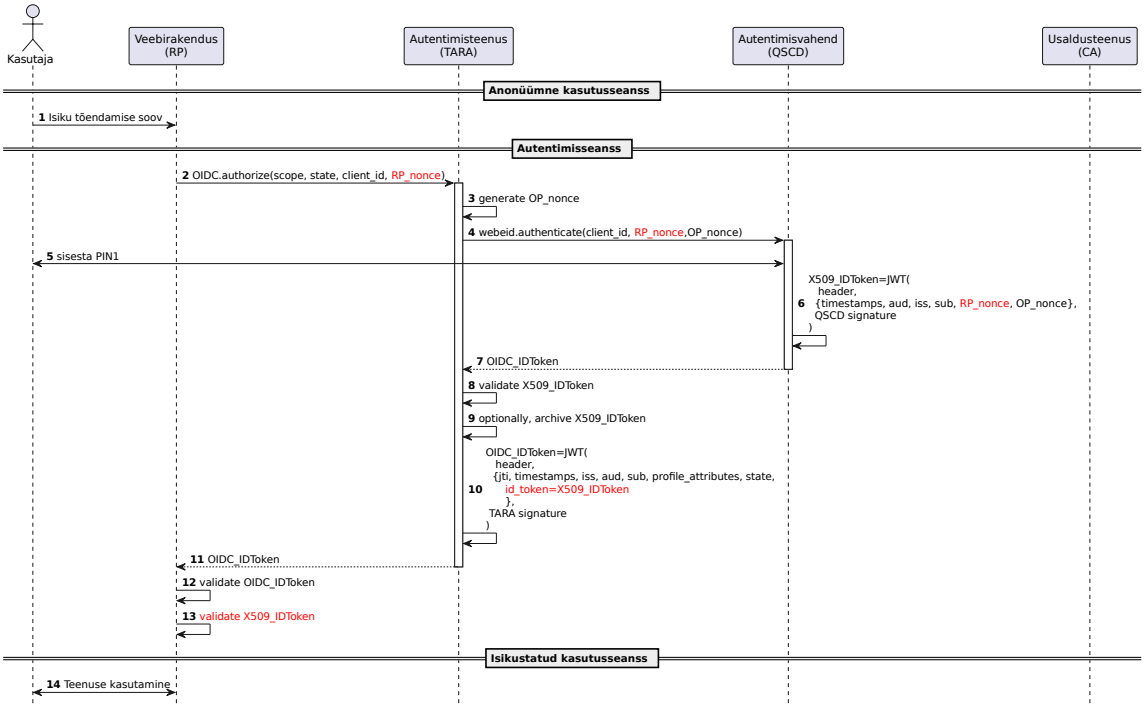
Joonis 3: Autentimine katkestatud usaldusankruga

Olukorda on võimalik parandada, kui koos isikuandmete tõendiga edastada ka kasutaja autentimisvahendi signatuur. Seda situatsiooni kirjeldab joonis 4. Joonisel kujutatud „autentimisvahend“ võib olla nii isikut tõendav dokument (ID-kaart) kui ka autentimisteenus, näiteks Mobiil-ID või Smart-ID, mis on omaette usaldusteenus ning mis väljastab sobivas formaadis autentimissignatuure (vt täpsemat ettepanekut jaotises 5.2.3).

Autentimisvahendi või autentimisteenuse kinnituse RP-le edastamisel on järgmised positiivsed omadused:

1. RP saab algallikast pärit autentimissignatuuri, mis on väljastatud vastavalt juriidiliselt reguleeritud usaldusteenuse reeglitele.

2. Komponentide ja teenuste hulk, mida RP peab usaldama, muutub selgemaks. Kui varasemalt pidi RP usaldama nii autentimisteenuse pakkujat ning kaudselt ka kõiki autentimisvahendite väljastajaid, siis nüüd on võimalik täpsemalt näha, milliseid autentimisvahendeid ning nende väljastajaid peab RP usaldama. Tõsi, otseselt usaldatavate komponentide arv võib isegi kasvada, kuna usaldusseosed on nüüd täpsemini teada. Lisaks muutub autentimise vahendusteenuse ründamine vähem ohtlikumaks.



Joonis 4: Autentimise läbiv turve usaldusankruni

RP ei pea talle edastatud kasutaja signatuuri kasutama, kui ta autentimisteenuse pakkujat täielikult usaldab. Juhul, kui ta otsutab ikkagi talle edastatud signatuuri kasutada, siis tuleb arvestada järgmiste negatiivsete omadustega:

1. RP peab tegema lisatööd vahendusteenusest saadud isikuandmete tõendi valideerimisel, et kontrollida lisaks veel autentimisvahendi moodustatud autentimissignatuure.

2. Autentimise vahendusteenused saavad kasutada ainult PKI-l põhinevaid autentimisvahendeid või krüptograafilisi autentimissignatuure väljastavaid autentimisteenuseid.

3. Uue autentimisvahendi või autentimisteenuse kasutuselevõtmine vahendusteenuse poolt tähendab lisatööd ka RP-le, kes peab hakkama valideerima uue vahendi poolt väljastatud autentimissignatuure. Isegi kui need signatuurid on samas formaadis, näiteks JWT (JSON-kodeeritud isikuandmete tõend – *JSON Web Token*), siis on ikkagi vajalik konfigureerida täiendavad usaldusankrud.

Selle küsimusega tegeleb detailsemalt edasi jaotis 5.2.

4 Turvanõuded autentimisprotokollidele

Aautentimisprotokoll peab olema turvaline, et ta saaks oma eesmärke täita ja arvestama nende teenuskanalitega, kus teda kasutada plaanitakse. Selleks, et hinnata praegu kasutatavate autentimisprotokollide turvalisust ning pakutava ühtse autentimisprotokollistiku turvalisust, peame loetlema konkreetsed ründed, mille vastu me soovime kaitset omada.

Selles analüüsis ei saa me aga anda ammendavat ja täielikku ülevaadet. Täielikuma analüüsi tegemiseks oleks vaja esmalt projekteerida konkreetne autentimisprotokoll ning selle teostus, loetleda kõik süsteemis olevad andmevarad (andmeelemendid) ning seejärel süstemaatiliselt tuletada kõikvõimalikud ohud, kus ründaja loeb, muudab või hävitab mõnda andmevara. Arvestada tuleb konkreetse süsteemi arhitektuuri ning autentimisprotokolli, kuna selliselt tuletatud ohud on lahenduse-spetsiifilised.

See on väga suur töö. Näiteks lahenduse Web eID kohta tehtud turvaanalüüsis [1] uuriti lähemalt kokku 33 ohtu 20 andmevara osas ning 31 ohtu jäeti dokumendist välja. Praeguse töö puhul ei ole selline detailsus võimalik ning analüüs peab olema kõrgemal ning abstraktsemal tasemel.

Seetõttu võtame aluseks kaks juhendmaterjali:

1. eIDAS rakendusmäärus [5] koos lisaga.
2. NIST SP800-63B – *Digital Identity Guidelines: Authentication and Lifecycle Management* [6].

Lisaks on Eestis avaldatud aastal 2017 *Eesti Vabariigi infosüsteemis autentimislahendustele kehtivad nõuded* [8], mis aga kahjuks ei anna konkreetsemaid turva-tehnilisi nõudeid ning piirdub üldisema juhendmaterjaliga. Seetõttu selles analüüsis nimetatud dokumendist juhinduda ei saa.

Tuleb märkida, et kirjanduses esitatavad nõuded autentimisprotokollidele (ning nendega seotud ründed) ei ole kuigi täpselt defineeritud ega sõnastatud. Tihti paistab, et osad nõuded on omavahel kattuvad ning mõne konkreetse ründe kaitseks sobivad mitmed nõuded. Nõuete tõlkimine, interpreteerimine ning omavahel võrdlemine on praeguses analüüsis loominguline ning ei ole täppisteadus. Kindlasti on võimalik pakkuda ka teistsuguseid võrdlusi. Täiendavad analüüsid, mis käsitleksid nõudeid ja ründeid veelgi granulaarsemalt, oleksid tulevikus kindlasti teretulnud. Lisaks tuleb arvestada, et Eestis kasutusel olev tsentraliseeritud digiidentiteedi mudel ning sellega seostatud autentimisvahendid moodustavad maailma mõistes üsna unikaalse komplekti ning ka seetõttu on väliste tingimuste sobitamine Eestis olevate tehniliste lahendustega keerukas.

4.1 eIDAS rakendusmääruse nõuded

eIDAS rakendusmäärus loetleb nõuded e-identimise süsteemidele, kus tuleb arvesse võtta nii kasutajate identiteedihaldusega seotud nõudeid, autentimisvahendite nõudeid kui ka autentimisprotokollide nõudeid. Tabelis 1 on väljavõte nendest nõuetest, mis on praeguse analüüsi jaoks olulised. Tuleb nentida, et [18] algtekstis on need nõuded sõnastatud tihti kohmakalt ning segaselt ja seepärast on siin analüüsis esitatud juba parandatud/tõlgendatud kirjeldus.

Rakendusmäärust täpsustab eIDAS koostöövõrgustiku juhendmaterjal [12] ning Saksa BSI regulatsioon [26].

eIDAS regulatsioonis lisatakse, et autentimisskeemi taseme „kõrge“ korral tuleb eeldada kõrge ründepotentsiaaliga ründajat. See tähendab [26] tõlgenduses CC komponendidele AVA_VAN.5 vastava läbistusründe tegemist, kuid puudub praktika, mida see tähendab autentimisprotokolli

korral, kuna SOG-IS veebisaidil[8] ei ole juhendmaterjali, kuidas tuleks autentimisprotokollide puhul võimalike rünnete ründepotentsiaali arvutada.

Tabel 1: eIDAS rakendusmääruse nõuded „kõrge“ turvatasemega autentimisprotokollidele.

Nõude tähis	Kirjeldus	[18] jaotise viide
EU.2FA	Autentimisprotokoll kasutab vähemalt kaht eri kategooriate autentimistegurit	2.2.1
EU.USER-CONTROL	Ainult autentimisvahendi omanik tohib saada vahendit kasutada ning teiste poolt autentimisvahendi väärkasutamine peab olema tõkestatud	2.2.1
EU.NO-TAMPER	Autentimisvahend peab olema kaitstud kopeerimis- ja manipuleerimisrünnete eest	2.2.1
EU.DYNAMIC	Autentimisprotokolli täitmise käigus loodavad tõendid ja kinnitused peavad olema iga autentimisseansi jaoks unikaalsed. Autentimisprotokolli abil peab saama tõendada, et kasutajal oli autentimise käigus kasutaja võtmepaarile juurdepääs	2.3.1
EU.NO-GUESS	Autentimisprotokolli täitmist ei tohi saada rünnata äraarvamisründega	2.3.1
EU.NO-EAVESDROP	Autentimisprotokolli täitmist ei tohi saada rünnata pealtkuulamisründega	2.3.1
EU.NO-REPLAY	Autentimisprotokolli täitmist ei tohi saada rünnata taasesitusründega	2.3.1
EU.NO-MITM	Autentimisprotokolli täitmist ei tohi saada rünnata vahemeheründe ega andmete manipuleerimisründega	2.3.1

4.2 NIST SP800-63B nõuded

NIST on avaldanud juhendmaterjali, milles esitatakse nõuded autentimisvahenditele ning autentimisprotokollidele. Tabelis 2 on väljavõte nõuetest, mis kehtivad kõige kõrgema turvatasemega autentimisvahenditele. Kuigi USAs kehtestatud nõuded ei ole otseselt Eestile kohustuslikud, siis võrdluseks ning põhjenduseks on siiski neid praegusel juhul hea kasutada. Näeme, et paljud nõuded kattuvad eIDAS nõuetega, mis on ootuspärane tulemus.

[8] https://www.sogis.eu/uk/supporting_doc_en.html

Tabel 2: NIST SP800-63B nõuded AAL3 turvatasemega autentimisprotokollidele.

Nõude tähis	Kirjeldus	[6] viide
NIST.2FA	Autentimisprotokoll peab kasutama kahte autentimistegurit	4.3
NIST.RATE_LIMIT	Autentimisprotokolli täitmist ei tohi saada rünnata äraarvamisründega	5.2.2
NIST.NO_PHISH	Autentimisprotokolli täitmist ei tohi saada rünnata vahemeheründega, näiteks RP võltsimine teenuskanalis	5.2.5
NIST.NO_API_MITM	Autentimisprotokolli täitmist ei tohi saada rünnata vahemeheründega, näiteks autentimisteenuse API võltsimise teel	5.2.6
NIST.NO_SECRETS	Autentimisteenus peab kasutama sobivaid autentimisvahendeid või muid võimalusi, et vähendada saladuste hoidmise vajadusi RP või autentimisteenuse juures	5.2.7
NIST.NO_REPLAY	Autentimisprotokolli täitmist ei tohi saada rünnata taasesitusründega	5.2.8
NIST.USER_INTENT	Autentimisvahendi kasutamise ning autentimisseansi kontekst peab kasutajale olema selgelt arusaadav	5.2.9

4.3 Sünteesitud nõuded Eesti autentimisprotokollidele

Koondame EU ning NIST nõuded ja esitame need tabelis 4. Põhjendamiseks toome ära ka konkreetsed ründed, mille õnnestumise tõenäosuse vähendamiseks iga nõue või turvameede on vajalik.

Nagu tabelist näha, siis nõuete ning rünnete vahel ei ole üks-ühele vastavust. Kõik nõuded vähendavad paljude erinevate rünnete riski ning paljud ründed vajavad riski vähendamiseks mitmete nõuete täitmist.

4.4 Autentimisprotokollide ründed

Tabelis 3 on kokkuvõtlik loetelu rünnetest, mille vastu autentimisvahendid ja autentimisteenused peavad kaitset omama. Loetletud ründed on kirjeldatud viisil, et nad oleksid abstraktsed ning universaalsed ning nendega arvestamine on oluline kõigile autentimisprotokollidele, sõltumata kasutatavast tehnoloogiast.

Tabel 3: Autentimisprotokollide rünnete kokkuvõte.

Lühend	Ründe tüüp	Kirjeldus
R.LOST		Kasutaja kaotab esemepõhise autentimisvahendi (kiipkaart, telefon, vms) või dubleeritud autentimisvahendi (nt pildistatud koodikaardi) ning ründaja kasutab leitud vahendit kasutaja nimel RP teenustesse autentimiseks.

Lühend	Ründe tüüp	Kirjeldus
R.GUESS	äraarvamis-rünne	Ründaja arvab ära kasutaja teadmuspõhise autentimisfaktori (PIN-koodi või parooli) ning kasutab seda kasutaja nimel RP teenustesse autentimiseks.
R.VIEW	pealt-kuulamis-rünne	Ründaja näeb, kuidas kasutaja sisestab teadmuspõhist autentimisfaktorit (PIN-koodi või parooli) ning kasutab seda kasutaja nimel RP teenustesse autentimiseks.
R.PHISH	vahemehe-rünne	Ründaja loob võltsitud RP teenuse ning meelitab kasutaja sinna autentima. Peale autentimist kasutab ründaja võltsitud teenusele edastatud autentimisandmeid (näiteks parooli), et kasutaja nimel õigesse RP teenusesse autentida.
R.MITM-RP	vahemehe-rünne	Ründaja loob võltsitud RP teenuse ning meelitab kasutaja sinna autentima. Peale autentimise algatamist pöördub ründaja kasutaja nimel õige RP teenuse poole ning alustab autentimisprotsessi kasutaja nimel. Kasutaja kinnitab autentimispäringu oma autentimisvahendiga ning RP teenus loob kasutaja nimel isikustatud seansi ründajaga.
R.MITM-API	side manipu-leerimisrünne	Ründaja loob võltsitud autentimisteenuse API ning suunab RP poolt tulevad päringud ümber enda teenusesse. Ründaja alustab kasutaja nimel autentimist RP teenuses ning annab RP-le võltsitud isikuandmete tõendi, mille alusel RP teenus loob kasutaja nimel isikustatud seansi ründajaga.
R.MITM-TSP	vahemehe-rünne	Ründaja kasutab autentimisteenuses olevat turvanõrkust, saavutab autentimisteenuse üle kontrolli ning saab seeläbi luua suvalisi isikuandmete tõendeid. Ründaja alustab kasutaja nimel autentimist RP teenuses ning annab RP-le võltsitud tõendi, mille alusel RP teenus loob kasutaja nimel isikustatud seansi ründajaga.
R.COMM-REPLAY	taasesitus-rünne	Ründaja kuulab pealt autentimisprotokollis kasutaja, RP, autentimisteenuse või autentimisvahendi vahel edastatud andmeid ning taas-esitab need uues autentimisseansis ning üritab RP teenusesse kasutaja nimel autentida.
R.COMM-TAMPER	side manipu-leerimisrünne	Ründaja (kes võib olla RP) meelitab kasutaja oma teenusesse autentima ning modifitseerib autentimisprotokollis edastatud andmeid või kombineerib mitme erineva autentimisseansi andmeid (näiteks autentimissignatuuri) selleks, et mõne muu RP teenusesse kasutaja nimel autentida.
R.QSCD-CLONE	dubleerimis-rünne	Ründaja dubleerib kasutaja autentimisvahendi või leiab kasutaja poolt dubleeritud (nt pildistatud koodikaardi vms) vahendi. Dubleeritud vahendit saab ründaja kasutada RP teenusesse kasutaja nimel autentimiseks.
R.QSCD-TAMPER	manipu-leerimisrünne	Ründaja kasutab autentimisvahendis olevat turvanõrkust ning manipuleerib vahendi turvamehhanismidega, mis võimaldab tal kasutada näiteks leitud autentimisvahendit ilma teadmuspõhise autentimisfaktorita. Manipuleeritud autentimisvahendit saab ründaja kasutada RP teenusesse kasutaja nimel autentimiseks.

Tabel 4: Eesti autentimisprotokollistike nõuded.

Nõude tähis	Kirjeldus	eIDAS nõue	NIST nõue	Ründed
EE.2FA	Autentimisprotokoll peab kasutama vähemalt kaht eri kategooriate autentimistegurit	EU.2FA	NIST.2FA	R.LOST, R.GUESS, R.VIEW, R.PHISH
EE.QSCD	Autentimisvahend peab olema kõrge turvalisusega ning olema kaitstud äraarvamis- ja pealtkuulamisrünnete eest	EU.NO-GUESS, EU.NO-EAVESDROP, EU.NO-TAMPER	NIST.RATE-LIMIT, NIST.NO-SECRETS	R.LOST, R.GUESS, R.VIEW, R.PHISH, R.QSCD-CLONE, R.QSCD-TAMPER
EE.USER-CONTROL	Ainult autentimisvahendi omanikul tohib olla võimalus vahendit kasutada ning teiste poolt autentimisvahendi väärkasutamine peab olema tõkestatud	EU.USER-CONTROL		R.LOST, R.GUESS, R.PHISH, R.MITM-RP
EE.USER-CONTEXT	Autentimisvahendi kasutamine ning autentimisseansi kontekst (kellele kasutaja ennast autendib ja mis teenuskanalis autentimine toimub) peab kasutajale olema selgelt arusaadav		NIST.USER-INTENT	R.MITM-RP, R.MITM-TSP
EE.DYNAMIC	Autentimisprotokolli täitmise käigus loodavad tõendid ja kinnitused peavad olema iga autentimisseansi jaoks unikaalsed. Autentimisprotokolli abil peab saama tõendada, et kasutajal oli autentimise käigus kasutaja võtmepaarile juurdepääs	EU.DYNAMIC		R.COMM-REPLAY, R.COMM-TAMPER
EE.NO-MITM	Autentimisprotokolli täitmist ei tohi saada rünnata vahemeheründega (näiteks RP võltsimine, autentimisteenuse võltsimine, autentimisteenuse API võltsimine, jms)	EU.NO-REPLAY, EU.NO-MITM	NIST.NO-PHISH, NIST.NO-API-MITM, NIST.NO-REPLAY	R.MITM-RP, R.MITM-API, R.MITM-TSP
EE.NO-TAMPER	Autentimisprotokolli täitmist ei tohi saada rünnata andmete manipuleerimisründega (näiteks autentimissignatuuri taasesitamine teises autentimiskontekstis)	EU.NO-REPLAY, EU.NO-MITM	NIST.NO-API-MITM, NIST.NO-REPLAY	R.COMM-REPLAY, R.COMM-TAMPER

5 Eesti autentimisprotokollistiku kavand

Eelmistes jaotistes tehtud analüüsi alusel kirjeldame ühtlustatud autentimisprotokollistiku, mis oleks kasutatav kõigi analüüsi käsitlusalas olevate autentimisteenustega (Mobiil-ID, Smart-ID, TARA, HarID) ning autentimisvahenditega (ID-kaart).

Protokollistik ei ole hetkel mitte ühegi RP (tuginev osapool – *Relying Party*) ega OP (autentimisteenuse pakkuja - *OIDC Provider*) standardtarkvaraga testitud ega praktikas realiseeritud. See on hetkel vaid üldistatud ettepanek, kus on kindlasti mõned puudulikud või lõpuni spetsifitseerimata tehnilised detailid. Protokollistiku edasi arendamiseks on vajalik ettepaneku laiapõhjaline testimine levinud riiulitarkvaraga ning võib-olla ka kompromisside tegemine kui selgub, et mingi konkreetne rakendustarkvara ei toeta ettepanekus tehtud valikuid.

Protokollistik koosneb kolmest osast:

1. Jaotises 5.1 kirjeldame autentimisprotokolli, mis on mõeldud kasutamiseks autentimisteenuste puhul.
2. Jaotises 5.3 kirjeldame autentimisprotokolli, mis on mõeldud kasutamiseks ID-kaardi puhul.
3. Jaotises 5.2 kirjeldame laiendust, mis võimaldab autentimisprotokollidel edastada autentimisvahendi signatuuri ning võimaldab läbivat turvalisust ka olukorras, kus mitmed autentimisteenused on ühendatud järjestikku.

5.1 Liidestusprotokoll autentimisteenuste kasutamiseks

Eesti autentimisteenuste kasutamise liidestusprotokoll põhineb protokollil OIDC (*OpenID Connect*) [24].

Autentimisprotokoll OIDC on tegelikult ehitatud pääsuhaldus- või delegeerimis-protokolli OAuth2 [13] peale. Protokoll OAuth2 on universaalne pääsuhaldusprotokoll, mille abil saab korraldada volitatud juurdepääsu suvalistele andmetele. Juurdepääsu reguleerimist võimaldavat ehituskivi kasutatakse protokollis OIDC selleks, et korraldada RP juurdepääsu OP serverist väljastatavatele kasutaja isikuandmetele. Isikuandmetele juurdepääsu korraldamise protsessi käigus peab OP kuidagimoodi autentimisseansis osaleva kasutaja tuvastama ning kontrollima isikusamasust, aga see on peaaegu nagu kõrvaline efekt. Ehk siis põhimõtteliselt kasutatakse protokolli OAuth2 laias laastus selleks, et RP poolt saata „pääsu reguleerimisserverisse“ (OP server, mis korraldab isikuandmetele juurdepääsu) konkreetsete isikuandmete väljastamise päring (edaspidi nimetame seda autentimispäringuks), hankida kasutaja nõusolek andmete väljastamiseks, tagastada RP-le andmete väljastamiseks vajalik volituskood ning lõpuks vahetada volituskoodi vastu autenditud kasutaja isikuandmed.

Autentimisprotokolli OIDC mudeli kohaselt ei ole isikuandmed isiku enda käes, vaid OP valduses. OP tuvastab autentimisseansis osaleva isiku ning kontrollib isikusamasust ning küsib isikuandmete edastamiseks tema käest luba. Kas OP-l on isikuandmete väljastamiseks enda sisemine andmebaas, kas ta kasutab autentimisvahendilt saadud isikuandmeid (näiteks ID-kaardile väljastatud isikusertifikaat) või saab ta need mingilt kolmandalt teenuselt, see ei ole enam protokolli OIDC skoobis.

Veidi täpsemalt on kirjeldatud sammud tabelis 5. Tabelis loetletud sammude juures on ka seos üldistatud autentimisprotsessi sammudega joonisel 2.

Tabel 5: Kasutaja autentimise sammud autentimisteenuste kasutamisel.

#	Tegija	Samm	Sõnumi nr joonisel 2	Kirjeldav jaotis
1.	RP	Autentimispäringu koostamine	2	5.1.3
2.	RP	Kasutaja suunamine OP teenusportaali koos autentimispäringuga	2	5.1.4
3.	OP	Autentimise läbiviimine	3, 4 ja 5	5.1.5
4.	OP	Autentimispäringu vastuse koostamine ja tagastamine	6	5.1.6
5.	RP	Autentimispäringu vastuse valideerimine	7	5.1.7
6.	RP	Isikuandmete tõendi päringu saatmine	8	5.1.8
7.	RP	Isikuandmete tõendi ja autentimissignatuuri valideerimine	9	5.1.9

5.1.1 RP registreerimine

Enne OP autentimisteenuse kasutamise alustamist peab RP ennast OP juures registreerima. Registreerimise käigus annab OP teenuse kasutamiseks RP-le loa. Lisaks kogub OP järgmise vajaliku info teenuse turvaliseks osutamiseks ning kasutaja autentimise turvaliseks läbiviimiseks.

Tabel 6: RP registreerimisel vajalikud andmed.

Andmeelement	Väärtuse näide	Selgitus
RP identifikaator	Näiteks RFC4122 UUIDv4 formaadis, `B776F8A2-3BC1-42AD-8D35-A755212E743A`	Identifikaator võimaldab eristada sama autentimisteenust kasutavaid RP-sid üksteisest. Identifikaatori formaat on teenusepakkuja valida.
RP autentimiseks jagatud saladus	Juhuslikult genereeritud parool, `hHU7Uv8nwNx9jB5m`	Kasutatakse RP-de poolt saadetud päringute autentimiseks. Vt. jaotist 5.1.2.1.
RP autentimise võtmepaar	RSA või EC privaatvõti, mis jääb RP valdusse ning sellele vastav avalik võti, mis esitatakse registreerimisel.	Kasutatakse RP-de poolt saadetud päringute autentimiseks kuid ka krüpteerimiseks. Vt. jaotist 5.1.2.2.

Naasmis-URIde loetelu	Massiiv
	`[`
	`https://example-rp.com/return`,
	`https://www.example-rp.com/cb`
	`]`
		Kasutatakse kontrollimiseks, kas autentimispäringus tellitud naasmis-URI on selle RP lubatud väärtuste seas. Kui RP-l on mitu veebisaiti, siis ta võib registreerida siin kõik kasutatavad naasmis-URI-d või siis registreerida iga veebisaidi jaoks erineva RP.

Vajadusel võib autentimisteenus registreerimisel koguda veel täiendavaid andmeid, näiteks autentimismeetodite loetelu, mida RP saab OP autentimisteenuses kasutaja autentimiseks kasutada, või soovitud teenustase, vms.

5.1.2 RP päringute autentimine

Tuleb tähele panna, et kõigi tabelis 5 loetletud päringute puhul peab toimuma päringusaatja autentimine OP poolt ja/või päringute sisu autentsuse ja tervikluse tagamine.

Päringusaatja (RP) identifitseerimine ja autentimine on vajalik järgmistel põhjustel:

1. OP poolt arveldusinfo või statistika kogumiseks. Autentimisteenus võib olla avatud ainult registreeritud klientidele ning võib-olla peab OP koguma infot, kuipalju iga RP on OP teenust kasutanud ning esitama RP-dele vastavalt kasutusele arveid. Arveldusinfo kasutatavuse tagamiseks on vajalik, et iga autentimispäringu saatja oleks autenditud ning ründaja ei saaks lihtsasti saata võltsitud päringuid, mis rikuks arveldusinfo usaldusväärsuse.

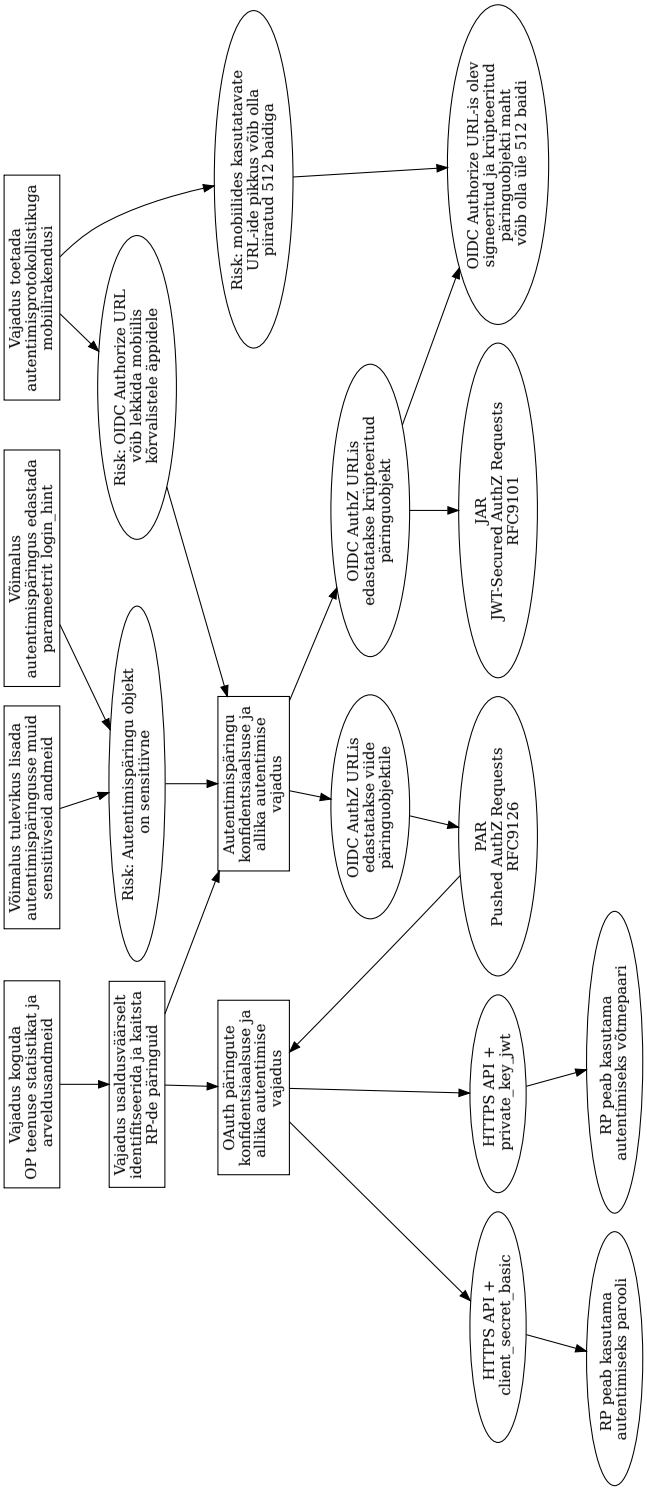
2. Protokolli OIDC sammudes, kus toimub pääsukoodi ja/või isikuandmete tõendi saamiseks volituskoodi esitamine, peab OP kontrollima, kas andmeid väljastatakse õigele soovijale. Kuigi ka volituskood peaks olema RP-ni liikunud üle usaldusväärse kanali, siis näeb protokoll OAuth2 ette täiendava turvameetmena päringu saatja autentimise juhuks, kui volituskood ise peaks siiski olema lekkinud. Sellisel juhul ei saaks ründaja lekkinud volituskoodi RP nimel kasutada, kui tal ei ole RP autentimisandmeid.

3. Autentimispäringus edastab RP ka naasmis-URI. OP peab kontrollima, kas see naasmis-URI väärtus on RP poolt registreeritud URI-de nimekirjas. Kontrolli tegemiseks peab autentimispäringu saatja olema identifitseeritud. Õnneks on protokoll OIDC projekteeritud sedaviisi, et isegi kui ründaja püüaks esineda mõne teise RP nimel ning meelitada kasutajat sedaviisi autentimist läbi viima, siis ta peaks kasutama selle konkreetse RP naasmis-URI ning kasutaja suunataks lõpuks tagasi RP õigesse veebisaiti. Täiendava turvameetmena on siiski ka päringu saatja autentimine kasulik, sest sellisel juhul ei saaks ründaja kasutaja autentimist isegi mitte alustada ning ta ei saaks kasutajat teise RP nimel autentimisteenusesse suunata. Segadusse ajavate võimaluste vähendamine aitab kaasa nõude `EE.USER_CONTEXT` täitmisele.

Näide 5.1: Parooli edastamise näide protokolli OAuth2 päringustes HTTP päiseväljas

```
POST /token HTTP/1.1
Host: server.example.com
Content-Type: application/x-www-form-urlencoded
Authorization: Basic
  Qjc3NkY4QTItM0JDMS00MkFELThEMzUtQTc1NTIxMkU3NDNBOnBhc3N3b3JkCg==

grant_type=authorization_code&
code=fsdfdsfsd&
redirect_uri=https://www.example-rp.com/cb
```



Joonis 5: OAuth2 ja OIDC päringute autentimise nõuete ja lahenduste sõltuvused

Näide 5.2: RP autentimiseks kasutatava JWT-tõendi näide

```
{
    "typ":  "JWT",
    "alg":  "RS256" | "ES256",
}
.
{
    "iss":  "B776F8A2-3BC1-42AD-8D35-A755212E743A",
    "sub":  "B776F8A2-3BC1-42AD-8D35-A755212E743A",
    "aud":  "https://example-op.com/auth-api-endpoint",
    "jti":  "QU6VF3MMKvgn2ZZK",
    "nbf":  "1642507495",
    "exp":  "1642507654"
}
.
"krüptograafiline signatuur"
```

Näide 5.3: JWT-tõendi edastamise näide protokolli OAuth2 päringutes, kasutades HTTP päisevälja

```
POST /token HTTP/1.1
Host: server.example.com
Content-Type: application/x-www-form-urlencoded
Authorization: Bearer eyJhbGciOiJIUzI1NiIXVCJ9TJV[...]r7E20RMHrHD

grant_type=authorization_code&
code=fsdfdsfsd&
redirect_uri=https://www.example-rp.com/cb
```

Protokolli OIDC juures on kasutusel olemuslikult kahte tüüpi päringuid:

1. OIDC-päringud – nendega edastab RP näiteks autentimissoovi, kuid see ei jõua OP-ni otse, vaid läbi kasutaja brauseri või läbi kasutaja mobiiltelefoni operatsioonisüsteemi. Seega ei saa nende päringute juures kasutada samu autentimisvahendeid nagu tavapäraste OAuth2 päringute juures. Nende päringute turvalisuse tagamisega tegeleb jaotis 5.1.4.
2. OAuth2-päringud – nendega edastab RP volituskoodi ning saab vastuseks isikuandmete tõendi. Need päringud saadetakse otse OP API otspunktidesse ning nende päringute juures saab kasutada tavapäraseid vahendeid, näiteks TLS-ühendusi ning HTTP *Basic* autentimist. Lisaks autentimisele soovitatakse nendes päringutes kasutada ka protokolli OAuth2 spetsiifilist turvameedet PKCE (*Proof Key for Code Exchange*).

Kõigi nenede tingimuste ja vajaduste arvessevõtmine on kokkuvõttes üsna keerukas. Joonisel 5 on näidatud nõuete ja lahenduste omavahelised sõltuvused. Õnneks selgub, et on olemas ka sellised tehnilised lahendused, mis võimaldavad kõiki vajadusi rahuldada ning RP-d saavad kasutada näiteks jagatud saladuse põhist autentimist, või võtmepaari-põhist autentimist.

5.1.2.1 Jagatud saladusega autentimine

Kasutada saab näiteks tavapärast HTTP *Basic* autentimist, kus RP lisab talle väljastatud parooli HTTP päisevälja `Authorization`. Näide on kuval 5.1.

5.1.2.2 Võtmepaariga autentimine

Kasutada saab standardi OIDC jaotises 9 ja standardites RFC7521 ning RFC7523 kirjeldatud spetsiaalseid JWT-tõendeid, mis kinnitavad privaatvõtmete teadmist, kuid ei edasta saladust ennast.

RFC7521 ja RFC7523 kohaselt peab RP koostama kuval 5.2 JWT-tõendi, koos päise, lasti ning JWT autentsust kinnitava signatuuriga. Vastavuses kasutatava võtmepaari krüptoalgoritmile, tuleb JWT päises kasutada kas väärtust „`RS256`“ või „`ES256`“.

Tuleb tähele panna, et kui need JWT-tõendid satuvad ründaja kätte, siis ta saab neid salvestada ning taasesitada. Seetõttu on oluline, et tõendite kehtivusaeg oleks lühike (näiteks 1 minut, arvestades serveri kellade võimalikku erisust), ning OP kontrolliks JWT-tõendite identifikaatoreid ning ignoreeriks korduvalt esitatud tõendeid. Tõendite esitamine peab seega toimuma endiselt üle HTTPS kanali. Nendest puudustest hoolimata saavutame me JWT-tõenditega, et pika-ajaliste saladuste (parool või privaatvõti) lekkimise oht väheneb.

Volituskoodi esitamise päringus toimub JWT-tõendi esitamine HTTP päiseväljas `Authorization` vastavalt RFC6750 reeglitele. Näide on kuval 5.3.

5.1.2.3 Turvamehhanismi PKCE kasutamine

RFC7636 ning standardi OAuth2.1 mustand [14] soovitavad tungivalt kasutada OAuth2 voogudes pretensioon-vastus-protokollil põhinevat turvameedet PKCE. Lühidalt tähendab PKCE kasutamine järgmiseid samme:

1. Enne OAuth2 päringu saatmist peab RP genereerima selle kasutusseansipõhise juhuarvu (parameeter `code_verifier`) ning salvestama selle seansiandmete juurde.
2. RP teisendab juhuarvu krüptograafilise funktsiooniga (näiteks räsifunktsiooniga SHA256) pretensiooniks, mille RP saadab OP serverile autentimispäringu kooseisus parameetris `code_challenge`.
3. Teatud tingimustel võib juhtuda, et autentimispäring koos parameetriga `code_challenge` ning autentimispäringu vastus koos volituskoodiga (parameeter `code`) lekib ründajale. Kui ründaja saaks seejärel teha RP nimel volituskoodiga päringu, siis saaks ta ise juurdepääsu protokollis OAuth2 kaitstavatele andmetele, meie kasutusjuhus siis kasutaja isikuandmetele.
4. Selle olukorra vältimiseks nõutakse, et RP saadaks isikuandmete tõendi päringus OP serverile parameetris `code_verifier` esialgselt genereeritud juhuarvu enda, mida ründajal pole.
5. OP server peab kontrollima, kas esimeses päringus saadud `code_challenge` on tõesti genereeritud `code_verifier` väärtusest.

Esialgselt oli see turvameede mõeldud protokollis OAuth2 avalike klientide (näiteks mobiilirakendused) jaoks, kes ei saa kasutada OAuth2 päringute autentimist, kuna sellised kliendid ei saa hoida pikajalisi saladusi. Praegu soovitab aga standardi OAuth2.1 mustand jaotises 7.6 kasutada seda kõigil klientidel, olenemata nende tüübist. Peale standardi OAuth2.1 valmimist on tõenäoline, et ka standard OIDC järgmine versioon hakkab nõudma turvamehhanismi PKCE kasutamist.

Käesolevas analüüsis ning joonisel 5 on juba selgunud, et OAuth2 päringute autentimine on niikuinii vajalik ning autentimisprotokollistiku profiil toetab niigi ainult konfidentsiaalseid kliente. Seetõttu võib esmapilgul tunduda, et turvamehhanismi PKCE kasutamine ei annaks Eestile midagi juurde. Siiski aitab see kaitsta sellise ründe eest, kus ründaja süstib enda autentimisseansiga seotud volituskoodi kasutaja seanssi.

Volituskoodi süstimise ründe sammud on järgmised:

1. Ründaja pöördub RP veebisaidi poole, alustab autentimist ning viib autentimise OP juures lõpuni. OP suunab ründaja brauseri RP veebisaiti tagasi, koos volituskoodiga (`code`).
2. Ründaja peatab oma brauseris ümbersuunamise ning kopeerib enda seansist naasmis-URI.
3. Ründaja meelitab kasutajat klõpsama ründaja naasmis-URI-l ning kasutaja edastab ründaja seansiga seotud volituskoodi RP veebisaidile.
4. Kui RP ei ole realiseerinud kõiki turvamehhanisme (autentimispäringu vastuses tuleb kontrollida parameetri `state` sobivust kasutaja seansiga) või kui ründajal on õnnestunud ka enda seansiküpsised kasutaja brauserisse süstida, siis aksepteerib RP selle päringu ning pöördub omakorda OP poole ning edastab sinna isikuandmete päringu.
5. Peale päringusaatja autentimist järeldab OP, et see RP on õigustatud küsima ründaja isikuandmeid (kuna tõesti, sellel RP-el on parasjagu pooleli autentimisseanss ründaja autentimiseks) ning tagastab isikuandmete tõendi.
6. RP loob kasutaja brauseriga ründaja nimel isikustatud seansi.

Võib tunduda, et ründe tulemus ei ole ründajale kuigi kasulik, kuid sõltuvalt RP veebisaidi ülesehitusest ning teenuse sisust võib siiski juhtuda, et ründaja suudab kasutajat edasi manipuleerides ikkagi mingit kahju tekitada. Isegi kui see rünne võimaldab kasutajaid lihtsalt segadusse ajada, siis ka selle kahju vältimine oleks asjakohane. Lisaks aitab turvamehhanismi PKCE kasutamine vältida RP-dele pandavat vastutust. Isegi, kui mõned RP-d jätavad ekslikult osad turvakontrollid tegemata, siis OP juures tehtavad täiendavad kontrollivad kaitsevad ka selliseid RP-sid.

5.1.3 Autentimispäringu sisu

Autentimispäringuga edastab RP kasutaja autentimise soovi. Eesti autentimisteenuste profiil kasutab OIDC standardi jaotises 3.1.2.1 kirjeldatud sõnumit. Sõnumis kasutatavad väljad on kirjeldatud tabelis 7. Autentimispäringu näide koos väljade sisuga on kuval 5.4.

Tabel 7: Eesti autentimisprofiilile vastava autentimispäringu koosseisu ettepanek.

Andme-element	Allikas	Kohustuslikkus	Selgitus
`scope`	OAuth 2.0	jah	Määrab, milliseid isikuandmeid RP soovib peale autentimist kasutaja kohta teada saada. Kohustuslik on kasutada vähemalt väärtust „`openid`“, mis viitab OIDC standardis defineeritud komplektile `id_token` (isikuandmete tõend). OP võib defineerida täendavaid väärtusi.

Andme-element	Allikas	Kohus-tus-likkus	Selgitus
response_type	OAuth 2.0	jah	Määrab kasutatava OAuth2 protokollivoo. Kohustuslik on kasutada väärtust „code“ mis on volituskoodivoog. Muud võimalused ei ole toetatud.
redirect_uri	OAuth 2.0	jah	Naasmis-URI, kuhu autentimisteenuse pakkuja peab peale autentimisprotsessi lõppu kasutaja brauseri või agendi suunama. Esitatud väärtus peab olema RP registreeritud URI-ide loetelus.
state	OAuth 2.0	jah	Päringule lisatud unikaalne väärtus CSRF taasesitusründe vältimiseks.
client_id	OAuth 2.0	jah	Päringu koostanud RP identifikaator.
nonce	OIDC	jah	Unikaalne väärtus, mida kasutatakse isikuandmete tõendi sidumiseks autentimisseansiga ning mille abil saab vältida tõendi taasesitusrünnet.
code_challenge	OAuth 2.1	jah	RP poolt genereeritud juhuarvust turvalise räsifunktsiooniga genereeritud pretensioon (RFC7636-s defineeritud turvameede PKCE). Selle meetme abil saab vältida volituskoodi süstimisrünnet.
code_challenge_method	OAuth 2.1	jah	Turvameetmes PKCE kasutatava räsifunktsiooni identifikaator. Kohustuslik on kasutada väärtust „S256“.
ui_locales	OIDC	ei	Autentimisteenuse kasutajaliidese keele valiku parameetrid.
acr_values	OIDC	ei	Kui autentimisteenus toetab erineva usaldustasemega autentimisvahendeid, siis edastatud väärtustega saab soovitud tasemeid määrata. Vaata jaotist 5.1.3.2.
login_hint	OIDC	ei	Arvatav kasutaja identifikaator. Kui RP on enda veebisaidis või äpis kasutaja identifikaatori juba kasutaja käest teada saanud, või on see näiteks brauseri küpsiste põhjal teada, siis saab kasutaja arvatava identifikaatori saata autentimisteenusele ning sedaviisi autentimisprotsessi lihtsustada ja kiirendada.

Näide 5.4: Autentimispäringu väljade näide

```
{
    "scope":                  "openid",
    "response_type":          "code",
    "state":                  "fjkfds78[...]",
    "redirect_uri":           "https://example-rp.com/callback",
    "nonce":                  "n-0S6_WzA2Mj",
    "code_challenge":         "E9Melhoa2OwvFrEMTJ[...]",
    "code_challenge_method": "S256",
    "ui_locales":             "et",
    "acr_values":             "eidas1-high",
    "login_hint":             "ETSI:PNOEE-38001085718"
}
```

5.1.3.1 Parameetri nonce kohustuslikkus

Kuigi standard OIDC ütleb, et volituskoodi voo korral ei ole parameetri nonce kasutamine kohustuslik, siis Eesti autentimisprofiilis on see siiski vajalik, et tagada nõude EE.DYNAMIC täitmine (vt tabel 4, jaotises 4.3). Vastasel juhul ei ole isikuandmete tõend ning autentimissignatuur enam iga autentimisseansi jaoks unikaalne ning RP ei saa otsustada, kas keegi taasesitab talle vanu tõendeid või mitte.

Kuigi ka väljas state olev juhuslikkus aitab CSRF-rünnet ning taasesitusrünnet vältida, on siinkohal tegemist OAuth2 protokolli väljaga ning selle taaskasutamine OIDC protokolli vastustes ei oleks õige, kuna OIDC standardi kohaselt ei ole isikuandmete tõendi (id_token) parameetrite hulgas parameetrit state. Parameeter nonce on spetsiaalselt mõeldud peale autentimisprotsessi lõpetamist loodud isikuandmete tõendi sidumiseks konkreetse autentimisseansiga. Eesti autentimisprotokoll läheb veelgi kaugemale, kasutades parameetrit nonce ka autentimissignatuuri sidumiseks konkreetse autentimiseansiga.

Seetõttu on vajalikud mõlemad, nii parameeter state kui ka nonce.

5.1.3.2 Väljade acr_values, acr ja amr kasutus

Väljaga acr_values saab RP täpsustada päringuga algatatud autentimisprotsessi reegleid. Näiteks, kui OP toetab mitmeid erineva usaldustasemega autentimisvahendeid (ID-kaart või näiteks parool), siis saab RP autentimispäringus määrata, millisel usaldustasemel ta soovib konkreetsel juhul kasutajat tuvastada. Juhul, kui autentimisteenuse pakkuja toetab ainult sama usaldustasemega, võrdväärseid autentimisvahendeid, siis ei pea seda välja kasutama.

acr_values väärtuste jaoks ei ole olemas globaalset standardit. Küll aga võib leida mitmeid näited, kuidas teised teenusepakkujad seda välja kasutavad:

1. Eesti autentimisteenus TARA: low, substantial, high
2. Soome FTN võrgustiku OIDC profiil: http://ftn.ficora.fi/2017/loa2, http://ftn.ficora.fi/2017/loa3, http://eidas.europa.eu/LoA/low, http://eidas.europa.eu/LoA/substantial, http://eidas.europa.eu/LoA/high
3. Lätis LVRTC poolt pakutav e-identimise süsteem eParaksts: urn:eparaksts:authentication:flow:mobileid, urn:eparaksts:authentication:flow:sc_plugin
4. Norra DigDir asutuse poolt pakutav e-identimise süsteem: Level3, Level4

Teiste eeskujul teeme ettepaneku, et Eesti autentimisprotokolli profiilis tuleks `acr_values` väärtustena kasutada järgmiseid variante:

- Väli on määramata – Autentimisvahendi valik jäetakse täielikult kasutajale ning OP kuvab talle kõik toetatud variandid.
- `EE-low` – Kasutaja autentimine toimub seaduse EUTS alusel hinnatud e-identimise süsteemiga tasemel „madal“. Praegu selliseid süsteeme Eestis pole, kuid need võivad tekkida.
- `EE-substantial` – Kasutaja autentimine toimub seaduse EUTS seaduse hinnatud e-identimise süsteemiga tasemel „märkimisväärne“. Praegu selliseid süsteeme Eestis pole, kuid need võivad tekkida.
- `EE-high` – Kasutaja autentimine toimub seaduse EUTS alusel hinnatud e-identimise süsteemiga tasemel „kõrge“. Praeguse on selliste süsteemide kandidaadid ID-kaart, Mobiil-ID ja Smart-ID.
- `http://eidas.europa.eu/LoA/low` – Kasutajal võimaldatakse autentida eIDAS „low“ tasemel teavitatud autentimisvahenditega.
- `http://eidas.europa.eu/LoA/substantial` – Kasutajal võimaldatakse autentida eIDAS „substantial“ tasemel teavitatud autentimisvahenditega.
- `http://eidas.europa.eu/LoA/high` – Kasutajal võimaldatakse autentida eIDAS „high“ tasemel teavitatud autentimisvahenditega.

Peale seda, kui on valminud ka EUTS rakendamise ning e-identimise süsteemide hindamisega seotud määrused, siis saab seda loetelu täiendada.

Tasemed ei ole üksteist automaatselt kaasavad. Ehk siis näiteks, kui RP soovib kasutajad autentida vahenditega, mis on kas keskmisel või kõrgel tasemel, siis peab RP edastama `acr_values` väärtusena `"EE-substantial EE-high"`.

Peale kasutaja autentimist lisab OP isikuandmete tõendi väljale `acr` kasutatud autentimisvahendi usaldustaseme.

Erinevalt TARA praegusest profiilist ei võimalda ettepanek `scope` väljas määrata autentimisvahendi tüüpi (näiteks ID-kaart või Mobiil-ID) järgnevatel põhjustel:

- Erinevate autentimisvahendite loetelu on ajas muutuv, mõni uus võib juurde tulla ja mõni ära langeda. See on lisa halduskulu RP-le.
- Üks autentimisvahend võib pakkuda erineva usaldustasemega kontosid. Näiteks kui kommerts Smart-ID peaks hakkama pakkuma madalama tasemega kontosid või seoses Mobiil-ID muutumisega mitte riiklikuks eID vahendiks. Seega RP võib teha vea ajades usaldustaseme `acr_values` ja autentimisvahendi tüübi segamini.
- Agregaatoril nagu TARA-l võimaldab valiku puudumine RP eest teha monitooringut ning näiteks ühe autentimisvahendi teenuse tõrke ajal vastav kasutaja valik mitte aktiivseks teha. Seega ei pea RP ise tegelema autentimisvahendite teenuste monitooringuga.
- Lisaks pole `scope` õige väli autentimisvahendi valimiseks, see peaks määrama isikuandmete tõendi kooseisu.

Toome näiteks, et mingitel turvakaalutlustel on RP-l vajadus lubada ainutl ID-kaarti, kuna sellel on garanteeritud lokaalne ühendus brauseriga. Lahendus oleks lisada `acr_values` valik, mis vastavaid vajadusi rahuldab – `EE-high-local-link`. Kui tulevikus peaks mõni muu

autentimisvahend ka sellele nõudele vastama, näiteks Smart-ID laadne lahendus, mis kasutab Webauthn protokolli brauseriga suhtluseks, saaks selle ka sinna lisada.

Lisaks on isikuandmete tõendi väljal `amr` kasutatud e-identimise süsteemi või autentimisvahendi identifikaator. Sellega saab RP vihje, mis tüüpi autentimisvahendit kasutati. See võib olla kasulik, kui RP kasutab oma äriprotsessides ka digiallkirjastamist, et RP saaks tellida kasutaja digiallkirja samalt vahendilt (kui autentimisvahend toetab ka digiallkirjastamise funktsiooni). Kindla vahendi määramiseks võib aga olla vajalik kasutatud autentimissertifikaadi seest dokumendinumbri välja otsimine.

Väljas `amr` kasutatavate väärtuste kohta on olemas standard RFC8176, kuid see ei ole kahjuks kuigi praktiline ega Eesti oludele kohandatav. Seetõttu soovitame, et kuna RIAl on EUTS kohaselt järelvalvepädevus, siis võiks RIA hakata pidama Eestis kasutusel olevate e-identimise süsteemide või autentimisvahendite registrit. Esialgne identifikaatorite komplekt võiks olla selline:

1. `id-card`
2. `mobile-id`
3. `smart-id`

Nimedele tuleb lisada ka näiteks versiooninumber või aastaarv, mis viitaks konkreetsele e-identimise süsteemi kirjeldavale dokumentatsioonile, nagu näiteks hetkel Smart-ID süsteemist olemas olevad kirjelduse versioonid 1.0[9] ja 3.0.[10] Võib ka kasutada URL skeemat, sarnaselt `acr_values` välja eIDAS tasemel teavitatud autentimisvahendite tasemetega.

Juhul, kui autentimine viidi läbi eIDAS Node võrgustiku teenustega, siis kasutatakse sealtkaudu saadud *Authentication Context Class Reference* väärtusi, näiteks `urn:oasis:names:tc:SAML:2.0:ac:classes:X509` vms.

Igaljuhul ei saa see Eesti autentimisprofiili ettepanek esitada lõplikku nimekirja. RP'd, kes otsustavad kasutada `amr` välja peavad aktiivselt jälgima muudatusi registris.

Kaalumist tasub ka `amr` välja kasutamisest loobumine. TARA olemasolevas profiilis täidab `amr` vajalikku rolli, kuna TARA võimaldab autentimisvahendi tüüpi määrata. Siin kirjeldatud ettepaneku puhul otsene vajadus puudub. Kui autentimisprofiilile saadud tagasisidest selgub, et selle välja kasutamiseks ei ole olulist vajadust, siis siis soovitame sellest loobuda.

5.1.4 Autentimispäringu terviklus ja konfidentsiaalsus tema edastamisel

OIDC protokolli kohaselt tuleb autentimispäring edastada autentimisteenuse API-le HTTP päringuna, kuid tehnilisi detaile on veelgi. Isegi, kui me kasutame OAuth-päringute autentimiseks jaotises 5.1.2 kirjeldatud vahendeid, siis autentimispäringut transporditakse teistmoodi (läbi kasutaja brauseri) ning samu vahendeid kasutada ei saa. Juhul, kui autentimispäringus on isikuandmeid, näiteks väljas `login_hint`, siis tuleb päringuobjekti lekkimise eest kaista.

Autentimisprofiili kirjeldamisel kaaluti järgmiseid võimalusi:

1. HTTP GET päringud ning URL päringuparameetrid. See on praegune levinud lahendus, mis on kirjeldatud OIDC jaotises 13.1. Probleem tekib sellisel juhul, kui kõigi soovitud väljadega varustatud autentimispäring konfidentsiaalsuse ja tervikluse kaitseks krüpteerida ja signeerida ning loodud andmeobjekt on suurem kui 512 baiti. Lauaarvutite brauserid saavad hakkama tõenäoliselt ka pikemate URL-idega kui 1024 baiti, kuid mobiiliplatformides võib olla URLide pikkus piiratud 512 baidiga.[11]

[9] https://www.ria.ee/sites/default/files/content-editors/EID/smart-id_tagatistaseme_kirjeldus.pdf
[10] https://www.ria.ee/sites/default/files/content-editors/EID/smart-id-skeemi-kirjeldus-abiv.pdf
[11] https://www.rfc-editor.org/rfc/rfc9101.html#section-5.2

2. HTTP POST päringud ning väljade esitamine päringu kehas oleva `application/x-www-form-urlencoded` vormina, vastavalt OIDC jaotisele 13.2 toodud tingimustele. Sellisel juhul ei ole meil enam URLi pikkuse probleemi, kuid mobiilirakenduste vahel ümbersuunamise korraldamiseks ei ole POST päringute kasutamine operatsioonisüsteemide poolt toetatud. Lisaks ei ole OIDC standardis POST päringute vastuvõtmise tugi OP tarkvaradele kohustuslik, mis võib vähendada riiulitarkvara kasutamise võimalusi.

3. OIDC standardi jaotis 6.2 annab võimaluse ka ainult autentimispäringu objekti viite edastamiseks, kuid autentimispäringu andmeobjektide majutamisega võib tekkida probleeme sellisel juhul, kui RP veebiserver ei ole OP serverist kättesaadav, näiteks privaatvõrgu või tulemüüride kasutamise tõttu. Standard RFC9126 kirjeldab võimaluse, kuidas RP saab eraldi päringus edastada autentimispäringu objekti OP-le, saab vastuseks unikaalse aadressi ning seejärel kasutab seda aadressi OIDC autentimispäringu saatmisel väljas `request_uri`. RFC9126 võimaldab edastada autentimispäringu sisu nii avatekstina kui ka krüpteerituna/signeerituna. Eesti autentimisprofiil jätab selle võimaluse lahti ning lubab mõlemat lahendust, kuna krüpteerimine pole enam otseselt vajalik, sest päring ei liigu enam läbi brauseri ja on TLS ühenduse poolt juba krüpteeritud.

OIDC autentimispäring tuleb siis edastada kahes osas. Esmalt tuleb OP serverisse saata päringuobjekt vastavalt RFC9126 reeglitele. Koodinäide on kuval 5.5. Selle päringu vastuseks tagastab OP server loodud päringuobjekti identifikaatori (vt kuva 5.6) ning seejärel tuleb läbi kasutaja brauseri või mobiiliplatformi saata levinud standardile OIDC vastav autentimispäring. Koodinäide on kuval 5.7.

Näide 5.5: Autentimispäringu objekti edastamine standardi PAR kohaselt

```
POST /auth_service/par HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Host: server.example-op.com
Authorization: Basic
  Qjc3NkY4QTItM0JDMS00MkFELThEMzUtQTc1NTIxMkU3NDNBOnBhc3N3b3JkCg==

scope=openid
&response_type=code
&client_id=B776F8A2-3BC1-42AD-8D35-A755212E743A
&state=fjkfds78[...]
&redirect_uri=https%3A%2F%2Fexample-rp.com%2Fcallback
&nonce=n-0S6_WzA2Mj
&code_challenge=E9Melhoa2OwvFrEMTJ[...]
&code_challenge_method=S256
&login_hint=ETSI:PNOEE-38001085718
```

Näide 5.6: Autentimispäringu objekti identifikaatori tagastamine standardi PAR kohaselt

```
HTTP/1.1 201 Created
Cache-Control: no-cache, no-store
Content-Type: application/json

{
  "request_uri": "urn:bwc4JK-ESC0w8acc191e-Y1LTC2",
  "expires_in": 90
}
```

Näide 5.7: Autentimispäringu saatmine standardi OIDC järgi, koos objekti identifikaatoriga

```
GET /auth_service?client_id=B776F8A[...]&request_uri=urn%3Abwc4JK-E[...]
  HTTP/1.1
Host: server.example-op.com
```

URLi parameetri `client_id` kasutamine on kohustuslik, kuna see on standardile OAuth2 vastav päring. URL parameetris `request_uri` esitatakse autentimispäringu objekti aadress URL-kodeerituna.

5.1.5 Kasutaja autentimine

Peale seda, kui kasutaja agent (brauseri või mobiilirakenduse) on RP koostatud autentimispäriguga OP autentimisteenusesse suunatud, teeb OP järgmised tegevused:

1. Autentimispäringu töötlemine ja kontrollimine.
2. Autentimisvahendi poolt allkirjastatava andmestruktuuri loomine (vt jaotis 5.2.3).
3. Kasutaja autentimine sobiva autentimisvahendiga ning vahendi abil autentimissignatuuri genereerimine.
4. Autentimispäringu vastuse tagastamine.

5.1.6 Autentimispäringu vastus

Autentimispäringu vastus on sõnum, millega autentimisteenuse pakkuja edastab info lõppenud autentimisprotseduuri kohta. Juhul, kui autentimine on edukas, siis antakse RP-le volituskood (`code`), millega teha isikuandmete tõendi päring. Kui autentimine ebaõnnestus või kasutaja loobus autentimisest, siis edastatakse info vastava veakoodiga (näiteks `user_cancel`). Autentimispäringu vastuse näide on kuval 5.8.

Näide 5.8: Autentimispäringu vastus

```
HTTP/1.1 302 Found
Location: https://www.example-rp.ee/callback?
  code=SplxlOBeZQQYbYS6WxSbIA&
  state=af0ifjsldkj
```

5.1.7 Autentimispäringu vastuse valideerimine

Protokollis OIDC tagastatava autentimispäringu vastusena kasutatakse standardile OAuth2 vastavat volituspäringu vastust ning seda tuleb valideerida vastavalt OAuth2 standardi jaotises 4.1.2 toodud reeglitele.

5.1.8 Kasutaja isikuandmete tõendi päring

Kasutaja isikuandmete saamiseks peab RP tegema täiendava päringu, vastavalt OIDC standardi jaotises 3.1.3.1 kirjeldatud sõnumile. Sõnumi näide on kuval 5.9.

Päringus tuleb kasutada täiendavat turvameedet PKCE ning edastada parameetris `code_verifier` esialgne juhuarv, millest genereeriti autentimispäringus edastatud parameeter `code_challenge`.

Näide 5.9: Isikuandmete tõendi päring

```
POST /token HTTP/1.1
Host: server.example-op.com
Content-Type: application/x-www-form-urlencoded
Authorization: Basic
  Qjc3NkY4QTItM0JDMS00MkFELThEMzUtQTc1NTIxMkU3NDNBOnBhc3N3b3JkCg==

grant_type=authorization_code
    &code=SplxlOBeZQQYbYS6WxSbIA
    &redirect_uri=https%3A%2F%2Fclient.example-rp.com%2Fcb
    &code_verifier=dBjftJeZ4CVP-mB92K27uhb[...]
```

Tabel 8: Eesti isikuandmete tõendi koosseisu kavand.

Andme-element	Kohus-tus-likkus	Selgitus
`iss`	jah	Tõendi väljastaja identifikaator
`sub`	jah	Autenditud kasutaja identifikaator vastavalt standardile ETSI EN 319-412-1 (näiteks `ETSI:PNOEE-38001085718`)
`nonce`	jah	Autentimispäringus RP poolt esitatud unikaalne nonss, mis aitab vältida tõendi taasesitusrünnet
`aud`	jah	Autentimise tellinud RP identifikaator ja veebidomeen, kuhu kasutaja sisse logis
`iat`	jah	Tõendi koostamise aeg
`exp`	jah	Tõendi aegumise aeg
`acr`	jah	Autentimisel kasutatud autentimisvahendi usaldustaseme klass
`amr`	jah	Autentimisel kasutatud autentimisvahendi tüüp
`dts`	jah	Autentimisvahendi poolt moodustatud autentimissignatuur eraldatud signatuuriga JWS-vormingus.
...		

5.1.9 Kasutaja isikuandmete tõendi valideerimine

Näide 5.10: Isikuandmete tõendi päringu vastus

```
HTTP/1.1 200 OK
Content-Type: application/json
Cache-Control: no-store
Pragma: no-cache

{
    "access_token": "SlAV32hkKG",
    "token_type": "Bearer",
    "expires_in": 3600,
    "id_token": "eyJhbGciOiJSUzI1N[...]"
}
```

Koos HTTP vastusega tagastatakse nii juurdepääsutalong kui ka kasutaja isikuandmete tõend. Vastuse näide on kuval 5.10. Kuna see on protokolli OAuth2 kohane vastus, siis tuleb tagastada ka `access_token` ja muud vajalikud väljad, mis ei ole tegelikult Eesti autentimisprotokollistikus vajalikud, kuna väljas `id_token` antakse kohe vastusega kaasa ka isikuandmete tõend. Isikuandmete tõend on JWT formaadis andmestruktuur, mille andmeelemendid on kirjeldatud tabelis 8. Vajadusel saab OP lisada isikuandmete tõendisse täiendavaid välju. Näiteandmetega moodustatud isikuandmete tõend on kuval 5.11.

Näide 5.11: Isikuandmete tõendi näide

```
{
    "alg": "RS256"
}
.
{
    "iss": "https://tara.ria.ee",
    "sub": "ETSI:PNOEE-38001085718",
    "nonce": "n-0S6_WzA2Mj[...]",
    "aud": [
        "https://www.example-rp.ee",
        "B776F8A2-3BC1-42AD-8D35-A755212E743A"
    ],
    "exp": 1642507495,
    "iat": 1642507295,
    "acr": "EE-high",
    "amr": [
        "id-card-2021"
    ],
    "dts": "eyJhb[...]FiIn0..0NXExcL[...]vC9xFjlg"
}
.
"tõendi väljastaja signatuur"
```

Isikuandmete tõendi valideerimiseks peab RP läbi tegema kõik järgmised sammud.

1. Kontrollima tõendit vastavalt standardi OIDC jaotisele 3.1.3.7 järgmiste sammudega:
    a) Kontrollima, kas tõend on väljastatud ning signeeritud usaldusväärse osapoole poolt (väli `iss`)
    b) Kontrollima, kas tõend on väljastatud õige RP jaoks (väli aud)
    c) Kontrollima, kas tõend on värske (väljad `iat` ja `exp`).
    d) Kontrollima, kas tõend on seotud seotud korrektse autentimisseansiga ning esialgse RP esitatud autentimispäringuga (väli nonce).
    e) Kontrollima, kas autentimine toimus soovitud usaldustasemega autentimisvahendiga (väljad `acr` ja `amr`).
2. Kontrollima väljas `dts` oleva autentimissignatuuri:
    a) Taaslooma signatuuri alla läinud andmed (RP genereeritud nonss, RP identifikaator, jms) ning kontrollima, et autentimissignatuur on antud nendele andmetele ning autentimissignatuur valideerub autentimissignatuuris endas esitatud isikusertifikaadiga (vt ka jaotis 5.2.5).
    b) Kontrollima, et isikusertifikaat on väljastatud samale identiteedile, mis on ka väljas sub.
    c) Kontrollima, kas isikusertifikaat on väljastatud usaldusväärse CA poolt, et sertifikaat kehtib ajaliselt ning ei ole tühistatud, OCSP-vastuste või CRL alusel.

d) Kontrollima, kas sertifikaadiahel kehtib ning ei ole tühistatud, OCSP-vastuste või CRL alusel.

Juhul, kui kõik tehnilised kontrollid on läbitud, alles siis saab RP järeldada, et väljas sub olev identifikaator on tõene selle autentimisseansi käigus autenditud isiku identiteet. Tõenäoliselt on väga kasulik, et nende sammude korrektseks läbiviimiseks luuakse RIA poolt laialtlevinud programmeerimiskeeltes teegid, nagu praegu on loodud näiteks lahenduses Web eID teek Java programmeerimiskeelele.[12]

5.1.10 Kasutusnäide

Protokolli kasutamise detailne näide olukorras, kus RP ning autentimisteenuse (Smart-ID) vahel on veel üks autentimist vahendav teenus (TARA), on joonisel 6. Joonisel ei ole kõik tehnilised detailid lõpuni spetsifitseeritud, kuid see näide peaks andma huvitavat mõtteainet ning illustreerib loodud protokolli potentsiaali lahendada väga üldiseid olukordi.

5.2 Autentimise usaldusankur

Jaotises 5.1 kirjeldatud autentimisprotokoll võimaldab pakkuda universaalset autentimisteenust. Siin jaotises põhjendame, miks on vajalik lisada autentimisprotokolli autentimissignatuuri (väli dts) edastamise võimalus, miks peavad RP-d seda kontrollima ning kuidas autentimissignatuuri esitada.

5.2.1 Autentimisteenuse usalduse küsimus

Tavapärase autentimisteenuse korral peab RP täielikult usaldama OP väiteid autenditud isiku kohta. Sellisel juhul saab ekslik, pahatahtlik või ründaja poolt ülevõetud OP edastada ka võltsitud isikuandmete tõendeid. Juhul, kui OP edastaks autentimisvahendi poolt loodud autentimissignatuuri, siis saab RP kontrollida, et autentimises osales kasutajale väljastatud autentimisvahend ning RP saab usaldada OP asemel autentimisvahendit.

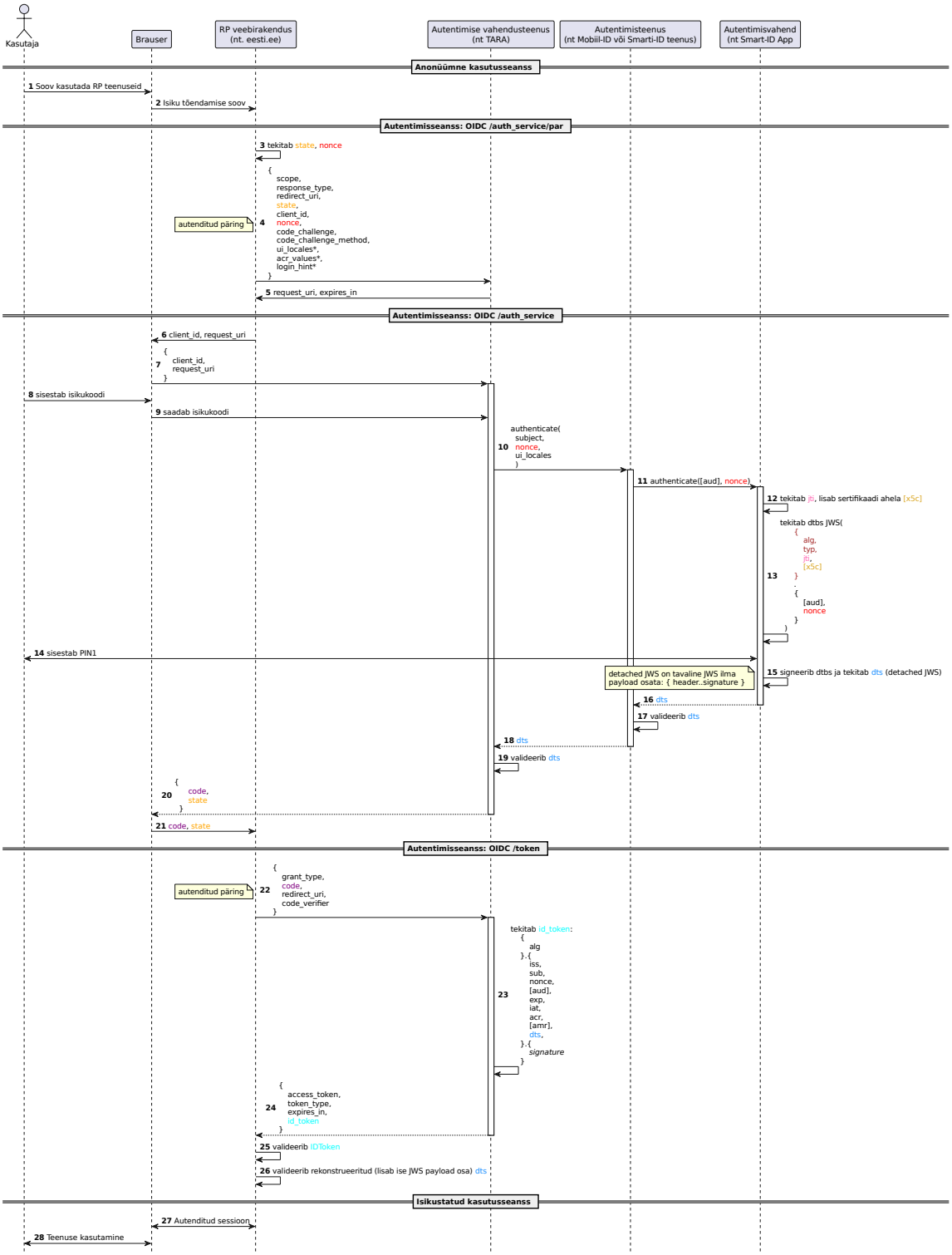
Kui RP peab täielikult usaldama OP tegevust, siis ei ole otseselt või kaudselt täidetud järgmised autentimise üldised nõuded (vt tabel 4):

1. EE.USER-CONTROL – „Ainult autentimisvahendi omanik tohib saada vahendit kasutada ning teiste poolt autentimisvahendi väärkasutamine peab olema tõkestatud“
2. EE.DYNAMIC – „... autentimisprotokoll peab tõendama, et kasutaja võtmepaar osales autentimises“
3. EE.NO-MITM – „Autentimisprotokoll peab olema kaitstud vahemeherünnete eest (naiteks RP võltsimine, autentimisteenuse võltsimine ...“

Sellegipoolest võib RP jaoks selline suurenenud risk olla aktsepteeritav järgmistel juhtudel:

1. autentimisteenuse pakkumust kirjeldav teenusleping pakub RP jaoks piisavaid garantiisid ning RP saab asjassepuutuvad riskid selle lepingu alusel OP-le üle kanda,
2. autentimisteenuse pakkuja on riiklikult reguleeritud usaldusteenus, mille nõuetele vastavust on hinnatud ning mis on RP jaoks sobival turvatasemel.
3. autentimisteenuse pakkuja käitab e-identimise süsteemi, mille nõuetele vastavust on hinnatud ning mis on RP jaoks sobival turvatasemel.

[12] https://github.com/web-eid/web-eid-authtoken-validation-java



Joonis 6: Autentimisprotokollistiku kasutamine läbi vahendaja

Olukorras, kus ühtegi nendest kolmest võimalusest ei saa kasutada ning sellise teenuse riskitase ei ole RP-le vastuvõetav, kuid autentimisteenus kasutab kõrge usaldustasemega autentimisvahendit, näiteks ID-kaarti, Mobiil-ID või Smart-ID, siis saab väikeste täiendustega autentimisprotokollis võimaldada RP-l usaldada PKI-põhist allkirja andmise vahendit ennast ning seeläbi vähendada autentimisteenuse usaldamise vajadust.

5.2.2 Privaatvõtme omanduse tõendamine

Põhimõtteliselt püüame me leida lahendust probleemile, kuidas RP saaks kontrollida, et autentimises osalenud kasutajal on juurdepääs just nimelt selle kasutajaga seostatud võtmepaarile ning mitte kellelgi teisel sellele võtmepaarile juurdepääsu pole. Krüptograafias nimetatakse seda probleemi „omanduse tõendamine“ (*proof-of-possession*). IETF töögrupid tegelevad samasuguse probleemi lahendamisega OAuth2.0 ning OIDC protokollides ning kirjanduses leiab järgmiseid lahendusi:

1. Standard RFC7800 kirjeldab ainult üldise JWT struktuuri välja `cnf`, millega saab kirjeldada selle võtmepaari infot, mille kohta omandust soovitakse tõendada, kuid standard ei lähe detailidesse, kuidas peaks tõendamine ise tegelikult toimuma.

2. Standardimustand `https://datatracker.ietf.org/doc/html/draft-ietf-oauth-dpop-04` kirjeldab võimalust, kuidas OAuth2.0 päringutes lisada HTTP päistesse signeeritud JWT struktuur, mille kättesaaja saab kontrollida, et saatjal oli juurdepääs privaatvõtmele. Standardimustand eeldab, et JWT kodeerimisel edastatakse ka last ning seal kopeeritakse need andmed, mis peaksid kättesaajal tegelikult juba olemas olema (näiteks väljad `nonce`, `htm`, `htu`). Standardimustand on kirjutatud spetsiifiliselt OAuth2 ning HTTP päringuid silmas pidades ning kirjeldatud sõnumite ületoomine autentimisse ei ole otsekohene.

3. OIDC standard näeb ette spetsiaalse OIDC teenusepakkuja tüübi SIOP (sõltumatu autentimisvahendi protokoll – *Self-Issued OP*), mis on kasutaja enda juures töötav teenus, mis väljastab isikuandmete tõendeid kasutaja enda kohta. Isikuandmete tõendi väljastamisel kinnitab SIOP, et tal on juurdepääs mingile konkreetsele võtmepaarile ning edastab ka selle informatsiooni isikuandmete tõendis. OpenID Foundation tegeleb praegu selle standardi järgmise versiooni arendamisega (`https://openid.net/specs/openid-connect-self-issued-v2-1_0.html`). Nii esialgne standard kui ka töös olev mustand eeldavad, et kodeerimisel edastatakse ka last ning seal kopeeritakse need andmed, mis peaksid RP-l juba olemas olema (näiteks väljad `nonce`, `exp`, `iat` jms).

Võib argumenteerida, et selline andmete üleliigne kopeerimine ei ole autentimise kontekstis hädavajalik ning võib osutuda isegi ohtlikuks (`https://cybersec.ee/storage/webeid_auth_proof.pdf`), kuna RP arendaja võib sattuda segadusse, milliseid väljasid ta saab usaldada ning milliseid mitte. Seetõttu jätame olemasolevad tehnilised lahendused kõrvale ning kirjeldame järgnevalt uut lahendust, kuidas tõendada privaatvõtme omandust just nimelt autentimise kontekstis ning eeldades Eesti PKI mudelit.

5.2.3 Autentimissignatuuri loomine

Autentimissignatuur on kasutaja autentimisvahendiga loodud krüptograafiline signatuur, millega signeeritakse järgmine minimaalne andmekomplekt:

1. `aud` – Massiiv autentimise tellinud RP ning autentimisteenuse pakkuja identifikaatoritega. ID-kaardiga autentimise korral on siin brauseri poolt kuvatud veebilehe aadress. Autentimisteenuste URL tuleneb RP poolt algselt saadetud `redirect_uri`-st.

2. `nonce` – RP poolt genereeritud juhuarv, mis edastati autentimispäringu `nonce` väljas.

3. `jti` – Autentimisteenuse või autentimisvahendi poolt genereeritud juhuarv.

5.2.3.1 Autentimissignatuuri väli `jti`

Väli `jti` (RFC7519 jaotis 4.1.7) on allkirjastatavate andmete hulka lisatud selleks, et suurendada signatuuride unikaalsust ning vähendada võimalust, et autentimisvahend töötaks pahatahtliku RP jaoks krüptograafilise oraaklina. Krüptograafia ajaloost on teada ründeid,[13] kus sedaviisi suudetakse leida kasutatav privaatvõti. Lisaks, kui pahatahtlik RP suudab autentimissignatuuri räsi ennustada, siis võib juhtuda, et ta saab signeeritavaid andmeid mingi muu autentimisseansi kontekstis taaskasutada. Põhimõtteliselt on `jti` näol tegemist kasutaja-poolse nonsiga ning selle esitamine eraldi väljana, mitte etteantud `nonce` väärtusega kokku segades, võimaldab RP-l endiselt kontrollida, et kas ka tema esitatud juhuslikkus on ikka signeeritud andmete hulgas.

Väli `jti` võimaldab autentimissignatuuri lisada juhuslikkust ainult autentimisvahendil endal, st näiteks ainult Web eID komponentidel `web-eid-app` või `web-eid-webextension`. Kuigi see kaitseb lõppkasutajat, siis autentimisteenuse pakkuja kaitse autentimisvahendit kontrolliva osapoole eest oleme praegu välja jätnud. Selle lahendamiseks saaks katsetada võimalust, et `jti` on massiiv juhuarvudest ning autentimisteenus genereerib oma juhuarvu, edastab selle autentimisvahendile ning autentimisvahend lisab sinna enda juhuslikkust. Sellisel juhul aga ei ühildu see enam standardiga JWS ning kuidas seda täpsemalt korraldada, pole hetkel veel dokumenteeritud.

5.2.3.2 Autentimissignatuuri väli `aud`

Massiivi `aud` sisu on ehk kõige keerulisem spetsifitseerida, kuna see sõltub tehniliselt autentimislahendudesest. Peab RP välja täpset sisu ette teadma, et oleks võimalik autentimissignatuuri verifitseerimine, vaata 5.2.4.2.

Autentimisvahendit otse kasutades probleeme pole, sest väärtus on brauseri pakutav `location.origin` ning RP saab selle ise tuletada. Näiteks kõige lihtsam on ID-kaardi kasutus Web eID abil.

Kui RP kasutab autentimiseenust ilma vahendajateta, saab `aud` olla `redirect_uri`. Siiski on `redirect_uri` vmt olemasolu omaette eeldus, et autentimisteenus pakub sedalaadi parameetrit oma liideses. Näiteks tänased Mobiil-ID ja Smart-ID REST API-d ei oma sarnast välja.

Kui RP kasutab autentimiseks vahendajat (näiteks TARA), siis autentimisvahendi nagu ID-kaart puhul on `aud` vahendaja domeeni aadressiga, mitte RP enda oma. Sellega saab RP arvestada ja probleemi üldiselt pole.

Kui RP kasutab autentimiseks vahendajat ning autentimisteenusena Smart-ID-d, siis teoreetiliselt saaks vahendaja autentimisteenusele RP-le vastava `aud` väärtuse edasi anda. Hetkel on see võimatu, kuna teenuste REST API'd ei toeta taolist parameetrit. Tulevikus võidakse sellist võimalust toetada. Autentimisteenus peaks muidugi lubama selle parameetri kasutust ainult teadaolevatele ja usaldatud vahendajatele.

Hetkel jätame läbi vahendaja edastatud `aud` välja seadmise võimaluse spetsifitseerimata. Vahendaja edastatud `aud` välja võib tulevikus alati juurde lisada, kuna autentimissignatuur ise on versioneeritav tänu `typ` väljale. Seejuures tuleb arvestada, et `aud` vorm sõltub `typ` väärtusest.

Erinevad potentsiaalsed `typ` väljast sõltuvad `aud` vormid (need on lihtsalt näited):

- `web-eid:1` - `origin`
- `web-eid:2` - `origin` + `server TLS hash`
- `service:2` - `redirect_uri`
- `service:3` - `rp_uuid`

[13] https://en.wikipedia.org/wiki/Adaptive_chosen-ciphertext_attack

- `service-proxy:1` - `redirect_uri` + `proxy_uri`
- ...

Kuna erinevate variantide puhul on ka välja sisu ise erinevev (näiteks UUID vs URI), siis peab ka iga väärtuse ees olema määratud tüüp, näiteks `uri:https://example.com/return` ja `uuid:2d12d94f-5d65-4667-9248-9504ebf2eb1b` jmt.

Kuigi massiv `aud` on olemas ka isikuandmete tõendis, siis peaks RP olema võimeline tuletama oodatud väärtust iseseisvalt. Teek, mis tegeleb autentimissignatuuri valideerimisega peaks sisendiks võtma peale autentimissignatuuri ja `nonce`-i RP `rediret_uri`, mitte isikuandmete tõendist tulnud `aud` väärtuse.

5.2.4 Allkirja vorming

Kuidas täpselt andmeid vormindatakse ning allkirja esitatakse, on veel hetkel lahtine. Laias laastus on meil järgmised valikud:

1. Minimaalsesse komplekti kuuluvate andmeelementide räsimine, räside üksteise järgi paigutamine, signeerimine ning edastamine andmetest eraldatud iseseisva signatuurina, nagu pakub Arnis Paršovs. Lühidalt saab ettepaneku kokku võtta nii: `SIGN(SHA256(aud) | SHA256(nonce))`.
2. Andmeelementide esitamine JSON struktuurina, signeerimine vastavalt JWS standardile ning edastamine andmetest eraldatud signatuurina (*detached*, `https://datatracker.ietf.org/doc/html/rfc7797`).

5.2.4.1 Lihtne räside ühendamine

Kui loobuda standardite järgimisest, siis põhimõtteliselt piisab vajalike andmete räsimisest, räside järjestikusest ühendamisest, seejärel allkirjastamisest ning signatuuri edastamisest. Kontrollija peab siis hankima samad andmed, samamoodi ühendama ning kontrollima kasutaja avaliku võtmega, kas signatuur on moodustatud just nimelt nendele andmetele.

See tähendab, et autentimissignatuuri moodustaja ning kontrollija peavad eelnevalt täpselt fikseerima, mismoodi toimub andmete esitamine baitides, nende vormindamine ning millist signeerimisalgoritmi kasutatakse. Juhul, kui kasutusel olevaid autentimisvahendeid on mitut tüüpi ning need autentimisvahendid toetavad erinevatel algoritmidel põhinevaid võtmepaare või mitut tüüpi allkirjastamise algoritme, siis info selliste valikute kohta tuleb edastada kuidagi muudmoodi. Juhul, kui tekib vajadus kaasata täiendavaid andmeväljasid, siis andmeformaadi versiooni esitamise võimalus puudub.

Selliste praktiliste kaalutluste tõttu jätame ülaltoodud autentimissignatuuri formaadi kõrvale.

5.2.4.2 Eraldiseisev signatuur JWS formaadis

Standard RFC7515 võimaldab esitada signeeritud andmeid JSON formaadis ning võimaldab fikseerida infot signeerimisalgoritmi, kasutatud võtmete ja muude detailide kohta. Kui tavaliselt sisestatakse JWS struktuuri ka signeeritavad andmed, kasutades selleks lastile ettenähtud asukohta, siis standard RFC7519 võimaldab esitada ka andmetest eraldiseisvat signatuuri. Eraldiseisva signatuuri kasutamine aitab kaasa sellele, et RP peab signatuuri valideerimiseks hankima usaldusväärsest allikast signeeritud andmed, ning seeläbi on ta sunnitud kasutama seansiandmete hoidlat, näiteks `nonce` leidmiseks.

Väli `jti` tuleb sellisel juhul esitada lasti asukoha asemel päises, kuna muidu ei saaks RP signeeritavaid andmeid enam taas-konstrueerida. Vastav võimalus on standardis JWT ette nähtud jaotises 5.3 ning standardi JWS jaotistes 4.1.11 ja 4.3. Vastav näide on kuval 5.12.

Näide 5.12: Autentimissignatuuri koostamiseks vajalike andmete näide

```
{
    "alg": "RS256",
    "typ": "web-eid:1",
    "jti": "a9fa7ef43137ea7595ab",
    "x5c": [
        "MIIE3jCC...TWVU+4=",
        "MIIC5zCC...9ViH0Pd"
    ]
}
.
{
    "aud": [
        "https://example-rp.com/callback"
    ],
    "nonce": "fjkfds78..."
}
```

JWS päises olevad kohustuslikud väljad:

1. `alg` tähistab signeerimisalgoritmi, millega kasutaja autentimisvahend loob autentimissignatuuri. Peab vastama JWA reeglitele.
2. `typ` tähistab Eesti autentimissignatuuri andmeformaadi tüüpi ning versiooni.
3. `jti` on autentimisteenuse või autentimisvahendi poolt genereeritud juhuslikkus.
4. `x5c` on autentimisvahendiga seotud X.509 isikusertifikaadi DER-vormingus sertifikaadiahel esitatuna Base64-vormingus. Kui me ei lisaks sertifikaadiahelat JWS-päisesse, siis ei oleks näiteks Web eID süsteemi poolt koostatud autentimissignatuuride valideerimine võimalik, kuna seal süsteemis ei edastata eraldi isikuandmete tõendit. Täna Eestis pole ahela edastamiseks vajadust olemas, sest väljastaja sertifikaadid on usaldatud, kuid see võib tulevikus muutuda ning mõistlik on kohe ka vastavat tuge protokollis omada.

Signeerimisele mineva sõnumi koostamiseks tehakse toimingud:

```
ASCII(BASE64URL(UTF8(JWS Protected Header)) || '.' || BASE64URL(JWS Payload))
```

Signeeritud JWS struktuuri esitamiseks kasutatakse kompaktset formaati (*compact*, RFC7515 jaotis 3.1), kuid JWS lasti ei lisata kodeeringusse ning vastav koht kodeeringus jäetakse lihtsalt tühjaks. Tulemuseks on baidijada, mille näide on kuval 5.13.

Näide 5.13: Autentimissignatuuri eraldiseisev kompaktne esitus Base64-vormingus

```
eyJhbGciOiJSUzI1NiIsInR5cCI6IndlYi1laWQ6MSIsImp0aSI6[...]
.
.
0NXExcLSCId5G[...]RLoH44vC9xFjlg
```

kus esimene punkt tähistab JWS päise lõppu ning tühja lasti algust ning teine punkt tähistab tühja lasti lõppu. Base64-vormindatud signatuur lisatakse autentimisteenuse pakkuja poolt isikuandmete tõendi välja `dts`. Välja nimi on valitud raamistiku Mobile Connect eeskujul (vt jaotis 2.6.1, `https://www.gsma.com/latinamerica/wp-content/uploads/2016/06/techdoc-MC-OpenID_Connect_Mobile_Connect_Profile-1.pdf`).

Autentimissignatuuri formaat on universaalne ehk kõik parameetrid on kohustuslikud sõltumata autentimisvahendist. Väli (`typ`) võimaldab tulevikus autentimissignatuuril vastavalt vajadusele edasi areneda.

5.2.5 Autentimissignatuuri valideerimine

RP peab autentimissignatuuri valideerimiseks signeeritud andmekomplekti konstrueerima järgmistest allikatest:

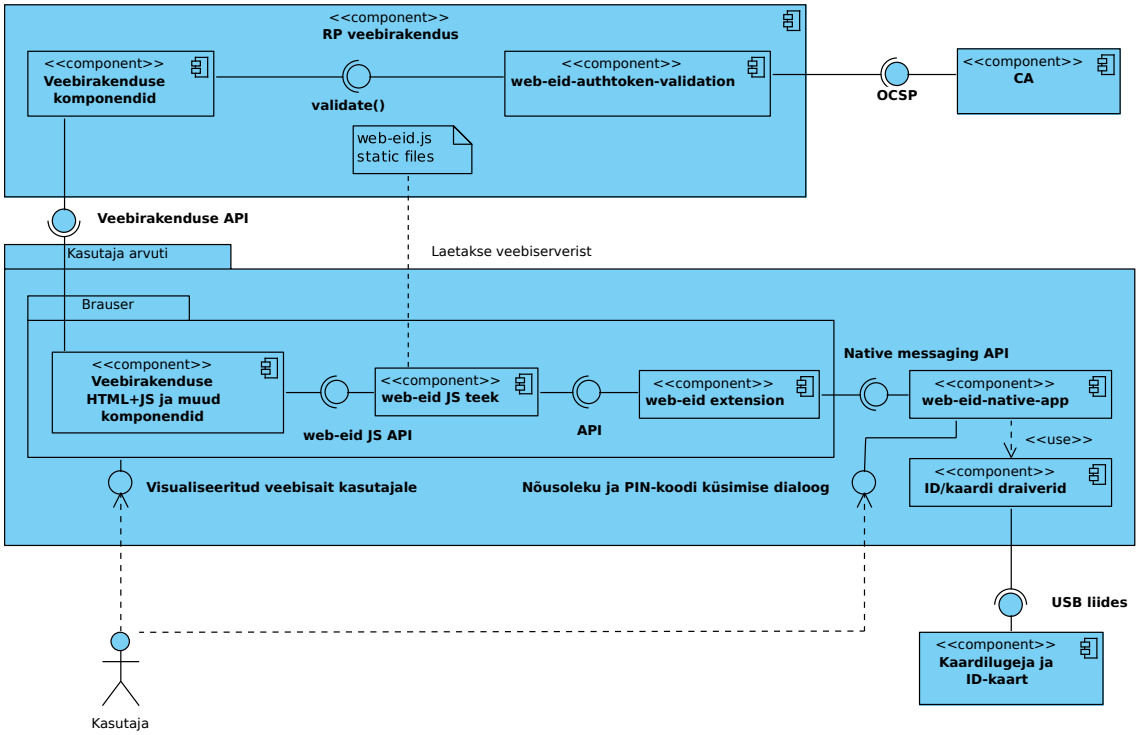
1. Autentimissignatuuri kaitstud päise seest tuleb võtta `alg` väärtus ning kontrollida, kas see on lubatud algoritmide nimekirjas.
2. Autentimissignatuuri kaitstud päise seest tuleb võtta `typ` väärtus ning kontrollida, kas see on lubatud formaatide nimekirjas.
3. Autentimissignatuuri kaitstud päise seest tuleb võtta `jti` väärtus ning kontrollida, et see ei oleks tühi.
4. Autentimissignatuuri kaitstud päise seest tuleb võtta `x5c` väärtus ning leida sealt isikusertifikaat ja kontrollida, et:
   - Isikusertifikaat peab ahelduma RP poolt usaldatud sertifikaadiväljastajaga.
   - Kõik sertifikaadid ahelast peavad valideeruma vastavalt sertifikaatide valideerimise reeglitele (ajaline kehtivus, hetke kehtivus jne).
   - Isikusertifikaadis kirjeldatud isik klapib isikuandmete tõendi `sub` väljaga ja RP eeldatud isikuga `login_hint` autentimispäringust.
5. RP seansiandmetest tuleb leida selle autentimisseansi jaoks genereeritud `nonce` väärtus.
6. RP seansiandmetest tuleb leida selle autentimisseansi jaoks sobiv `aud` väärtus (`redirect_uri`).

Kogutud andmetest tuleb koostada samasugune päis ja last ning kontrollida standardteegiga, kas esitatud autentimissignatuur on loodud nendele andmetele ning selle privaatvõtmega, mis vastab kasutaja isikusertifikaadile. Kasutaja sertifikaat tuleb hankida autentimissignatuuri päise väljast `x5c`.

5.3 Liidestusprotokoll autentimisvahendite kasutamiseks

Jaotis 5.1 kirjeldas liidestusprotokolli, kus RP suunab kasutaja agendi (brauseri või mobiiliäpi) autentimisteenusesse, mis siis korraldab tegeliku autentimise. Kui RP soovib kasutada autentimisvahendit „otse“, siis on vajalik kasutada autentimisvahendite tarkvarakomponentide pakutavat APIt. Siin jaotises kirjeldame täpsemalt, millist APIt peavad autentimisvahendid pakkuma ning kuidas selle kasutamine käib.

Siinse jaotise eesmärgiks on kirjeldada üldistatud mudelit, nii et kui tulevikus tekib ID-kaardi kõrvale mõni teine kasutaja brauseri poolt „otse“ kasutatav autentimisvahend (näiteks FIDO2-ühilduv autentimisvahend) või mõni ID-kaardiga autentimist realiseeriv teistsugune



Joonis 7: RP ja Web eID komponentide skeem

tarkvaralahendus (näiteks ID-kaardiga üle NFC-liidese suhtlev mobiilirakendus), siis saaks järgida sama liidestusprotokolli.

Liidestusprotokolli kirjeldame lahenduse Web eID eeskujul. Joonisel 7 on toodud komponentskeem RP ja autentimise alamsüsteemi Web eID komponentidega.

5.3.1 Autentimisvahendi kasutamise sammud

Autentimisvahendiga autentimine koosneb tabelis 9 toodud sammudest. Tabelis olevad sammud on seostatud ka üldise autentimisprotsessi skeemiga joonisel 2.

Tabel 9: Kasutaja autentimise sammud autentimisvahendi kasutamisel.

#	Tegija	Samm	Sõnumi nr joonisel 2	Kirjeldav jaotis
1.	RP	Autentimispäringu koostamine ja edastamine	2	5.3.3
2.	Autentimis-vahend	Autentimise läbiviimine	3, 4 ja 5	5.3.4
3.	Autentimis-vahend	Autentimispäringu vastuse ja autentimissignatuuri koostamine ja tagastamine	6	5.3.5
4.	RP	Autentimispäringu vastuse ja autentimissignatuuri valideerimine	7	5.3.6
5.	RP	Isikuandmete hankimine	8 ja 9	5.3.7

5.3.2 Autentimisvahendi kasutamise seadistamine

Kuigi autentimisvahendiga liidestumiseks ei pea RP kelleltki spetsiaalset luba taotlema ega kusagil registreeruma, siis ikkagi on vajalik läbi viia järgmised ühekordsed seadistused.

1. RP integreerib oma veebirakendusega autentimise alamsüsteemi teegid (Web eID puhul näiteks teegid Java ja JavaScript programmeerimiskeeltele).
2. RP seadistab veebirakenduse usaldama konkreetseid CAsid, kes väljastavad autentimisvahenditega seotud isikusertifikaate.
3. RP seadistab veebirakenduses kasutatavad veebiaadressid ja domeenid.
4. RP täiendab oma veebirakendust, et ta kasutaks autentimise läbiviimiseks autentimisteegi poolt pakutavat API-t.

5.3.3 Autentimispäringu koostamine ja edastamine

RP veebirakendus peab koostama autentimispäringu, kus on järgmised andmed:

1. `challengeNonce` – RP veebirakenduse brauseris töötav komponent peab serverist ise hankima selle seansi jaoks genereeritud nonsi (pretensiooni), mis kaasatakse autentimisvahendiga allkirjastatud andmete hulka. Eesti autentimisprotokollistikus `nonce` väli.
2. `options` – autentimise juhtimiseks vajalikud seadistused, näiteks kasutajaliidese keel jms. Eesti autentimisprotokollistikus näiteks `ui_locale` väli.

5.3.4 Autentimise läbiviimine

Autentimise käivitamiseks peab RP veebirakendus välja kutsuma autentimisvahendi API vastava meetodi, mille sisendiks on 5.3.3 jaotises kirjeldatud väljad.

Näiteks olemasoleva Web eID korral `webeid.authenticate(challengeNonce, options)`. Muud autentimisvahendid ja -teegid peavad pakkuma sarnast API-t.

Autentimisteek teeb seejärel järgmised tegevused:

1. hangib usaldusväärsel viisil brauseri käest kasutajale kuvatud veebisaidi aadressi (`origin`)
2. kuvab kasutajale dialoogiakna, milles kasutaja saab otsustada, kas ta nõustub RP veebirakenduse sooviga kasutajat autentida
3. vormindab signeerimisele minevad andmed ning saadab selle andmestruktuuri räsi ID-kaardile signeerimiseks
4. kui kasutajal on klahvistikuga ID-kaardi lugeja, palutakse kasutajal sisestada PIN-kood lugeja klahvistikuga, vastasel korral küsib autentimisteek PIN-koodi arvuti klaviatuurilt ning saadab PIN-koodi ID-kaardile koos räsiga.

5.3.5 Autentimispäringu vastuse koostamine

Peale autentimise läbiviimist peab autentimisteek koostama autentimispäringu vastuse ning vormindama autentimissignatuuri. Tehniliselt on selleks palju erisuguseid võimalusi, järgmistes jaotistes kirjeldame süsteemi Web eID ning siin analüüsis eelnevalt kirjeldatud ettepanekut.

5.3.5.1 Autentimissignatuur süsteemis Web eID

Web eID koostab[14] autentimispäringu vastuse, mille näide on kuval 5.14.

Näide 5.14: Lahenduse Web eID autentimispäringu vastus

```
{
    "unverifiedCertificate": "MIIFozCCA4ugAwIBAgIQHFpdK-zCQsFW4...",
    "algorithm": "RS256",
    "signature": "HBjNXIaUskXbfhzYQHvwjKDUWfNu4yxXZha...",
    "format": "web-eid:1.0",
    "appVersion": "https://web-eid.eu/web-eid-app/releases/v2.0.0"
}
```

Väljas `unverifiedCertificate` esitatakse kasutaja isikusertifikaat. Sellise nimega väli tähendab, et tegemist ei ole usaldusväärse sertitifikaadiga, vaid üksnes abistavate andmetega, et viia läbi täiendavaid kontrolle.

Väljas `algorithm` esitatakse kasutatud signeerimisalgoritmi nimi ning väljas `signature` esitatakse autentimissignatuur. Kasutatakse jaotises 5.2.4.1 kirjeldatud lihtsamat lahendust autentimissignatuuri formaatimiseks ning seal on väärtus `SIGN(hash(origin)+ hash(challenge))`.

Väljas `format` esitatakse autentimispäringu vastuse vormingu versioon ning väljas `appVersion` esitatakse päringuvastuse koostanud tarkvarakomponendi versioon.

5.3.5.2 Universaalne autentimissignatuuri vorming

Käesolev analüüs soovitab kasutada standardipõhiseid lahendusi andmete vormindamiseks ning teha seda samamoodi nagu on kirjeldatud jaotises 5.2.4.2. Andmetest eraldatud JWS signatuuri kasutamisel on samad omadused nagu Web eID lähenemisel:

1. RP peab signatuuri alla kaasatud andmed lugema enda andmehoidlast (`nonce`, `aud`)
2. Signatuuri alla on võimalik lisada ka veebisaidi HTTPS sertifikaadi räsi kui autentimisvahend selle kuidagi brauserist kätte saab. Sellisel juhul tuleb kokku leppida täiendav autentimissignatuuri tüüp, näiteks `web-eid-with-rp-cert:1`. Veebisaidi HTTPS sertifikaadi räsi lisamine võimaldab teenusepakkujal tuvastada keerukama ründe, kus ründajal on õnnestunud kasutaja brauser veenda usaldama ründaja sertifikaati ning kuvama ründaja lehte korrektse domeenina. See meede tuvastab ka mõnedes asutustes legitiimselt kasutatavaid HTTPS SSL proksisid. Kas sedalaadi prokside kasutamine on normaalne või viitab vahemeheründele, pole RP-l võimalik kindlaks teha.

Lisanduvad veel järgmised eelised, mida Web eID vormingul ei ole:

1. Kasutatakse standardipõhist formaati, mida saab genereerida ja valideerida riiulitarkvaraga.
2. Automaatselt on toetatud kõik standardis JWA loetletud signeerimis- ja räsimisalgoritmid.
3. Signatuuri alla lisatakse autentimisvahendi poolt genereeritud juhuslikkust (`jti`), mis aitab vähendada võimalust, et autentimisvahend töötab krüptograafilise oraaklina ning

[14] https://web-eid.github.io/web-eid-system-architecture-doc/web-eid-auth-token-v2-format-spec.pdf

pahatahtlik RP suudab ennustada signeerimisele minevate andmete sisu ning võib-olla autentimissignatuuri taaskasutada või manipuleerida.

5.3.6 Autentimispäringu vastuse ja autentimissignatuuri valideerimine

Autentimispäringu vastuse valideerimisel peab RP tegema järgmised üldised sammud:

1. Kontrollima, kas autentimispäringu vastus ja autentimissignatuur on loodud õige autentimiseansi kohta. Selleks tuleb leida seansiandmete hoidlast õige seanss ning hankida seansiandmete hulgast eelnevalt genereeritud `challengeNonce` ehk `nonce`, konstrueerida autentimissignatuuri alla läinud andmed ning kontrollida signatuuri kehtivust.
2. Kontrollima, kas autentimispäringu vastus ja autentimissignatuur on loodud õige RP ja õige veebirakenduse jaoks. Selleks tuleb hankida konfiguratsioonist veebirakenduse domeen ning konstrueerida autentimissignatuuri alla läinud andmed ning kontrollida signatuuri kehtivust.
3. Kontrollima, kas autentimissignatuuri teinud autentimisvahendi sertifikaat on usaldusväärne (väljastatud usaldusväärse CA poolt), et sertifikaat ei ole aegunud ega tühistatud. Viimase kontrollimiseks tuleb kasutada CA poolt pakutavaid teenuseid, näiteks CRL nimekirjad või OCSP teenus.

Süsteemi Web eID autentimisteek `web-eid-authtoken-validation-java` pakub kõigi kolme kontrolli jaoks abifunktsiooni `tokenValidator.validate(token, challengeNonce)`, kus `token` on autentimissignatuur. Funktsioon tagastab autentimises kasutatud autentimisvahendi sertifikaadi, millest veebirakendus saab välja lugeda kasutaja identiteedi.

5.3.7 Isikuandmete hankimine

Peale seda, kui kõik eelmises jaotises kirjeldatud kontrollid on läbitud, saab RP alles järeldada, et autentimissignatuuri päise väljalt `x5c` saadud isikusertifikaadi väljas `Subject` olev identifikaator on tõene selle autentimisseansi käigus autenditud isiku identiteet.

5.3.8 Kasutamise näide

Detailne näide, kuidas saab autentimist korraldada kui kasutada autentimisvahendit läbi autentimise teegi, on toodud joonisel 8.

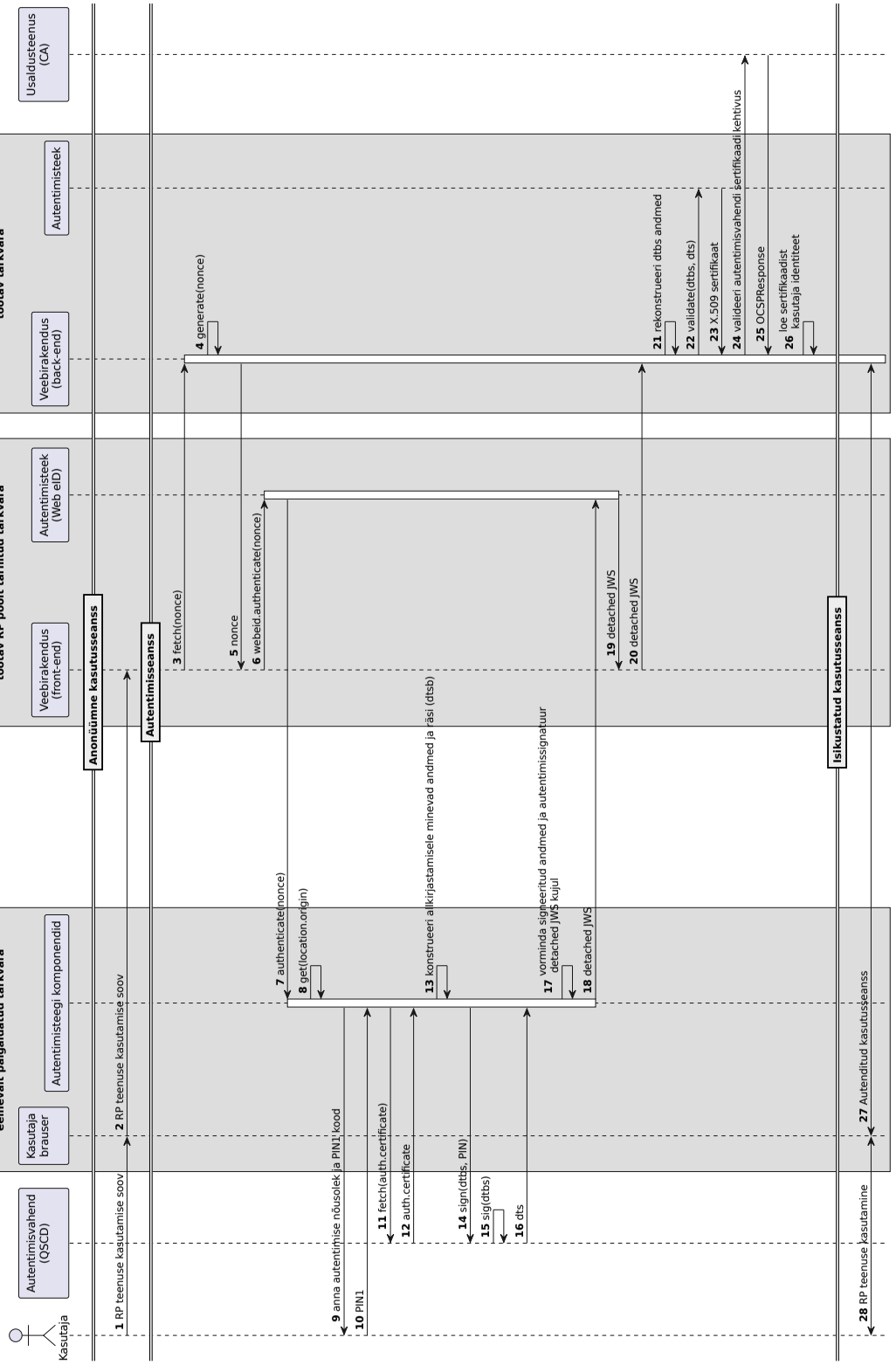
5.4 Autentimisprofiili rakendatavus ja ühilduvus

5.4.1 Autentimisteenuse TARA erisused

TARA praegune teenus[15] erineb väljapakutud Eesti autentimisprofiilist. Olulisemad erisused on järgmised:

1. TARA ei toeta autentimispäringu objekti eraldi edastamist ning objekti viite edastamist päringu-URLis (RFC9126) ning turvameetme PKCE kasutamist.
2. TARA ei nõua autentimispäringu välja `nonce` täidetust.
3. TARA ei võimalda autentimissignatuuri edastamist RP'ni ning ei täida seega dünaamilise autentimise nõuet `EE.DYNAMIC`.

[15] `https://e-gov.github.io/TARA-Doku/TehnilineKirjeldus`



Joonis 8: Autentimisvahendi kasutamise näide

4. Isikuandmete tõendis ei kasutata ETSI standardi EN319-412-1 kohast identifikaatorit (näiteks ETSI:PNOEE-38001085718)

5. TARA ei toeta välja `login_hint` kasutust ning väljade `acr_values` ning `amr` sisu tuleks muuta.

6. TARA ei vasta kunagi `scope` väljaga vastuses, kui see erineb sellest, mida päriti. Nt. kui autentimispäringu väljas `scope` oli `email` aga autentimise käigus ei õnnestunud kasutaja e-posti aadressi välja selgitada. See on vastuolu OIDC standardi jaotisega 3.1.3.3 ning RFC6749 jaotistega 3.3, 4.1.4, 5.1.

7. TARA lubab `scope` väljas määrata lubatud autentimisvahendeid. Soovitame sellest loobuda.

Kui soovida Eesti autentimisprofiili rakendada autentimisteenusele TARA, siis tuleks TARA tunduvalt edasi arendada.

5.4.2 Autentimisteenuse GOVSSO erisused

GOVSSO pakub ühekordset sisselogimise teenust. Sisuliselt on tegu eraldi OIDC teenusega, mis delegeerib autentimise protseduuri TARA autentimisteenusele ning pakub SSO funktsioonidena lisaks seansi värskendamise ja väljalogimise API-sid.

SSO funktsioonid ei ole väljapakutud Eesti autentimisprofiili skoobis. GOVSSO poolt realiseeritud täiendused, võrreldes teenusega TARA, on samamoodi rakendatavad ka sellisel juhul, kui teenus TARA töötaks vastavalt Eesti autentimisprofiili kavandile. GOVSSO-st ongi mõistlik mõelda kui ühest protokolli OIDC profiilist.

Kui Eesti autentimisprofiili soovida rakendada teenusele GOVSSO, siis on üldjoontes vaja teha sarnaseid muudatusi nagu ka TARA korral. Isegi vähem, sest näiteks GOVSSO juba praegu ei luba väljas `scope` määrata autentimisvahendeid.

5.4.3 Mobiil-ID ja Smart-ID teenuste erisused

Mobiil-ID ja Smart-ID autentimisteenused kasutavad praegu firmapärast API-t, mis ei ole OIDC protokolliga ühilduv. Kui Eesti autentimisprofiili soovida rakendada Mobiil-ID ja Smart-ID autentimisteenusele, siis tuleks nende teenuste API täiesti uuesti ehitada.

Praktilisem lahendus on Mobiil-ID ja Smart-ID teenusepakkujal pakkuda OIDC portaali oma API-de ees, mis pakub Eesti autentimisprofiiliga OIDC protokolli.

5.4.4 eIDAS autentimisvõrgustik

EU määruse [17] alusel loodud eIDAS autentimisvõrgustik koosneb liikmesriikides töötavatest eIDAS-sõlmedest, mis vahendavad liikmesriikide vahel autentimispäringuid ning autentimisvastuseid. Võrgu sõlmed kasutavad sisemiselt nende sõnumite edastamiseks ning turvamiseks protokolli SAML.

Eesti autentimisteenuste profiil ning eIDAS autentimisvõrgustik ei ole omavahel ühilduvad ega kattuvad. Juhul, kui Eesti RP tellib mõne teise liikmesriigi füüsilise isiku autentimist, siis peab Eesti eIDAS-sõlm tegema ära vajaliku tõlkimise Eesti autentimisprotokollistiku sõnumite ning eIDAS autentimisvõrgustiku sõnumite vahel.

Lisaks tõlkimise probleemile, tekib eIDAS autentimisvõrgustikku kasutades veel lisaks probleem, et eIDAS võrgustik ei toeta läbivat turvalisust ega kasutaja autentimisvahendi signatuuri edastamist. See tähendab, et Eesti RP peab liikmesriigi füüsilist isikut autentides tahes tahtmata usaldama Eesti eIDAS-sõlme ning liikmesriigi eIDAS-sõlme ning ta ei saa tugineda ainult liikmesriigi väljastatud autentimisvahendi turvalisusele. See aga tähendab, et

tegelikult on eIDAS-sõlmedel üli-kriitiline roll. Nende pahatahtlikul ülevõtmisel saaks esitada võltsitud isikuandmete tõendeid suvalise EU kodaniku kohta.

Me ei näe hetkel tehnilisi võimalusi, kuidas seda olukorda parandada ning loodame, et eIDAS regulatsiooni järgmine versioon eIDAS2 ning EUDIW (digikukru) arendamine võib ehk siinkohal aidata.

6 Täiendavad ning uudsed õngitsusrünnete vastased meetmed

Siin jaotises kirjeldame võimalusi, kuidas Eestis kasutusel olevad autentimisteenused või -vahendid saaksid suurendada ründekindlust vahemeherünnete ning õngitsusrünnete vastu.

Enamik nendest võimalustest ei ole rakendatavad kõigil kasutusjuhtudel, nad ei anna täielikku ründekindlust, nende rakendamine võib olla seotud täiendavate riskidega või valepositiivsete tulemustega ning nende rakendamine võib vajada hoolikat plaanimist, reguleerimist ning jälgimist. Seetõttu ei saa neid meetmeid soovitada kohustuslikena, kuid osadel juhtudel on neid siiski mõistlik kaaluda.

6.1 Taasesitusründed ja nendega seotud tähelepanekud

Õngitsusründed ning taasesitusründed võivad olla probleemiks paljudes kohtades. Eestis kasutusel olevad autentimisprotokollid peavad olema turvalised ning selliste rünnete eest kaistud nii isoleeritud olukordades kui ka üksteisega kombineerituna. See tähendab lisakohustusi nii autentimisteenuste pakkujatele kui ka -teenuste kasutajatele.

6.2 Serveripoolsed võimalused

6.2.1 Brauseri ja autentimisvahendi aadressi võrdlemine

Kui autentimisvahendina kasutatakse eraldiolevat seadet (Mobiil-ID, Smart-ID või mõni muu telefonil põhinev vahend), kuhu saadetakse autentimispäring, siis saab OP (vajadusel koostöös RP-ega) võrrelda kasutaja agendi (brauseri või mobiilirakenduse) ning kasutaja autentimisvahendi IP-aadressi või asukohta.

See aitab üsna tüüpilise õngitsusründe korral (vt ka `R.MITM-RP`), kus ründaja ühendub RP teenusega oma brauserist ning alustab RP teenuses kasutaja nimel autentimisseanssi. Kasutaja autentimisseadmesse saabub autentimispäring ning kui kasutaja ei ole küllalt hoolikas, siis võib ta segadusse sattuda ning kinnitada ründaja poolt algatatud autentimisseansi. Sellist olukorda aitaks avastada just nimelt autentimise algatanud agendi ja autentimisvahendi asukoha võrdlemine. Kui asukoht on kardinaalselt erinev, siis tuleks autentimisseanssi käsitleda riskantsemana ning potentsiaalse ründeolukorrana.

Kuigi võrdlemise idee on lihtne, siis selle praktiline teostamine vajab päris mitme asjaolu kaalutlemist:

1. Andmekaitse – Juhul, kui OP ei suuna kasutaja brauserit RP teenusesse, siis peab OP kasutaja IP-aadressi ja/või tuvastatud asukoha spetsiaalselt RP-le edastama. Või siis vastupidi - RP peab peale autentimist spetsiaalselt edastama autentimisvahendi IP-aadressi ja/või tuvastatud asukoha OP-le. Kuna IP-aadress ja asukoht on isikuandmed, siis tuleb sellisest andmete omavahelisest jagamisest ja töötlemisest kasutajat andmekaitsetingimustes teavitada. Praeguses analüüsis soovitatud autentimisprotokollistik eeldab, et kasutaja brauser suunatakse OP teenusesse. Sellisel juhul jõuab kasutaja brauseri IP-aadress ja asukoht tahes-tahtmata ka OP-ni ning olukord on veidi lihtsam. OP-le jääb aga endiselt teavituskohustus ning andmekaitsetingimuste täiendamise vajadus.

2. Valepositiivsed juhud – Brauseri või telefoni IP-aadressi tuvastamine ei anna alati õigeid tulemusi ning näiteks ettevõtete privaatvõrkude, prokside, VPN-ide jms vahendite tõttu võib juhtuda, et kuigi arvuti ja telefon on sama kirjutuslaua peal, siis nende ühendus OP teenustega liigub mööda täiesti erinevaid kanaleid ja erinevad IP-aadresse kasutades. Seetõttu ei saa ainult IP-aadresside võrdluse alusel autentimistulemust kindlalt tühistada ning tuleb kasutada graduaalset ning riskipõhist lähenemist.

3. Kasutaja alarmeerimine – RP ja OP seisukohast on mugavaks lahenduseks kuvada kasutajale täiendav hoiatus kui OP on avastanud brauseri ja autentimisvahendi asukohaerinevuse. Sellise meetme rakendamisel tuleb kasutajate testrühmaga kontrollida, kas nad saavad hoiatusest aru ning kas nad reageerivad hoiatusele õigesti. Senine infoturbepraktika on näidanud, et veebisaitide HTTPS sertifikaatide hoiatustele kasutajad tähelepanu ei pööra ning pigem ignoreerivad seda. Seetõttu tuleks sellise asukohaerinevuse hoiatuse sõnumit ning kasutajale pakutavaid valikuid väga hoolikalt plaanida ning nende efektiivsust jälgida.

4. Täiendavate meetmete valmisolek – Kui IP-aadresside võrdlemise järel leitakse, et see on riskantne autentimisseanss, siis peab OP või RP olema valmis rakendama mingit lisameedet, mis annaks täiendava kindluse kas siis autentimise tühistamiseks või vastupidi - autentimistulemuse aksepteerimiseks. Mõningate äriprotsesside puhul on võimalik kasutusele võtta näiteks tehingu limiite või muid riske vähendavaid meetmeid, kuid see ei ole universaalne ning ei ole kõikjal rakendatav.

6.2.2 Brauseri või mobiilirakenduse eksemplaride jälitamine

Kui autentimise käigus suunatakse kasutaja brauser OP teenusportaali, siis tehniliselt on võimalik brauserite eksemplare küpsiste ja muude vahenditega jälitada ning seeläbi autentimise käigus kontrollida, kas *see* kasutaja on varasemalt *seda* brauserit edukalt kasutanud. Kui jah, siis saab OP järeldada, et see on väikse riskiga autentimisseanss, kuna kasutaja kasutab samasugust seadet nagu ka eelmistel kordadel. Kui ei, siis võib endiselt tegemist olla sama kasutajaga, kes lihtsalt kasutab seekord esimest korda oma uut arvutit või uut brauserit, kuid on ka võimalus, et see on ründaja, kes on kasutaja nimel alustanud autentimiseanssi enda brauseriga. OP asemel võib jälitamist teostada ka RP.

Samalaadset loogikat saab rakendada ka mobiilirakenduste korral. Tõsi küll, seda ainult koostöös RP-de ja OP-de vahel. Kui RP mobiilirakendus suunab kasutaja OP mobiilirakendusse, siis saab RP lisada eksemplari identifikaatori ning OP saab jälitada, millisest rakendusest ja millisest rakenduse eksemplarist see päring tuli. Kui kasutaja ajaloost lähtub, et ta on varem edukalt sama rakenduse eksemplari autentimisel kasutanud, siis on tegemist madalama riskiga olukorraga.

Nagu eelmises jaotises kirjeldatud meetme puhul, on ka jälitamise rakendamine väga paljude tahkudega:

1. Andmekaitse – Brauserite ja äppide erinevate eksemplaride jälitamine tuleb kasutajatingimustes ning andmekaitsetingimustes kasutajale selgelt avaldada ning seda saab teha vaid tema nõusolekul. See tähendab, et osad kasutajad loobuvad sellisest võimalusest ning nende puhul peab autentimisprotsess töötama endist viisi. Seega ei saa jälitamise rakendamine olla 100 protsendiliselt efektiivne.

2. Uute brauserite käsitlemine – Sellised olukorrad, kus kasutaja hakkab autentimisteenust kasutama mõnest seadmest esmakordselt, tuleb korrektselt lahendada. Jällegi on RP-de ja OP-de jaoks mugav lahendada see olukord täiendava kasutajadialoogiga ja täiendava küsimusega (nt „*Kas te olete praegu arvutis, mida te ei ole kunagi varem selle autentimisvahendiga kasutanud?*“), kuid see tuleb põhjalikult läbi katsetada ja veenduda, et kasutajad saavad nendest dialoogidest õigesti aru ning käituvad vastavalt.

3. Täiendavate meetmete valmisolek – Jällegi, kui jälitamise kasutamisel selgub, et see on riskantsem autentimisseanss, siis peab OP või RP olema valmis rakendama mingit lisameedet, mis annaks täiendava kindluse kas siis autentimise tühistamiseks või vastupidi - autentimistulemuse aksepteerimiseks.

6.3 Veebilehe aadressi kontrollimine autentimisvahendis

Üks põhilisi probleeme õngitsus- ja vahemeherünnete puhul on see, et kasutajale on pandud kohustus ja vastutus veenduda, et ta on RP õigel veebilehel või RP õiges mobiilirakenduses. Juhul, kui kasutaja ei ole küllalt hoolikas ning eksib, siis võib ta sattuda ründaja veebilehele ning alustada autentimist sealt.

Kõige lihtsamal juhul on ründaja registreerinud eraldi domeeni, mis võib kasutajale tunduda usaldusväärne või sarnane (`https://www.eesti.ee` või `https://www.eesti-valitsus.com`) ning teda meelitatakse sealt autentimist alustama. Samal ajal alustab ründaja kasutaja nimel autentimist õigel RP veebisaidil. Kasutaja ei pane erisust tähele ning kinnitab oma Mobiil-ID või Smart-ID autentimisvahendis ründaja algatatud autentimispäringu.

Olukorda saaks parandada, kui brauser „informeeriks“ autentimisvahendit, millise aadressiga veebisait on kasutajale kuvatud ning autentimisvahend saaks kasutaja eest selle kontrollimise (kas RP saadetud autentimispäring on seotud brauseris kuvatud veebilehega) ära teha. Põhimõtteliselt samamoodi käituvad näiteks FIDO autentimisvahendid ning ka ID-kaardiga autentimislahendus Web eID, kus brauser edastab veebilehe `origin` väärtuse autentimisvahendile ning autentimisvahend kaasab selle autentimissignatuuri alla. RP saab vastuse saamisel kontrollida, kas autentimissignatuur on ikka temale mõeldud ning terve hulk õngitsus- ja vahemeheründeid muutub tunduvalt raskemaks.

Järgnevas jaotises uurime võimalusi, kuidas saaks brauseritega sellise sidekanali luua. Probleemi uurimisel tuleb arvestada kahte tahku:

1. Kuidas tagada väärtuse `origin` usaldusväärsust ning vältida ründaja poolt selle võltsimist või taasesitamist?
2. Mis sidekanalitega saab seda väärtust `origin` edastada?

6.3.1 Kasutajale kuvatud veebisaidi aadressi tuvastamine

Veebisaidi aadressi hankimiseks on palju võimalusi. Osad võtted on ründekindlamad ning siin jaotises anname nendest ülevaate.

6.3.1.1 Serverist saadetud info

Kõige lihtsam võimalus on kasutada veebisaidi serveris olevat infot selle kohta, mis aadressil veebisait töötab. See on serveris töötavatele komponentidele lihtsalt kättesaadav ning nad saavad selle info veebisaidi HTML või JS koodis kasutaja brauserisse edastada. Kahjuks ei ole aga mitte kuidagi võimalik tagada, et vahemehe ründe teostaja ei kopeeriks veebisaidi lähtekoodis esitatud infot enda veebisaiti ning ei esitaks seda omakorda kasutaja brauserisse. Seetõttu ei ole see võimalus vahemeheründe tõkestamiseks sobiv.

6.3.1.2 JavaScript

Järgmiseks on võimalik kasutada brauserite poolt pakutavaid API-sid, et pärida `origin` väärtust kohapealt, brauseri enda käest. Ka see lahendus ei ole ründekindel, kuna vahemeheründe käigus saab ründaja lisaks RP veebisaidi lähtekoodi kopeerimisele ka koodi modifitseerida ning täiendada. Ründaja saab lisada võltsitud veebisaidile JS koodi, mis ei küsi `origin` väärtust brauserilt, vaid kasutab ründaja poolt eelkodeeritud „korrektset“ väärtust. Seetõttu ei ole ka see võimalus vahemeheründe tõkestamiseks sobiv.

6.3.1.3 Turvatud JavaScript

Veel üks variant on püüda brauseris käivitatavat JS koodi kuidagi kaitsta, et ründajal oleks seda keerulisem modifitseerida. Näiteks on võimalik kasutada JS koodi minimeerimist, sogastamist või muid vahendeid. See võib väiksemate kogemustega ründajaid tõepoolest heidutada ning nende ründe teha mõnevõrra keerulisemaks ning ettevalmistamise veidi ajamahumaks.

Siiski on selge, et pikemas perspektiivis ei saa need vahendid olla võimekamate ründajate vastu efektiivsed. RP või autentimisteenuse pakkuja peab olema valmis rünnete ilmnemisel kiirelt reageerima, oma kaitsetaktikat muutma ja vajadusel täiendavaid turvameetmeid rakendama.

6.3.1.4 Brauseri laiendus

Kui me saame kasutaja brauserisse paigaldada brauseri laiendusi, siis saab juba laiendus ise kasutada teistsuguseid API-sid, mis võimaldavad laiendustel küsida brauseri käest kuvatava veebilehe aadressi. Veebisaidi JS kood peab sellisel juhul saatma ainult sõnumi autentimisprotsessi algatamise kohta ning laiendus korraldab ülejäänu.

Web eID on üheks selliseks näiteks, mille puhul on vajalik kasutaja arvutisse paigaldada nii brauseri laiendus (`web-eid-webextension`) kui ka spetsiaalne rakendus (`web-eid-app`), mis oskab kasutaja käest küsida PIN-koodi ning üle USB-liidese ID-kaardiga sidet pidada.

Selline lahendus annab tunduvalt parema ründekindluse. Juhul, kui kasutaja arvutis on selline brauseri laiendus juba paigaldatud ning sideprotokoll võimaldab autentimisvahendil kontrollida, kas talle edastatud sõnum on pärit autentsest laiendusest, siis ei saa võrgus tegutsev MITM-ründaja enam seda olukorda võltsida ega taasesitada.

Kui kasutajal ei ole aga veel brauseri laiendust paigaldatud, siis saab ründaja realiseerida laienduse funktsioonid ka võltsitud veebisaidi JS koodis ning sedaviisi kasutaja autentimisvahendile laiendust teeselda. Seda juhul, kui brauseri laiendus ja autentimisvahend kasutavad sellist sideprotokolli, mis on kättesaadav ka ründaja JS koodile. Juhul, kui sideprotokolli kasutamiseks peab ründaja realiseerima enda laienduse, siis peab ta lisaks veel kasutaja meelitama võltsitud laiendust paigaldama.

6.3.1.5 WebAuthn

WebAuthn [30] on W3C standard ning brauserites laialdaselt[16] realiseeritud API, mis võimaldab veebisaitidel kasutada läbi brauseri kättesaadavaid autentimisvahendeid. WebAuthn API-t kasutades on võimalik veebisaidil välja kutsuda brauseritesse sisseehitatud kood, mida ründaja ei saa mõjutada ning mis võimaldab üle CTAP (*Client to Authenticator Protocol*) protokolli edastada veebisaidi aadressi.

Protokoll seab küll erinevaid piiranguid ning ei ole mõeldud töötama tavapärase PKI-põhise autentimisvahendiga, kuid selle tugi on enamikesse brauseritesse sisse ehitatud ning seda kasutades saaks autentimisvahend teada, millisel veebilehel olles autentimist alustati.

WebAuthn korral luuakse iga RP jaoks autentimisvahendis unikaalne võtmepaar. RP ülesanne on salvestada avalik võti ning siduda see kasutaja kontoga. PKI ehk sertifikaadid puuduvad, igal kasutajal on üks kuni mitu võtit iga RP jaoks. Kui aga autentimist ei teosta iga RP ise, vaid kasutatakse näiteks ühist autentimisportaali, siis oleks vaja WebAuthn võtmete registreerimisprotseduur läbi teha ainult ühise autentimisportaali jaoks.

Mobiiliseadme rakenduses realiseeritud autentimisvahend võib lisaks oma PKI-põhisele autentimisvõtmele genereerida WebAuthn võtmed iga RP/autentimisportaali jaoks ning kasutada WebAuthn protokolli vähemalt ühte liiki vahemeherünnete ära hoidmiseks.

[16] `https://fidoalliance.org/fido2/fido2-web-authentication-webauthn/`

6.3.2 Brauseri ja mobiili vahelise sidekanali võimalused

6.3.2.1 QR-koodi skaneerimine

Üheks kõige lihtsamaks sidepidamise kanaliks on ehk võimalus kuvada veebilehel masinloetav QR-kood (*QR code*) ning lugeda seda mobiiltelefoni kaameraga. Veebisait saab QR-koodis esitada näiteks seansi identifikaatorit ja/või veebilehe aadressi ning telefonis töötav autentimisvahend saab seda lugeda. Rootsi Bank-ID lahendus kasutab isegi dünaamilisi QR-koode,[17] mida uuendatakse iga sekund ning mis suurendab edastatavat infohulka ning teeb ründajale QR-koodi kopeerimise veidi raskemaks.

QR-koodi kasutamine võib olla osadel juhtudel otstarbekas, lihtne ning odav lahendus. Sellel lahendusel on aga järgmised puudused:

1. QR-koodi skaneerimine annab ainult ühesuunalise sidekanali. Vastuste jaoks peab kasutama mingit täiendavat sidekanalit.

2. Veebisaidi poolt genereeritud QR-koodi edastamine toimub kanalisisese sidega (versus ribaväline side) ning ta kuvatakse kasutajale koos ülejäänud veebisaidi sisuga. Ründaja, kes saab kasutajale enda veebisaidis vahendada RP veebisaidi sisu, saab samamoodi vahendada ka genereeritud QR-koodi, ükskõik, kas see QR-kood genereeritakse pildi kujul veebiserveris või JavaScript koodi poolt veebibrauseris. Isegi kui QR-koodi genereerib brauseri laiendus ning kuvab selle brauseri aknas, ka siis on ründajal võimalus põhimõtteliselt see kopeerida, kasutades näiteks tervet virtualiseeritud operatsioonisüsteemi. Seetõttu ei ole QR-koodiga võimalik õngitsusründeid täielikult vältida. Jah, neid saab teha ründajale veidi raskemaks (näiteks kasutades dünaamilist QR-koodi) ning rünnetest saab välistada sellised teenuskanalid, näiteks telefonikõne, kus ei saa visuaalset infot edastada.

3. QR-koodi saab kasutada ainult juhul, kui kasutaja brauser ja autentimisrakendus töötavad erinevates seadmetes, näiteks lauaarvutis ning mobiiltelefonis. Kui kasutajal on ainult üks seade, näiteks ta kasutab nutitelefonis RP mobiilirakendust ning autentimisrakendust, siis ei saa ta mitte kuidagi autentimisrakendusega oma telefoni ekraani pildistada. Sellisel juhul tuleb kasutada teistsuguseid võimalusi, kuidas samas seadmes töötavad mobiilirakendused saavad omavahel sidet pidada.

4. QR-koodi skaneerimine vajab kasutaja poolt telefonis autentimisrakenduse käivitamist, skaneerimise funktsiooni valimist ning telefoni suunamist arvuti ekraanile. Osad telefonid toetavad QR-koodi skaneerimist ka tavalise pildistamise rakendusega, kuid ka selline kasutusvoog nõuab kasutajalt lisasamme võrreldes praeguse olukorraga. Kasutatavuse uuringutega tuleb veenduda, et sellised täiendavad sammud on kasutajatele vastuvõetavad ning ei vähenda tunduvalt kasutajamugavust.

6.3.2.2 Web NFC, Web USB, Web Bluetooth

Veebibrauserid pakuvad veebisaitidele JavaScriptis kasutamiseks mitmesuguseid Web-perekonna API-sid.[18] Neist telefoniga suhtlemist võimaldavad Web NFC, Web USB, WebHID, Gamepad, Web Bluetooth ja eelnevalt kirjeldatud Web Authentication (WebAuthn) API.

Web NFC on hetkel veel piiratud ainult NDEF (*NFC Data Exchange Format*) sõnumite lugemise ja kirjutamisega. Tulevikus võib see muidugi muutuda. Aruande kirjutamise ajal on ainus brauser, mis toetab liidest Web NFC, Chrome Android.

Web USB API on mõeldud mitte-standardsete USB-seadmetega suhtlemiseks. Standardsete USB-seadmete jaoks on eraldi liidesed WebHID API ja Gamepad API. Spetsiaalselt

[17] https://www.bankid.com/utvecklare/guider/teknisk-integrationsguide/qrkoder
[18] https://developer.mozilla.org/en-US/docs/Web/API

autentimisprotseduuri tarbeks mobiilseadme USB-kaabliga arvutiga ühendamine ei ole tõenäoliselt ei mugav ega alati ka turvaline tegevus.

Web Bluetooth API on mõeldud BLE (*Bluetooth Low Energy*) seadmetega suhtlemiseks. Näiteks võimaldab see veebilehel juhtida BLE valgustit või lugeda kasutaja südamelöögilugejat. BLE protokollis on kaks osapoolt, üks on klient (*Central*) ja teine server (*Peripheral*). Üks klient saab ühenduda mitme serveriga. Serverid on tavaliselt, aga mitte alati, piiratud ühe kliendiühendusega.

Peale ühenduse loomist (*pairing*) võib valikuliselt toimuda ka krüpteeritud ühenduse loomine (*bonding*), kus vahetakse võtmed järgneva turvalise seansi loomiseks (operatsioonisüsteemide vahel, mitte lõpprakenduste).

Telefonid töötavad tavaliselt kliendi rollis, ühendudes paljude seadmetega. iOS ja Android platvormid suudavad töötada ka serveri rollis ning lasevad sedaviisi mõnel teisel teisel kliendil, näiteks PC veebibrauseril, ühenduda telefonis töötava mobiilirakendusega.

Web Bluetooth API on toetud Chromium põhistes brauserites, aga mitte Apple Safaris ega Mozilla Firefoxis.

Kõik mainitud APId on suuresti Google arendatud ning ainuke neist, mida Mozilla on nõustunud toetama, on Gamepad API. Mozilla peab enamikke mainitud APIdest kahjulikeks, kuna nad võimaldavad vigade ja nõrkuste avaldumisel tekitada potentsiaalselt suurt kahju.[19]

Võimalik, et Web Bluetooth API-t arendatakse edasi ning ta muutub aktsepteerivaks ka Mozillale. Seni on aga küsitav, kas turvariskidega APIt peaks kasutama autentimisel. Lisaks on kõik API-d arendusfaasis ning ei ole stabiilsed.

Samuti on kasutaja telefonis töötava autentimisrakenduse ühendamine näiteks avalikuks kasutamiseks mõeldud arvutiga seotud täiendavate riskidega.

Kõik Web-perekonna APId on kasutatavad veebilehtede JavaScript koodi poolt ning see tähendab, et ikkagi on võimalik vahemeherünne, kus ründaja võtab enda kontrolli all olevast brauserist RP poolt loodud sõnumid, transpordib need enda veebisaidi koosseisus kasutaja brauserisse ning edastab need siis telefonile. Vahemeheründe probleemiga Web Bluetooth ei tegele.

6.3.2.3 CTAP

CTAP on WebAuthn standardi pool kasutatav sideprotokoll, mille abil saab kasutada nii NFC, USB kui ka Bluetooth ühendusi. Kui autentimisvahendis realiseerida selle protokolli tugi, siis saaks brauseris kuvatud veebisait lihtsalt teha WebAuthn API funktsiooni kutse ning brauser korraldab ülejäänud tegevused veebisaidi eest ära. Tegemist oleks standardipõhise ning väga turvalise lahendusega, mida kasutatakse FIDO autentimisvahendites ning mille turundamise, arendamise ja testimisega tegelevad globaalsed suurfirmad.

CTAP protokolli kasutamisel Eesti kontekstis on aga järgmised puudused:

1. FIDO autentimisvahendite ja standardiga WebAuthn seotud brauserite funktsioonid, kasutajaliides ning dialoogiaknad arvestavad ainult globaalseid brauseri tootjate huve. Nemad teevad oma otsuseid ning projekteerivad oma kasutajaliidese selliselt, et kasutajal oleks kõige parem kasutada just nimelt FIDO autentimisvahendeid. Kui Eestis liidestatakse protokolle WebAuthn ning CTAP kasutades klassikalisel PKI-l põhinevad autentimisvahendid, siis ei pruugi kõik dialoogiaknad ega veateated olla asjakohased. Näiteks kasutatakse autentimisvahendi tähenduses brauserites praegu sõna *security key*. Erinevad brauserid ja operatsioonisüsteemid kasutavad mõistete jaoks erinevaid termineid ning praegusel hetkel ei ole need dialoogid ka eesti keelde tõlgitud. See tähendaks, et Eesti peaks osalema aktiivselt standardiloomes ning mõjutama W3C ning FIDO standardeid, et brauserite loodav kasutajakogemus sobiks ka PKI-põhiste autentimisvahenditega.

[19] https://github.com/mozilla/standards-positions/issues/95

2. FIDO standardeid väljatöötav konsortsium „FIDO Alliance“ korraldab ka FIDO autentimisvahendite sertifitseerimist. Võib juhtuda, et brauserid ei ole ühel hetkel nõus kasutama selliseid autentimisvahendeid, mis ei väljasta FIDO standardite kohaseid atesteeringuid ning mis ei ole sertifitseeritud seadmete nimekirjas.[20] See tähendab, et kui Eesti autentimisvahendite arendajad võtavad kasutusele protokolli CTAP, siis nad peaksid täiendavalt tegelema ka oma autentimisvahendi sertifitseerimisega. See on täiendav arenduskulu.

6.3.2.4 Brauseri laiendusel põhinev sidevõimalus

Kui kasutaja arvutisse saab lisada tarkvarakomponente või brauseri laiendusi, siis on võimalik kasutusele võtta ükskõik milline sidekanal, eeldusel, et arvuti ja telefonide riistvara seda toetab. Sellisel juhul on valikus nii traadita side lahendused (WiFi, Bluetooth) või näiteks kasvõi ultraheli. Transpordikanali peale on võimalik ehitada juba turvaline krüptograafiline protokoll, mida kasutades saab brauseri laiendus edastada kuvatud veebilehe aadressi autentimisvahendile.

Sellisel lahendusel on üks peamine eelis, võrreldes eelnevate võimalustega:

1. Omatehtud lahendus ei sõltu brauserite poolt veebisaitidele pakutavatest ametlikest sidepidamise APIdest (Web Bluetooth või WebAuthn) ning saab ära kasutada täpselt sellist sidekanalit, mida autentimisvahend kõige paremini toetab. Samuti ei ole enam oluline, kas kõik brauserid ja kõik operatsioonisüsteemide kombinatsioonid sidepidamise API-t toetavad või kas brauserite tehnilises võimekuses aja jooksul midagi muutub. Seetõttu võiks selline lahendus olla töökindlam.

Tuleb aga arvestada järgmiste probleemidega:

1. Lahenduse väljatöötamise kulud on tõenäoliselt suuremad, kui näiteks WebAuthn API-t kasutava lahenduse korral. Luua tuleks igale operatsioonisüsteemile omarakendus, võib-olla isegi erinevatele operatsioonisüsteemi versioonidele erinevad rakendused. Nende komplektide arendamine ning haldamine on täiendav kulu.

2. Lahenduse kohta info levitamiseks ning selleks, et kasutajad üldse kaaluksid oma arvutisse vajaliku lisakomponentide paigaldamist, tuleb läbi viia spetsiaalsed teavituskampaaniad. Kindlasti jäävad alles sellised kasutajad, kes ei soovi seda tarkvara enda arvutisse paigaldada või kelle arvutis see tarkvara millegipärast lihtsalt ei tööta korrektselt. Seetõttu ei oleks sellisele lahendusele tuginev turvameede kunagi 100% efektiivsusega.

3. Kuigi lahendus ei sõltuks brauserite sidepidamise API-dest, siis alles jääb ikkagi sõltuvus API-dest, mis võimaldavad brauserite laienduste paigaldamist ja kasutamist. Need API-d ei ole üle brauserite standardiseeritud ning varasem kogemus ID-kaardi tarkvara arendamise ja toetamisega on näidanud, et brauseritootjad soovivad neid API-sid aasta-aastalt ikkagi muuta. Seetõttu tuleb omatehtud lahenduse puhul arvestada juurde ka pidev moderniseerimise ja täiendamise vajadus, et lahendust muutuvas maailmas käigus hoida.

6.3.3 Kokkuvõte

Jaotistes 6.3.1 ja 6.3.2 kirjeldati mitmeid lahendusi, mis kirjeldavad kuidas autentimisvahendile saaks edastada brauseris kuvatud veebisaidi aadressi ning seeläbi vältida teatud liiki õngitsus- ja vahemeheründe. Tabelis 10 on kokkuvõte, mis loetleb aadressi hankimise võimalusi ning kirjeldab millised sidevõimalused on omavahel kasutatavad. Lisatud on ka kombinatsiooni turvalisuse hinnang:

[20] https://fidoalliance.org/certification/fido-certified-products/

- kombinatsioon on ebaturvaline – me saame kirjeldada praktiliselt läbiviidavaid efektiivseid ründeid sellise turvameetme vastu,
- kombinatsioon on väheturvaline – ründaja peab kulutama rohkem aega ning ressursse, et turvameedet edukalt murda,
- kombinatsioon on turvaline – me ei tea efektiivsed ründeid.

Tuleb tähele panna, et isegi kui QR-koodi kasutamine veebikanalis ei aita sealsamas toimuvate õngitsusrünnete vastu, siis QR-koodi rakendamine veebis võib aidata näiteks telefonikõnedes toimuvate õngitsusrünnete vastu, kuna ründaja ei saa enam nii lihtsasti telefonikõne käigus ohvrile edastada äpi poolt visuaalselt kontrollitavat infot. Sel juhul peaks aga veebikanalis QR-koodi kasutusele võtmine andma midagi kasulikku ka veebikasutajatele endile, näiteks kasutusmugavust, vastasel juhul ei pruugi kasutajad seda omaks võtta.

Kokkuvõtteks paistavad tabelist 10 välja järgmised lahendusvõimalused:

1. Omaloodud laiendus, mis pakub veebisaidile autentimispäringu algatamiseks API-t, saab brauserist kuvatud veebisaidi aadressi ning suhtleb autentimisvahendiga, kas vahendipõhise protokolliga või näiteks protokolliga CTAP.
2. Veebisaidi või autentimisportaali poolt brauserite WebAuthn-kohaste standardfunktsioonide kasutamine ja autentimisvahendi poolt protokolli CTAP toetamine.

Eesti eID ökosüsteemis võetakse juba kasutusele lahendus Web eID ning selle projekti käigus arendatakse välja ka brauseri laiendus ning tegeldakse selle levitamise ja haldamisega. Kuna laiendus on juba olemas, siis tehnilisest seisukohast oleks väga positiivne, kui seesama komponent `web-eid-webextension` oskaks lisaks ID-kaardile suhelda ka näiteks Mobiil-ID ja Smart-ID autentimisvahenditega. Kui seeläbi õnnestuks vähendada Eestis õngitsusründeid ja vahemeheründe kasvõi poole võrra (arvestades, et mitte kõigil juhtudel ei tarvita kasutaja sisselogimiseks eraldi arvutit ning mitte kõik rünnatavad kasutajad ei paigalda endale vajalikku tarkvara, jne), siis võivad kasutajate rahalised kahjud aastas väheneda sadade tuhandete eurode võrra.[21,22]

Veelgi enam, selliste standardipõhiste protokollide kasutamine loob teisigi täiendavaid võimalusi. Näiteks, kui lisada Web eID komponendile `web-eid-webextension` protokolli CTAP kasutamise võimalus, siis tekib Eesti riigil tehniline võimekus kasutada eID autentimisvahenditena ka FIDO autentimisvahendeid. Võib-olla ei ole see vajalik ega kasulik kodanikele väljastatavate tavapäraste isikuttõendavate dokumentide puhul, kuid mingisuguses spetsiifilisemas kasutusjuhus, näiteks riigiametnike töökohustuste käigus autentimise korraldamiseks võib see olla otstarbekas.

6.4 RP mobiilirakenduse ja eID autentimisrakenduse side

Mobiiliplatformides ei ole õngitsus- ja vahemeheründed niivõrd levinud kui veebisaitide korral, kuid põhimõtteliselt on samasugused ründed võimalikud ka mobiilirakenduste korral. Ründaja kontrolli all olev mobiilirakendus võib olla kujundatud samamoodi nagu ehtne RP mobiilirakendus ning kasutajale võib tunduda, et see on õige rakendus. Kui kasutaja alustab autentimist ründaja mobiilirakendusest, siis saab ründaja enda seadmes samal ajal alustada kasutaja nimel autentimist RP mobiilirakenduses. Kasutaja eID autentimisrakendusele saabuv

[21] https://tehnika.postimees.ee/6682958/alatu-skeem-kurjategijad-koorisid-ohvreid-smart-id-pettustega

[22] https://youtu.be/KsdEZ1zybHA?t=2575

Tabel 10: Veebisaidi aadressi hankimise ja sidekanalite kombinatsioonide turvalisus. N/A tähistab mitte-toimivat või mitte-rakendatavat kombinatsiooni.

Side-kanalid	Veebisaidi aadressi allikad				
	Server	JavaScript	Turvatud JavaScript	Brauseri laiendus	WebAuthn
QR-kood	ebaturvaline	ebaturvaline	väheturvaline	väheturvaline	N/A
Web-perekonna APId	ebaturvaline	ebaturvaline	väheturvaline	N/A	N/A
CTAP	N/A	N/A	N/A	turvaline	turvaline
Muu lahendus	N/A	N/A	N/A	turvaline	N/A

autentimispäring tundub kasutajale õige ning ta kinnitab selle. Selle tulemusena loovad ründaja seadmes olev RP mobiilirakendus ning RP tagasüsteem isikustatud kasutusseansi kasutaja nimel.

Kui RP mobiilirakendus ning eID autentimisrakenduse vahel saaks korraldada andmevahetust, siis saaks eID autentimisrakendus veenduda, et see on õige RP ehtne rakendus ning mitte ründaja oma.

6.4.1 Rakenduste sidevõimalused

Android ja IOS platformidel töötavad rakendused spetsiaalses piiratud õigustega liivakastis ning rakenduste võimalused omavahel andmeid vahetada on suhteliselt piiratud. Platformid pakuvad ametliku võimalusena „Universal Links“ ning „App Links“ lahendusi.

6.4.1.1 Universal Links

„Universal Links“[23] on IOS vahend, kuidas üks mobiilirakendus saab käivitada URL-idega identifitseeritud funktsioone, mis asuvad teistes rakendustes. Funktsiooni kutse käigus vahetab IOS aktiivse rakenduse väljakutsutava rakenduse vastu. Kutsele saab lisada parameetreid ning sedaviisi korraldada andmevahetust.

Kasutatavate URL-ide ja väljakutsutavate mobiilirakenduste seosed tuleb RP poolt oma domeenis deklareerida[24] spetsiaalses RP veebisaidis asuva failiga `apple-app-site-association`, mis tuleb publitseerida aadressil `https://www.example-rp.com/.well-known/apple-app-site-association`. Faili sisu näide on kuval 6.1.

[23] `https://developer.apple.com/ios/universal-links/`

[24] `https://developer.apple.com/documentation/Xcode/supporting-associated-domains`

Näide 6.1: IOS rakenduste sidumine RP veebisaidi nimeruumiga

```
{
  "applinks": {
      "details": [
        {
            "appIDs": [ "ABCDE12345.com.example.app",
  "ABCDE12345.com.example.app2" ],
            "components": [
                {
                    "/": "/buy/*",
                    "comment": "Matches any URL whose path starts with /buy/"
                }
                [...]
            ]
        }
        [...]
      ]
  }
}
```

Neid faile kasutab IOS operatsioonisüsteem otsustamiseks, millist mobiilirakendust välja kutsuda ning sedaviisi saab RP kindlaks teha, et päringu-URLi kutse jõuab õigesse rakendusse.

Selliselt väljakutsutavas URL-is saab määrata parameetreid samamoodi nagu tavalistes brauserites kasutatavates URL-ides.

Kutse tegemiseks peab IOS rakendus kasutama `open(_:options:completionHandler:)` või `openURL` API-t.

6.4.1.2 App Links

„App Links“[25] on Androidi platformi lahendus, mille abil rakendused saavad URL-idega välja kutsuda teiste mobiilirakenduste funktsioone.

URL-ide ja rakenduste omavaheliseks sidumiseks nõuab Androidi operatsioonisüsteem faili `assetlinks.json` publitseerimist asukohas `https://www.example-rp.com/.well-known/assetlinks.json`. Faili sisu näidis on kuval 6.2.

[25] `https://developer.android.com/training/app-links`

Näide 6.2: Androidi rakenduste sidumine RP veebisaidi nimeruumiga

```
[
    {
        "relation": ["delegate_permission/common.handle_all_urls"],
        "target": {
            "namespace": "web",
            "site": "https://www.google.com"
        }
    },
    {
        "relation": ["delegate_permission/common.handle_all_urls"],
        "target": {
            "namespace": "android_app",
            "package_name": "org.digitalassetlinks.sampleapp",
            "sha256_cert_fingerprints":
  ["10:39:38:EE:45:[...]:C3:39:FC:FC:8E:C1"]
        }
    }
]
```

6.4.2 Liidestusprotokoll mobiilirakenduste kasutamisel

Kui RP mobiilirakendusest välja kutsuda OP autentimisrakenduse funktsioone (põhimõtteliselt siis saata OP-le autentimispäringut), saame kasutada samasugust autentimisprotokollistikku, nagu RP veebisaitide ning OP autentimisportaalide puhul (5.1). Seda ideed on hakatud nimetama „app2app“ lahenduseks ning täpsemalt kirjeldatakse näiteks OpenID Foundation blogis.[26]

Siin kirjeldame, milliste erisustega tuleks *app2app* lahenduse korral arvestada:

1. Autentimispäringu sisu – Kui veebisaitide korral peab RP kasutama välja `redirect_uri` väärtusena RP veebisaidis olevat URL-i, siis nüüd tuleb selleks väärtuseks kasutada sellist URL-i, millele reageerib RP mobiilirakendus. Muus osas on autentimispäringu sisu samasugune.

2. Autentimispäringu edastamine – RP tagaserver peab autentimispäringu objekti saatma OP-le vastavalt standardile RFC9126 ning saab vastu selle objekti URI. Seejärel peab RP mobiilirakendus kutsuma OP mobiilirakenduses realiseeritud autentimisfunktsioonile viitava URL-i, kasutades mobiiliplatformi vahendeid. URL-ile lisatakse parameetri `request_uri` väärtuse autentimispäringu objekti identifikaator.

3. Autentimine – Peale seda, kui mobiiliplatform on RP rakenduse viinud tahaplaanile, käivitanud OP autentimisrakenduse ning selle kasutaja fookusse toonud, saab OP rakendus autentimispäringu kätte. See päring tuleb edastada OP tagasüsteemile, mis kontrollib autentimispäringu korrektsust ning alustab autentimisseanssi. OP autentimisrakendus viib läbi kasutaja autentimise ning OP tagasüsteem koostab autentimispäringu vastuse.

4. Autentimispäringu vastus – Vastus koostatakse `redirect_uri` põhjal ning sinna URIsse pannakse kaasa volituskood. Kui brauserite puhul toimub brauseri tagasisuunamine RP

[26] https://openid.net/2019/10/21/guest-blog-implementing-app-to-app-authorisation-in-oauth2-openid-connect/

veebisaidile, siis nüüd peab OP mobiilirakendus tegema RP mobiilirakendusse viitava `redirect_uri` kutse.

5. Autentimispäringu vastuse valideerimine – RP mobiilirakendus saab vastuse kätte ning edastab selle RP tagasüsteemile, mis valideerib parameetri `state`.

6. Isikuandmete tõendi päring – RP tagasüsteem teeb OP teenusele samasuguse isikuandmete tõendi päringu nagu autentimisteenuse kasutamisel, saab vastu isikuandmete tõendi, valideerib vastuse ning loob RP mobiilirakenduse ning RP tagasüsteemi vahelise isikustatud seansi.

6.4.3 Mobiilirakenduste eksemplaride jälitamine

Jaotises 6.2.2 kirjeldati, kuidas veebibrauserite eksemplare küpsistega jälitada. Samasugust meetodit saab kasutada ka mobiilirakenduste korral, RP ja OP koostöös selleks, et saavutada täiendavat turvalisust.

RP mobiiilrakendus peab siis genereerima juhusliku identifikaatori, mille ta edastab autentimispäringu käigus OP-le. Juhul, kui OP tuvastab, et kasutaja on seda mobiilirakendust juba eelnevalt edukalt kasutanud, siis võib autentimisseansi lugeda väiksema riskiga olevaks. Juhul, kui kasutaja kasutab seda rakendust esmakordselt, siis on olukord riskantsem ning OP peaks rakendama täiendavaid kontrollimeetmeid.

6.5 Muud võimalused vahemeheründe tuvastamiseks

Teaduskirjanduses on mitmeid viiteid lahendustele, mis püüavad spetsiaalselt mitmekordsete pretensioon-vastus protokollide ja muude meetodite abil avastada vahemeheründeid. Võib-olla kõige varasem katse tehti juba aastal 1984, Rivest ja Shamir poolt, kes kirjeldasid protokolli *Interlock* [23]. Protokollist on küll hiljem avastatud nõrkusi [3].

Hea ülevaate näiteks finantsrakendustes ning lähiväljasides kasutatavate meetodite kohta annab Brelurut, Gerault ja Lafourcade koostatud uuring [4], mis tegeleb süstemaatiliselt kirjanduses esinevate *distance bound* protokollide ja nendega seotud rünnete kirjeldamisega.

Chaum'i protokoll, mida kirjeldatakse artiklis [25] on oma olemuselt samuti mitmekordne pretensioon-vastus protokoll, kus kasutatakse krüpteerimist, ühesuunalisi funktsioone ning krüptograafilisi kinnistusi (*commitments*). Protokoll on üsna keerukas ning selle kasutamine veebirakendustes ning autentimisvahendite juures ei ole esmapilgul intuitiivne.

Eelpool toodud protokollide juures tunduvad kasulikud ka kontrollitava täitmisajaga funktsioonid (*verifiable delay functions*) ning viitega krüptogrammid (*delay encryption*) [22].

Võib-olla kõige lähemal meie analüüsi probleemile on artikkel [28], kus Ulqinaku, Lain ja Capkun pakuvad välja huvitava meetodi, mille abil brauseris käivitatavat JS koodi vahemeheründe eest kaitsta. Nad kombineerivad JS koodi sogastamise, krüpteerimise/dekrüpteerimise, spetsiaalse mitmekordse pretensioon-vastus protokolli ning tegevuste ajalise kestvuse mõõtmise selleks, et tõenäosuslikult tuvastada ründaja olemasolu RP veebisaidi ning autentimisvahendi vahel. Juhul, kui rünnet ei ole, toimub nende loodud protokolli täitmine kasutaja brauseril ning autentimisvahendil normaalse kiirusega. Juhul, kui ründaja üritab vahemeherünnet, siis ta peab mõned toimingud tegema mitmekordselt ning see paistab autentimisvahendile välja tunduvalt pikema viitena. Artiklis on hinnatud, et kirjeldatud meetodi rakendamine võimaldab tuvastada kasutaja ligiduses (sama WiFi võrk või sama asula) asuva ründaja umbkaudu 70% tõenäosusega ning kaugemal asuva ründaja kuni 100% tõenäosusega.

Võib juhtuda, et mitmete teadustulemuste kombineerimisega ning paljude erinevate meetodite koostöös õnnestuks luua vahemeherünnet avastav autentimisprotokoll, mis on rakendatav ka Eestis kasutatavate autentimisvahendite juures. Tekib aga küsimus, kas sellise

täiendava protokolli väljatöötamine on hädavajalik, kui brauseri laienduste ja/või protokollide WebAuthn ja CTAP kombineerimisega õnnestuks saavutada samalaadne olukord.

7 Autentimisprotokollistiku kehtestamise õiguslik analüüs

7.1 Analüüsi ulatus

Eesti digiidentiteedi raamistik on mitmetest komponentidest koosnev süsteem, mida iseloomustab keerukas ülesannete jaotus nii avaliku- kui ka erasektori osapoolte vahel. Selle peamised funktsioonid on:

1. digiidentiteedi väljaandmine ja elutsükli haldus - võimaldada igale isikule digiidentiteedi olemasolu ja selle elutsükli haldamine.
2. digiidentiteedi kasutamine - võimaldada igale isikule oma digiidentiteedi turvaline kasutamine. See toimub Eesti digiidentiteedi raamistikus kahel moel:
    - digiidentiteedi abil saab kontrollida isikusamasust digitaalselt (ITDS § 15^5 lg 3, § 18^1 lg 2),
    - digiidentiteedi kaudu saab isik anda digitaalallkirju.

Nii Eesti riik (RIA) kui ka erasektori osapooled pakuvad erinevaid tarkvaralahendusi ja kliendituge digiidentiteedi kasutamiseks, sh isikusamasuse digitaalseks kontrollimiseks.

Antud peatükis keskendutakse digiidentiteedi kasutamisele ulatuses, mis puudutab isikusamasuse digitaalset kontrollimist. Muud Eesti digiidentiteedi raamistiku osad on käsitlusalast väljas - neid puudutatakse üksnes niivõrd, kuivõrd see on vajalik, et vastata püstitatud õiguslikele küsimustele.

Kuna Eestis ei väljastata juriidilistele isikutele digitaalset tuvastamist võimaldavat sertifikaati ega digitaalset allkirjastamist võimaldavat sertifikaati, siis on juriidilised isikud selle analüüsi käsitlusalast väljas.

Selle peatüki koostamisel on arvesse võetud, et Eesti õiguses (ITDS, EUTS, HoS, TsÜS) ja Euroopa Liidu õiguses (eIDAS) kasutatakse digiidentiteedi valdkonnas erinevaid õigustermineid, millest osad tähistavad ühtesid ja samu õigusmõisteid, teised aga erineva sisu või mahuga õigusmõisteid. Kuna selle analüüsi eesmärgiks ei ole nende õigusterminite kasutust ühtlustada, siis võimalike vastuolude ületamiseks on lähtutud analüüsi tarbeks koostatud eriterminitest (vt alampeatükk 1.3). Õigusnormi tsiteerimisel on kasutatud vastava õigusnormi originaalteksti või selle eestikeelset tõlget, kuid tsitaadi joonealuses viites on esitatud sama õigusnormi mõte ka selle analüüsi eriterminitega.

7.2 Asjaolude kirjeldus

2017. a avaldas RIA dokumendi pealkirjaga "Eesti Vabariigi Infosüsteemis autentimislahendustele kehtivad nõuded (autentimisnormatiiv)"[9]. See on soovitusliku iseloomuga dokument, mille õiguslik tähendus, siduvus ja õigusjõud on ebaselged.

Selle uuringu tulemusena töötati välja ühtlustatud autentimisprotokollistiku ettepanek (vt eelmine peatükk), mis oleks kasutatav kõigi uuringu käsitlusalas olevate autentimisteenustega (Mobiil-ID, Smart-ID, TARA, HarID) ning autentimisvahenditega (ID-kaart). Ettepaneku kohaselt täidaks autentimisprotokollistik kahte otstarvet:

1. lihtsustab RP-de liidestumist autentimisvahendite ja -teenustega (sh ümberlülitumist ühelt autentimisvahendilt või -teenuselt teisele),
2. suurendab autentimisvahendite ja -teenuste kasutamise turvalisust.

RIA soovib autentimisprotokollistikku kehtestada eelkõige avaliku sektori teenusepakkujatele, kuid ei välista, et tulevikus võidakse seda laiendada kõigile teenusepakkujatele. Isegi kui autentimisprotokollistiku kasutusala oleks piiratud üksnes avaliku sektori teenusepakkujatega, peaks selle abil olema siiski võimalik autentida nii Eesti kui ka teiste ELi liikmesriikide kasutajaid.

RIA soovib teada, kellele ja millises vormis oleks võimalik autentimisprotokollistiku ettepanekut kehtestada Eestis kehtiva õiguse alusel.

7.3 Õiguslikud küsimused

Õiguslikus analüüsis otsitakse vastuseid järgmistele küsimustele:

1. kas RIAl on kehtiva õiguse järgi pädevus kehtestada reegleid autentimisprotokollistiku kohta?
2. millist õiguslikku tähendust, siduvust ja jõudu saaks autentimisprotokollistiku reeglitele anda?
3. kellele võib RIA selliseid reegleid kehtestada?

7.4 Kohalduv õigus

Esitatud küsimustele vastamiseks tuleb kohaldada Eesti ja ELi õigust. Järgnevas alampeatükis kirjeldatakse täpsemalt vastavaid õigusakte ja nende kohaldamisala.

7.4.1 Eesti õigus

Eesti siseriiklikus õiguses on reguleeritud peamiselt digiidentiteedi haldusega seotud küsimusi:

1. ITDS – kehtestab dokumendikohustuse (igal Eestis elaval Eesti kodanikul, kes on üle 15-aastane, peab olema isikutunnistus) ja reguleerib Eesti Vabariigi poolt Eesti kodanikele ja välismaalastele isikut tõendavate dokumentide väljaandmist (ITDS § 1 lg 1). ITDS reguleerib ka digitaalset tuvastamist võimaldava sertifikaadi ja digitaalset allkirjastamist võimaldava sertifikaadi kandmist isikuttõendavasse dokumenti, nende kehtivuse peatamist ja taastamist ning kehtetuks tunnistamist (ITDS §§ 9^4 - 9^6, § 13 lg 1^2-1^3, § 19^1, § 20^2, § 20^4 lg 1, § 20^6 lg 5, § 20^{14}, § 34^2).
2. EUTS – reguleerib e-identimist ja e-tehinguteks vajalikke usaldusteenuseid ning riikliku järelevalve korraldust ulatuses, milles need ei ole reguleeritud eIDASes (EUTS § 1 lg 1). Samas, e-identimise kohta on EUTSis ainult üks peatükk (käsitleb e-identimise süsteemide usaldusväärsuse taseme hindamise nõudeid, tingimusi ja korda), mida ei rakendata ITDSi alusel välja antud isikut tõendavatel dokumentidel põhinevate e-identimise süsteemide suhtes (EUTS § 1 lg 5). See tähendab, et EUTS ei kohaldu Eesti poolt Euroopa Komisjonile teavitatud e-identimise süsteemide suhtes, mis käsitlevad riigi väljastatud (digitaalseid) isikutunnistusi (Mobiil-ID ja ID-kaart). Varasemalt on leitud [21] (lk 7 ja 13), et EUTS ega eIDAS ei reguleeri isikutuvastamist võimaldavat sertifikaati ning selle peatamist või tühistamist, kuna see allub ITDSile.
3. HoS – sätestab kriisireguleerimise, sealhulgas hädaolukorraks valmistumise ja hädaolukorra lahendamise ning elutähtsate teenuste toimepidevuse tagamise õiguslikud alused (HOS § 1 lg 1). HOS määrab elutähtsate teenustena mh elektroonilise isikutuvastamise ja digitaalse allkirjastamise (HOS § 36 lg 1 p 8). HoS § 37 lg 2 alusel kehtestatud Ettevõtlus- ja infotehnoloogiaministri määruses on täpsustatud elektroonilise isikutuvastamise ja

digitaalse allkirjastamise kui elutähtsa teenuse kirjeldust ning esitatud selle toimepidevuse nõuded.

Digiidentiteedi kasutamise spetsiifilist regulatsiooni on Eesti õiguses vähe:

1. ITDS – ITDS § 18^1 käsitleb isikusamasuse kontrollimise viise, mis hõlmavad mh isikusamasuse digitaalset kontrollimist masin-masin olukordades. Selle järgi võib avalik-õigusliku teenuse elektroonilise osutamise teha sõltuvaks isiku nõusolekust kasutada ITDSi alusel välja antud isikutunnistusele, elamisloakaardile või digitaalsele isikutunnistusele kantud digitaalset tuvastamist ja digitaalset allkirjastamist võimaldavat sertifikaati, s.t kui isik keeldub, võib jätta teenuse osutamata (ITDS § 18^1 lg 3).

2. TsÜS – TsÜS § 80 lg 1 järgi loetakse tehingu elektrooniline vorm võrdseks tehingu kirjaliku vormiga, kui seaduses ei ole sätestatud teisiti. Elektroonilise vormi üks tingimusi on elektrooniline allkirjastamine tehingu teinud isikute poolt (TsÜS § 80 lg 2 p 3). Peamised nõuded elektroonilisele allkirjale on esitatud TsÜS § 80 lg-s 3, mille kohaselt loetakse elektrooniliseks allkirjaks ka digitaalallkirja.

3. RIA põhimäärus - sätestab RIA pädevuse riigi infosüsteemi ja küberturvalisuse valdkonnas (RIA põhimääruse § 1 lg 1, § 7). RIA põhimääruse kohaselt on RIA üheks põhiülesandeks autentimist, digitaalallkirjastamist ja krüpteerimist võimaldava tarkvara ning internetipõhise autentimis- ja allkirjastamissüsteemi arendamise, haldamise ja majutamise korraldamise ning nende kasutamise koordineerimine (RIA põhimääruse § 8 lg 3 p 1)).

Kuna digiidentiteedi üks peamisi kasutusvaldkondi on avaliku sektori e-teenused, siis kohalduvad digiidentiteedi kasutamisele ka riigi infosüsteemi valdkonna normid:

1. AvTS - kõigi riigi ja kohaliku omavalitsuse andmekogude pidamisel on kohustuslik kasutada riigi infosüsteeme kindlustavaid süsteeme (AvTS § 43^9 lg 3). Riigi infosüsteemi kindlustavateks süsteemideks on mh infosüsteemide turvameetmete süsteem ja infosüsteemide andmevahetuskiht (AvTS § 43^9 lg 1 p-d 4) ja 5)). AvTS alusel teostab RIA haldus- ja riiklikku järelevalvet kahe riigi infosüsteemi kindlustava süsteemi üle (infosüsteemide turvameetmete süsteemi rakendamine, infosüsteemide andmevahetuskihiga liitumine) (AvTS § 44 p 2, § 53^1 lg 1). Riikliku järelevalve teostamisel võib RIA kohaldada KorSis sätestatud riikliku järelevalve erimeetmeid KorSis sätestatud alusel ja korras (AvTS § 53^1 lg 2).

Üldisemal tasandil reguleerivad digiidentiteedi kasutamist küberkaitset puudutavad nõuded:

1. EUTS – EUTS § 4 sedastab usaldusteenuse osutaja kohustuse teavitada pädevat asutust eIDAS artikli 19 lõike 2 kohasest turvaintsidendist viivitamata, kuid mitte hiljem kui 24 tunni jooksul pärast sellest teadasaamist. Riiklikku ja haldusjärelevalvet eIDASes ning EUTSis sätestatud nõuete täitmise üle teostab RIA (EUTS § 22).

2. KüTS – KüTS sätestab ühiskonna toimimise seisukohast oluliste ning riigi ja kohaliku omavalitsuse üksuse võrgu- ja infosüsteemide pidamise nõuded, vastutuse ja järelevalve ning küberintsidentide ennetamise ja lahendamise alused (KüTS § 1 lg 1). Muuhulgas kohustab KüTS teenuse osutajaid rakendama alaliselt organisatsioonilisi, füüsilisi ja infotehnilisi turvameetmeid küberintsidendi ennetamiseks või lahendamiseks ning selle mõjude ennetamiseks ja leevendamiseks (KüTS § 7 lg 1). KüTS kohustab tagama riigil endal oma süsteemide turvalisuse (KüTS § 9). Ka elutähtsa teenuse osutaja on kohustatud rakendama KüTSis sätestatud meetmeid (KüTS § 3 lg 1 p 1). KüTSis ja selle alusel kehtestatud õigusaktides sätestatud nõuete täitmise üle teeb riiklikku ja haldusjärelevalvet

RIA (KüTS § 14 lg 1). Seejuures riikliku järelevalve jaoks on KüTSis kehtestatud nii erisused kui ka erimeetmed (KüTS § § 15-16), samuti haldusjärelevalve meetmed (KüTS § 17).

7.4.2 Kohalduv ELi õigus (eIDAS)

Euroopa Liidu tasandil on digiidentiteedi haldamise ja kasutamisega seotud küsimusi reguleeritud peamiselt eIDAS määruses ja selle rakendusaktides, millest on selle uuringu jaoks olulisemad järgmised:

1. eIDAS-1501 – sätestab koostalitlusvõime raamistiku tehnilised ja käitusnõuded, et tagada nende e-identimise süsteemide koostalitlusvõime, millest liikmesriigid komisjonile teatavad [17] (art 1).
2. eIDAS-1502 – sätestab reeglid teatatud e-identimise süsteemi alusel väljastatud autentimisvahendite madala, märkimisväärse või kõrge usaldusväärsuse taseme kindlaksmääramiseks [18] (art 1.1).

7.4.2.1 eIDASe eesmärgid ja kohaldamisala

eIDASt kohaldatakse liikmesriikide poolt teavitatud e-identimise süsteemide ja liidus asuvate usaldusteenuse osutajate suhtes (eIDAS art 2 lg 1).

eIDASe üks eesmärke on kõrvaldada takistused vähemalt selliste autentimisvahendite piiriüleselt kasutamiselt, mida liikmesriikides kasutatakse avalike teenuste autentimisel (eIDAS põhjenduspunkt 12). Eesmärk ei ole sekkuda liikmesriikides loodud e-identiteedi haldamise süsteemide ja nendega seotud taristute küsimuses, vaid tagada, et juurdepääsul liikmesriikide pakutavatele piiriülestele internetipõhistele teenustele oleks võimalik turvaline e-identimine ja autentimine[27] (eIDAS põhjenduspunkt 12).

eIDASe teiseks eesmärgiks ergutada autentimisvahendite piiriülest kasutamist ka erasektoris (eIDAS põhjenduspunkt 17):

> *Liikmesriigid peaksid ergutama erasektorit vabatahtlikult kasutama teavitatud süsteemi kuuluvaid e-identimise vahendeid identimiseks,*[28] *kui see on vajalik internetipõhiste teenuste või e-tehingute puhul. Selleks peaks liikmesriigi pakutav autentimisvõimalus olema väljaspool kõnealuse liikmesriigi territooriumi asuvatele erasektori tuginevatele isikutele*[29] *kättesaadav samadel tingimustel kui kõnealuses liikmesriigis asuvatele erasektori tuginevatele isikutele. Teavitav liikmesriik võib erasektori tuginevate isikute puhul kindlaks määrata autentimisvahenditele juurdepääsu tingimused, kus võib olla teade selle kohta, kas teavitatud süsteemi kuuluvad autentimisvahendid on erasektori tuginevatele isikutele juba kättesaadavad.*

Liikmesriikidel on vabadus kasutada või juurutada autentimisvahendeid juurdepääsuks internetipõhistele teenustele ning otsustada, kas kaasata nende vahendite pakkumisse ka erasektor (eIDAS põhjenduspunkt 13). Ühelgi liikmesriigil pole kohustust teavitada Euroopa Komisjoni e-identimise süsteemidest – riigid saavad valida, kas teavitada kõikidest riigisiseselt vähemalt avalikele internetipõhistele teenustele juurdepääsuks kasutatavatest e-identimise süsteemidest, teha seda mõne puhul või üldse mitte (eIDAS põhjenduspunkt 13).

[27] eIDASe eestikeelses tõlkes kasutatakse fraasi *turvaline e-identimine ja e-autentimine*, kus termini *autentimine* algusesse on lisatud ebavajalik täiendus *e-*. Korrektsem oleks öelda *turvaline e-identimine ja autentimine*

[28] Korrektsem oleks tõlkida *kasutama autentimiseks autentimisvahendeid, mis kuuluvad teavitatud süsteemi.*

[29] eIDAS originaalteksti eestikeelne tõlge kasutab terminit *tuginevatele isikutele*, siin analüüsis kasutame terminit *RPdele.*

7.4.2.2 Vastastikuse tunnustamise põhimõte

Seatud eesmärkide saavutamiseks paneb eIDAS art 6 lg 1 liikmesriikidele kohustuse tunnustada autentimisvahendeid vastastikuse tunnustamise põhimõtte alusel (vt ka eIDAS põhjenduspunkt 15):

> *Kui ühes liikmesriigis nõutakse vastavalt siseriiklikule õigusele või haldustavale avaliku sektori asutuse osutatavale internetipõhisele teenusele juurdepääsuks e-identimist e-identimise vahendi abil ja e-autentimist,*[30] *tunnustatakse selles liikmesriigis teises liikmesriigis väljastatud e-identimise vahendit*[31] *kõnealuse internetipõhise teenuse piiriüleseks autentimiseks, kui täidetud on järgmised tingimused:*
>
> *a) e-identimise vahend*[32] *on väljastatud e-identimise süsteemi kohaselt, mis on kantud komisjon poolt vastavalt artiklile 9 avaldatud nimekirja;*
>
> *b) e-identimise vahendi*[33] *usaldusväärsuse tase vastab usaldusväärsuse tasemele, mida avaliku sektori asutus nõuab kõnealusele internetipõhisele teenusele juurdepääsuks esimesena nimetatud liikmesriigis, või on sellest usaldusväärsuse tasemest kõrgem, eeldusel et selle e-identimise usaldusväärsuse tase on märkimisväärne või kõrge;*
>
> *c) asjaomane avaliku sektori asutus kasutab kõnealusele internetipõhisele teenusele juurdepääsuks usaldusväärsuse taset, mille tase on märkimisväärne või kõrge.*

Avaliku sektori asutused võivad tunnustada nende osutatavate internetipõhiste teenuste piiriülese autentimise eesmärgil ka madala usaldusväärsuse tasemega autentimisvahendit, mis on väljastatud Euroopa Komisjoni poolt vastavalt eIDAS artiklile 9 avaldatud nimekirjas oleva süsteemi kohaselt (eIDAS art 6 lg 2).

7.4.2.3 E-identimise süsteemidest teavitamine

eIDAS sätestab mõned tingimused selle kohta, milliseid autentimisvahendeid peab tunnustama ja kuidas e-identimise süsteemidest peaks teavitama (eIDAS põhjenduspunkt 14).

> *Need tingimused peaksid aitama liikmesriikidel luua vajalikku usaldust üksteise e-identimise süsteemide vastu ning vastastikku tunnustada e-identimise vahendeid,*[34] *mis kuuluvad nende teavitatud süsteemidesse. Vastastikuse tunnustamise põhimõtet tuleks rakendada juhul, kui teavitava liikmesriigi e-identimise süsteem täidab teavitamise tingimusi ja teavitus on avaldatud Euroopa Liidu Teatajas. Vastastikuse tunnustamise põhimõtet tuleks siiski järgida ainult internetipõhiste teenuste autentimisel. Juurdepääs kõnealustele internetipõhistele teenustele ja nende lõplik osutamine taotlejale peaksid olema tihedalt seotud õigusega selliseid teenuseid siseriiklikes õigusaktides sätestatud tingimustel tarbida.*

E-identimise süsteemist teavitamise üheks vältimatuks tingimuseks on ELi liikmesriigi RP võimalus mõistlikult kontrollida elektrooniliselt saadud isikutuvastusandmeid (eIDAS art 7 p f):

[30] eIDASe eestikeelses tõlkes kasutatakse fraasi *e-identimist e-identimise vahendi abil ja e-autentimist*, kus termini „*autentimist*“ algusesse on lisatud ebavajalik täiendus „*e-*“. Korrektsem oleks tõlkida *e-identimist e-identimise vahendi abil ja autentimist*

[31] eIDAS originaalteksti eestikeelne tõlge kasutab terminit *e-identimise vahend*, siin analüüsis kasutame terminit *autentimisvahendit*.

[32] vt eelmine joonealune märkus.

[33] vt eelmine joonealune märkus.

[34] eIDAS originaalteksti eestikeelne tõlge kasutab terminit *e-identimise vahendeid*, siin analüüsis kasutame terminit *autentimisvahendeid*.

teavitav liikmesriik tagab internetipõhise autentimise võimaluse nii, et teise liikmesriigi territooriumil asuv tuginev isik saab kinnitada[35] *elektrooniliselt saadud isikutuvastusandmeid. Teavitav liikmesriik võib kindlaks määrata kõnealuse autentimise kasutustingimused tuginevatele isikutele, kes ei ole avaliku sektori asutused. Piiriülene autentimine on tasuta, kui autenditakse avaliku sektori asutuse internetipõhist teenust. Liikmesriigid ei kehtesta autentimiskavatsusega tuginevate isikute suhtes ebaproportsionaalseid tehnilisi tingimusi, mis takistavad või raskendavad märkimisväärselt teavitatud e-identimise süsteemide koos[talitlus]võimet.*

E-identimise süsteemist teavitamisel Euroopa Komisjonile peab liikmesriik muuhulgas esitama:

1. autentimise kirjelduse, s.t kuidas teavitav liikmesriik tagab internetipõhise autentimise võimaluse nii, et teise liikmesriigi territooriumil asuv tuginev isik saab kinnitada elektrooniliselt saadud isikutuvastusandmeid (eIDAS art 9 lg 1 p f), eIDAS art 7 p f)). Kui see kirjeldus muutub, siis tuleb esitada komisjonile ka selle iga hilisem muudatus (eIDAS art 9 lg 1).

2. autentimise või selle ohustatud osa peatamise või tühistamise korra (eIDAS art 9 lg 1 p g)).

7.4.2.4 Autentimisvahendite usaldusväärsuse tasemed

Komisjonile teavitatud e-identimise süsteemis määratakse süsteemi raames väljastatud autentimisvahenditele madal, märkimisväärne ja/või kõrge usaldusväärsuse tase (eIDAS art 8 lg 1), mis peab vastama järgmistele nõuetele (eIDAS art 8 lg 2):

1. *madal usaldusväärsuse tase osutab e-identimise süsteemi kuuluvale e-identimise vahendile,*[36] *mis on isiku väidetava või tema poolt kinnitatud isikusamasuse tuvastamiseks piiratud määral usaldusväärne ning mille kirjeldamisel osutatakse sellega seotud tehnilistele kirjeldustele, standarditele ja menetlustele, sealhulgas tehnilisele kontrollile, mille eesmärk on vähendada isikuandmete väärkasutamise või muutmise ohtu;*
2. *märkimisväärne usaldusväärsuse tase osutab e-identimise süsteemi kuuluvale e-identimise vahendile,*[37] *mis on isiku väidetava või tema poolt kinnitatud isikusamasuse tuvastamiseks olulisel määral usaldusväärne ning mille kirjeldamisel osutatakse sellega seotud tehnilistele kirjeldustele, standarditele ja menetlustele, sealhulgas tehnilisele kontrollile, mille eesmärk on vähendada märkimisväärselt isikuandmete väärkasutamise või muutmise ohtu*
3. *kõrge usaldusväärsuse tase osutab e-identimise süsteemi kuuluvale e-identimise vahendile,*[38] *mis on isiku väidetava või tema poolt kinnitatud isikusamasuse tuvastamiseks kõrgema usaldusväärsuse tasemega kui märkimisväärse usaldusväärsuse tasemega e-identimise vahend ning mille kirjeldamisel osutatakse sellega seotud tehnilistele kirjeldustele, standarditele ja menetlustele, sealhulgas tehnilisele kontrollile, mille eesmärk on hoida ära isikuandmete väärkasutamist või muutmist.*

[35] Korrektsem oleks kasutada termini *kinnitada* asemel terminit *kontrollida*.

[36] eIDAS originaalteksti eestikeelne tõlge kasutab terminit *e-identimise vahendile*, siin analüüsis kasutame terminit *autentimisvahendile*.

[37] vt eelmine joonealune märkus.

[38] vt eelmine joonealune märkus.

Usaldusväärsuse tasemed[39] kajastavad, mil määral on autentimisvahend isikusamasuse tuvastamiseks usaldusväärne, andes kindluse, et autentimise abil väljaselgitatud isiku identiteet on õige (eIDAS põhjenduspunkt 16):

> *Tagatistasemed*[40] *peaksid kajastama, mil määral on e-identimise vahend isikusamasuse tuvastamiseks usaldusväärne, andes seega kindluse, et ennast teatud isikuna esitlev isik on tõepoolest isik, kellele need isikuandmed on omistatud. Tagatistaseme liik sõltub sellest, mil määral on see e-identimise vahend usaldusväärne isiku väidetava või tema poolt kinnitatud isikusamasuse tuvastamiseks, võttes arvesse menetlusi (näiteks isikusamasuse tõendamine ja kontrollimine ning autentimine), haldustegevust (näiteks e-identimise vahendeid väljastav üksus ja selliste vahendite väljastamise menetlus) ja rakendatavat tehnilist kontrolli. [...] Kehtestatavad tingimused peaksid olema tehnoloogiliselt neutraalsed. Vajalikke turvanõudeid peaks olema võimalik saavutada erinevate tehnoloogiate abil.*

Komisjoni rakendusaktiga eIDAS-1502 on kehtestatud minimaalsed tehnilised kirjeldused, standardid ja menetlused, mille suhtes määratakse autentimisvahendite jaoks kindlaks madal, märkimisväärne või kõrge usaldusväärsuse tase (eIDAS art 8 lg 3). Nende üheks lähtealuseks on muuhulgas autentimisvahendi enda ning autentimisprotokolli[41] usaldusväärsus ja kvaliteet. Rakendusaktis eIDAS-1502 sätestatud kirjeldustes ja menetlustes on lähtutud rahvusvahelisest standardist ISO/IEC 29115, mis on peamine rahvusvaheline standard autentimisvahendite usaldusväärsuse tasemete valdkonnas (eIDAS-1502 põhjenduspunkt (3)).

Rakendusakti eIDAS-1502 lisas esitatud kirjeldusi ja menetlusi kasutatakse teatatud e-identimise süsteemi alusel väljastatud autentimisvahendite usaldusväärsuse taseme täpsustamiseks, määrates selleks kindlaks mh autentimise usaldatavuse ja kvaliteedi (eIDAS-1502 art 1 lg 2 p c)). Määruse eIDAS-1502 lisa jaotises 2.3 olevas tabelis (vt tabel 11) on esitatud nõuded igale sellise autentimisprotokolli usaldusväärsuse tasemele, mille kaudu füüsiline või juriidiline isik kasutab autentimisvahendit selleks, et kinnitada RP-le oma isikusamasust.

Tabel 11: Autentimismehhanismi usaldusväärsuse nõuded.

Usaldusväärsuse tase	Vajalikud komponendid
Madal	1. Enne isiku identiteediandmete loovutamist tuleb usaldusväärselt kontrollida autentimisvahendit ja selle kehtivust.
	2. Kui isiku identiteediandmed on salvestatud autentimismehhanismi osana, peab see teave olema turvatud, et kaitsta seda kadumise või rikkumise, sh väljaspool võrku analüüsimise eest.
	3. Autentimismehhanism rakendab e-identimise vahendi kontrollimiseks turvameetmeid, et oleks väga ebatõenäoline, et baasoskustest suurema ründepotentsiaaliga ründaja suudaks näiteks mõistatamise, pealtkuulamise, taasesituse või side manipuleerimise abil autentimismehhanismi häirida.

[39] eIDASe eestikeelses tõlkes kasutatakse terminit *tagatistasemed*.

[40] eIDAS originaalteksti eestikeelne tõlge kasutab terminit *tagatistasemed*, siin analüüsis kasutame terminit *usaldusväärsuse tasemed*.

[41] eIDAS-1502 originaalteksti eestikeelne tõlge kasutab terminit *autentimismehhanism*, siin analüüsis kasutame terminit *autentimisprotokoll*.

Usaldusväärsuse tase	Vajalikud komponendid
Märkimisväärne – nõuded, mis peavad olema täidetud lisaks madala taseme nõuetele.	1. Enne isiku identiteediandmete loovutamist tuleb e-identimise vahendit ja selle kehtivust usaldusväärselt kontrollida dünaamilise autentimisega.
	2. Autentimismehhanism rakendab e-identimise vahendi kontrollimiseks turvameetmeid, et oleks väga ebatõenäoline, et keskmise ründepotentsiaaliga ründaja suudaks näiteks mõistatamise, pealtkuulamise, taasesituse või side manipuleerimise abil autentimismehhanismi häirida.
Kõrge – nõuded, mis peavad olema täidetud lisaks madala ja märkimisväärse taseme nõuetele.	Autentimismehhanism rakendab e-identimise vahendi kontrollimiseks turvameetmeid, et oleks väga ebatõenäoline, et suure ründepotentsiaaliga ründaja suudaks näiteks mõistatamise, pealtkuulamise, taasesituse või side manipuleerimise abil autentimismehhanismi häirida.

7.4.2.5 E-identimise süsteemide koostalitlusvõime ja turvalisus

E-identimise süsteemide usaldusväärse piiriülese vastastikuse tunnustamise põhitegur on e-identimise süsteemide turvalisus - sellega seoses teevad liikmesriigid liidu tasandil koostööd e-identimise süsteemide koostalitlusvõime ja turvalisuse küsimustes. Kui e-identimise süsteemid võivad nõuda RP-delt teatava riist- või tarkvara kasutamist riigi tasandil, eeldab piiriülene koostalitlusvõime, et nimetatud liikmesriigid ei kehtestaks selliseid nõudeid väljaspool tema territooriumi asuvatele RPdele ega nõuaks nendega seotud kulude katmist (eIDAS põhjenduspunkt 19):

> *Sellisel juhul tuleks sobivaid lahendusi arutada ja need välja töötada koos[talitlus]võime raamistiku piires. Teisalt ei ole võimalik vältida tehnilisi nõudeid, mis tulenevad riigisiseste e-identimise vahendite tehnilisest kirjeldusest ja mis tõenäoliselt mõjutavad selliste elektrooniliste vahendite (nt kiipkaardid) kasutajaid.*

Lisaks teevad liikmesriigid liidu tasandil koostööd ka tehnilise koostalitlusvõime saavutamiseks (eIDAS põhjenduspunkt 20):

> *Liikmesriikide koostöö peaks olema suunatud teavitatud e-identimise süsteemide tehnilisele koos[talitlus]võimele, et soodustada usalduse ja turvalisuse kõrget taset, mis vastab riski astmele. Liikmesriikidevaheline teabevahetus ja parimate tavade jagamine nende vastastikuse tunnustamise eesmärgil peaks nimetatud koostööle kaasa aitama.*

7.4.3 Õiguslike suhete määratlemine

Selleks, et otsustada, mis tingimustel saab autentimisprotokollistiku reguleerimiseks kasutada Eesti õigust ja mis tingimustel ELi õigust, tuleb täpsustada autentimisprotokollistiku vahendusel toimivaid õiguslikke suhteid. Selleks on vaja selgitada:

1. kuidas autentimisprotokollistik paikneks Eesti digiidentiteedi raamistikus,

2. mil määral mõjutab autentimisprotokollistik Eesti poolt eIDASe alusel teavitatud olemasolevate e-identimise süsteemide ja teiste ELi liikmesriikide poolt eIDASe alusel teavitatud riiklike e-identimise süsteemide koostalitlusvõimet.

Autentimisprotokollistiku paiknemist ja mõju riiklike e-identimise skeemide koostalitlusvõimele kirjeldab joonis 9. See sisaldab ülevaadet, kuidas RP saaks autentimisprotokollistiku abil autentida füüsilist isikut, kes kasutab kõrge usaldusväärsuse taseme autentimisvahendit, mida ei pea, aga võib olla kirjeldatud mõnes Eesti poolt teavitatud e-identimise süsteemis.

Joonise 9 kohaselt on autentimisprotokollistik Eesti digiidentiteedi raamistiku komponent, mille kaudu teostatakse Eesti või välisriigi füüsilise isiku autentimist RP jaoks, kes võib olla nii Eesti kui ka välisriigi juriidiline isik. Seega võimaldab autentimisprotokollistik autentimist kolmes olukorras:

1. **Eesti RP autendib Eesti füüsilist isikut**, kes kasutab Eestis tunnustatud kõrge usaldusväärsuse taseme autentimisvahendit, mis ei pea tingimata olema kirjeldatud Eesti teavitatud e-identimise süsteemis. See olukord eeldab, et Eesti RP on liitunud Eesti autentimisteenuse pakkuja teenustega.

2. **Eesti RP autendib välisriigi füüsilist isikut**, kes kasutab kõrge usaldusväärsuse taseme autentimisvahendit, mida on kirjeldatud mõne muu ELi liikmesriigi teavitatud e-identimise süsteemis. See olukord eeldab, et

   a) Eesti RP on liitunud Eesti autentimisteenuse pakkuja teenustega, mis on liidestatud eIDAS-sõlmega ja

   b) välisriigi füüsiline isik kasutab eIDAS sõlmega liidestumiseks välisriigi autentimisteenuse pakkujat.

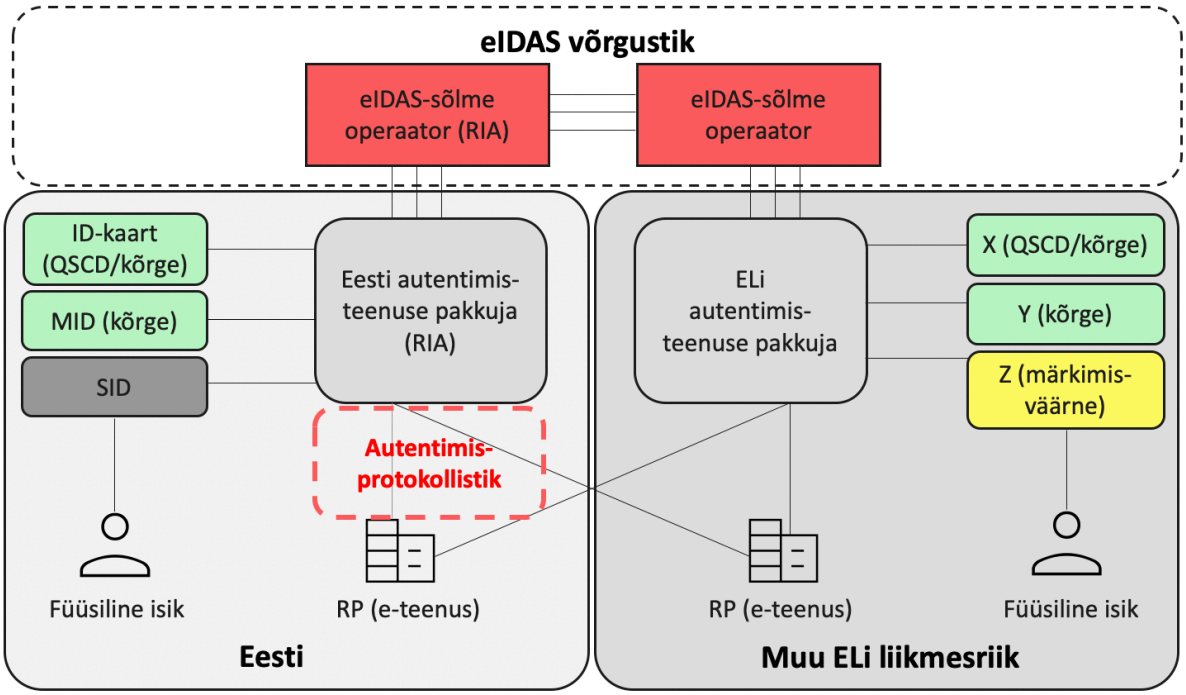
3. **ELi liikmesriigi RP autendib Eesti füüsilist isikut**, kes kasutab Eestis tunnustatud kõrge usaldusväärsuse taseme autentimisvahendit, mis ei pea tingimata olema kirjeldatud Eesti teavitatud e-identimise süsteemis. See olukord eeldab, et ELi liikmesriigi RP on liitunud Eesti autentimisteenuse pakkuja teenustega.

Kõigil kolmel juhul suhtleb RP Eesti autentimisteenuse pakkujaga autentimisprotokollistiku vahendusel, kuid ainult 2. juhul lisandub suhtlus eIDAS-sõlmega. Sellegipoolest võivad eIDAS reeglid kohalduda nii 2. kui ka 3. juhul, kui kasutatakse autentimisvahendit, mida on kirjeldatud mõne ELi liikmesriigi teavitatud e-identimise süsteemis.

Jooniselt 9 nähtub, et autentimisprotokollistikku saab rakendada Eesti autentimisteenuse pakkuja ja Eesti või välisriigi RP vahelises suhtes. Välisriikidest saavad kõne alla tulla eelkõige ELi liikmesriigid, kellel on eIDASe vastastikuse tunnustamise põhimõttest tulenev kohustus aktsepteerida oma e-teenustele juurdepääsu lubamiseks teiste liikmesriikide autentimisvahendeid. Seetõttu jätame käsitlusalast välja mitte-ELi liikmesriigid, ehkki põhimõtteliselt ei ole välistatud ka selliste riikide teenusepakkujate liitumine Eesti autentimisprotokollistikuga. Vaatamata sellele on ka ELi liikmesriikide puhul olukordi, kus autentimine on korraldatud muul moel kui autentimisprotokollistiku vahendusel:

a) Eesti füüsilise isiku ja teise ELi liikmesriigi autentimisteenuse pakkuja vahelises suhtes, mis toimub otse eIDAS-sõlme vahendusel. See juht eeldab, et Eesti füüsiline isik kasutab kõrge usaldusväärsuse tasemega autentimisvahendit, mida on kirjeldatud Eesti teavitatud e-identimise süsteemis.

b) Eesti autentimisteenuse pakkuja (RIA) ja teise ELi liikmesriigi füüsilise isiku vahelises suhtes, mis toimub otse eIDAS-sõlme vahendusel. See juht eeldab, et teise ELi liikmesriigi



Joonis 9: Juriidilise maastiku selgitav joonis

füüsiline isik kasutab kõrge usaldusväärsuse tasemega autentimisvahendit, mida on kirjeldatud teise ELi liikmesriigi teavitatud e-identimise süsteemis.

c) Eesti RP (e-teenus) ja teise ELi liikmesriigi autentimisteenuse pakkuja vahelises suhtes, mis toimub teise ELi liikmesriigi kohalike reeglite järgi.

d) juhul, kus teise ELi liikmesriigi RP (e-teenus) autendib sama ELi liikmesriigi füüsilist isikut, kes kasutab samas ELi liikmesriigis tunnustatud kõrge usaldusväärsuse tasemega autentimisvahendit, mis ei pea tingimata olema kirjeldatud selle ELi liikmesriigi teavitatud e-identimise süsteemis. See juht eeldab, et teise ELi liikmesriigi RP (e-teenus) on liitunud sama ELi liikmesriigi autentimisteenuse pakkuja teenustega, autentimine toimub sama ELi liikmesriigi kohalike reeglite järgi.

e) juhul, kus teise ELi liikmesriigi RP (e-teenus) autendib kolmanda ELi liikmesriigi füüsilist isikut, kes kasutab kolmandas ELi liikmesriigis tunnustatud kõrge usaldusväärsuse tasemega autentimisvahendit, mis ei pea tingimata olema kirjeldatud selle ELi liikmesriigi teavitatud e-identimise süsteemis. See juht eeldab, et teise ELi liikmesriigi RP (e-teenus) on liitunud kolmanda ELi liikmesriigi autentimisteenuse pakkuja teenustega, autentimine toimub selle kolmanda ELi liikmesriigi kohalike reeglite järgi.

7.5 Õiguslik analüüs

7.5.1 RIA pädevus autentimisprotokollistiku kehtestamiseks kehtiva õiguse alusel

Selle analüüsi esimeseks püstitatud õiguslikuks küsimuseks oli, kas RIAl on kehtiva õiguse järgi pädevus kehtestada reegleid autentimisprotokollistiku kohta. Vastus sellele küsimusele sõltub RIAle tema põhimäärusega määratud tegevusvaldkondadest ja ülesannetest.

RIA on Majandus- ja Kommunikatsiooniministeeriumi valitsemisalas tegutsev valitsusasutus, kellel on juhtimisfunktsioon ja kes täidab avalikke ülesandeid, samuti muid tema pädevuses olevaid ülesandeid õigusaktides ettenähtud alustel ja ulatuses (RIA põhimääruse § 1 lg 1). RIA teostab oma ülesandeid kahes valdkonnas (RIA põhimääruse § 7):

1. riigi infosüsteemi valdkond - siin on RIA ülesandeks mh korraldada autentimist, digitaalallkirjastamist ja krüpteerimist võimaldava tarkvara ja internetipõhise autentimis- ja allkirjastamissüsteemi arendamist, haldamist ja majutamist ning koordineerida nende kasutamist (RIA põhimääruse § 8 lg 3 p 1).
2. küberturvalisuse valdkond - siin on RIA ülesanded järgmised (RIA põhimääruse § 8 lg 4):

    1) korraldab kriitilise informatsiooni infrastruktuuri kaitset;
    2) korraldab infosüsteemide turvameetmete süsteemi arendamist ja koordineerib infoturbemeetmete rakendamist;
    3) täidab küberturvalisuse seaduse § 5 tähenduses ühtse kontaktpunkti ja küberturbe intsidentide lahendamise üksuse ülesandeid ning koordineerib küberintsidentide ennetamist ja lahendamist;
    4) korraldab küberturvalisust ohustavate riskide seiret, analüüsi ja ohtudest teavitamist;
    5) juhib välisprojekte ameti pädevuse piires;
    6) teostab õigusaktide alusel haldus- ja riiklikku järelevalvet, haldussunni rakendamist ja väärtegude kohtuvälist menetlemist.

RIA pädevustest nähtub, et RIAl on haldus- ja riikliku järelevalve pädevus, haldussunni rakendamise ja väärtegude kohtuvälise menetlemise õigus kehtivate õigusaktide alusel üksnes küberturvalisuse valdkonnas (RIA põhimääruse § 8 lg 4 p 6). Õigusliku aluse haldus- ja riikliku järelevalve teostamiseks küberkaitse valdkonnas annavad RIAle järgmised normid:

1. EUTS § 22 – RIA teostab riiklikku ja haldusjärelevalvet eIDASes ning EUTSis sätestatud nõuete täitmise üle.
2. KüTS § § 14-17 – RIA teostab riiklikku ja haldusjärelevalvet KüTSis ja selle alusel kehtestatud õigusaktides sätestatud nõuete täitmise üle.
3. AvTS § 44 p 2 ja § 53^1 lg 1 – RIA teostab riiklikku ja haldusjärelevalvet AvTSi ja selle alusel kehtestatud õigusaktide täitmise üle, täpsemalt infosüsteemide turvameetmete süsteemi rakendamise ning infosüsteemide andmevahetuskihiga liitumise üle.

7.5.2 Autentimisprotokollistiku kasutamise reeglite kehtestamise õiguslikud vormid kehtiva Eesti õiguse alusel

7.5.2.1 Autentimisprotokollistiku kasutamise reeglid kui riikliku järelevalve meede

RIA on riikliku järelevalve teostajana korrakaitseorgan KorS § 6 lõike 1 tähenduses. Oma ülesannete täitmisel on RIAl õigus rakendada asjakohaseid korrakaitse üldmeetmeid ning vastavates seadustes sätestatud erimeetmeid (EUTS § 23, KüTS § 15, AvTS § 53^1 lg 2).

Üheks korrakaitse üldmeetmeks on teavitamine ohu ennetamisest, ohukahtlusest, ohust või korrarikkumisest (teadaanded, soovitused, hoiatused) (KorS § 26 lg 1). Praktikas arvatakse siia alla ka korrakaitseorgani juhendiloome, mille kaudu antakse soovitusi parima praktika kujundamiseks. Seega põhimõtteliselt saaks RIA kui korrakaitseorgan kehtestada nii EUTS,

KüTS kui ka AvTSist tuleneva riikliku järelevalve pädevuse raames soovitusliku iseloomuga juhendi autentimisprotokollistiku kasutamise kohta ning teostada selle täitmise üle riiklikku järelevalvet.

Sellisel juhendil oleks siiski olulised piirangud:

1. õiguslikult mittesiduv - juhendi reeglid ei oma õigusakti staatust ning RIA ei saa vahetult nõuda nende täitmist ega sanktsioneerida nende rikkumist.

2. ei laiene haldusjärelevalvele - riiklikku järelevalve meetmeid ei saa kohaldada haldusjärelevalvemenetluses, s.t ühe haldusorgani või halduskandja poolt teise haldusorgani või halduskandja suhtes tema tegevuse õiguspärasuse ja otstarbekuse üle järelevalve teostamisel (KorS § 1 lg 7, VVS § 75, VVS § 75^1 lg 1 ja 3). Seega autentimisprotokollistiku peamise adressaadi - avaliku sektori asutuste - suhtes ei saaks juhendit kehtestada kui riikliku järelevalve üldmeedet vastavalt KorS § 26 lg-le 1.

7.5.2.2 Autentimisprotokollistiku kasutamise reeglid kui haldusjärelevalve meede

RIA on ka haldusjärelevalve teostaja VVS 6. jao tähenduses (VVS § 75^1 jj). VVSis sätestatud haldusjärelevalve meetmed ja KüTSis sätestatud haldusjärelevalve meeted aga ei sisalda võimalust kehtestada haldusorganitele jt haldusekandjatele soovituslikke juhiseid küberkaitse valdkonnas.

Kui riiklik järelevalve hõlmab seaduse järgi ohu ennetamise tegevusi (KorS § 2 lg 4) ja võimaldab seega kehtestada soovituslikke juhiseid ohu ennetamiseks (KorS § 26 lg 1), siis haldusjärelevalve puhul ei ole ennetamise tegevused nii selgelt hõlmatud. Seega puuduvad võimalused kehtestada soovituslikke reegleid autentimisprotokollistiku kasutamiseks haldusjärelevalve korras.

7.5.2.3 Muud võimalused autentimisprotokollistiku kasutamise reeglite kehtestamiseks

Autentimisprotokollistik on seotud Eesti digiidentiteedi raamistikus kõige otsesemalt digiidentiteedi kasutamise valdkonnaga – see võimaldab isikusamasuse digitaalset kontrollimist eri RPde poolt samadel alustel. Eesti õiguses on digiidentiteedi kasutamise valdkonna spetsiifilisi reegleid väga vähe, küll aga kohalduvad siin riigi infosüsteemi ja küberkaitset puudutavad normid KüTSis, EUTSis ja AvTSis. Järgnevalt analüüsime, millised on alternatiivsed võimalused KüTSi, EUTSi ja AvTSi alusel autentimisprotokollistiku jõustamiseks avaliku ja erasektori osapooltele.

Autentimisprotokollistiku efektiivseks kasutuselevõtuks on vajalik, et seda juurutaksid ühelt poolt autentimisteenuste ja autentimisvahendite pakkujad ja teiselt poolt ka RPd. Kuivõrd RIA esmaseks eesmärgiks on võtta autentimisprotokollistik kasutusele avaliku sektori e-teenustes, siis peaks eelkõige tagama autentimisprotokollistiku reeglite täitmise avaliku sektori autentimisteenuste ja autentimisvahendite pakkujate ning RPde poolt. Niisiis vajab selgitamist, kas KüTS, EUTS või AvTS sisaldavad piisavaid norme, mille abil avaliku sektori osapooled saaksid autentimisprotokollistiku kasutusele võtta.

KüTS: Autentimisprotokollistik kui turvameede

KüTS § 6 sätestab järgmised küberturvalisuse tagamise põhimõtted:

1. *isiklikkuse põhimõte – süsteemi turvalisuse tagamist korraldab teenuse osutaja;*
2. *tervikliku kaitse põhimõte – teenuse osutaja teeb kindlaks võimalikud ohud süsteemile ning rakendab süsteemi kaitseks kohaseid korralduslikke ja tehnilisi abinõusid;*

3. *kahjuliku mõju vähendamise põhimõte – teenuse osutaja rakendab küberintsidendi korral vajalikku hoolsust ja abinõusid, et vältida küberintsidendi mõju laienemist ja võimalikku levikut teisele süsteemile, ning teavitab küberintsidendist [KüTSis] sätestatud järelevalveasutust;*
4. *koostööpõhimõte – küberturvalisuse tagamisel ja küberintsidentide lahendamisel teevad osalised koostööd ja võtavad vajaduse korral arvesse süsteemide ja teenuste omavahelist seotust ning sõltuvust.*

KüTSi tervikliku kaitse põhimõttest tuleneb, et peamine vastutus võrgu- ja infosüsteemi turvalisuse eest on KüTSi alusel küberturvalisuse tagamiseks kohustatud teenuse osutajatel. KüTS § 7 lg 1 paneb teenuse osutajale kohustuse rakendada alaliselt organisatsioonilisi, füüsilisi ja infotehnilisi turvameetmeid, et ennetada küberintsidente ning ennetada või leevendada nende tõttu avalduvat mõju (teise sõltuva) teenuse toimepidevusele või süsteemi turvalisusele. KüTS § 7 lg 2 järgi peab teenuse osutaja turvameetmete rakendamisel mh koostama ja dokumenteerima süsteemi riskianalüüsi ning võtma kasutusele abinõud küberintsidendi mõju ja leviku vähendamiseks.

Ülalkirjeldatud teenuse osutaja kohustused kehtivad mõnede erisustega ka riigi ja kohaliku omavalitsuse üksustele (KüTS § 7 lg 4, § 9 lg 1). Nimelt, riigi ja kohaliku omavalitsuse üksuse süsteemi turvalisuse tagamisel peavad olema täidetud AvTSi alusel infosüsteemide turvameetmete süsteemile kehtestatud nõuded (KüTS § 9 lg 2 ja AvTS § 43^9 lg 1 p 4).

Autentimisprotokollistiku üks peamine otstarve on suurendada autentimisvahendite ja -teenuste kasutamise turvalisust. Seega saab autentimisprotokollistikku käsitleda kui turvameetmeid KüTS § 7 lg 1 tähenduses, mida teenuse osutajad, sh riik ja kohaliku omavalitsuse üksused, saavad rakendada küberintsidentide ennetamiseks ning nende mõjude leevendamiseks. RIAl kui küberkaitse valdkonna riikliku- ja haldusjärelevalveorganil on võimalik kontrollida, kas teenuse osutajad on võtnud kasutusele piisavad turvameetmed oma süsteemide kaitseks KüTS § 7 lg 1 tähenduses ning täitnud muid KüTS § 7 lg 2-s nimetatud kohustusi (süsteemi riskianalüüsi teostamine, süsteemi seire, abinõud küberintsidendi mõju ja leviku vähendamiseks jms). Kui autentimisprotokollistik on RIA poolt avalikustatud ja tunnustatud kui kasulik turvameetmete süsteem, siis saab RIA:

1. teha haldusjärelevalve korras ettekirjutusi autentimisprotokollistiku kasutuselevõtmiseks nii riigi ja kohaliku omavalitsuse üksuste haldusorganitele (KüTS § 14 lg 1, VVS § 75^1 lg-d 1 ja 3) kui ka muudele haldusekandjatele (KüTS § 14 lg 1, VVS § 75^1 lg-d 1 ja 4),
2. teha riikliku järelevalve korras ettekirjutusi ja kohaldada haldussunnivahendeid autentimisprotokollistiku kasutuselevõtmiseks muude teenuse osutajate suhtes (KorS § 28).

Teenuse osutajatel hetkel kehtiva õiguse alusel aga vabadus valida, milliseid turvameetmeid nad kasutavad. Seega, isegi kui osad teenuse osutajad otsustavad autentimisprotokollistikuga liitumise kasuks, ei pruugi seda teha kõik teenuse osutajad. Ka autentimisprotokollistikuga liitumise tähtaega ei ole õigusaktides kindlaks määratud, mistõttu võib see praktikas jääda venima. Järelikult ei saa autentimisprotokollistikku hetkel kehtiva õiguse järgi rakendada ühtlaselt ja üheaegselt kõigi teenuse osutajate suhtes, kes pakuvad autentimisteenuseid ja -vahendeid või kontrollivad kasutajate isikusamasust. See tähendab, et autentimisprotokollistiku rakendamisega kaasnevad kasulikud mõjud ei pruugi saabuda küllalt kiiresti ning viibimine võib kaasa tuua hoopis kahjulikke mõjusid.

EUTS: Autentimisprotokollistiku reeglid kui usaldusteenuste nõuete järgimise juhend

EUTS § 12 lg 1 annab valdkonna eest vastutavale ministrile ja RIAle õiguse kehtestada soovituslikke juhendeid kvalifitseeritud usaldusteenuse osutajale ja usaldusteenusele ning usaldusnimekirja kantud kvalifitseerimata usaldusteenuse osutajale ja usaldusteenusele

sätestatud nõuete järgimiseks. See juhendiloome pädevus puudutab aga üksnes eIDASes ja EUTSis sätestatud nõuete järgimist usaldusteenuste kontekstis. Kuna autentimine ei ole eIDASe tähenduses usaldusteenus, siis vastav juhendiloome pädevus ei laiene autentimisega seotud nõuetele. Seega EUTS § 12 lg 1 alusel see soovituslik juhend ei sobi autentimisprotokollistiku reeglite kehtestamiseks.

AvTS: Autentimisprotokollistik kui infosüsteemide turvameetmete süsteemi komponent

AvTS § 43^9 lg 3 järgi on riigi infosüsteemi kindlustavate süsteemide kasutamine kohustuslik kõigi riigi ja kohaliku omavalitsuse andmekogude pidamisel. Üheks riigi infosüsteemi kindlustavaks süsteemiks on infosüsteemide turvameetmete süsteem AvTS § 43^9 lg 1 p 4 tähenduses. Kui autentimisprotokollistikku saaks käsitleda osana infosüsteemide turvameetmete süsteemist, võiks see kehtiva õiguse alusel olla kohustuslik element riigi ja kohaliku omavalitsuse andmekogude pidamisel. See küsimus vajab täiendavat õiguslikku analüüsi, mis ei ole selle uuringu skoobis ning vajaks eraldi käsitlemist.

Siinkohal tuleb silmas pidada, et infosüsteemide turvameetmete süsteemi kohustuslikkus on piiratud üksnes andmekogude pidamisega - see ei laiene kehtiva õiguse alusel muudele riigi infosüsteemi osadele ega ka väljaspoole riigi infosüsteemi. Järelikult ei saaks AvTS § 43^9 lg 3 alusel teha autentimisprotokollistiku kasutamist kohustuslikuks autentimisteenuste ja -vahendite pakkujatele ega RPdele, kui nad ei tegele andmekogude pidamisega AvTS tähenduses.

7.5.3 Autentimisprotokollistiku kasutamise reeglite kehtestamine ELi õiguse alusel

Eelmises osas käsitletud õiguslikud vormid autentimisprotokollistiku kasutamise reeglite kehtetamiseks Eesti õiguse alusel ei pakkunud ammendavaid lahendusi. Seetõttu käsitleme põgusalt ka ELi õigusest tulenevaid võimalusi autentimisprotokollistiku reguleerimiseks.

eIDASe järgi peab liikmesriik tagama internetipõhise autentimise võimaluse nii, et teise liikmesriigi territooriumil asuval RPl on võimalik kontrollida elektrooniliselt saadud isikutuvastusandmeid. Seejuures ei tohi liikmesriigid kehtestada autentimiskavatsusega RPde suhtes ebaproportsionaalseid tehnilisi tingimusi, mis takistavad või raskendavad märkimisväärselt teavitatud e-identimise süsteemide koostalitlusvõimet (eIDAS art 7 p f). Järelikult, kui Eesti riik kehtestab autentimisprotokollistiku ka teiste ELi liikmesriikide RPde suhtes, siis ei tohi see eIDAS art 7 p f kohaselt takistada või raskendada Eesti ja teiste ELi liikmesriikide e-identimise süsteemide koostalitlusvõimet.

Selle uuringu jaotises 5.4.4 on leitud, et eIDAS-sõlmede abil toimuv autentimisprotsessi osa ei ole Eesti autentimisprotokollistikuga kattuv ning on sellest eraldi. See tähendab, et Eesti autentimisprotokollistiku kaudu toimuvale autentimisprotsessile võib lisanduda eIDAS-sõlmede abil toimub autentimisprotsess.

Juhime tähelepanu, et Eesti autentimisprotokollistiku kasutuselevõtu korral Eesti teenusepakkujate poolt süveneks juba praegu eksisteeriv erinevus Eesti ja ELi kodanike autentimisel Eesti RP poolt, kui ELi kodaniku autentimisel kasutatakse lisaks Eesti autentimisprotokollistikule ka eIDAS-sõlme:

1. Eesti kodanike puhul on võimalik valideerida autentimissignatuuri ja seeläbi veenduda, et autenditakse konkreetset Eesti kodanikku;

2. ELi kodanike puhul seda teha ei saa, s.t tuleb usaldada eIDAS-sõlme väidet, et autenditakse konkreetset ELi kodanikku.[42]

[42] Sama probleem on ka Eesti kodanike autentimisel praegu kasutusel olevate TARA ja HarID vahendusteenuste kaudu

Leiame, et see erinevus väärib laiemat arutelu käimasoleva eIDAS määruse muutmise ettepaneku[43] valguses.

eIDAS art 6 lg 1 järgi peab liikmesriik tunnustama piiriülesel autentimisel teise liikmesriigi autentimisvahendit oma e-teenustele juurdepääsu andmisel, kui see autentimisvahend on kirjeldatud teise liikmesriigi poolt Euroopa Komisjonile teavitatud e-identimise süsteemis ning vastab usaldusväärsuse tasemele *märkimisväärne* või *kõrge*. eIDAS art 12 lg 1 kohaselt peavad teavitatud riiklikud e-identimise süsteemid olema koosvõimelised ning selle saavutamiseks on eIDAS art 12 lg 2 alusel loodud koosvõime raamistik, mille rakendamiseks on Euroopa Komisjon võtnud vastu eIDAS-1501 rakendusakti. eIDAS-1501 rakendusakti art 2 p 1) järgi peab e-identimise koostalitlusvõimelise arhitektuuri osaks olema isikute piiriüleses autentimises osalev ühenduspunkt – eIDAS-sõlm –, mis suudab edastuse ära tunda ja seda töödelda või selle teistele sõlmedele edasi saata, pakkudes ühe liikmesriigi riigisisese e-identimise taristule liidest andmevahetuseks teiste liikmesriikide riigisiseste e-identimise taristutega.

Tuleb tähele panna, et eIDAS-sõlmede puhul ei rakendada samasuguseid turvanõudeid nagu liikmesriikide autentimisprotokollide[44] puhul, sest eIDAS-sõlmede nõudeid reguleerib eIDAS-1501, autentimisprotokollide nõudeid aga eIDAS-1502.[45] Selliselt on eIDAS-sõlmed e-identimise koostalitlusvõimelise arhitektuuri nõrgaks lüliks, kuna nende puhul ei nõuta autentimiskinnitustes autentimissignatuuri valideerimist. Sisuliselt tähendab see seda, et Eesti teenusepakkujal ega RPl ei ole võimalik veenduda, kas end ELi liikmesriigi kodanikuna presenteeriv lõppkasutaja on sama isik, kes ta väidab end olevat.

Sama kehtib ka muu ELi liikmesriigi teenusepakkuja puhul, kes üritab autentida Eesti kodanikust lõppkasutajat eIDASe vastastikuse tunnustamise põhimõtte alusel - ehkki Eesti autentimisvahendid väljastavad autentimiskinnituses autentimissignatuuri vaikimisi igal autentimisel, ei nõuta eIDAS-sõlmes selle valideerimist. eIDAS nõuab küll liikmesriikide autentimislahendustelt meetmeid vahemeherünnete vastu, aga seda nõuet ei ole kehtestatud eIDAS-sõlmedele. Isegi kui ühe liikmesriigi teenusepakkuja saab ja soovib valideerida teise liikmesriigi autentimissignatuuri autentimiskinnituses, siis eIDAS-sõlm seda hetkel praktikas ei võimalda. Niisiis on tekkinud olukord, kus autentimine väljaspool eIDAS-sõlme võib olla usaldusväärsem kui eIDAS-sõlme kaudu.

Näeme siin nii vajadust kui ka võimalust eIDASe alusel autentimisreeglite tugevdamiseks ja ühtlustamiseks ELi tasandil. eIDASe muutmise ettepaneku kohaselt plaanitakse käiku võtta nn e-kukkur, mille abil peab olema võimalik kindlalt veenduda e-kukru omaniku isikusamasuses. Seda saab PKI-põhises süsteemis tehniliselt teostada e-kukru privaat- ja avaliku võtme kontrollimise teel, s.t e-kukru kaudu autentimisel tuleks nõuda autentimiskinnituses lõppkasutaja signatuuri valideerimist.

eIDAS põhjenduspunktis 19 selgitatakse piiriülese koostalitlusvõime eeldusi - kui e-identimise susteemid võivad nõuda RP-delt teatava riist- või tarkvara kasutamist riigi tasandil, siis ei tohiks nimetatud liikmesriigid kehtestada selliseid nõudeid väljaspool oma territooriumi asuvatele RPdele ega nõuda nendega seotud kulude katmist. Teiste liikmesriikide RPdelt teatud riist- või tarkvara kasutamise nõudmiseks tuleb sobivaid lahendusi arutada ja need välja töötada koostalitlusvõime raamistiku piires. eIDAS põhjenduspunkti 20 kohaselt peavad liikmesriigid tegema koostööd ka tehnilise koostalitlusvõime saavutamiseks, et soodustada usalduse ja turvalisuse kõrget taset, mis vastab riski astmele - sellele peaks kaasa aitama liikmesriikidevaheline teabevahetus ja parimate tavade jagamine nende vastastikuse tunnustamise eesmärgil.

[43] Commission proposes a trusted and secure Digital Identity for all Europeans. 03.06.2021. Internet: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2663.

[44] eIDAS-1502 originaalteksti eestikeelne tõlge kasutab terminit *autentimismehhanism*, siin analüüsis kasutame terminit *autentimisprotokoll*

[45] vt eelmine joonealune märkus.

Eelnevast saab järeldada, et autentimiskinnituses autentimissignatuuri valideerimise nõudmiseks peab selle lahenduse eelnevalt läbi arutama koostalitlusvõime raamistiku piires ning heaks kiitma liikmesriikidevahelises koostöös (näiteks parima tavana).

7.5.4 Vastused õiguslikele küsimustele

Selle peatükis otsisime kehtiva õiguse analüüsi põhjal vastuseid järgmistele küsimustele:

1. Kas RIAl on pädevus kehtestada reegleid autentimisprotokollistiku kohta?

   RIAl puudub kehtiva õiguse järgi õigusloome pädevus, s.t ta ei saa kehtestada kolmandatele isikutele siduvaid reegleid. Küll aga saab RIA kehtestada kolmandatele isikutele soovituslikke juhiseid riikliku järelevalve teostamise korras. See ei ole siiski piisav lahendus, sest RIA soovib autentimisprotokollistikku kehtestada eelkõige avaliku sektori teenusepakkujatele, kelle suhtes RIAl on üksnes haldusjärelevalve teostamise pädevus. Nii riikliku kui ka haldusjärelevalve teostamise pädevus on RIAl vaid küberturvalisuse valdkonnas.

2. Millist õiguslikku tähendust, siduvust ja jõudu saaks autentimisprotokollistiku reeglitele anda?

   Kui autentimisprotokollistik on RIA poolt avalikustatud ja tunnustatud kui kasulik lahendus, siis võivad nii avaliku sektori kui ka erasektori teenusepakkujad käsitleda seda kui turvameetmete süsteemi. KüTS § 7 lg 1 ja § 9 lg 1 koosmõjus on mitte ainult erasektori teenuse osutajatel, vaid ka riigi ja kohaliku omavalitsuse üksuse teenuse osutajatel kohustus rakendada alaliselt organisatsioonilisi, füüsilisi ja infotehnilisi turvameetmeid, et ennetada küberintsidente ning ennetada või leevendada nende tõttu avalduvat mõju (teise sõltuva) teenuse toimepidevusele või süsteemi turvalisusele. Kui seda kohustust ei täideta, saab RIA rakendada avaliku sektori asutuste suhtes haldusjärelevalve meetmeid ning erasektori asutuste suhtes riikliku järelevalve meetmeid KuTS § § 14-17 alusel. Alternatiivselt saab autentimisprotokollistikku käsitleda ka osana riigi infosüsteemi kindlustavast infosüsteemide turvameetmete süsteemist AvTSi § 43^9 lg 1 p 4 järgi. Nii võiks autentimisprotokollistik olla kohustuslik element riigi ja kohaliku omavalitsuse andmekogude pidamisel, kuid see küsimus vajab täiendavat õiguslikku analüüsi. Tuleb arvestada, et infosüsteemide turvameetmete süsteem on kohustuslik üksnes andmekogude pidamisel (AvTSi § 43^9 lg 3) - see ei laieneks autentimisteenuste ja -vahendite pakkujatele ega RPdele, kui nad ei tegele andmekogude pidamisega AvTSi tähenduses.

3. Kellele võib RIA selliseid reegleid kehtestada?

   RIA saab kehtestada kolmandatele isikutele soovituslikke juhiseid üksnes küberturvalisuse valdkonnas riikliku järelevalve teostamisel.

8 Kokkuvõte ja soovitused

8.1 Eelanalüüsi kokkuvõte

Projekti käigus uuriti Eestis kasutusel olevaid autentimisprotokolle ning töötati välja ühtse autentimisprotokollistiku kavand (vt jaotis 5.1), mis sobib kasutamiseks nii autentimisteenuste juures (näiteks TARA) kui ka autentimisvahendite juures (näiteks ID-kaart, Mobiil-ID, Smart-ID).

Kavandatud Eesti autentimisprotokollistik põhineb OIDC protokollil. Seda protokolli kasutavad juba Eestis teenused TARA ning HarID, kuid võrreldes praeguse praktikaga on väljapakutud kavandis täiendavaid elemente, mis tagavad suurema turvalisuse ning eIDAS regulatsiooni nõuete täitmise. Enamus kasutuselevõetud turvamehhanisme on OIDC laiendatud standardipere osad ning me näeme, et lähemas tulevikus muutuvad need täiendused niikuinii kohustuslikuks.

Lisaks täiendavate standardite rakendamisele loodi autentimisprotokollistiku jaoks ka unikaalne, Eesti-spetsiifiline laiendus, mis võimaldab autentimisteenuse pakkuja poolt loodavas autentimiskinnituses edastada autentimisvahendi loodud signatuuri (vt jaotis 5.2). Sellise laienduse kasutuselevõtmine võimaldaks vähendada riski, et autentimisteenuse pakkuja on ründaja poolt üle võetud ning ründaja võltsib autentimiskinnitusi. Autentimissignatuuri esitamiseks kasutati ID-kaardi autentimissüsteemi „Web eID“ jaoks loodud autentimissignatuuri formaati ning laiendati seda.

Projekti lähteülesande kohaselt uuriti ka täiendavaid võimalusi, kuidas Eestis saaks vähendada vahemehe- ja kalastusrünnete riski. Protokollistiku kavandis on juba mõned meetmed kasutusele võetud, kuid töö käigus selgus, et ainult autentimisprotokollidesse lisatavate meetmetega ei ole võimalik kõigi rünnete eest kasutajaid kaitsta. Osad kaitsemeetmed tuleb rakendada autentimisvahendites. Aruande jaotises 6 kirjeldatakse vastavaid võimalusi.

Kuna aruanne tuli esitada eesti keeles, siis moodustab üllatavalt mahuka osa autentimisega seotud mõistete sõnastik (vt jaotised 1.2 ja 1.3). Selgus, et paljude mõistete jaoks ei ole veel eestikeelseid üldlevinud termineid ning mõned aruandes kasutatud terminid on uued. Loodame, et sõnastikku saab edaspidistes töödes taaskasutada ning täiendada. Soovitame tulevikus ühtlustada ka juriidilised ja tehnilised mõisted ning terminid, mis on praegu mõnes kohas vastuolulised, samuti leida võimalus Eesti ja ELi õiguslike terminite paremaks ühtlustamiseks.

Olulise osa projektist moodustas juriidiline analüüs (vt jaotis 7), millistele tingimustele peab autentimine Eestis vastama ning kuidas saab RIA seda protokollistikku kehtestada.

8.2 Järgmised sammud

Autentimisprotokollistiku kavandi ellu viimiseks soovitame kliendil jätkata järgmiste sammudega:

1. Autentimisteenuste kirjeldamine masinloetavate andmetega – praegune eelanalüüs on mõeldud arhitektidele ning ekspertidele ning siin on kirjeldatud protokollide sõnumite näidised ning toodud ära põhjendused, miks on tehtud üks või teine valik. Selleks, et protokollistiku kasutuselevõtmine oleks süsteemiülemate ja programmeerijate poolt kiirem, tuleb peale protokollistiku heakskiitmist välja töötada ka masinloetavad metaandmed.

2. Autentimisteenuste automaatne testimine – Autentimisprotokollistikule vastamist saab osaliselt kontrollida automatiseeritud vahenditega. OIDC arendamisega tegelev *OpenID Foundation* pakub selleks väljatöötatud testikomplekte ning nende kohandamine Eesti autentimisprotokollistikus tehtud valikutega aitaks kiirendada autentimisteenuste loomist ja täiendamist.

3. Autentimisprotokollistiku katsetamine enamlevinud süsteemitarkvaradega – praeguse eelanalüüsi käigus ei saanud põhjalikult kontrollida protokollistiku ühilduvust olemasolevate tarkvaradega, kuigi analüüsi käigus hangitud tagasiside põhjal juba tehti mõned lihtsustavad valikud. Testimise käigus saab välja selgitada, kas on vajalik mõnedes asutustes kasutuselolevate tarkvarade täiendamist või uuendamist.

4. Autentimisprotokollistiku kehtestamine sobiva õigusaktiga – kehtiva õiguse kohaselt on RIAl võimalik anda autentimisprotokollistiku kasutamiseks soovituslik juhis riikliku järelevalve subjektidele küberkaitse valdkonnas, kuid see ei laiene haldusjärelevalve subjektidele. Kui RIA avaldab autentimisprotokollistiku kui täiendava turvameetmete süsteemi, on teenuse osutajatel KüTSi järgi kohustus hinnata selle kasutuselevõttu küberintsidentide ennetamiseks ja nende mõjude vähendamiseks. Autentimisprotokollistiku reeglitele tugevama õigusjõu andmiseks tuleb kaaluda, kas kehtestada need seaduse alusel (nt KüTS või AvTS) või laiendada RIA pädevust juhiste andmise õigusega, mida saaks rakendada nii riikliku kui ka haldusjärelevalve subjektidele.

Nende sammude tegemisega saab Eesti tublisti edasi liikuda selleks, et eID ökosüsteemi täiustada – autentimisteenuste pakkujad ning tarbijad saaksid paremini toimiva „turuplatsi“ ning täiendavatel pakkujatel oleks lihtsam turule tulla ja tarbijatel mugavam teenuseid vahetada.

Kahjuks ei tähenda see, et edaspidi tööd enam teha pole vaja. Maailmas toimub praegu digitaalse identiteedi, autentimisprotokollide ja autentimisvahendite osas väga kiire areng, peamiselt seetõttu, et ka ülejäänud maailm on hakanud sarnaselt Eestile digitaalse identiteedi vajalikkusest ning kasulikkusest aru saama. Kiire areng tähendab muutusi ning Eesti peab:

(1) ülejäänud maailma arengute ja lahendustega kursis olema,

(2) osalema nende loomises ning suunama vajalikke standardeid endale sobivalt.

Vastasel korral riskib Eesti, et 5 aasta pärast on ta mahajäänud lahendusi kasutav „saareke“, kes enam uuemat tehnoloogiat kasutusele võtta ei saa.