TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond
Informaatikainstituut

IDN70LT

Alvar Nõmmik 111677IAPM

Raamistikupõhine Raportite süsteemi kaardistamine AS Sertifitseerimiskeskuses Smart-ID projekti näitel

Magistritöö

Juhendaja: Tarmo Veskioja
Doktorikraad
Teadur

Tallinn
2016

Autorideklaratsioon

Kinnitan, et olen koostanud antud lõputöö iseseisvalt ning seda ei ole kellegi teise poolt varem kaitsmisele esitatud. Kõik töö koostamisel kasutatud teiste autorite tööd, olulised seisukohad, kirjandusallikatest ja mujalt pärinevad andmed on töös viidatud.

---------- ----------

(*kuupäev*) (*allkiri*)

Annotatsioon

Töös läbitakse AS Sertifitseerimiskeskuses käimasoleva Smart-ID projekti näitel protsess, mis aitab kaardistada erinevate osapoolte nõudeid täitva raportite süsteemi.

Igapäevaste tööülesannete täitmiseks ja otsuste tegemiseks on igal rollil vaja informatsiooni. Näiteks tootejuht vajab ülevaadet, kuidas teenuse käitumine on muutunud pärast versiooniuuendust. Samas klienditugi tegeleb konkreetse tõrke uurimisega ning peab vaatama vaid ühte terviksessiooni. Sellest tulenevalt kaardistatakse esmalt rollid ning nende infovajadused.

Autori hinnangul on vajalik juurutada metoodikat, mis võimaldab süstemaatiliselt läheneda raportite loomise protsessile.

Eesmärk on leida standardne arhitektuuri raamistik, mis aitab kaasa raportite infosüsteemi loomisele. Raamistik peab võimaldama saada ülevaade erinevatest rollidest, kes on raportitest huvitatud ja kirjeldama nende eesmärgid ning andmevajadused. Raamistiku abil tekib ülevaatlik pilt seostest erinevate rollide, raportite ning Smart-ID infosüsteemi vahel.

Lõputöö põhilised tulemused on:

1. Valmib eestikeelne metoodika dokument, mis kirjeldab ära raportite süsteemi loomise protsessi, mis on kasutatav ka teiste infosüsteemide puhul. Lisas 1 on metoodika ülevaatlikult esitatud ingliskeelsena.

2. Kaardistatakse infovajadused (nõuded infosüsteemile) – mis andmeid peab Smart-ID infosüsteem salvestama.

3. Kaardistatakse nõuded raportite infosüsteemile – millised raportid on vaja ning mis nõuded tekivad sellest tulenevalt kasutatavale vahendile.

Lõputöö on kirjutatud eesti keeles ning sisaldab teksti 62 leheküljel, 6 peatükki, 20 joonist, 5 tabelit.

Abstract

The aim of the thesis is to go through the process of creating the reporting system based on ongoing Smart-ID project in AS Sertifitseerimiskeskus.

The author is required to implement a methodology that allows for a systematic approach to the process of creating reports.

It is important to get an overview of the actual data needs – what information is needed to hold in the information system and it's logs. The need for provided data derives directly from the requirements of different stakeholders. It is necessary to map the links between systems using the Integrated Architecture Framework. [1]

The main results of the thesis are:

1. Estonian methodology document that will describe the process of creating the reporting system. Appendix 1 briefly describes used methodology in English.
2. Overview of the information needs to the Smart-ID system (data that needs to be provided to reporting system)
3. Requirements for the reporting system. What reports are needed and which related requirements arise.

The thesis is in Estonian and contains 62 pages of text, 6 chapters, 20 figures, 5 tables.

Lühendite ja mõistete sõnastik

SK	AS Sertifitseerimiskeskus
Splunk Enterprise	Vahend, mis pakub logihalduse ning raportite loomise funktsionaalsust.
Nagios	Monitooringu vahend, mida SK teenuste jälgimiseks kasutab.
API	***Application Programming Interface*** Liides, mida saab kasutada programmiga suhtlemiseks ja mille läbi on võimalik laiendada programmi funktsionaalsust.
Räsi	***Hash*** Digitaalne „sõrmejälg“ andmetest. Moodustatud kokku lepitud räsi funktsiooni abil.
Kolmas osapool	***Relying Party*** Sõltuv osapool, klient või partner, kes teenust kasutab.
Autentimine	***Authentication*** Isiku tuvastamine digitaalselt. Smart-ID kontekstis allkirjastatakse kasutaja autentimise privaatvõtmega kolmanda osapoole poolt valitud räsi.
Allkirjastamine (digitaalne)	***Signing (digital)*** Dokumendi räsi ja kasutaja allkirjastamise salajast võtit kasutades arvutatakse vastavalt kasutatavale krüptograafilisele räsifunktsioonile allkirja räsi.
IP	**IP address** Võrgus asuva seadme aadress.
SMS	***Short Message Service*** Tekstisõnumite saatmise teenus mobiiltelefonidel.

CA	***Certificate Authority*** Olem, mis väljastab digitaalseid sertifikaate.
Sertifikaat	***Certificate*** CA poolt välja antud elektrooniline tõend, mis seob isiku ja avaliku võtme. Võimaldab kontrollida isiku samasust.
IAF	***The Integrated Architecture Framework*** Integreeritud Arhitektuuri Raamistik. Loodud abivahendina, et luua seoseid IT ja äriloogika vahel.
OS	***Operating system*** Süsteemne tarkvara, mis haldab riistvara ja tarkvara ressursse (arvuti)süsteemis.

Jooniste nimekiri

Tabelite nimekiri

Sisukord

1. Sissejuhatus

Järjest enam räägitakse andmeanalüüsist ning mainitakse sõna „Suurandmed“ ning varasemast rohkem tekib suures mahus meta-andmeid. Autori arvates on SK –s liialt vähe tähelepanu pööratud reaalse andmevajaduse kirjeldamisele, mis on eelduseks vajalike raportite loomiseks. Raportite andmevajadusele ja funktsionaalsetele nõuetele tuleks mõelda juba infosüsteemi loomise algfaasis. Hilisemad muudatused võivad osutuda liialt kulukateks ning vajada süsteemi toimimise loogika täielikku ümber tegemist.

AS Sertifitseerimiskeskus (SK) on riiklikult akrediteeritud sertifitseerimis- ja ajatempliteenusele ning sellega seotud tarkvara arendusele ja opereerimisele keskendunud ettevõte.

SK põhitegevusteks on:

- sertifitseerimis- ja ajatempliteenuse pakkumine;
- digitaalallkirjastamise tehnoloogia ja rakenduste väljatöötamine;
- valideerimisteenuste pakkumine. [1]

SK on Mobiil-ID tulevikukindluse ja parema eksporditavuse suurendamiseks koostöös enda arenduspartneritega uurinud Mobiil-ID edasi arenduse võimalusi. Uuringute tulemusena on jõutud Mobiil-ID-le alternatiivne isikutuvastuse ja digitaalallkirjastamise lahenduseni, mille puhul ei ole vaja spetsiaalset SIM kaarti. Privaatvõtmed on hoitud serveri ja kasutaja telefoni vahel jagatud osakutena. Siinses magistritöös kutsutakse edaspidi seda lahendust Smart-ID’ks (SK sisene projekti nimi).

Smart-ID näol on tegu hajussüsteemiga, mis koosneb serveri-poolsetest komponentidest, kolmanda osapoole teenustest, telefoni operatsioonisüsteemist ning -rakendusest. Mitmed sõltuvused muudavad keeruliseks ja samas väga oluliseks regulaarse teenuse kvaliteedi mõõtmise ning potentsiaalse tõrkekoha välja selgitamise. Smart-ID projekti puhul on logimise nõuete loomisel kasutatud Tiit Hallase magistritööd [2], mis aga ei keskendu logimisele raportite loomise perspektiivist lähtudes. Raportite infosüsteem on toetav teenus, mis võimaldab erinevatel pädevusaladel saada ülevaadet jälgitavast infosüsteemist.

Töö teostamiseks leitakse sobiv raamistik, mis võimaldaks süstemaatiliselt läheneda raportite süsteemi nõuete kirjeldamisele ning kirjeldada seosed infosüsteemiga, mille andmete põhjal raporteid teostatakse.

Töö struktuur on esitatud joonisel 1.

1.1 Taust ja probleem

Seoses Smart-ID süsteemiga on asutusesisestel- ja kolmandatel osapooltel erinevad infovajadused, mille rahuldamiseks on tarvis spetsiifilisi raporteid ja analüüse. Näiteks teenusejuhile on vajalik teenusega seotud ülevaatlik statistika – näiteks kuidas erinevate süsteemi versioonidega muutub süsteemi käitumine. Klienditoel on olulisem ühe spetsiifilise olukorra uurimine ja kliendi probleemi lahendamine.

Ülaltoodud infovajaduste lahenduseks oleks juurutada keskne raportite infosüsteem, mis kogub kokku erinevate teenuste toimimise info ning võimaldaks nende põhjal erinevaid infovajadusi täitvaid otsinguid teostada. Statistilised otsingu tulemused peaks olema võimalik esitada ka graafilisel kujul.

Huvitatud osapoolteks võivad asutusesiseselt olla näiteks: tootejuht, teenusejuht, IT haldus, kasutajatugi. Ettevõtte-välisteks osapoolteks võivad olla kolmandad osapooled (kliendid, partnerid) ning infosüsteemi kasutajad.

Tüüpiline algatatud protsess läbib mitmeid erinevaid servereid ning keskkondi, kuid selle käigus maha salvestatavaid kirjeid võib olla kohati väga keerukas üheks tervikuks kokku siduda. Põhjuseks on ühtse identifikaatori puudumine.

Raportite koostamist raskendab ka asjaolu, kui tekkivas logis pole kõiki vajalikke andmeid. Tuleb põhjalikult läbi mõelda, mis andmed on tarvilik salvestada, et raportitele esitatud andmevajaduse nõudeid täita.

SK töötaja Mikk Mähar poolt teostatud diplomitöös „Keskse logihalduslahenduse rakendamine AS-is Sertifitseerimiskeskus“ valiti sobiliku logianalüüsi vahendina välja „*Splunk Enterprise*“. Töös läbiviidud analüüsi kohaselt vastas toode kõige paremini ettevõtte poolt seatud nõuetele. [3].

Splunk on võimekas logihaldus ja andmeanalüüsi vahend, mis võimaldab koguda logide andmed erinevate seadmete ja rakenduste lõikes. Päringud meenutavad kohati andmebaasi süntaksile sarnast päringute loomise keelt. Mugavaks kasutamiseks on loodud veebipõhine

graafiline kasutajaliides, mis võimaldab kasutajal luua uusi või kasutada juba varem defineeritud otsinguid. [4]

Kuna hetkel ons AS Sertifitseerimiskeskuses käimas Smart-ID projekt, mis on arenduse faasis, siis kasutatakse projektis loodavat süsteemi antud töös näitena.

1.2 Ülesande püstitus

Magistritöö eesmärk on leida standardne raamistik raportite loomiseks, Smart-ID projekti näitel läbitakse punktid, mis võimaldavad:

1) kaardistada raportitest huvituvad rollid;
2) leida rollide nõuded raportitele – mis raporteid näha soovitakse;
3) selgitada välja infovajadus – analüüsida, mis andmed on tarvilikud raportite teostamiseks ja koostada selle põhjal andmemudel ja nõuded, mis oleks jälgitavale infosüsteemile sisendiks;
4) veenduda olemasoleva vahendi sobilikkuses raportite teostamiseks või valida välja uus;

Töö tulemusest saadav kasu on:

1. Valmib metoodika, mida aluseks võttes saab kaardistada raportite loomiseks vajalikud eeldused mistahes teisele SK infosüsteemile.
2. Smart-ID projekti raportite süsteemi loomise võimaldamiseks kaardistatakse selleks vajalikud eeldused – huvituvad rollid, infovajadus ja nõuded raportitele ja raportite loomise vahendile.
3. Smart-ID projekti näitel läbitakse metoodikas kirjeldatud punktid ning selle tulemusena saab anda hinnangu raamistiku sobivuse kohta.

1.3 Metoodika

Antud peatüki eesmärk on valida metoodika, mis aitaks kaasa raportite infosüsteemi juurutamisele SK-s. Metoodikaga koos valitakse välja ka sobilik raamistik infosüsteemide

vaheliste seoste kirjeldamiseks. Raamistik peab omama võimekust kaardistada süsteemide toimimise loogika üldisel tasemel, keskendumata detailselt lahenduse disaini loomisele. Raamistik peab võimaldama piisavat paindlikkust, et muuta kirjeldamise protsessi ettevõttele sobivamaks. Antakse ülevaade teenuste toimimise loogikatest ning omavahelistest seostest. Kaardistatakse nõuded.

1.3.1 Ettevõtte arhitektuuri raamistike tutvustus

Zachmani raamistik „*The Zachman Framework for Enterprise Architectures*“ on laialdaselt kasutatud ettevõtte arhitektuuri dokumenteerimise ja arendamise raamistik. Raamistiku vertikaalne tasand vastab küsimustele „mida?“, „kuidas?“, „kus?“, „kes?“, „millal?“ ja „miks?“. Horisontaalse taseme vaated on: planeerija-, omaniku-, projekteerija-, ehitaja-, alltöövõtja vaade ja toimiv organisatsioon. [5]

Teine tuntud arhitektuuri raamistik on Integreeritud arhitektuuri raamistik „*Integrated Archidecture Framework*“, mis on välja töötatud Capgemini poolt. Arendus algas 1993. aastal ning on järjepidevalt parimatele praktikatele tuginedes arenenud. Tegemist on väga paindliku raamistikuga ning võimaldab kohanduda vastavalt ettevõtte vajadustele. See koosneb horisontaalsetest abstraktsest tasemetest, mis vastavad küsimustele: „miks?“, „mida?“, „kuidas?“, „millega?“. Vertikaalne tasand vaatab äri, informatsiooni, informatsioonisüsteemide ja tehnoloogia infrastruktuuri taset. (Lisa 2) [6]

1.3.2 Sobiliku raamistiku valik

Antud projekti raames keskendutakse infosüsteemide kirjeldamise tasemele. Eesmärk on leida raamistik, mis oleks piisavalt abstraktse tasemega, et ülevaatlikult kirjeldada ideaalset tulemust. Samas peaks olema võimalus laiendada raamistikku juba kitsamatele vaadetele. Võrreldavad raamistikud on omavahel väga sarnased ja omavad kattuvaid alamosi. IAF meenutab Zachmani lihtsustatud versiooni, pakkudes kolmanda dimensioonina juurde põhjalikuma äri ja turvalisuse vaate kirjeldamise. [7]

Ettevõtte arhitektuuri raamistike hindamise skaala, mille alusel toimub arhitektuuri raamistike hindamine:

1 pall: ei kajasta teemat.

2 palli: kajastab teemat ebapiisavalt.

3 palli: saab teemaga aktsepteeritavalt hakkama.

4 palli: saab hästi hakkama teema kajastamisega.

Tabel 1 - Ettevõtte arhitektuuri raamistike võrdlus

	Hinnang (4 palli skaalal)	
Kriteerium	Zachmani raamistik	IAF
Äri fookus	2	3
Raamistiku põhjalikkus	4	3
Rakendamise lihtsus	2	3
(tehnoloogia) Paindlikkus	3	4
Kokku	**11**	**13**

Hindamise põhjal selgus, et IAF pakub paindlikumat ning suurema äri fookusega lähenemist. Põhiliseks plussiks on rakendamise lihtsus: IAF-is antakse rakendamisest hea ülevaade ning näpunäited, kuidas kombineerida paindlikult näiteks erinevate UML mudelitega.

1.3.3 Metoodika kirjeldus

Töö teostamiseks osutus kahest võrreldud raamistikust paremaks Integreeritud Arhitektuuri Raamistik (*The Integrated Architecture Framework - IAF*). [6]

Töö käigus keskendutakse IAF infosüsteemi vaatele, mille puhul läbitakse neli abstraktset taset.

Esimeses osas antakse ülevaade Smart-ID infosüsteemist:

1. Antakse ülevaade infosüsteemist, mille andmete põhjal raporteid teostama hakatakse:
    1.1. Kirjeldatakse konteksti taset (tekib ülevaade, miks infosüsteem loodud on).
    1.2. Kirjeldatakse kontseptuaalset taset (tekib ülevaade, mida infosüsteem teeb - kasutuslood).
    1.3. Kirjeldatakse loogilist taset (tekib ülevaade, kuidas süsteem toimib - jadadiagramm).

1.4. Kirjeldatakse füüsilist taset (tekib ülevaade mis vahendeid kasutatakse füüsilisel tasemel)

Teises osas keskendutakse raportite infosüsteemi vajaduste kaardistamisele:

2. Antakse ülevaade raportite infosüsteemist:
   2.1. Kirjeldatakse konteksti taset
   2.2. Kirjeldatakse kontseptuaalset taset (kasutuslood erinevate osapoolte vaates – mida süsteem tegema peaks).
   2.3. Kirjeldatakse loogilist taset (soovilood – kuidas süsteem toimima peaks)

Kolmandas osas keskendutakse Smart-ID infosüsteemi nõuete kaardistamisele.

3. Püstitatakse nõuded infosüsteemile (Kaardistada - sisendiks eelnevad kaks punkti).

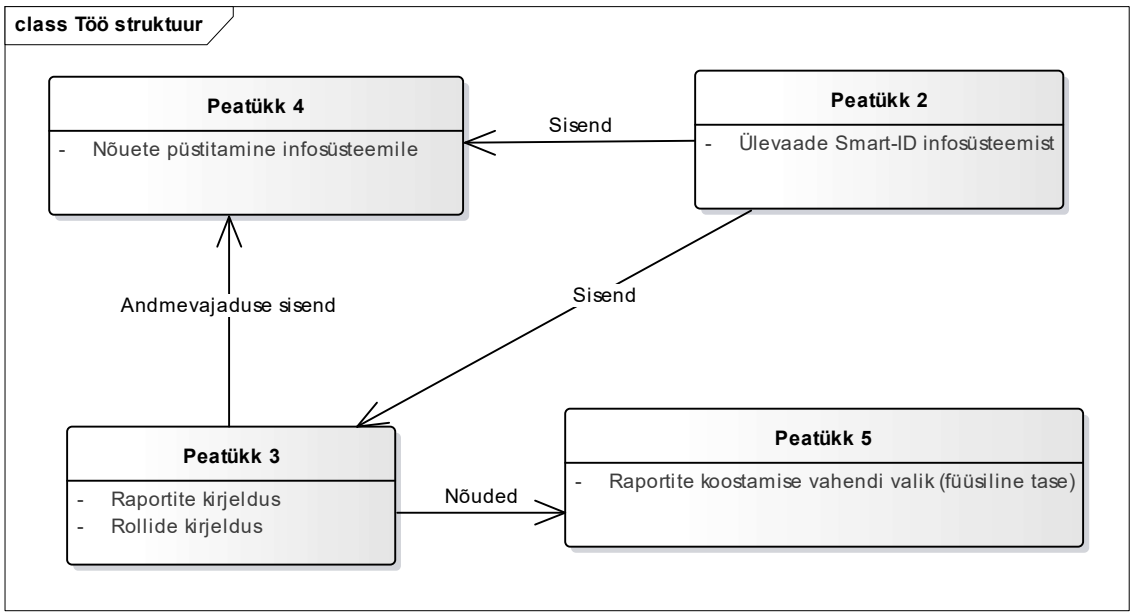
a) Milliseid andmeid on vaja raportite / monitooringute teostamiseks?
b) Mis andmeid oleks tarvis erinevates serverites olevate logikirjete seostamiseks?
c) Mis andmed on olemas / juba logitakse?
d) Mis andmeid oleks juurde vaja?

Neljandas osas tegeletakse raportisüsteemi füüsilise taseme kirjeldamisega. Vaadatakse üle sobilikkus nõutud raportite teostamiseks.

4. Raportisüsteemi füüsiline tase (nõuded raportite koostamise / analüütika vahendile – Vastab küsimusele: millega?)

- Mis funktsioonid peavad olema toetatud, et nõutud raportid / monitooringud teostada. Sobiliku analüütika vahendi valik.
- Analüüs, kas olemasoleva või väljavalitud vahendi puhul on nõuded täidetud.
- Mis oleks vaja lisada / või mõne muu vahendiga teostada?

1.4 Ülevaade tööst



Joonis 1 - Töö struktuur

Töö teises peatükis kirjeldatakse Smart-ID infosüsteemi põhilisi kasutuslugusid. Antakse ülevaade Smart-ID infosüsteemist – peamistest funktsionaalsustest ja süsteemi komponentide seostest. Peatükk võimaldab paremini aru saada raportite soovilugude ja infosüsteemi loginõuete seostest ning on neile sisendiks.

Kolmas peatükk keskendub raportite kirjeldustele. Kaardistatakse erinevad raportitest huvituvad rollid. Antakse ülevaade intervjuudest, et selgitada välja, milliseid raporteid on tarvilik infovajaduste täitmiseks koostada. Pakutakse sisendit raportite koostamise vahendile esitavate nõuete analüüsiks ning Smart-ID süsteemile.

Neljandas peatükis toimub eelnevaid peatükke sisendiks võttes infosüsteemile nõuete püstitamine. Selgitatakse välja infovajadus ning nõuded Smart-ID logidele.

Viiendas peatükis kaardistatakse funktsionaalsed nõuded raportite koostamise vahendile. Selgub, millist võimekust peaks vahend omama. Vaadeldakse valitud raportite loomise vahendi võimalusi ning sobivust.

Töö teostamisel on kasutatud Integreeritud Arhitektuuri raamistikku, mis võimaldab arusaadavalt esitada infosüsteemide vahelisi seoseid.

Antud raamistik koosneb neljast tasemest:

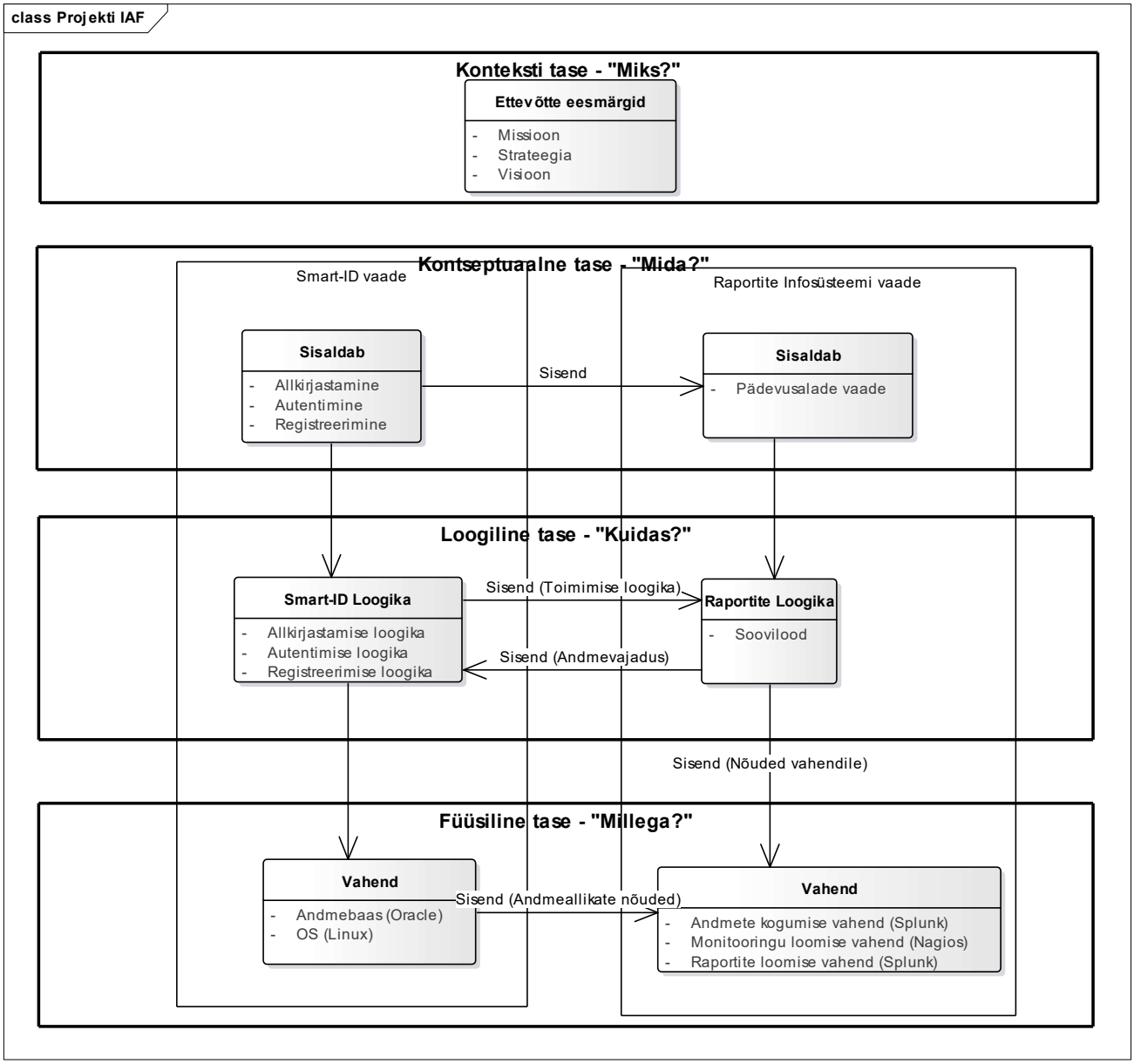
1. Konteksti tase – vastab küsimusele „Miks?“. Infosüsteemi üldine tase, mis keskendub eesmärkidele, strateegiale ja visioonile, millel ettevõte põhineb.

2. Kontseptuaalne tase – vastab küsimusele „Mida?“. Tase, kus kaardistatakse probleemid, mida on vaja lahendada.

3. Loogiline tase – vastab küsimusele „Kuidas?“. Tase, mis aitab leida ideaalse tulemust , mis on lahendusest sõltumatu. Analüüsi väljundiks on soovitud tulemuse visioon.

4. Füüsiline tase – vastab küsimusele „Millega?“. Piiritletud nõuete ja juhistega tase, mis on seotud loogilise taseme tulemuse „tõlkimisega“ ettevõtte struktuuri. [8]

Antud projekti raames kasutatakse infosüsteemide põhist vaadet ja keskendutakse süsteemidevahelistele seostele (Joonis 2).



Joonis 2 - Integreeritud Arhitektuuri vaade

2. Ülevaade Smart-ID infosüsteemist

Peatüki eesmärgiks on anda ülevaade infosüsteemist, mille kohta raporteid realiseerida soovitakse.

Läbi käiakse kõik raamistikus käsitletud tasemed (Lisa 2):

Kontseptuaalsel tasemel antakse ülevaade, miks Smart-ID vajalik on.

Kontseptuaalsel tasemel antakse ülevaade, mida süsteemis teha saab ning mis on peamised funktsionaalsused.

Loogilisel tasemel antakse ülevaade, mis moodi süsteem loogika mõttes toimib. Kasutuslood võimaldavad kirjeldada funktsionaalsust, mis on olulised pädevusala, süsteemi või tarkvara jaoks.

Füüsiline tase annab ülevaate, milline on abstraktsel tasemel süsteemi ülesehitus. Tekib arusaamine, mis vahendeid kasutatakse andmete ja logide hoiustamiseks. Tulemus annab sisendi raportite infosüsteemile, esitades nõuded andmete hankimise võimekusele. [8]

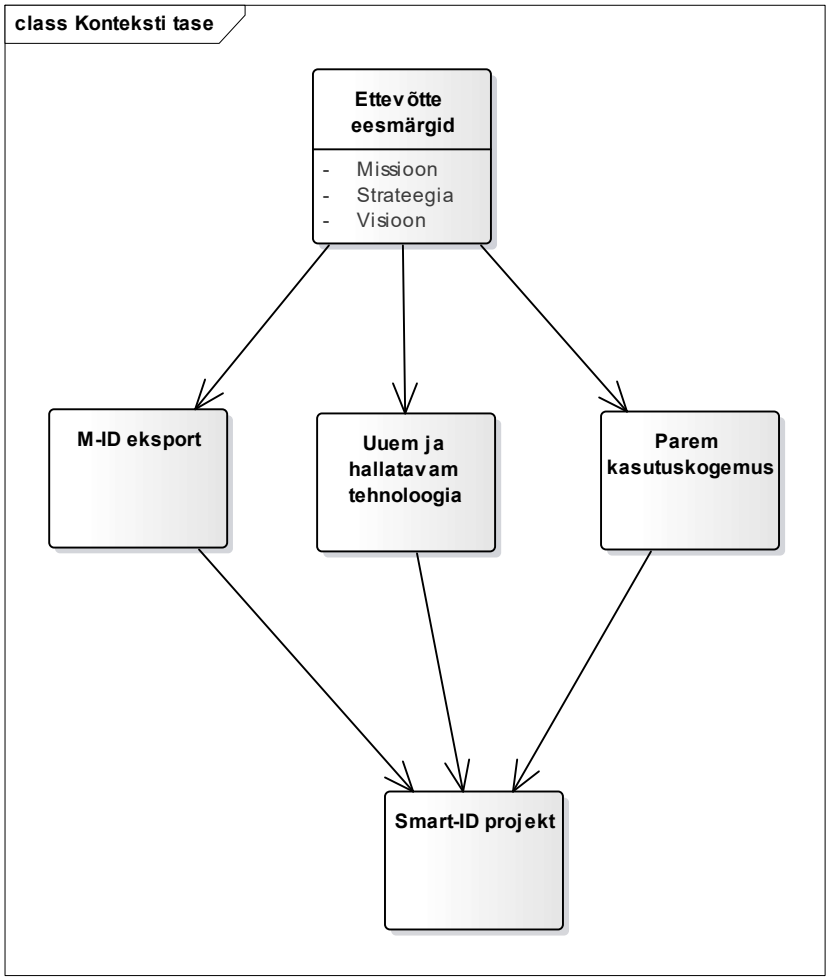
2.1 Smart-ID konteksti tase

Smart-ID on Mobiil-ID-le alternatiivne isikutuvastuse ja digitaalallkirjastamise lahendus, mille puhul ei ole vaja spetsiaalset SIM kaarti. Privaatvõtmed on hoitud serveri ja kasutaja telefoni vahel jagatud osakutena.

Ettevõttele pakub Smart-ID suuremat võimekust eksportida Mobiil-ID-d. SIM kaartidel põhineva lahenduse miinuseks on keeruline väljastusprotsess. SIM kaart on vaja toota, väljastada kliendile ja seejärel aktiveerida. Kliendile tekitab see ebameeldivusi, kuna Mobiil-ID kasutusele võtmisel tuleb välja vahetada SIM kaart, mis eeldab esinduses kohapeal käimist.

Mobiil-ID puhul kasutatakse andmeühendusena serveri ja telefoni vahel SMS-e. siis Smart-ID puhul on kasutusel internetiühendus. SIM rakenduse asemel on kasutusel mobiilirakendus, mis lisab võimalusi kasutajakogemuse tõstmiseks. Mobiilirakenduse kasutamine avab mitmeid uusi võimalusi, kuidas teenuse kvaliteeti mõõta ja parandada.

SIM kaardi nõudest loobumine võimaldab Smart-ID-d võtta kasutusele seadmetes, kus sim kaart puudub (nt. mõned tahvelarvutid)



Joonis 3 - Smart-ID konteksti tase

Joonisega kirjeldatakse ettevõtte eesmärkide ja projekti vaheline seos. Projekt aitab kaasa ettevõtte eesmärkide täitmisel.

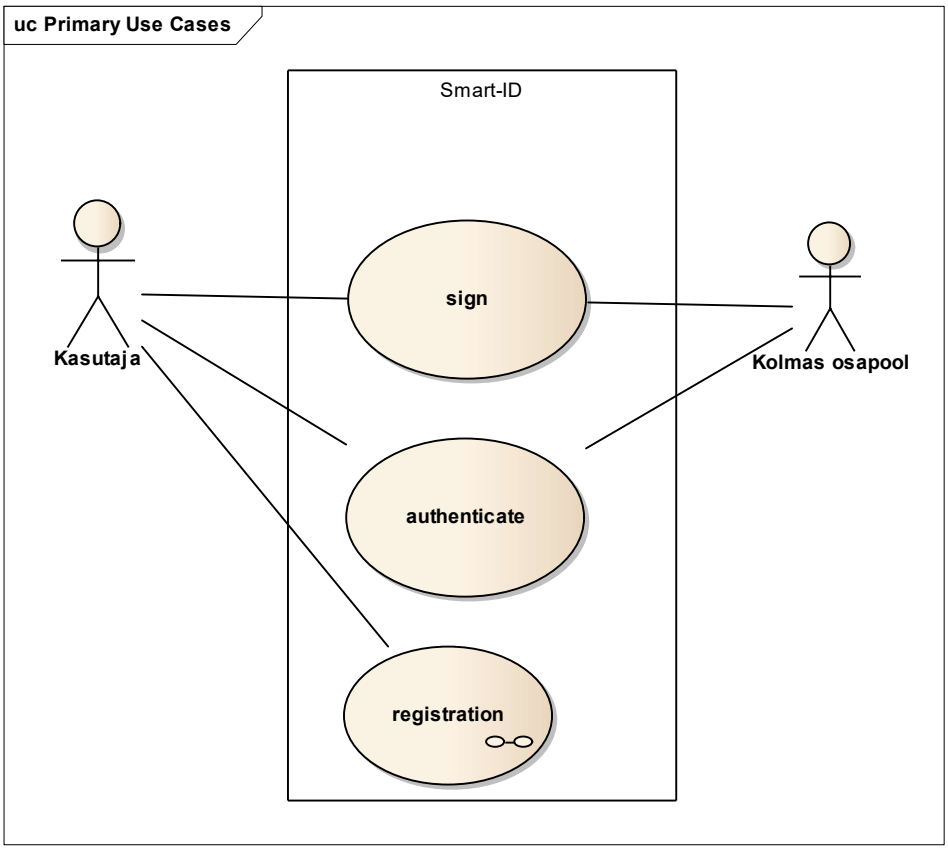
2.2 Smart-ID kontseptuaalne tase

Smart-ID kolm põhilist kasutus-stsenaariumit on autentimine (kasutaja tuvastamine), allkirjastamine ja registreerimine.

1. Registreerimise protsessi käigus luuakse kasutajale uus profiil, genereeritakse privaatvõtmed ning seotakse reaalse isikuga.

2. Allkirjastamise protsessi käigus signeerib kasutaja Kolmanda osapoole süsteemis loodud dokumendi räsi.

3. Autentimise protsessi puhul soovib kasutaja siseneda Kolmanda osapoole infosüsteemi.



Joonis 4 - Smart-ID kasutuslood

2.3 Smart-ID loogiline tase

Smart-ID loogiline tase koosneb kolmest põhilisest funktsionaalsusest: registreerimine, autentimine ja allkirjastamine. Järgnevalt keskendutakse igale funktsionaalsusele eraldi.

2.3.1 Registreerimine

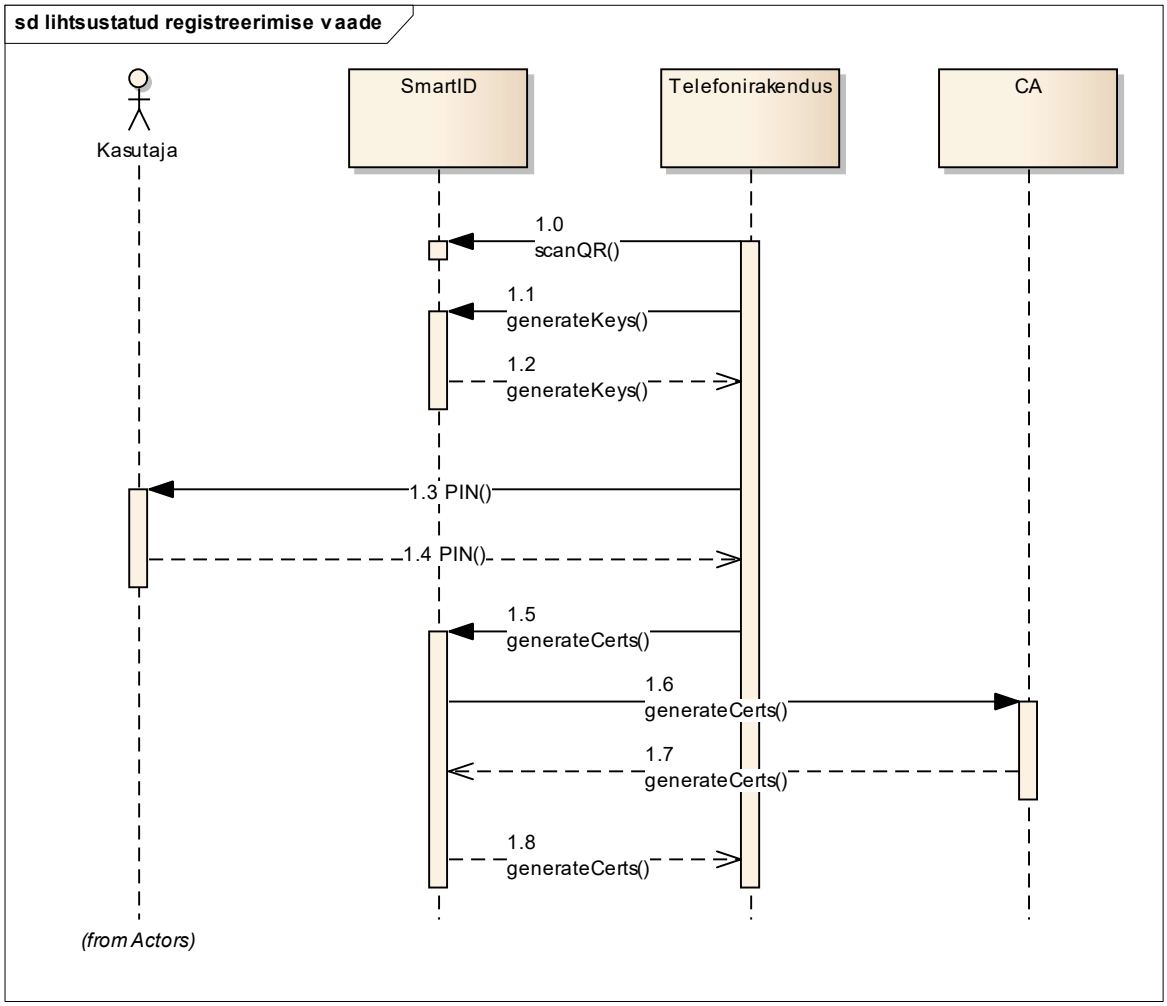
Kasutaja loob uue Smart-ID konto, mille käigus genereeritakse teenuse kasutamiseks (allkirjastamine / autentimine) tarvilikud võtmed ning seejärel seostatakse reaalne isik loodud võtmetega. Eesti puhul on võimalik kasutada kvalifitseeritud digitaalset isikutuvastust – ID kaart või mobiil-ID. [9] Riikide lõikes võib protsess erineda. Seega kasutusloo puhul keskendutakse registreerimise üldisele protsessile, mille käigus genereeritakse kasutajale privaatvõtmed.

Smart-ID konto registreerimise eeldused:

- Smart-ID mobiilirakendus on paigaldatud nutitelefoni.
- Kasutaja alustab registreerimise protsessi Smart-ID portaalis.

Põhiline lihtsustatud kasutuslugu:

1. Telefonirakendus skaneerib QR koodi
2. Telefonirakendus käivitab võtmete genereerimise protsessi
3. Telefonirakendus küsib PIN1 ja PIN2 koodi
4. Kasutaja sisestab PIN1 ja PIN2
5. Telefonirakendus käivitab sertifikaadi loomise protsessi
6. Smart-ID süsteem edastab sertifikaadi päringu CA –le
7. CA tagastab sertifikaadid Smart-ID rakendusele
8. Smart-ID rakendus edastab sertifikaadid telefonirakendusele



Joonis 5 - Registreerimise jadadiagramm

2.3.2 Autentimine

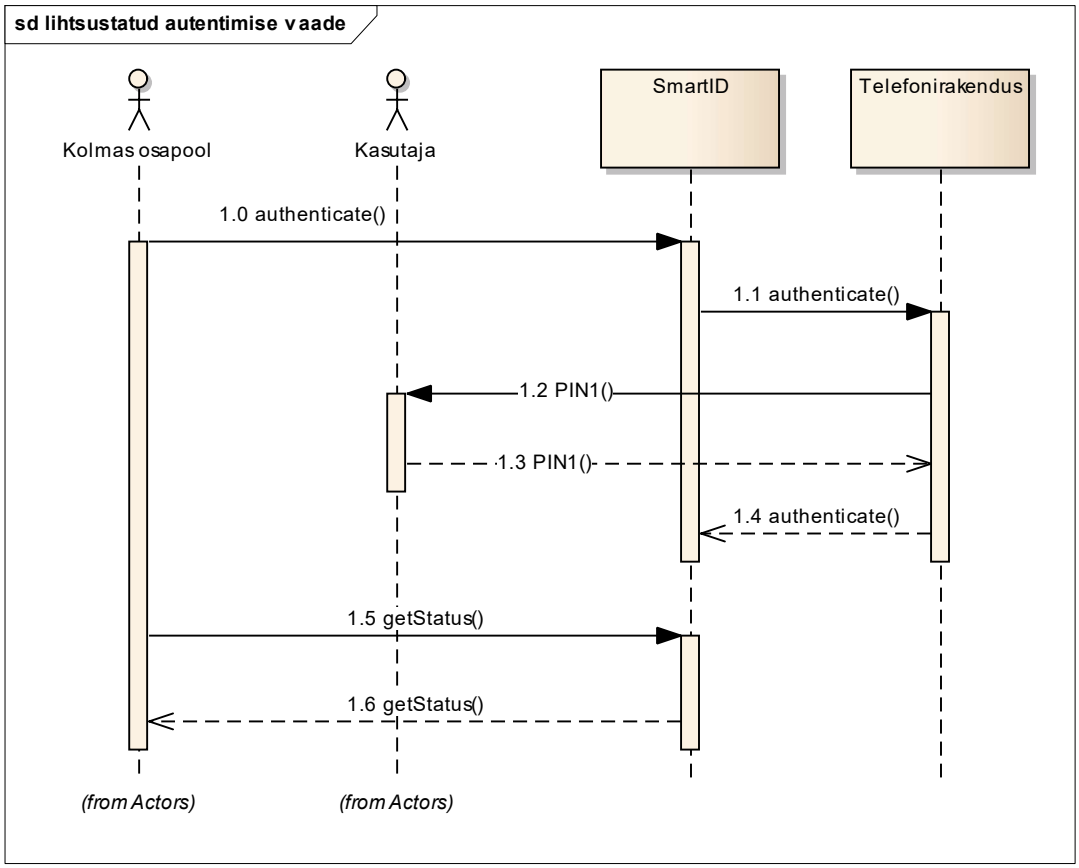
Autentimise käigus selgitatakse välja, kes on süsteemi pääseda sooviv isik. Tihtilugu on infosüsteemides kasutusel kasutajanime ja parooli kombinatsioon, mis ei pruugi turvalisuse tagamiseks olla piisav. Smart-ID pakub lisaturvalisust – autentimise eelduseks on eelnevalt läbitud protsess, mille käigus tekib nutitelefoni kasutajaga seotud profiil koos võtmetega.

Smart-ID autentimise eeldused:

1. Smart-ID mobiilirakendus on paigaldatud nutitelefoni.
2. Kasutaja on registreerinud Smart-ID profiili
3. Kasutaja alustab autentimise protsessi „Kolmanda osapoole“ portaalis, infosüsteemis või rakenduses.

Autentimise põhiline lihtsustatud kasutuslugu:

1) Kolmanda osapoole teenus edastab autentimispäringu.
2) Smart-ID teenus edastab päringu Kasutaja telefoni.
3) Kasutajalt küsitakse PIN1.
4) Kasutaja sisestab PIN1.
5) Mobiilirakendus suhtleb Smart-ID teenusega ning kasutaja saab tuvastatud.
6) Kolmanda osapoole teenus edastab päringu sessiooni staatuse kohta.
7) Smart-ID edastab Kasutaja andmed ja allkirjastatud räsi.



Joonis 6 - Autentimise jadadiagramm

2.3.3 Allkirjastamine

Digitaalne allkiri võimaldab elektrooniliselt sõlmida lepinguid, Digitaalallkirja olemust ning kasutamist reguleerib Eestis "Digitaalallkirja seadus" ehk DAS, mis võeti vastu 7. märtsil 2000. aastal.

Digitaalne allkiri on seaduse silmis võrdne omakäelise allkirjaga. Kõik Eesti ametiasutused on kohustatud võtma vastu digitaalselt allkirjastatud dokumente. [10]

Alates 1. juulist 2016 jõustub eIDAS regulatsioon, mille eesmärk on kõrvaldada takistused e-identimise vahendite piiriülesel kasutamisel, mida liikmesriikides kasutatakse avalike teenuste autentimisel. See tähendab, et digitaalset identifitseerimist on võimalik teostada piiriüleselt kõigis Euroopa Liidu riikides. [11]

Smart-ID mõistes on tegemist dokumendist genereeritud räsi allkirjastamisega, kasutades mobiiltelefoni- ja serverirakendust.

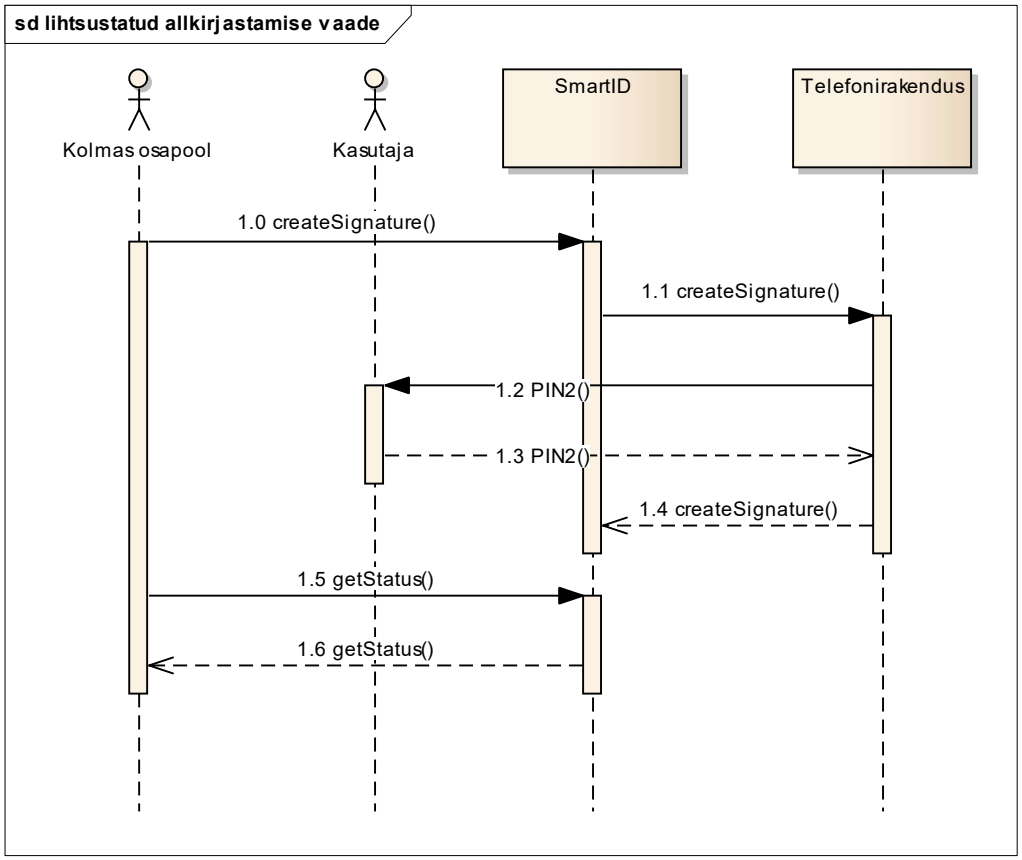
Smart-ID allkirjastamise eeldused:

1. Smart-ID mobiilirakendus on paigaldatud nutitelefoni.
2. Kasutaja on registreerinud Smart-ID profiili.
3. Kasutaja alustab allkirjastamise protsessi „Kolmanda osapoole“ portaalis.

Allkirjastamise põhiline lihtsustatud kasutuslugu:

1) Kolmanda osapoole teenus edastab allkirjastamise päringu (allkirjastatava dokumendi räsi).
2) Smart-ID teenus edastab päringu Kasutaja telefoni.
3) Kasutajalt küsitakse PIN2.
4) Kasutaja sisestab PIN2.
5) Mobiilirakendus suhtleb Smart-ID teenusega ning luuakse allkirjastatud räsi.
6) Kolmanda osapoole teenus edastab päringu sessiooni staatuse kohta.

7) Smart-ID edastab Kasutaja poolt allkirjastatud räsi.



Joonis 7 - Allkirjastamise jadadiagramm

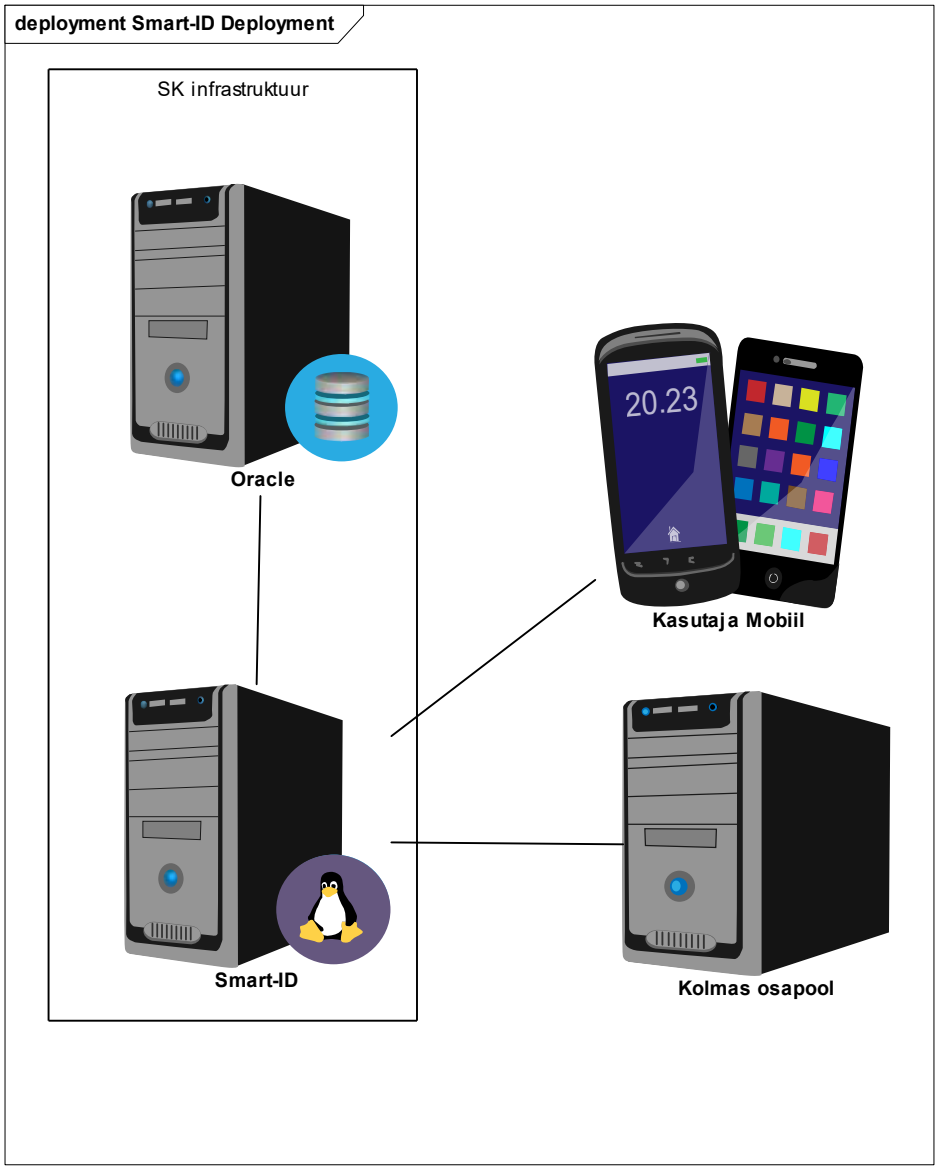
2.4 Smart-ID infosüsteemi füüsiline tase

Peatükis antakse ülevaade, mis vahendeid kasutatakse süsteemi füüsilisel tasemel. Peatüki eesmärk on anda sisend raportite infosüsteemile võimekusest, mis on vajalik süsteemi poolt loodud andmete kätte saamiseks. Lisaks tutvustatakse süsteemi seoseid erinevate osapooltega.

Smart-ID kasutab infosüsteemi spetsiifiliste andmete hoidmiseks Oracle andmebaasi. Infosüsteemi tegevuste käigus tekib rakenduse logi, mis kirjutatakse failidesse. Smart-ID näol on tegu hajussüsteemina, mis koosneb serveri poolsetest komponentidest ning on horisontaalselt skaleeritav.

Lisaks ettevõtte sisesele suhtlusele vahetab Smart-ID teenusega sõnumeid ka Kolmanda osapoole teenused ning kasutaja mobiiltelefonis asuv rakendus. Kõik osapooled loovad tegevuse käigus enda juurde andmeid, kuid ettevõttel puudub ligipääs mobiiltelefoni ja kolmanda osapoole logidele. Liideste kaudu on võimalik mobiilirakendusel ning kolmandal osapoolel mingil määral infot edasi anda. SK kontrolli all on nii mobiilirakendus, kui ka API-d, seega on võimalus kohandada neid vastavalt vajadusele.

Leppima peab infoga, mida edastatakse Smart-ID infosüsteemile läbi API-de. Päringute sisu hoitakse logides või andmebaasis.



Joonis 8 - Smart-ID füüsiline tase

3. Raportite kirjeldus

Magistritöös lähtutakse Mike Cohn poolt esitatud kasutuslugude kirjeldamise metoodikast, milles on oluline, et lood kajastaksid võimalikult detailselt pädevusala soove. Seetõttu peab vältima tehnilist žargooni ning olema esitatud „ärivaate“ keeles. Metoodika sai valitud arusaadavuse ja lihtsuse tõttu. Parimat ülevaadet nõuetest omab otseselt raportitest huvitatud pädevusala. Kõige lihtsama vahendit selles pakub kirjeldada kasutajate poolt esitatavad soovid raportite infosüsteemile [12].

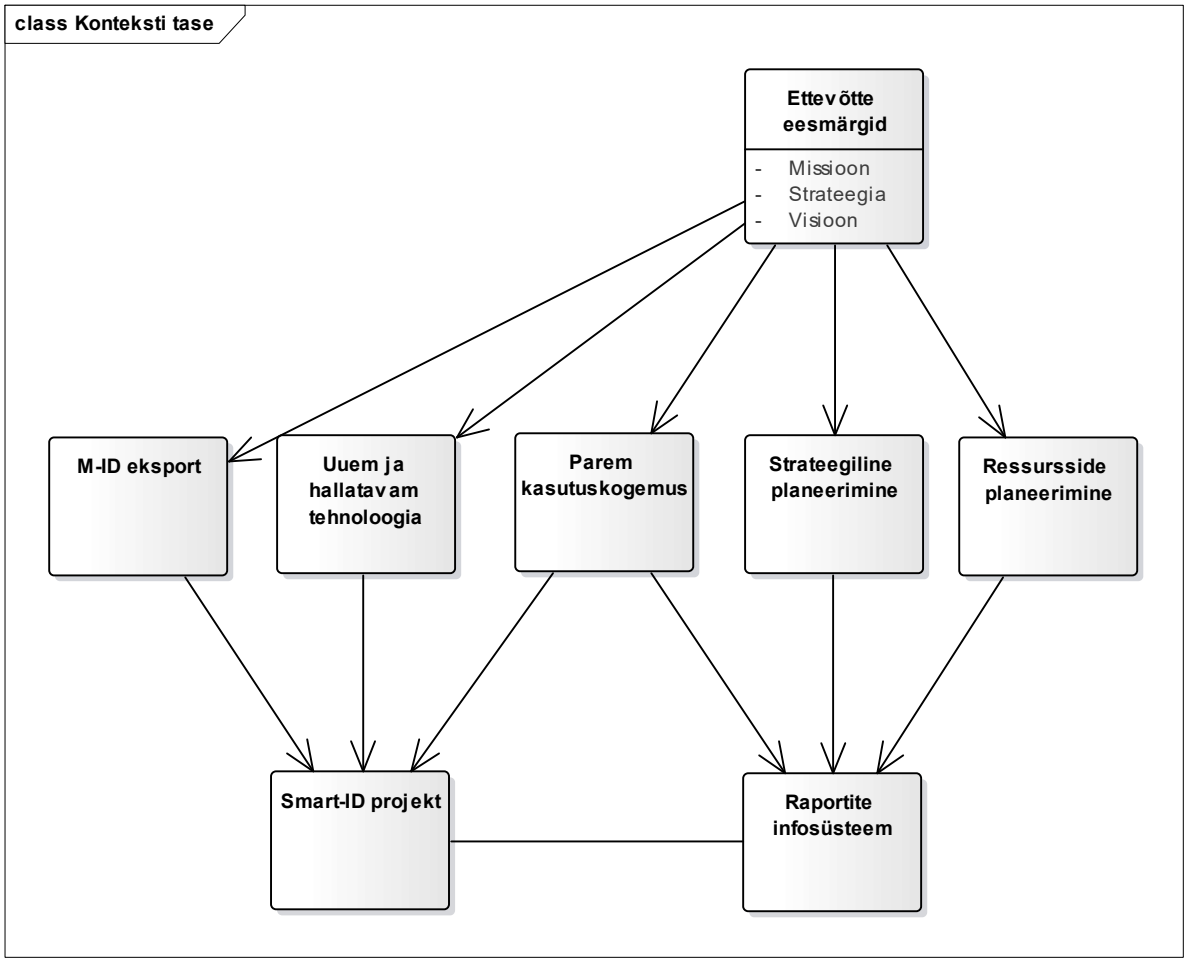
Antud peatükis toimub raportite / jälgimissüsteemide defineerimine. Ülevaate saamiseks:

1. Kirjeldatakse raportite infosüsteemi konteksti taset – antakse ülevaade, miks süsteem ettevõttele vajalik on.
2. Kirjeldatakse kontseptuaalset taset ja antakse ülevaade, mida infosüsteem teeb (pädevusalade vaade).
3. Kirjeldatakse loogilist taset ja antakse ülevaade, kuidas süsteem toimima peaks (st milliseid raporteid on tarvis?). Selleks:
   3.1 Teostatakse intervjuud erinevate osapooltega, mis formuleeruvad raportite soovilugudena.
   3.2 Kategoriseeritakse / grupeeritakse sisu järgi (intervjuude põhjal tekkinud soovide grupeerimine ning raportivajaduste grupeerimine sarnaste nõuete järgi).
   3.3 Planeerimine raportite loomine, et asetada raportid tähtsuse alusel järjekorda.

3.1 Raportite infosüsteemi konteksti tase

Ettevõtte soovib eesmärkide täitmiseks saada informatsiooni, mis toetaks strateegilise planeerimise, ressursside planeerimise ning parema kasutuskogemuse pakkumise protsessi.

Mainitud tegevuste täitmiseks on sisendina vaja infot, mille hankimist saab lihtsustada raportite infosüsteem.



Joonis 9 - Raportite infosüsteemi konteksti tase

Joonisega kirjeldatakse ettevõtte eesmärkide ja projekti vaheline seos. Projekt aitab kaasa ettevõtte eesmärkide täitmisel.

3.2 Raportite infosüsteemi kontseptuaalne tase

Pädevusala väljendab osapoolt, kellel on huvi saada Smart-ID infosüsteemi raporteid. „Kes?“ tähistab isikut, kes on pädevusala huvide eest vastutajaks ning kellega abiga koostatakse soovilood. Kasutaja ja kliendi soovidest on kõige parem ülevaade teenusejuhil. Sellest johtuvalt otsustati nende rollide puhul kasutada nende rollide huvide eest vastutavana teenusejuhti.

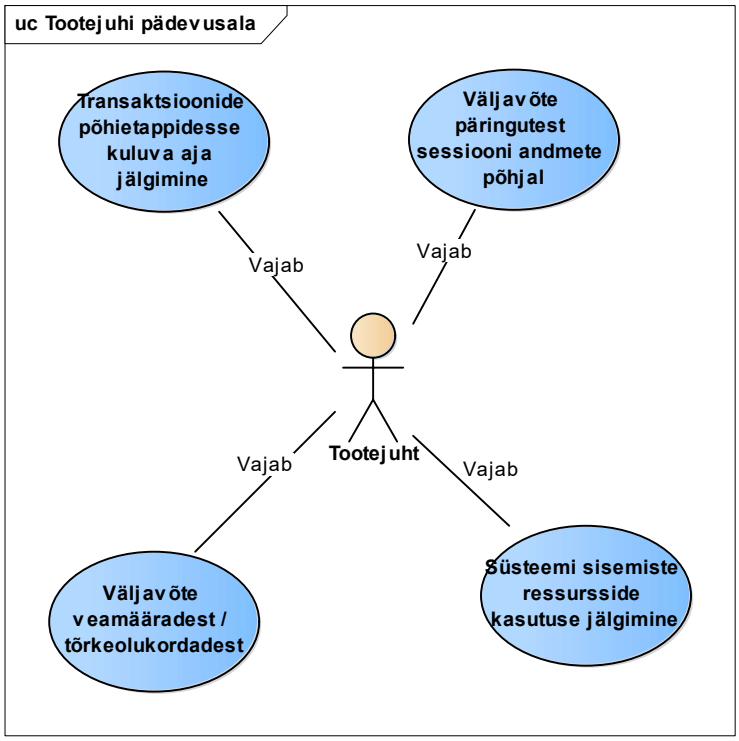
Tabel 2 - Pädevusalade nimekiri

Pädevusala	**Kes?**
Tootejuht	Urmo
Teenusejuht	Liisa
IT haldus	Jaanus

Kasutajatugi	Ave
Kasutaja	Liisa
Kolmandas osapool (klient)	Liisa

3.2.1 Tootejuhi pädevusala

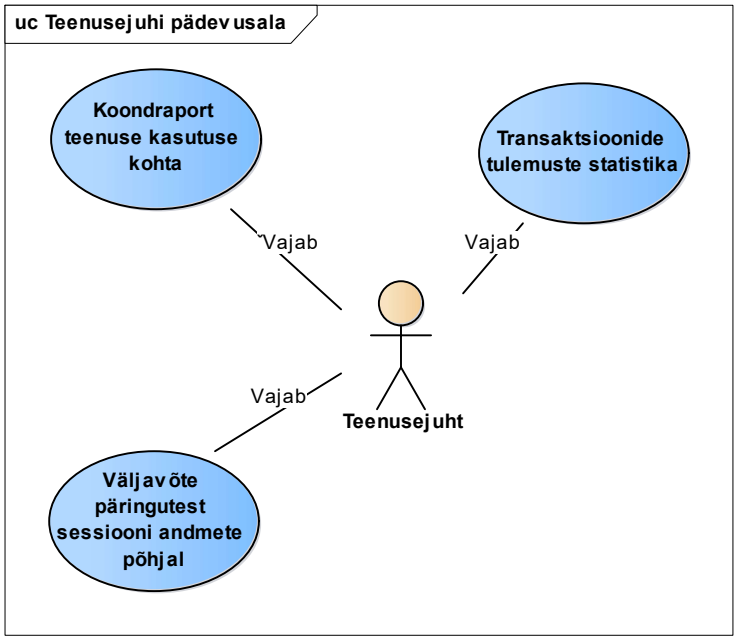
Tootejuhi põhiliseks huviks on saada ülevaade teenuse toimimise kohta: kui kaua kestavad tehtavad operatsioonid ajaliselt ning mis on vigade määr. Vajalik sisendiks, et toote kvaliteeti mõõta ja vajadusel paremaks muuta. Lisaks huvitab tootejuhti teenuse kasutus erinevate seadmete lõikes, et teada mis keskkondade toetamine on olulisem ning mis vähem.



Joonis 10 - Tootejuhi kasutusjuhud

3.2.2 Teenusejuhi pädevusala

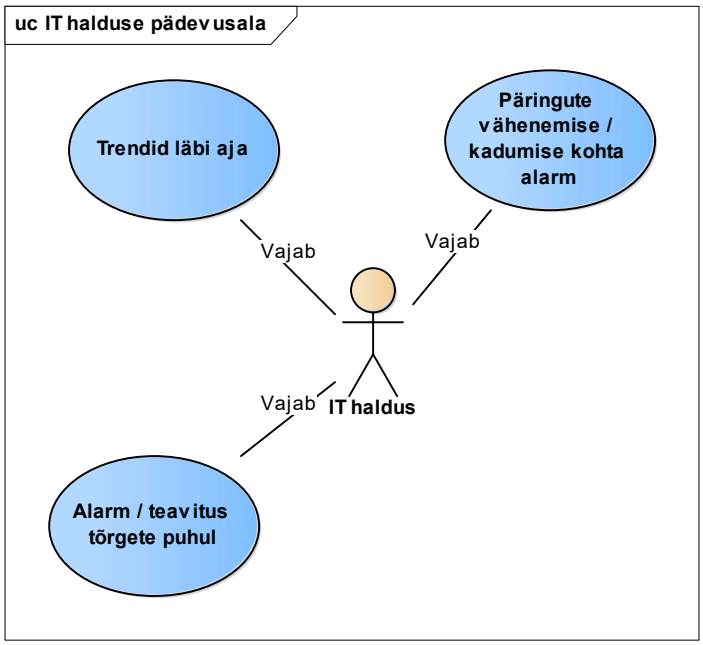
Teenusejuhi põhiliseks huviks on saada ülevaade teenuse toimimisest: kui palju on erinevaid kasutajaid ning mis päringuid teostatakse.



Joonis 11 – Teenusejuhi kasutusjuhud

3.2.3 IT halduse pädevusala

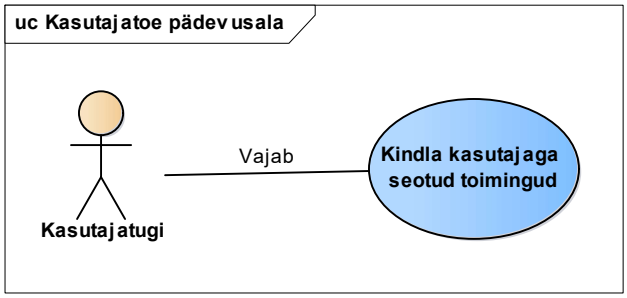
IT haldus vastutab teenuse toimimise eest ning peab tagama süsteemi tõrgeteta töö. Selleks peab olema võimekus märgata tõrkeid süsteemis, et neile operatiivselt reageerida. Ühtlasi soovitakse saada ülevaadet trendide kohta, et olla valmis vajadusel süsteemi võimsust tõstma enne, kui vähene ressurss probleemiks saab.



Joonis 12 - IT halduse kasutusjuhud

3.2.4 Kasutajatoe pädevusala

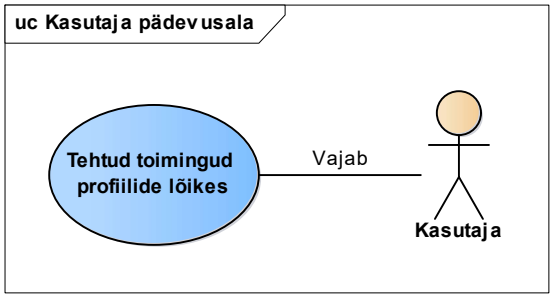
Kasutajatoe põhiülesanneteks on aidata kasutajat tõrgete lahendamisel, et leida probleemide põhjus ning lahendus.



Joonis 13 – Kasutajatoe kasutusjuhud

3.2.5 Kasutaja pädevusala

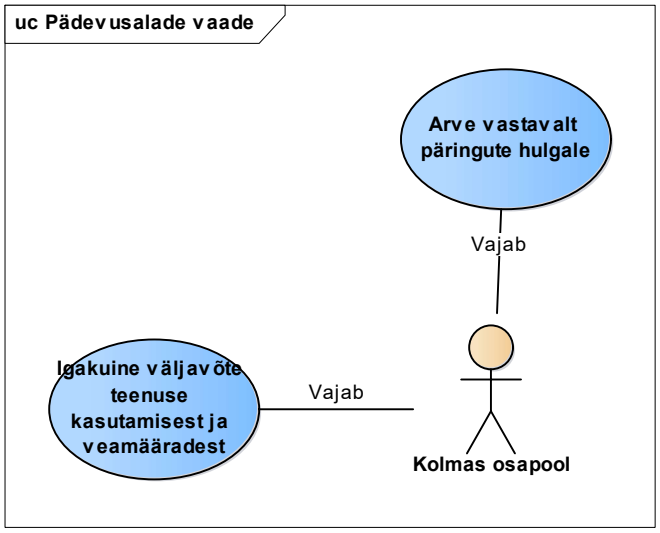
Kasutaja on huvitatud sellest, et oleks võimalus näha kõiki enda tehtud toiminguid. Pädevusala vajab võimalust oma tegevustest tagantjärgi ülevaate saamiseks – veendumaks näiteks selles, et profiili ei oleks kasutatud kasutaja teadmata.



Joonis 14 - Kasutaja kasutusjuhud

3.2.6 Kolmanda osapoole pädevusala

Kolmanda osapoole soov on pakkuda oma kliendile võimalust Smart-ID-ga oma süsteemi logida või allkirjastada dokumente. Seetõttu soovitakse eelkõige saada informatsiooni teenuse kvaliteedi ja kasutamise mahtude kohta.



Joonis 15 - Kolmanda osapoole kasutusjuhud

3.3 Raportite infosüsteemi loogiline tase

Raportite nõuded on kirja pandud soovilugudena.

Alljärgnevalt on lähtutud (Tabel 2) kirjeldatud rollide tabelist. Viiakse läbi vestlused raportitest huvitatud pädevusalade vastutavate isikutega ja formuleeritakse soovilood (Cohn, „User Roles“). [12]

3.3.1 Tootejuhi raportite soovilood

Tootejuhi jaoks olulised soovilood:

1. Jälgida transaktsiooni põhietappides kuluvat aega (näiteks: päring sisse, „push“ sõnum välja, PIN ära sisestanud jne).
2. Väljavõte:
   2.1. päringute arvu kohta tipptundidel;
   2.2. erinevate mobiiltelefoni mudelitega tehtavatest päringutest;

2.3. kasutavate rakenduste / OS versioonide osas;

2.4. teenuse kasutajatest vanuse ja soo põhjal;

2.5. päringute hulga kohta reaalajas (teatud tüüpi päringuid ajaühikus).

3. Võimalus näha veamäärade osakaalusid:

3.1. mis etapis on viga toimunud;

3.2. mis põhjusel on viga toimunud (nt x% ebaõnnestus, kuna telefon välja lülitatud, st mis takistused on teenuse kasutamisel) (sh. ka erinevate OS / rakenduse versioonide osas).

4. Süsteemi sisemine jälgimine (lõimede arv, andmebaasiühendused, jne)

3.3.2 Teenusejuhi raportite soovilood

Teenusejuhi jaoks on olulised järgmised soovilood:

1. Koondraport teenuse kasutuse kohta, kui palju on ajaühiku jooksul:

1.1 autentimisi;

1.2 allkirjastamisi;

1.3 registreerimisi;

1.4 erinevaid aktiivseid „profiile“;

1.5 unikaalseid kasutajaid;

1.6 kasutajate arv kolmanda osapoole teenuse lõikes;

1.7 käimasolevaid transaktsioone;

2. Saada ülevaade:

2.1 transaktsioonide kestvuse kohta (kuu keskmine erinevate transaktsioonide lõikes);

2.2 kliendi tegevustest kasutuskogemuse parandamiseks (nupuvajutused koos erinevates etappides kulunud ajaga).

3. Transaktsioonide tulemuste statistika (üleüldine / telefonimudelite lõikes?).

3.3.3 IT halduse raportite soovilood

IT halduse jaoks on olulised järgmised soovilood:

1. Võimalus näha:

   1.1. trende läbi aja (päringute arv x ajavahemikus tundide kaupa / kasutajate arv);

   1.2. prognoose teenuse kasutuse kasvu osas.

2. Saada päringute vähenemise / kadumise kohta alarm (tavapärasest märgatavalt väiksem päringute hulk või täielik puudumine)

3. Saada tõrgete kohta alarm (vigade määr kõrgem lubatust)

4. Võimalusel liidestus praegu kasutuses oleva monitooringu vahendiga - Nagios

3.3.4 Kasutajatoe raportite soovilood

Kasutajatoe jaoks on olulised järgmised soovilood:

1. Võimalus näha kindla kasutajaga seotud toiminguid (sessiooniga seotud etapid tõrke tuvastamiseks)

3.3.5 Kasutaja raportite soovilood

Kasutaja jaoks on olulised järgmised soovilood:

Võimalus näha:

1. Tehtud toiminguid seadmete lõikes (erinevad Smart-ID profiilid, mis kliendile kuuluvad).
2. Päringuid kogus.
3. Päringu tüüpi (st. kas on autenditud, allkirjastatud).
4. Kolmanda osapoole teenust, kus päring algatati.
5. Päring algatamise algusaega.

3.3.6 Kolmandate osapoolte raportite soovilood

Kolmanda osapoole jaoks on olulised järgmised soovilood:

1. Võimalus näha ebaõnnestunud päringute hulka ajalooliselt (viimase 12h vead 1h lõikes);
2. Saada iga kuu:
    2.1. teenuse kasutusraport (õnnestunud / positiivse tulemuseni jõudnud päringud);
    2.2. vigade raport (kolmanda osapoole algatatud ebaõnnestunud päringud kellaaegadega);
    2.3. arve vastavalt tehtud päringute hulgale.

3.4 Raportite loomise planeerimine

Järgnevalt hinnatakse kasutuslugude vajalikkust ning vastavalt sellele tükeldatakse raportid iteratsioonideks. See võimaldab tükeldada raportite loomisel tehtavat tööd väiksemateks osadeks.

Iteratsioonideks jagamisel lähtuti sellest, et kokku saaksid sarnase profiiliga soovilood. Samuti lähtuti raportite vajaduse prioriteedist.

Esimese iteratsioonina soovitakse saada infot kasutajaga seotud tegevuste kohta ning selle põhjal statistikat teha.

„Kasutuslood“ veerg tähistab peatükis 3.3 esitatud vastava pädevusala sooviloo numbrit.

Tabel 3 - Raportite planeerimine iteratsioonideks

Iteratsioon	**Kasutuslood**
Iteratsioon 1	Tootejuht (2); Teenusejuht(1); Kasutajatugi (1)
Iteratsioon 2	IT haldus (2, 3)
Iteratsioon 3	Tootejuht (1,3,4); Teenusejuht(2, 3); IT haldus (1, 4); Kolmas osapool (1, 2.1, 2.2)
Iteratsioon 4	Kasutaja; Kolmas osapool (2.3)

4. Nõuete püstitamine infosüsteemile

Peatükis selgitatakse välja, milliseid on andmevajadused – mis info on vaja salvestada sessiooni käigus, et oleks võimalik teostada soovilugudes kirjeldatud raportid. Töö sisendiks on kahe eelmise peatüki tulemused – kasutuslugudest selgus süsteemi arhitektuuriline pool ning raportite soovilugudest selgus, mida tahetakse süsteemi juures mõõta.

Kaardistatakse funktsionaalsused, mis on vajalikud soovitud raportite koostamiseks.

Andmevajaduse leidmiseks otsime vastused metoodikas esitatud küsimustele:

Milliseid andmeid on vaja raportite / monitooringute teostamiseks?

Mis andmeid oleks tarvis erinevates serverites olevate logikirjete seostamiseks?

Mis andmed on olemas / juba logitakse?

Mis andmeid oleks juurde vaja?

4.1 Andmevajaduse kirjeldus

Järgnevas osas teostatakse soovilugude põhjal kokkuvõte ning kaardistatakse, milliseid andmeid on tarvis, et raporti koostamine oleks võimalik.

Andmed, mida on vaja sessiooni käigus maha logida, võttes arvesse raportite soovilugusid on:

Tabel 4 - Andmevajadused

Nõue (Võimalik sorteerida päringud)	**Vajalik parameeter**
X ajavahemikus;	Päringu tegemise aeg
Telefoni mudeli põhjal;	Telefoni mudel
Telefoni OS ja versiooni järgi;	Telefoni OS ja versioon
Kasutaja profiili järgi;	Profiil

Kindla isiku põhjal;	Isikukood, riik
Päringu tüübi järgi (nt autentimine, allkirjastamine, registreerimine)	Päringu tüüp
Päringu etapi järgi (logitakse sessiooni etapp – nt PUSH sõnumi saatmine)	Päringu etapp
Päringu tulemuse järgi (OK / ERROR)	Päringu tulemus
Vea põhjuse info järgi (nt Timeout, vale PIN)	Vea põhjus (koodina või tekstina)
Kolmanda osapoole teenuse järgi (nt xPank)	Kolmanda osapoole nimetus, IP
Vanuse ja soo põhjal (kui võimalik)	Sugu, vanus (Eesti ja Leedu kodanike puhul piisaks isikukoodist)

Kaardistame saadud graafiku põhjal andmemudeli.

Etapi andmeolemiga seotud info:

1. Alguse aeg – vajalik, et aru saada, millal alustati etapi protsessimist
2. Lõpu aeg – vajalik, et aru saada, millal lõpetati etapi protsessimine (võimalik mõõta etapi läbimiseks kulunud aeg)
3. Etapi nimetus – identifikaator, mis eristab erinevaid etappe
4. Staatus – näitab etapi staatust – kas päring lõppes edukalt.
5. Põhjus – identifikaator, mis kirjeldab etapi lõppemise detailset põhjust (nt päringu aegumine)
6. Sessiooni ID – tähistab iga sessiooni kohta käivat unikaalset tunnust.
7. Etapi algataja IP – Serveri IP, mis algatas antud etapi.
8. Etappi teostava serveri IP – Serveri IP, kus tegeletakse käimasoleva etapi protsessimisega

Päringu andmeolemiga seotud andmed:

1. IP – Päringu teinud serveri aadress
2. Kolmanda osapoole teenuse nimi – Eelnevalt kokku lepitud Kolmanda osapoolt tähistav nimetus
3. Kasutaja isikukood – kasutajat tähistav isikukood (unikaalne riigi piires)
4. Kasutaja riik – Kasutaja elukohta tähistav kirje
5. Päringu aeg – millal päring süsteemi saabus.
6. Päringu tüüp – Mis päringuga on tegemist (nt allkirjastamine, autentimine)
7. Sessiooni ID – tähistab iga sessiooni kohta käivat unikaalset tunnust.

Kolmanda osapoole andmeolemiga seotud andmed:

1. Nimi – Tähistab Kolmanda osapoole nime
2. Registrikood – Tähistab Kolmanda osapoole registrikoodi
3. IP – Tähistab Kolmanda osapoole poolt kasutatavaid aadresse
4. Teenuse nimi – Tähistab Kolmanda osapoole poolt kasutatavaid teenusenimetusi

Kasutaja andmeolemiga seotud andmed:

1. Isikukood
2. Nimi
3. Riik
4. Sugu
5. Sünniaeg
6. ID – Kasutajat identifitseeriv unikaalne tunnus

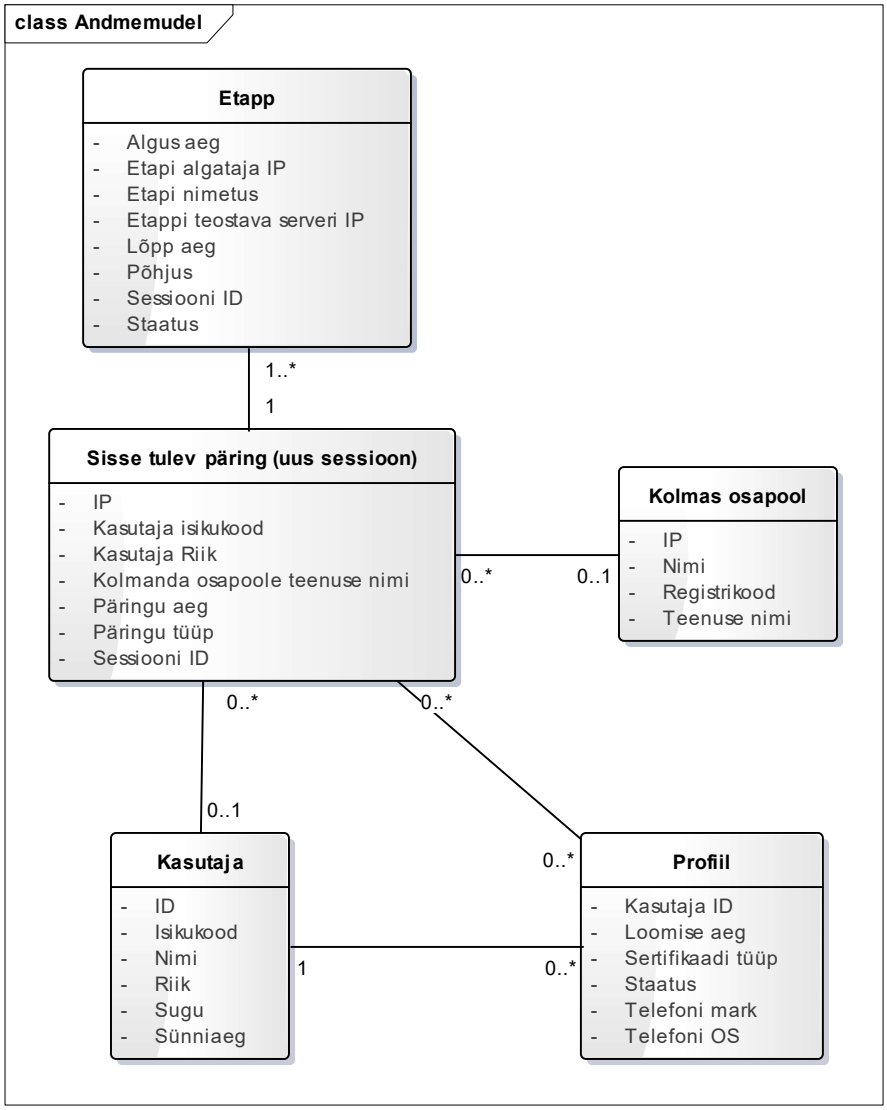
Profiili andmeolem seotud andmed:

1. Loomise aeg
2. Sertifikaadi tüüp
3. Staatus
4. Telefoni mark
5. Telefoni OS
6. Kasutaja ID – Unikaalse kasutajaga seotud tunnus

Päringuga võib seotud olla seotud kuni üks konkreetne kasutaja ja kolmas osapool.

Kasutajal võib olla mitu profiili, profiil on aga seotud ühe konkreetse kasutajaga.

Sisse tuleb päring koosneb ühest kuni mitmest etapist, mida sessiooni käigus läbitakse. Etapp on seotud ühe kindla sisse tuleva päringuga.



Joonis 16 - Raportisüsteemi andmete domeenimudel

4.2 Logikirjete sidumine ja etappide ajakulu leidmine

Transaktsioonide põhietappides kuluva aja leidmiseks on tarvis kasutada ühtset sessiooni ülest ID –d, mille abil erinevates Smart-ID süsteemi komponentides ja serverites olevad logikirjed kokku siduda.

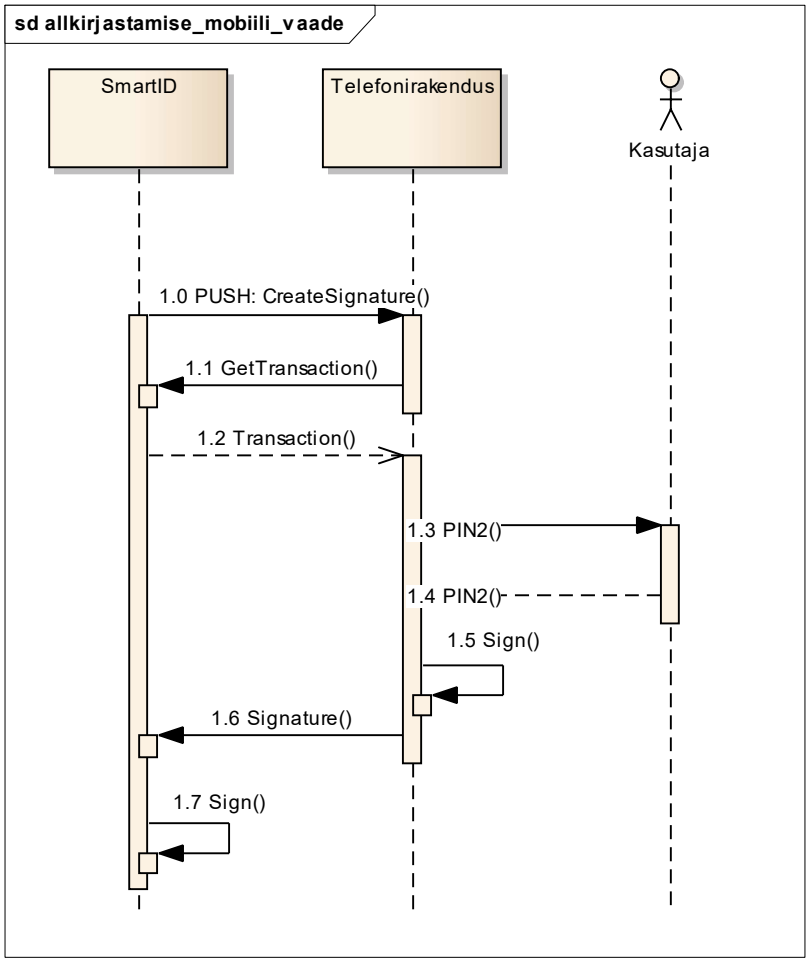
Samuti on vajalik logida maha iga etapi juures täpne aeg.

4.2.1 Mobiilirakenduse nõuded ajakulu leidmiseks

Mobiilirakenduse logidele ligipääs puudub ning ei soovita, et kogu tekkiv logi edastataks Smart-ID teenusele. Selleks, et mobiilirakenduses läbitud etappide kestvust hiljem analüüsida, peaks seadmes endas ajakulu mõõtma. Serverisse peaks jõudma API kaudu vaid oluline info, näiteks põhietappide vahele jääv aeg.

Allkirjastamise ja isikutuvastamise puhul:

1. „push“ sõnumi kätte saamisest (1.0) kuni päringu tagasi saatmiseni (1.1) kulunud aeg;
2. Smart-ID serverisse päringu tegemise (1.1) ka vastuse saamise (1.2) vahele jäänud aeg;
3. serveri päringu tagasi jõudmise (1.2) PIN dialoogi kuvamisele (1.3) kulunud aeg;
4. PIN dialoogi kuvamisest (1.3) PIN sisestamiseni (1.4) kulunud aeg;
5. PIN sisestamise (1.4) ja Signeerimise protsessi lõpuni (1.5) kulunud aeg;
6. signeerimise protsessi (1.5) ja signatuuri serverile tagasi saatmiseni kulunud aeg.



4.2.2 Smart-ID komponentide logimise nõuded

Kõigi Smart-ID API-liideste puhul tuleks fikseerida:

1. Päringu tegija IP;
2. Päringu vastuvõtja IP;
3. Päringu vastuvõtmise / väljasaatmise aeg;
4. Päringu tüüp ja etapp;
5. Sessiooni identifikaator.

Päringu tegija IP ja vastuvõtja IP on oluline, et tekiks arusaamine päringu liikumise teekonnast – milliseid klastri servereid päring läbib. Informatsioon aitab tuvastada vajadusel tõrkeid põhjustav server.

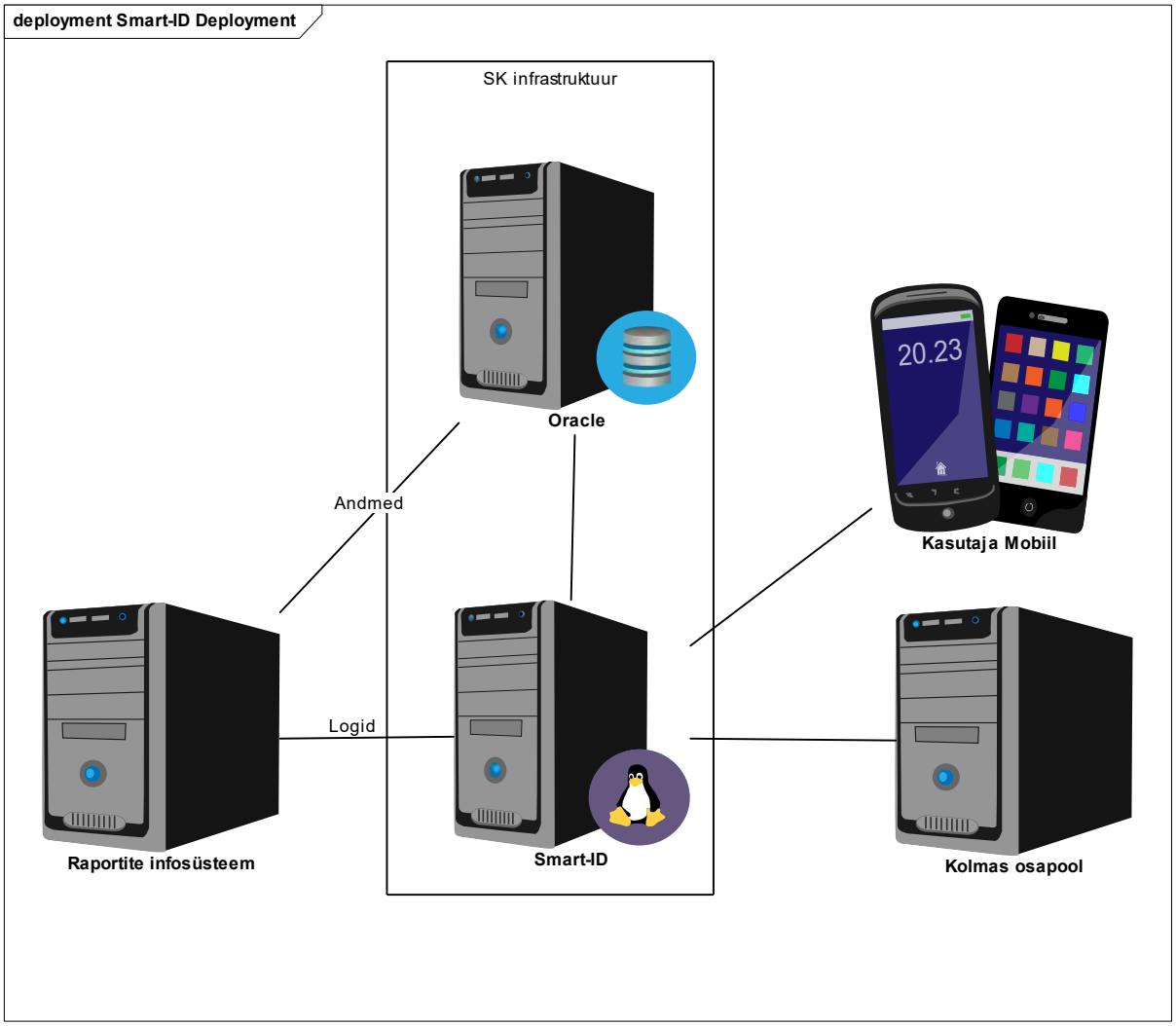
Päringu vastuvõtmise ja väljasaatmise aja salvestamine annab ülevaate etapis kulunud ajast – on oluline, et kaardistada ajakulu etappide lõikes.

Päringu tüübi ja etapp on vajalik salvestada, et tekiks võimekus sorteerida päringuid tegevuste lõikes. Seeläbi saab edastada statistikat erinevate päringute koguste kohta ning on võimalik märgata, kus etapis on kõrge vea tekkimise määr.

Sessiooni identifikaator peab läbivalt olema kajastatud iga logikirje loomise puhul. Kirje eesmärgiks on olla ühine nimetaja, mis võimaldab siduda logikirjed ühtseks sidusaks tervikuks.

5. Raportite koostamise süsteemi füüsiline tase

Peatükis otsitakse vastust küsimusele: „Millega soovitud raportid luua?“. Vastuse saamiseks kaardistatakse nõuded raportite koostamise vahendile. Tutvustatakse olemasolevat vahendit ning seejärel hinnatakse, kas tegemist on piisavalt võimeka tööriistaga vajaminevate raportite teostamiseks.



Joonis 17 - Raportite koostamise süsteemi füüsiline tase

5.1 Nõuded raportite koostamise vahendile

Nõuded raportite koostamise vahendile päringute tegemisel:

- peab võimaldama siduda kokku erinevates serverites olevad ja eri komponentide poolt loodud kirjed üheks terviklikuks sessiooniks;
- võimekus eristada erinevaid andmetüüpe (nt Telefoni OS kirjed);

- võimalus filtreerida ajaliselt välja soovitud tulemused;
- peab suutma arvutada trende ajalooliste andmete põhjal (nt prognoos, kui suur on päringute maht x aja pärast);
- võimekus teha andmebaasipäringuid, et logikirjetele lisaks kasutada andmebaasis olevat infot;
- lugeda kokku otsingu parameetritele vastavad tulemused.

Vahend peab võimaldama:

- koguda infosüsteemi poolt loodavaid andmeid – logifailidest, kui ka vajadusel andmebaasist;
- kasutajapõhist ligipääsu (kasutajapõhine ligipääs ning võimalus määrata rolli põhiselt õigusi);
- graafiliselt kujutada päringute tulemusi;
- luua ja kujundada kasutaja vajadustele vastav töölaud, mis sisaldab tööks vajalikke raporteid;
- raportite saatmist (e – mailiga);
- reaalajas raportite esitamine (perioodiliselt uuendatav esitlus viimase x ajahulga tegevustest).

5.2 Olemasoleva analüütika vahendi tutvustus

SK töötaja Mikk Mähar poolt teostatud diplomitöös „Keskse logihalduslahenduse rakendamine AS-is Sertifitseerimiskeskus“ valiti sobiliku logihaldus vahendina välja „*Splunk Enterprise*“. Splunk on võimekas logihaldus ja andmeanalüüsi vahend, mis võimaldab koguda kokku logide andmed erinevate seadmete ja rakenduste lõikes. Seejärel on võimalik kogutud andmete põhjal luua raporteid ning analüüse. Selleks on loodud võimekas veebipõhine graafiline kasutajaliides, mis võimaldab kasutajal luua uusi otsinguid või kasutada olemasolevaid. [3].

Splunk võimaldab:

- koguda ja indekseerida logisid ning andmeid;
- teostada otsinguid, analüüse kasutades graafilist kasutajaliidest;

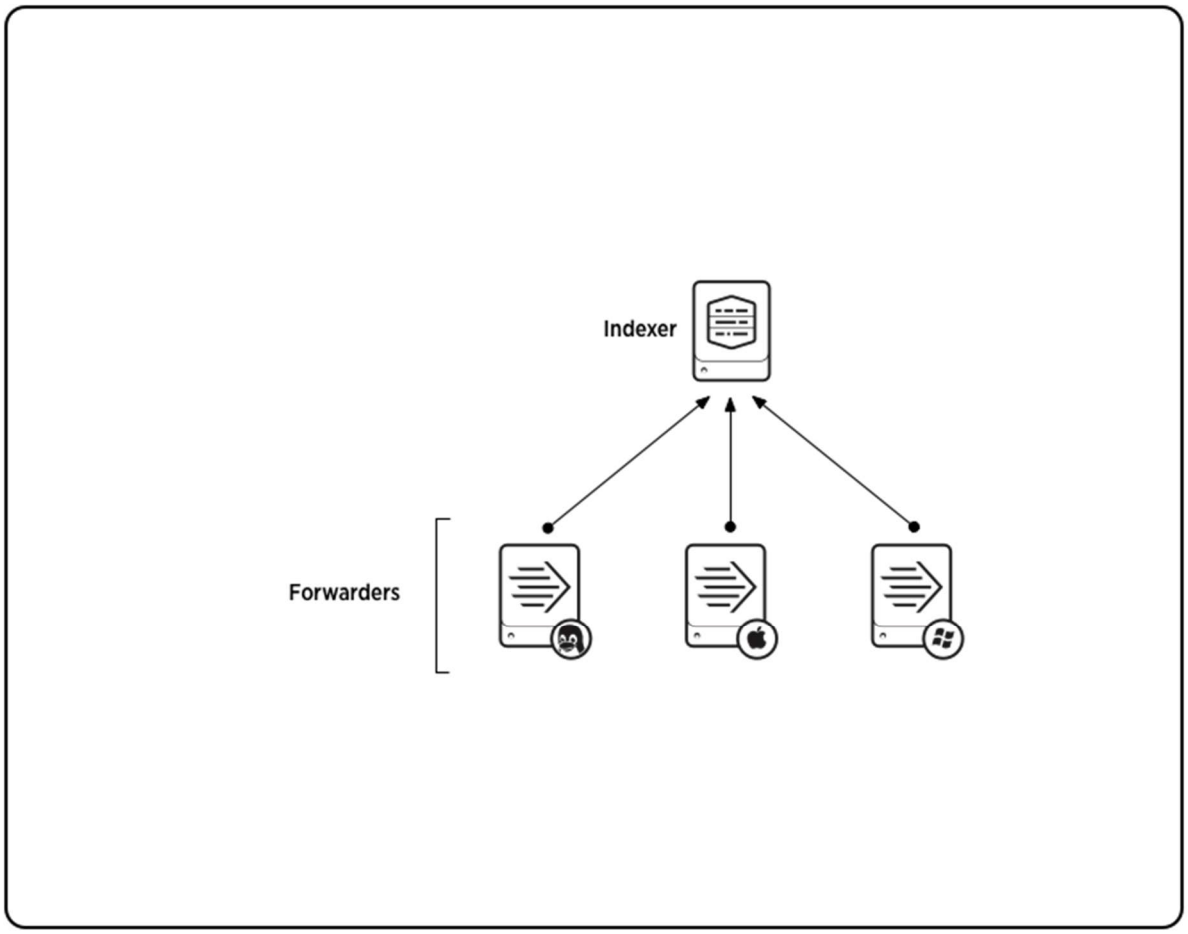
- visualiseerida tulemus graafikuna;
- luua kasutajapõhine töölaud vajalike raportitega;
- raporteid sisaldava PDF loomine ja saatmine;

5.2.1 Splunk *Universal Forwarder*

Splunk „*Universal Forwarder*“ on võimekas vahend, mis võimaldab koguda ja seejärel edastada süsteemseid andmeid Splunk Enterprise serverile.

Põhilisteks omadusteks on:

- meta-andmete märgendamine
- seadistatav puhverdamine
- andmete tihendamine
- SSL põhine turvaline andmekanal
- Võimekus kasutada mistahes võrguporti



Joonis 18 - Splunk Universal Forwarder

[13]

5.2.2 Splunk DB Connect 2

Splunk võimaldab kasutada mitmeid rakendusi (add-ons), mis lisavad võimekust raportite loomisel. Splunk DB Connect sisaldab nelja põhilist võimekust:

- Andmebaasi import – võimaldab importida tabeleid, ridu, veerge andmebaasist Splunk Enterprise serverisse, mis seejärel indekseerib andmed.
- Andmebaasi eksport – võimaldab eksportida andmed Splunk Enterprise serverist tagasi relatsioonilisse andmebaasi.
- Andmebaasi andmete sidumine – võimaldab teostada andmebaasipäringuid ja seeläbi siduda baasis olevaid andmeid logikirjetega, mis tulevad rakendusserverist.

- Andmebaasipäringud – võimaldab kasutada andmebaasipäringuid Splunk otsingutes. [14]

5.2.3 Splunk ja Nagios liidestus

SK –s on keskse monitooringu vahendina kasutusel Nagios [15]. Splunki ja Nagiose liidestuse tarvis on loodud „*Analytics for Nagios*“. Vahend võimaldab saata Nagiosele Splunki poolt defineeritud otsingu tulemusi. Lisaks pakub võimalust tuua Nagiose monitooringu tulemused paremaks visuaalseks esitluseks hoopis Splunki. [16]

5.3 Olemasoleva vahendi sobivuse hindamine

Peatükis analüüsitakse Splunk sobivust raportite ja monitooringute realiseerimise vahendina. Järgnevalt reastatakse nõuded ning hinnatakse vahendi sobivust.

Tabel 5 – Splunk-i sobivuse hindamine

Nõue	**Vastavus**
Peab võimaldama siduda kokku erinevates serverites olevad ja eri komponentide poolt loodud kirjed üheks terviklikuks sessiooniks;	Nõue täidetud – võimalik siduda logikirjed kokku üheks „sündmuseks“
Võimekus eristada erinevaid andmetüüpe (nt Telefoni OS kirjed);	Nõue täidetud (Automaatselt on võimalik andmetüüpe eristada, kui kasutada süntaksit – nt. tel_os=Telefoni_OS)
Võimalus filtreerida ajaliselt välja soovitud tulemused;	Nõue täidetud
Peab suutma arvutada trende ajalooliste andmete põhjal (nt prognoos, kui suur on päringute maht x aja pärast);	Nõue täidetud – võimalik kasutada näiteks „*predict*“ funktsionaalsust [17]
Võimekus teha andmebaasipäringuid, et logikirjetele lisaks kasutada andmebaasis olevat infot;	Nõue täidetud - Splunk DB Connect 2 abiga võimalik saavutada.

Lugeda kokku otsingu parameetritele vastavad tulemused.	Nõue täidetud – „*count*“ päringu abil teostatav sarnaselt relatsioonilise andmebaasi süntaksile. [17]
Vahend peab võimaldama	
koguda infosüsteemist andmeid – logifailidest, kui ka vajadusel andmebaasist;	Nõue täidetud – (Universal Forwarder ja Splunk DB Connect 2)
kasutajapõhist ligipääsu;	Nõue täidetud
graafiliselt kujutada päringute tulemusi;	Nõue täidetud
luua ja kujundada kasutaja vajadustele vastav töölaud, mis sisaldab tööks vajalikke raporteid;	Nõue täidetud
raportite saatmist (e – mailiga);	Nõue täidetud
reaalajas raportite esitamine.	Nõue täidetud

Tabeli põhjal selgib, et Splunk vastab kõigile seatud nõuetele. Kuna Splunki kasutamine eeldab kasutaja põhist autentimist, seega tuleb eelnevalt huvitatud isikutele luua neile kohandatud töölauad. Kasutajate päringute puhul on mõttekas lahendada ülesanne eraldi veebilehena. Andmete pärimiseks oleks samas võimalik võimalusel kasutada Splunk API –t [18]

6. Kokkuvõte

Tööl oli kaks suuremat eesmärki. Esiteks leida universaalne raamistik, mida saaks kasutada raportite loomiseks mistahes SK infosüsteemi puhul. Raamistik annab võimaluse luua ülevaatliku pildi infosüsteemide arhitektuurist ja aitab kaardistada süsteemidele esitatavad nõuded.

Teiseks eesmärgiks oli läbida raportite loomise metoodika Smart-ID projekti näitel, et tekiksid eeldused raportite loomiseks ning veenduda metoodika sobilikkuses.

Autor leiab, et kõik seatud eesmärgid täideti. Selgus, et valitud metoodika abil saab edukalt kirjeldada eeldused raportite infosüsteemi juurutamiseks.

Infosüsteemide vaheliste seoste kirjeldamiseks kasutati standardset raamistikku – sobivaimaks osutus Integreeritud Ettevõtte Arhitektuuri Raamistik (*Integrated Enterprise Archidecture Framework - IAF*).

Nii Smart-ID infosüsteemi kui raportite infosüsteemi kirjeldamiseks läbiti neli abstraktset taset, mille käigus vastati küsimustele: „miks?“, „mida?“, „kuidas?“ ja „millega?“. Selle käigus kaardistati erinevate osapoolte andmevajadused, tekkisid funktsionaalsed nõuded raportisüsteemile ja ülevaade andmevajadustest – mis andmeid peab Smart-ID infosüsteem pakkuma.

Smart-ID näitel läbiti metoodikas kirjeldatud etapid:

1. Kaardistati Smart-ID raportitest huvituvad pädevusalad
2. Leiti pädevusalade nõuded Smart-ID süsteemi kohta käivatele raportitele

Raportite defineerimisel selgus, et saadav kasu seisneb näiteks selles, et:

a) Tekib suutlikkus süsteemi jõudluses ja tõrkemäärades toimuvaid trende märgata, neile proaktiivselt reageerida ning efektiivselt jõuda probleemi põhjustava komponendi või sessiooni etapini.

b) Tekib võimekus pakkuda ettevõtte äripoolele ülevaadet teenuse kasutamises erinevate analüüside ja raportite näol.

c) Tekib võimekus pakkuda suuremat läbipaistvust teenuse toimimisest Kolmandatele osapooltele (klientidele).

3. Selgitati välja nõuded Smart-ID infosüsteemile – mis andmed on vaja pakkuda. Antud peatükki saab kasutada sisendina Smart-ID infosüsteemi logimise nõuetele.

4. Valmis analüüs raportite loomise vahendile Splunk, mis näitas, et kasutusel oleval vahendil on kõik nõutud omadused olemas.

Ettepanekud edasiarenduseks:

Nõuded raportitele põhinevad pädevusaladega tehtud intervjuudel. Metoodika eeldab, et pädevusala omab kõige paremat ülevaadet oma infovajadustest seoses vaatlusaluse infosüsteemiga. Tegemist võib olla mõnevõrra ohtliku eeldusega, mistõttu saaks töös kasutatud raamistiku skoopi laiendada ning kaardistada objektiivsema ülevaate saamiseks lisaks infosüsteemide vaatele ka äri- ning informatsiooni vaateid.

Summary

Thesis had two major objectives. First was to find a universal framework that can be used to generate reports for any information system in SK. The framework provides an opportunity to create a comprehensive overview and helps to map the systems requirements.

Second goal was to go through the methodology using Smart-ID project as an example. The goal is to define requirements to create reports and to make sure about the suitability of the methodology.

Architecture Integrated Enterprise Framework – IAF was selected as suitable framework to describe relations between information systems.

There are used four levels of abstractions which answer to the questions: "why?", "what?", "how?" and "with what?“ to describe reporting and Smart-ID infosystem.

The data needs of different stakeholders were mapped. It helped to find out what kind of data should the Smart-ID information system provide to the reporting system.

The author believes that the stated objectives were met.

Using Smart-ID system as an example the following steps were completed using selected methology:

1. Stakeholders that are interested of reports based on Smart-ID information system were mapped.

2. Smart-ID information system reports based on the needs of interested stakeholders were described.

Defining reports showed that the reports provide the following information about Smart-ID:

a) performance and capacity of the system;

b) trends of the system to proactively respond to and to effectively reach to the problem-causing component;

c) the usage of the Smart-ID service;

d) greater transparency of the system functioning to the third parties (customers)

3. We have identified the requirements to the Smart ID information system (the information that is required by the reporting system). This chapter can be used as input to the Smart-ID information system logging requirements.

4. Requirements to the reporting tool (Splunk) were analysed and all of the required properties were met.

Suggestions for further development:

Requirements for reports are based on interviews with actors of competence. The methodology assumes that competence has the best overview of their needs for information regarding the information system. It can be somewhat dangerous assumption. The scope of the framework used in this thesis could be extended to map business and information views to get more objective picture of the needs.

Kasutatud kirjandus

[1] „Ettevottest,“ AS Sertifitseerimiskeskus, [Võrgumaterjal]. Available: https://sk.ee/ettevottest/. [Kasutatud 23 04 2016].

[2] T. Hallas, *Logging Requirement Analysis and Specification for Development Based on Governmental Institutions of Estonia,* Tallinn, 2014.

[3] „Operational Intelligence, Log Management, Application Management, Enterprise Security and Compliance - Splunk,“ [Võrgumaterjal]. Available: http://www.splunk.com/. [Kasutatud 2016 04 23].

[4] M. Mähar, *Keskse logihalduslahenduse rakendamine AS-is Sertifitseerimiskeskus,* Tallinn, 2014.

[5] N. F. W. S. Carol O'Rourke, Enterprise Architecture Using the Zachman Framework, Course Technology, 2003.

[6] M. W. H. H. M. S. A. H. Jack van't Wout, The Integrated Architecture Framework Explained: Why, What, How, Springer, 2010.

[7] J. Schekkerman, How to Survive in the Jungle of Enterprise Architecture Frameworks: Creating or Choosing an Enterprise Architecture Framework, 2006.

[8] E. P. M. W. ,. J. C. C. S. Martin Op't Land, in *Enterprise Architecture: Creating Value by Informed Governance*, Springer, 2009.

[9] „Isikut tõendavate dokumentide seadus – Riigi Teataja,“ [Võrgumaterjal]. Available: https://www.riigiteataja.ee/akt/ITDS. [Kasutatud 01 05 2016].

[10] „Digitaalallkirja seadus – Riigi Teataja,“ [Võrgumaterjal]. Available: https://www.riigiteataja.ee/akt/694375?leiaKehtiv. [Kasutatud 02 05 2016].

[11] E. P. J. E. L. NÕUKOGU, „EUROOPA PARLAMENDI JA NÕUKOGU MÄÄRUS (EL) nr 910/2014,“ [Võrgumaterjal]. Available: http://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:32014R0910&from=EN. [Kasutatud 08 05 2016].

[12] M. Cohn, User Stories Applied For Agile Software Development, Addison-Wesley Professional, 2004.

[13] "About forwarding and receiving - Splunk Knowledgebase," Splunk, [Online]. Available:

http://docs.splunk.com/Documentation/Splunk/latest/Forwarding/Aboutforwardingandreceivingdata. [Accessed 01 05 2016].

[14] "Splunk DB Connect 2 | Splunk Apps," Splunk , [Online]. Available: https://splunkbase.splunk.com/app/2686/#/documentation. [Accessed 01 05 2016].

[15] "Nagios - The Industry Standard In IT Infrastructure Monitoring," [Online]. Available: https://www.nagios.org/. [Accessed 01 05 2016].

[16] „Analytics for Nagios | Splunk Apps,“ [Võrgumaterjal]. Available: https://splunkbase.splunk.com/app/352/. [Kasutatud 01 05 2016].

[17] „Commands by category - Splunk Knowledgebase,“ [Võrgumaterjal]. Available: http://docs.splunk.com/Documentation/Splunk/6.4.0/SearchReference/Commandsbycategory. [Kasutatud 01 05 2016].

[18] "Basic concepts - Splunk Knowledgebase," Splunk, [Online]. Available: http://docs.splunk.com/Documentation/Splunk/latest/RESTUM/RESTusing. [Accessed 01 05 2016].

Lisa 1 - Description of methodology (English)

Based on Integrated Architecture Framework (IAF):

1. Provide an overview of the information system of which reports are made
    1.1. Describe the contextual level (overview – why the information system is made).
    1.2. Describe the conceptual level (overview – what is the functionality of the information system - usecases).
    1.3. Describe the logical level (overview of how the system works – sequence diagram, user stories).
    1.4. Describe the physical level (overview – with what is data storage realised)
2. Provide an overview of the reporting information system
    2.1. Describe the contextual level (overview – why the information system is made).
    2.2. Describe the conceptual level (overview of different roles, their usecases and what is system functionality)
    2.3. Describe the logical level (user stories – to describe how should system act)
3. Setting requirements for information system (mapping input based on the two previous points).
    3.1. What data is needed for creating the reports / monitorings?
    3.2. What data would be needed to associate logged data in different servers?
    3.3. Which data is already logged?
    3.4. What data should be added?
4. Reporting system pysical level (With what reports are made?)
    4.1. Describe requirements for the the reports / analytics tool - which functions need to be supported by the required tool. Picking the suitable tool.
    4.2. The analysis of whether an existing or chosen tool has fulfilled the requirements.
    4.3. What would be required to add / other means to carry out?

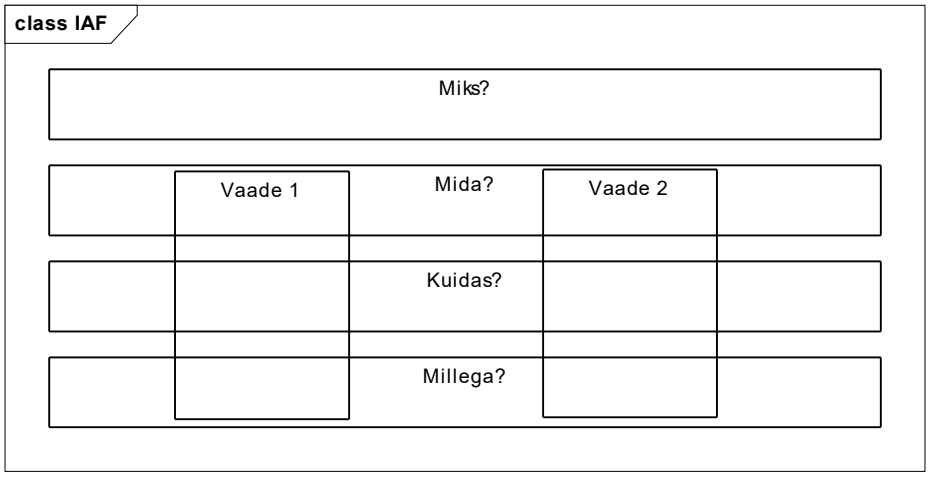
Lisa 2 – Integreeritud Arhitektuuri Raamistik - IAF

IAF sisaldab nelja abstraktsuse taset, mis võimaldab probleemi jagada väiksemateks osadeks, muutes lahenduse leidmise seeläbi lihtsamaks.

Tasemed vastavad küsimustele: Miks?, Mida?, Kuidas?, Millega? Esmalt saadakse ülevaade põhjustest, miks projekt loodud on. Seejärel saadakse ülevaade nõuetest, mida lahendus peab täitma. Kolmandana esitatakse ideaalne lahendus, kuidas süsteem peaks toimima, ilma konkreetset lahendust pakkumata. Viimaks otsustatakse, mis füüsilist komponenti käsitada ideaalse lahenduse loomiseks. Abstraktsed tasemed esitatakse horisontaalselt arhitektuuri teemadega.

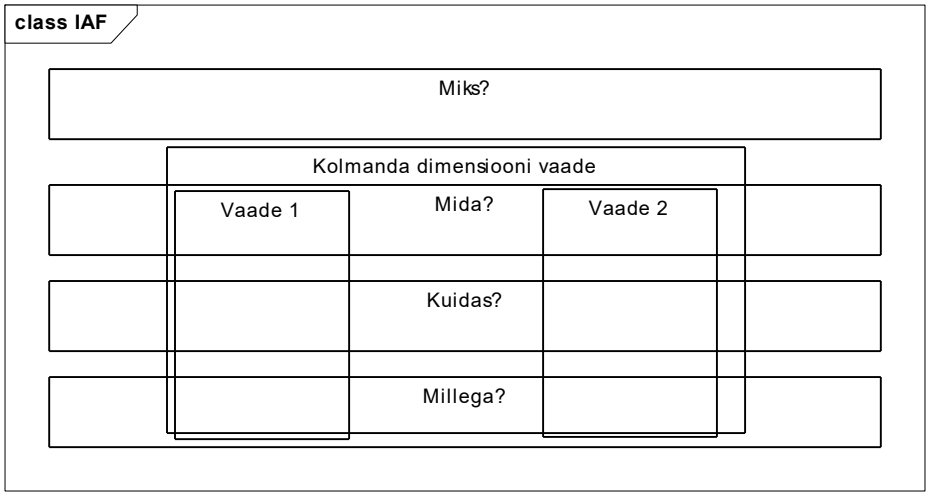
Joonis 19 - Lisa2 IAF Abstraktsed tasemed

Vaated (*Aspect Areas*) kujutavad formaalseid piire arhitektuuri lahenduste vahel. Iga vaade keskendub erinevale arhitektuuri mõõtmele, samas lisades informatsiooni üleüldisele arhitektuurile. Vaja on teada vaadete tausta, et saaks nad katta abstraktse tasemega. Vaated katavad „mida“, „kuidas“ ja „millega“ abstraktsed tasemed. „Miks“ abstraktne tase omab ülevaatlikult strateegiaid ja trende, mis on kohandatavad kõigile vaadetele. Vaated esitatakse IAF diagrammil vertikaalselt.



Joonis 20 - Lisa2 IAF Vaated

IAF kasutab tihti ka kolmandat dimensiooni, et kujutada aspekte, mis on osa kõikidest teistest vaadetest, kuid tuleks esitleda eraldi, et tagada arhitektuuri täielikkus ja kokku sobivus. Tavaliselt sisaldab see kvaliteedi- või mittefunktsionaalseid aspekte, nagu turvalisus (*security*), teenuse kvaliteet (*quality of service*) ja juhtimine (*Governance*).



[6]