TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Aleksandra Kuznetsova

Teadmise puudumise protokolli integreerimine infosüsteemidesse Smart Wallet näitel

Magistritöö

Juhendaja: Priit Raspel
Infotehnoloogia
teaduskond

Tallinn 2023

Sissejuhatus

Andme- ja küberkaitse muutuvad iga aastaga populaarsemaks teemaks, sest inimesed aina rohkem kasutavad oma mobiilseadmed maksmiseks, autentimiseks ja digitaalselt allkirjastamiseks. Seoses sellega Euroopa Liidu poolt kehtestatud eIDAS määrus, mis on seotus elektroonilise identiteediga, uuendatakse ja kehtestatakse uusi kontrollimise meetmeid kohandatud eIDAS 2.0 määruses. Uuendatud määrus kohustab Euroopa Liidu riike parandama turvameetmeid, laiendama kohaldamisala ning tutvustama ID-rahakoti. [1]

Peamine uuendus eIDAS 2.0 kontekstis on digitaalne rahakott ehk ID-rahakoti ehk EUID-rahakoti kasutuselevõtt. Iga Euroopa Liidu riik peab kohandama digitaalse rahakotti oma standarditega, tehnoloogiatega ja turvameetmetega. Digitaalse rahakotti all mõistetakse tarkvara, mida nii eraisikud kui ka ettevõtted saavad oma nutitelefoni alla laadida. Sellise rakenduse peamine eesmärk pakkuda võimalust salvestada ja hallata oma elektroonilise identifitseerimise ja usaldusteenustega seotud sertifikaate ja tõendeid ühes kohas. [1]

Käesoleva magistritöö eesmärk on läbi viia uue teenuse äri-, süsteemi- ja riskianalüüsid, mis on kohandatud Eesti standarditega, tehnoloogiatega ja turvameetmetega. Magistritöö tulemuseks on kirjeldatud teenuse kavand, mille põhjal saab arendama hakata uue teenuse. Uue teenuse olulisemaks komponendiks on krüptograafiliselt kodeeritud andmevahetus teadmise puudumise protokolli abil.

Hetkeseisuga puudub Eestis digitaalse rahakotti lahendus, mis võimaldaks sertifikaatide ja tõendite salvestamine ühe nutiseadme peale. Magistritöö analüüsi käigus võetakse arvesse eIDga seotud riiklik seadus ning luuakse kohandatud rakenduse kavand.

Magistritöö struktuur on ehitatud järgmiselt:

1. Esimeses peatükis autor kirjeldab probleemi, sellega kaasnevaid piiranguid ja kirjeldab analüüsi metoodikaid.

2. Teises peatükis autor kirjeldab ettevõtete tegevus- ja koostööala ning kirjeldab ellu viidud lahendusi.

3. Kolmandas peatükis autor annab ülevaade kasutatavas komponendist ja sarnasest kontseptsioonist, mis on välja pakutud Euroopa Liidu poolt.

4. Neljandas peatükis autor keskendub äri- ja süsteemianalüüsi peale ja kaardistab funktsionaalsed ja mittefunktsionaalsed nõuded.

5. Viiendas peatükis kirjeldab loodava süsteemi arhitektuuri ja disaini.

6. Kuuendas peatükis viiakse läbi riskianalüüsi, kus tuuakse välja teenusega seotud riske, riskide tekitamise tõenäosus, riskide mõju süsteemile ja meetmed riskide kontrollimiseks.

1 Ülesandepüstitus

1.1 Taust

Tänapäeval inimesed kasutavad interneti rohkem kui kunagi varem. Iga aastaga muutub küber- ja andmekaitse aina olulisemaks, kuna euroopa liidu regulatsioonid ja määrused läbivad sagedasi uuendusi. Lähtudes rangetest regulatsioonidest peavad ettevõtted kohandama oma teenuseid nii, et autentimise viis oleks turvaline. Vältimaks andmete leket, on igapäevastel internetitegevustel vaja turvalist keskkonda. Selle alla kuuluvad nii tundlike isiklike andmete kaitsmist kui ka teadlikkust küberturvalisuse põhimõtetest, kvaliteetseid tarkvara- ja riistvaralahendusi.

Andmete lekke vältimiseks tuleb kasutusele võtta autentimis lahendus, mis võimaldavad vajaliku teabe jagamist, aga samal ajal ei paljasta isiklike andmeid. Teadmise puudumise protokoll (*Zero knowledge proof või ZKP inglise keeles*) on krüptograafiline informatsiooni vahetamise meetod, kus isik saab tõestada väite, mis sisaldab teatud informatsiooni, seeläbi säilitades privaatse konteksti konfidentsiaalsuse. Selline lähenemine aitab vältida andmete leket ja muudab andmete pärimise ning tõestamise protsessi infosüsteemides tõhusamaks. Lisaks, teadmise puudumise protokolli kasutades on võimalik saavutada privaatsuse ja turvalisuse tasakaalu internetipõhistes teenustes ja süsteemides, kus kasutajad soovivad jääda anonüümseks või kaitsta oma isiklikke andmeid.

Teadmise puudumise protokolli hakatakse kasutama Euroopa Liidu piires uues kontseptsioonis nimega „EUDI Wallet“. EUDI Wallet või nutikas rahakott, mis on nutitelefoni põhine hoidla. EUDI Wallet'isse saab inimene lisada informatsiooni, näiteks juhiload ja tõendid, võimaldades Euroopa kodanikel ja ettevõtjatel jagada oma identiteediandmeid turvalisel ja mugaval viisil. [1]

1.2 Probleemi püstitus ja magistritöö eesmärk

Määrus (EL) 910/2014, tuntud kui eIDAS-määrus (elektroonilised identifitseerimis-, autentimis- ja usaldusteenused), on Euroopa reguleeriv raamistik, mis kehtestab elektroonilise

identifitseerimise ja usaldusteenuste reeglid ja standardid Euroopa Liidu liikmesriikides. [2] Infotehnoloogia arenguga uuendab Euroopa Liit eIDAS-määrust, mille eesmärk on hõlbustada turvalist ja sujuvat digitaalset suhtlust ELi liikmesriikides. Selle uuendusega avaldas Euroopa Komisjon uue kontseptsiooni EL Digitaalse Identiteeti rahakott (EU Digital Identity Wallet), mille põhiliseks tehnoloogiaks on teadmise puudumise protokoll ehk teatud informatsiooni turvaliselt viisil jagamine. Rahakotti eesmärk on võimaldada Euroopa kodanikel ja ettevõtjatel turvalisel ja mugaval viisil jagada oma identiteediandmeid. [3]

Käesoleva magistritöö probleem on turvaline andmete jagamine teadmise puudumise protokolli abil ja selle tehnoloogia integreerimine infosüsteemi Smart Wallet'i näitel, mida oleks võimalik kasutada Eestis. Magistritöö eesmärk on viia läbi analüüs teadmise puudumise protokollist, sellest tehnoloogiast, rakendamisest ja luua vajalik äriline ja tehnoloogiline kontsept uue põlvkonna eID teenuste osutamiseks vastavalt uuendatud eIDAS versioonile.

1.3 Võimalikud piirangud

Piiranguteks võib nimetada erinevaid faktoreid. Praegusel ajal on kätte saadaval üpriski palju informatsiooni krüptofraafilistest operatsioonides ja teadmise puudumise protokollist (ZKP), paraku on need väga tehnilised. Enamasti käsitletakse töötamise algoritme ja teoreeme. Lisaks sellele, kõik ISO standardid on tasulised ja nende kätte saadavus on üsna piiratud.

Käesoleva magistritöö piiranguks võib nimetada eIDAS ja eIDAS 2.0 määrused, mis seovad piiranguid ja reguleerivad riikide tegevusi. Autentimise teenused nõuavad kõrgemat turvalisust, mis omakorda nõuab tugevat analüüsi ja keerulist arendust.

1.4 Kasutatavad metoodikad

Käesolevas magistritöös rakendatakse erinevaid meetodeid probleemi analüüsimise ja lahenduse leidmiseks. Magistritööd alustatakse ülesande ja probleemi püstitamisega, millele järgneb kirjanduse analüüs ja ülevaade. Kirjanduse ülevaade hõlmab teadmise puudumise protokolli võimalikke variatsioone, kasutusalasi ja rakendus võimalusi. Seatakse reeglid uue kontseptsiooni väljatöötamiseks. Kasutatavad metoodikad, mis on selles magistritöö kasutusel, võib jagada kaheks: ärianalüüsi- ja süsteemianalüüsi metoodikad.

1.4.1 Ärianalüüsi metoodikad

- Ärireeglid: on formaalselt väljendatud juhised, mis kirjeldavad, kuidas ettevõte toimib ja milliseid tegevusi, otsuseid ja protseduure tuleb järgida ettevõtte igapäevatöös. Autor kasutab ärireegleid selleks, et kirjeldada teenuse reeglid.

- Äriinfo mudel: on visuaalne esitlus ärireeglitest. Magistritöös autor kasutab äriinfo mudelit selleks, et visualiseerida ärireegleid.

- Motivatsiooni mudel: raamistik, mida autor kasutab organisatsiooni äristrateegiate, eesmärkide ja motivatsioonide esitamiseks ja analüüsimiseks. Motivatsiooni mudel pakub struktureeritud viisil organisatsiooni strateegiliste algatuste määratlemiseks, dokumenteerimiseks ja kommunikeerimiseks. Motivatsiooni mudel aitab mõista, kuidas Nortali ja SK missioon ja visioon on seotud selle strateegiatega ja kuidas neid strateegiaid mõjutavad sise- ja välistegurid. [4]

- Väärtusvoo kaardistamine: Lean-haldustööriist, mida autor kasutab teenuse protsessi visualiseerimiseks, analüüsimiseks ja täiustamiseks. Diagrammi eesmärk on visualiseerida protsessi, tuvastada raiskamine ja arendada strateegiaid selle vähendamiseks. [5]

- BPMN - Business Process Model and Notation on graafiline notatsioon, mis võimaldab visualiseerida ja dokumenteerida äripritsessi. BPMN aitab paremini protsessi mõista nii analüütikutel, kui ka arendajatele. [6]

- SWOT analüüs: strateegiline tööriist, mida autor kasutab teenuse tugevuste (Strengths), nõrkuste (Weaknesses), võimaluste (Opportunities) ja ohtude (Threats) hindamiseks. See aitab paremini mõista teenuse sise- ja välist keskkonda ja kujundada tõhusaid strateegiaid. [7]

- SIPOC diagramm: tööriist, mida autor kasutab protsesside modelleerimiseks ja analüüsimiseks. Eriti protsesside, mis hõlmavad erinevate osapoolte koostööd. SIPOC aitab protsessi paremini mõista, tuvastada protsessiga seotud osapooli ja nende vajadusi. Aitab kaasa protsessi täiustamises ja optimiseerimises. [8]

1.4.2 Süsteemianalüüsi metoodikad

- Kasutusmallide mudel: visuaalne esitus süsteemi funktsionaalsetest nõuetest, mis autor kasutab, et paremini näidata süsteemi kasutajate või osapoolte seisukohast. See on väärtuslik kommunikatsiooni- ja dokumenteerimisvahend projektis osalevatele osapooltele, kuna sest see annab kõrgetasemelise ülevaate süsteemi käitumisest ilma tehniliste üksikasjadeta. [9]

- Evitusdiagramm: UML'i osa, mida autor kasutab tarkvarakomponentide füüsilise paigutuse modelleerimiseks võrguinfrastruktuuris. Need osad esitlevad visuaalselt kuidas tarkvarakomponendid, riistvara ja võrgu elemendid suhtlevad ja on seadistatud reaalses keskkonnas. [10]

- Komponentmudel: on tarkvaraarhitektuuriline lähenemisviis, kus tarkvarasüsteem jagatakse väiksemateks, iseseisvateks ja omavahel seostatud komponentideks. Komponentmudelit kasutatakse laialdaselt tarkvaraarenduses, et luua süsteeme, mis on skaleeritavad, hooldatavad ja laiendatavad. [11]

- MoSCoW: prioriteetsusmudel, mida autor kasutab antud projektis funktsionaalsete nõuete prioriseerimiseks. Selle mudeli nimi tuleneb selle viiest peamisest kategooriast: Must have (peab olema), Should have (peak olema), Could have (võiks olla), Won't have (ei pea olema), ja Would like (sooviksid). [12]

- FURPS+: on akronüüm, mis tähistab erinevaid tarkvara arenduse ja hindamise kvaliteediomadusi. Funktsionaalsus, kasutatavus, usaldusväärsus, jõudlus, toetavus on konkreetsed omadused, mis esinevad selles mudelis. Mudel on kasutusel tarkvaraarenduse valdkonnas, et tagada arendatava tarkvara mittefunktsionaalsete nõuetele vastavust, samuti ka teistele olulistele kvaliteedi- ja kasutatavuskriteeriumidele. [39]

- Andmemudel – on mudel, mis kirjeldab, kuidas andmed on korraldatud, talletatud ja seotud süsteemis või andmebaasis. Antud magistritöö autor kasutab relatsioonilist andmemudelit selleks, et näidata seosed andmete vahel. Andmemudelid pakuvad raamistikku, mis aitab mõista ja kujundada, kuidas andmed on struktureeritud ja kuidas nendega toimida. [13]

2 Kokkuvõte

Käesoleva magistritöö eesmärgiks oli teostada uue süsteemi analüüsi ja kavandamist. Magistritöö käigus autor analüüsis valdkonna kirjandust, mille põhjal tegi vajalikud analüüsiga ja arhitektuuriga seotud mudelid, kirjeldas süsteemi nõuded ning tõi välja riskid. Eesmärgi saavutamiseks, autor viis läbi järgmisi tegevusi:

1. Sõnastas ja kirjeldas valdkonna probleemi;
2. Kirjeldas ettevõtete koostöö ja tuleviku plaanid;
3. Kirjeldas ja analüüsis valdkonna kirjandust ning tõi välja kavandatava süsteemiga seotud kontseptsioon;
4. Koostas vajalikke ärimudeleid, mille põhjal kirjeldas ärinõuded;
5. Koostas ja kirjeldas kasutusmallide mudelit;
6. Tõi välja ja prioriseeris kavandatava süsteemi funktsionaalsed ja mittefunktsionaalsed nõuded;
7. Koostas kavandatava teenuse arhitektuurilise lahenduse koos vajalikke mudelitega;
8. Tõi välja riskid, mis on seotud uue teenusega, riskide tõenäosust, mõju süsteemile ja riskide kontrollimise meetmed.

Magistritöö lõpptulemusena ettevõtetel võimalik alustada Smart Walleti arendustöödega.

Magistritöö autori hinnangul püstitatud eesmärgid on saavutatud.