Eesti
tuleviku heaks

Euroopa Liit
Euroopa
Regionaalarengu Fond

Alternatiivsete kanalite kasutamise analüüs ja pilootprojekt

HANGE: 225494

04.12.2020

Majandus- ja Kommunikatsiooni-ministeerium

Riigi Infosüsteemi Amet

Põllumajanduse Registrite ja Informatsiooni Amet

SOLITA

Sisukord

Mõisted

Alternatiivsed kanalid	Suhtluskanalid, mille kaudu saab klientidega infot vahetada. Näiteks Facebook Messenger, Whatsapp, Viber, iMessage, Telegram, Skype, SMS jt
Klient	Kodanik või ettevõtja (sh e-residendid), kes kasutab avalikku teenust
Liidestuja	Alternatiivsete kanalite kasutamiseks on vaja luua eraldiseisev rakendus ehk liidestuja. Liidestujal on kindel protokoll teenuse kasutamiseks sõltumata sellest, kes liidestujaks on, näiteks teenuse liidestamiseks eesti.ee ja/või riikliku postkastiga. Teenuse liidestamine ning sõnumite saatmine AS IS kujul alternatiivsete kanalitega on samuti liidestuja ülesanne.
MKM	Majandus- ja Kommunikatsiooniministeerium
PRIA	Põllumajanduse Registrite ja Informatsiooni Amet
RIA	Riigi Infosüsteemi Amet
PPA	Politsei- ja Piirivalveamet
AKI	Andmekaitse inspektsioon
SKA	Sotsiaalkindlustusamet
KOV	Kohalik omavalitsus
MSP	*Message Service Provider* - sõnumite edastamise platvorm (näiteks LiveChat, Zendesk jmt platvormid)
API	*Application Program Interface* – rakendustarkvara liides
PoC	*Proof of Concept* ehk prototüüp
ALT süsteem	Analüüstav liidestuja komponent, millest analüüsi käigus luuakse PoC
Sessioon	Sessiooni all mõeldakse kliendiga peetud vestlust, mis koondab endas tervikuna vestluse algust selle lõppemiseni. Üldjuhul mõnest minutist kuni mõne tunnini
Facebook Leht	Facebook Page, ehk asutuse poolt kasutatavat lehte Facebooki keskkonnas, kus hoitakse ja edastatakse infot asutuse kohta, kasutatakse turunduslikel eesmärkidel? ning suheldakse klientidega vestluste kaudu kui klient pöördub läbi selle asutuse poole.

Lühikokkuvõte

Alternatiivsete kanalite kasutamise analüüsi- ja pilootprojekti eesmärgiks on analüüsida võimalusi, kuidas lihtsustada ja muuta efektiivsemaks suhtlust riigi ja kodanike vahel kasutades kaasaegseid kommunikatsioonikanaleid ja nende pakutavaid võimalusi. Kanalite all peetakse siinkohal silmas vestlusel (*chat*) põhinevaid rakendusi nagu näiteks Facebook Messenger, WhatsApp, Apple iMessages, Signal, jt. Uute kanalite kasutuselevõtu puhul on oluline, et paraneks kasutajakogemus, väheneks riigipoolne halduskoormus ning laieneks kaasatavate kodanike hulk. Projekt valmis perioodil 09.2020-12.2020 koostöös MKM, RIA, PRIA ja Solita spetsialistidega.

Analüüs esimeses etapis intervjueeriti kaasatud riigiasutusi (MKM, RIA, PRIA, PPA, Sotsiaalkindlustusamet, Häirekeskus ja Maanteeamet) saamaks tagasisidet, milline on nende alternatiivsete kanalite kasutamise hetkeolukord, võimalikud kasutuslood, liidestamise võimalused olemasolevate asutuste süsteemidega ning ootused tulevikule. Intervjuudest selgus, et hetkel kasutatakse alternatiivseid kanaleid minimaalselt ning kasutuslugudena nähakse võimalusi tutvustada ja juhendada kodanikke teenuste kasutamisel ning edastada neile teateid uue kanali kaudu reaalajas teavitamise eesmärgil. Enamik asutusi integreeriks loodavad lahendused juba kasutatavate kliendihaldussüsteemidega, kuna seal on neil kõige ajakohasem info klientide kohta ning võimekus edastada isikuandmeid sisaldavaid dokumente kui selleks vajadus tekib.

Teiseks analüüsiti turul enamlevinud alternatiivseid kanaleid, nende võimekust teostada kasutuslugudes ettenähtud toiminguid ning vastavust turvalisuse ja andmekaitse nõuetele. Lisaks vaadeldi ka sõnumivahetuse platvormide (MSP) kasutusvõimalusi ning reaalse lahenduse juures kasutamise mõttekust ja kõikide lahenduste kasutamise kulusid.

Detailsemalt võrreldi 6 erinevat kanalit ning 3 sõnumivahetuse platvormi põhilisi omadusi nagu näiteks sõnumisaatmise algatamise võimalus asutuse poolt, API olemasolu ja kasutamise võimalused, andmete hoidmise asukoht, teenuse hind, jms. Võrdluse tulemusena sai prototüübi loomiseks välja valitud lahendus, kus kasutatakse Whatsapp ja Facebook Messenger kanaleid ning MSP-na MessageBird platvormi. Selle põhjal loodi ka vastava kanali lahendust kasutavad kasutajaliidese vaated.

Eraldi vaadeldi veel klientide autentimise ja digitaalse allkirjastamise võimalusi mille tulemusena leiti, et kuna alternatiivseid kanaleid kasutatakse peamiselt mobiilirakendustena, siis on kasutatavad SmartID ning MobiilID lahendused. Need variandid said ka prototüübis edukalt ja suuremate kuludeta kasutusele võetud. Lisaks uuriti, mis vahenditega saaks mõõta kasutajakogemuse taset ning klientide rahulolu.

Üks eraldiseisev valdkond mida analüüsi käigus uuriti väga põhjalikult oli alternatiivsete kanalite kasutamisega kaasnevad õiguslikud nõuded ja piirangud. Kuna kliendid ja asutused edastavad alternatiivsete kanalite kaudu erinevaid isikuandmeid, siis kohalduvad nii andmetele kui nende töötlejatele GDPR-is tulenevad nõuded. Suuremad riskikohad antud kontekstis on vastutavate ja volitatud töötlejate vastutus, nendevaheliste andmetöötluslepingute siduvus ja kolmandates riikides andmete töötlemine. Viimane punkt on üks olulisemaid piiranguid kanalite kasutamisel, kuna enamik alternatiivseid kanaleid pakkuvatest ettevõtetest on peakorteriga Ameerika Ühendriikides ja neil on lepingu järgi õigus ka seal andmeid töödelda. See aga läheb vastuollu Euroopa Komisjoni nõudega kus andmeid tohib edastada vaid piisava andmekaitse tasemega riigile või tema kindlaksmääratud sektorile. Hetkel on käimas arutelu EU ja Ameerika Ühendriikide vahelise

uue kokkuleppe saavutamiseks andmete turvaliseks ning kontrollitud edastamiseks, mis võiks tuua lahenduse lahenduste kasutamisel tekkivatele riskidele. Tuleb mainida, et varasemalt loodud kokkulepped raamistikud „*privacy shield*“ ja „*safe harbour*“[1] on tänaseks oma olemuselt õigusruumi vaatest osutunud tühiseks ning vajadus toimiva koostöö osas tuleb leida.

Õigusliku analüüsi tulemusena selgus, et alternatiivsete kanalite kaudu teenuste pakkumine on hetkel üsnagi piiratud nii tehnoloogiliselt kui kanalite valikuga. Täpsemaks piirangute mõistmiseks tehti kolmele peamisele kasutusloole ka andmekaitsealane mõjuhinnang, mis analüüsis põhjalikult kasutatavaid infosüsteeme, nende kliente ja kasutuses olevaid andmekoosseise.

Mõjuhinnangu tulemusel identifitseeriti kanalite kasutamisel 8 erinevat riski, millest kaks olid kõrge, 5 keskmise tasemega ja 1 madala taseme risk (detailsemalt Andmekaitse mõjuhinnangu peatükis). Enamiku neist riskidest saab maandada kui vestluse andmed kustutatakse alternatiivsest kanalist regulaarselt peale vestluste lõppu, kuid mõnel juhul tuleb rakendada ka teisi tehnilisi lahendusi ja piiranguid. Samas selgus, et tugevalt autentimist nõudvaid kasutuslugusid (isikuandmete edastamiseks suhtluses käigus) antud kanaleid kasutades rakendada ei saa, kuna tänane õigusraamistik tingib ebamõistlike riskide võtmist asutusele, kui nad kasutavad populaarsemaid alternatiivseid kanaleid.

Turvaanalüüsi käigus kujunes alternatiivsete kanalite täislahenduse ISKE klassiks K2T1S1. Sellest järeldub, et süsteemi käideldavus (K2) peab olema suurem kui 99% aastas; Terviklikkust (T1) on teada infoallikas, selle muutmise või hävitamise fakti on võimalik tuvastada, kontrollida ajakohasust erijuhtudel ja vastavalt vajadusele; Konfidentsiaalsus (S1) määrab, et info on asutusesiseseks kasutamiseks ning juurdepääs teabele on lubatud vaid juurdepääsu taotleva isiku õigustatud huvi korral.

Oluline info iga loodava infosüsteemi kohta on ka infosüsteemi aredus- ja halduskulud (ehk kulumudel). Antud analüüsist tulenevalt sai loodud kulumudel kahe alternatiivse lähenemise jaoks – esimeseks lahendus, kus kasutatakse sõnumiedastuseks MSP teenust ning teine lahendus, kus MSP funktsionaalsus arendatakse ise. Detailne ülevaade koos eeldustega on eraldi lahti kirjutatud kulumudeli peatükis, ent võib öelda, et MSP rolli ise arendades ja hallates on süsteemi halduskulud üle kahe korra suuremad kui teenust mõnelt MSP teenusepakkujalt ostes.
Süsteemide arendustöid hinnates võeti arvesse, et kasutatavad tehnoloogiad oleksid kaasaegsed ja võimalusel vabavaralised ning arendajate poolt laialdaselt kasutusel.

Valitud tehnilise lahenduse kohta arendati lahenduse prototüüp ning kirjeldati lahenduse arhitektuur ja tehnilised nõuded. Prototüüp realiseeriti kolme iteratsiooni tulemusena. ALT süsteem on oma olemuselt liidestumise komponent alternatiivsete kanalite ja asutuses kasutatava vestluse tööriista vahel. Komponendi rolliks on hallata suurt hulka erinevaid kanaleid (nt PPA'l on kasutusel mitmeid Facebooki lehti, lisaks võib olla asutusel kontosid WhatsApp'is, Instagram'is vms) ja koondada sissetulevad vestlused asutuse juturoboti või klienditeenindaja töölauale. Kuna töö raames realiseeriti vaid liidestuja komponent, siis loodav prototüüp ei moodusta veel terviklahendust nt klienditeenuse pakkumiseks alternatiivsest kanalist vaid loob alused lahenduse loomiseks järgnevates etappides. Terviklahenduse loomiseks tuleb võtta kasutusele asutusse klienditoe töölaud, mis

1 https://en.wikipedia.org/wiki/EU%E2%80%93US_Privacy_Shield

võimaldaks efektiivselt klientidega suhelda. Sellist töölaua ja juturoboti funktsionaalsust uuriti paralleelses riigi keskse juturoboti analüüsis[2].

Esimese liidestuja versioon keskendus MSP (MessageBird) ja eelistatud kanali (Facebook Messenger) integreerimises riigiportaali eesti.ee riikliku postkastiga, kusjuures kogu vestluse ajalugu talletuks riiklikku postkasti. Teise iteratsiooni puhul tuli aga lähenemist muuta kuna andmekaitsealase mõjuhinnang ei võimalda tugevat autentimist kasutada ja seega jäi ära ka integratsioon riigiportaali eesti.ee riikliku postkastiga. Lahendust lihtsustati seega selliselt, et selle kaudu saaks vastata Facebooki/Whatsappi kanalite kaudu sisse tulnud sõnumitele ja prototüüp loodi RIA testlehekülje vastu. Kolmandas iteratsioonis täiendati prototüüpi selliselt, et see ei sõltuks riiklikust postkastist vaid oleks paigaldatav kõikide asutuste lahendustesse koos juturobotiga.

Kokkuvõttes saab koostatud analüüsi ja arendatud prototüübi põhjal öelda, et alternatiivsete kanalite kasutamine Eesti riigiasutustes on võimalik ja vajalik ning tulevikus võetakse levinumad kanalid teatud kasutusjuhtude jaoks kasutusele. Kui lahenduse leiavad avalike pilveteenustena pakutavate platvormidel olevad andmekaitse alased riskid, siis võib kasutatavate teenuste arv mitmekordistuda. Edasiste arenduste osas võiks alternatiivsete kanalitena kasutusse võtta täiendavalt kodulehele paigaldatavad vestluse aknad ja üldiste teadete edastamiseks WhatsApp lahendused, mis on integreeritud juturoboti funktsionaalsusega.

[2] https://riigihanked.riik.ee/rhr-web/#/procurement/1976512/general-info

Sissejuhatus

Käesolev projekt on käivitatud analüüsimaks alternatiivsete kanalite kasutamise võimalikkust Eesti riigiasutuste ja klientide vahel.

Täna toimub enamus suhtlust asutuste ja nende klientide vahel läbi teeninduskeskkondade ning e-kirja teel. Samas on viimastel aastatel oluliselt suurenenud teavituste hulk ning asutustel on soov neid mahte veelgi kasvatada. Samuti soovitakse liikuda kodanike teavitamisest kodanikega suhtlemisele ning neid „nügida“ ehk suunata kasutama kasutama nende igapäevaselt kasutatavaid suhtluskanaleid, mis tagab parema kättesaadavuse riigi poolt pakutavate võimaluste ja kohustuste osas. Selliseid vajadusi on väljendanud kõik suuremad ametid nagu näiteks PPA, MTA, Statistikaamet ja PRIA. Kahjuks on traditsioonilised kanalid asünkroonsed (nt e-kirja või SMS saatmine, mis saadetakse *no-replay* formaadis välja) ning ei võimalda kiiret ja vahetut suhtlust, mida on vaja näiteks eriolukorra ja/või massteavituste puhul.

Üheks võimalikuks viisiks teavituste kohaletoimetamise parendamiseks oleks alternatiivsete kanalite (Facebook, Whatsapp, Viber, iMessage, jt.) kasutusele võtmine, mis võimaldaks kriitilisi ja elutähtsaid teavitusi klientidele kiiremini või isegi reaalajas kohale toimetada. Samas puudub täna täpne teadmine, millistele tehnilistele nõuetele peaks lahendus vastama, millised riskid ja piirangud võivad kaasneda, millises ulatuses saab teavitusi saata jne.

2019. aasta statistika järgi kasutab enamik Eesti inimesi interneti, aktiivseid sotsiaalmeedia kliente on üle poole elanikkonnast ja Statistikaameti 2017. aasta uuring näitas, et üle 90% noortest tarbib internetiteenuseid mobiiliseadmest. Äripäeva sotsiaalmeedia kasutamise uuring[3] näitab, et aastal 2020 kasutas Eestis 750 000 inimest sotisaalmeedia kanaleid ja viimase aasta juurdekasv oli 4,2%, populaarsemateks keskkondadeks olid Facebook, Instagram, LinkedIn ja Twitter. Seega on mõistlik keskenduda analüüsis sotsiaalmeediale ning suhtluskanalitele, mida kasutatakse mobiiliseadmega. 2020 aasta riigiportaali rahulolu uuringust[4] selgus, et kliendid eelistavad e-posti ja telefoni (SMS) kommunikatsiooni kanalite järel sotsiaalmeedia suhtluskanaleid (kogu valimist 5% ja e-residentidest 15%).

Antud projekti eesmärk on üheltpoolt analüüsida alternatiivsete kanalite kasutamist klientide teavitamiseks ja nendega suhtlemiseks, eesmärgiga vähendada vajadust edasi arendada erinevaid eraldiseisvaid kasutajaliideseid, vähendada riigiga suhtlemisel koormust ja parandada kasutajamugavust. Analüüsi tulemuseks on teadmine, kas ja millistel tingimustel oleks võimalik alternatiivsete kanalite kasutamine klientidega suhtlemiseks.

Antud analüüsi käigus keskendutakse riigiportaali eesti.ee riikliku liidestamise võimalikkusele 5 alternatiivsete kanalitega. Alternatiivsete kanalitega liidestumiseks tuleks luua eraldiseisev rakendus ehk liidestuja, millel on omakorda kindel protokoll teenuse liidestamiseks riikliku postkastiga. Tulevikus peaks kliendil olema võimalik valida, millise kanali kaudu ta soovib riigilt teavitusi saada ja riigiga suhelda.

Paralleelselt toimub ka alternatiivse(te) kanali(te)ga liidestamise prototüübi (PoC) loomine antud kontseptsiooni tehnoloogiliseks katsetamiseks. PoC kontseptsiooni käigus tuleks läbi liidestuja liidestada riiklik postkast analüüsi raames välja valitud alternatiivse(te) kanali(te)ga ja luua klientide autentimiseks, kontode sidumiseks ja kontaktide haldamiseks võimalus

3 https://www.bestsales.ee/uudised/2020/02/06/uuring-eestlaste-interneti-ja-sotsiaalmeedia-kasutus-aastal-2020

4 https://www.ria.ee/sites/default/files/kantar_emor_riigiportaali_eesti.ee_rahuloluanaluus_koondaruanne.pdf

riikliku postkasti juurde. Liidestamise eesmärgiks on saada praktiline kogemus ja õppetund, mida tuleks edasistel liidestamistel arvestada ja millised on riskid.

Analüüs on jaotunud 6 teemasse, kus kõigepealt vaatleme projekti jooksul tehtud muudatusi võrreldes algse analüüsiga, seejärel kaardistame ärivajadused, alternatiivsete kanalite funktsionaalsuse, koostame õigus ja andmekaitseanalüüsi ning lõpuks toome välja loodud prototüübi tehnilise lahenduse koos alternatiivsete kulumudelitega.

Projekti jooksul toimunud fookuse muudatused

Peatüki loomise põhjuseks on projekti jooksul omandatud uutest teadmistest (mis ei olnud hankijale ja pakkujale teada analüüsi alguses) tulenevalt parimale lähenemise keskendumine ja sobivaima prototüübi loomiseks.

Analüüsi esimese etapi alguses selgus, et vähemalt täna ei võimalda alternatiivsed kanalid oma olemuselt asendada e-kirja või SMS teenust ehk alustada vestlust kliendiga. Asutusel on võimalik enamikes alternatiivsetes kanalites vastata peale suhtluse algatamist kliendi poolt, kuid siin esinevad piirangud, mis võimaldavad vastata 1-7 päeva jooksul. WhatsApp ja Viber pakuvad oma platvormidel vestluse alustamist, ehk teate edastamise võimalust oluliste piirangutega ning tasu eest. Kuna Viber ei ole Eestis piisavalt levinud suhtlusplatvorm[5], siis keskenduti analüüsis teadete edastamisele kanalis WhatsApp (kasutades *Templates ehk sõnumi mallidel põhinevat*eate formaati). Edasises töös ilmnes kanalile piirang, millega riigiasutusi üldjuhul platvormi kasutama ei lubata, kuna võib tekkida oht poliitilise propaganda edastamiseks. Samas leidis kinnitust, et kuigi WhatsApp Business Templates kasutamisel on piirangud, näiteks on vajalik kooskõlastada teavituste sisu/mall, siis juurdepääs riigiasutustel on võimalik. Sellest lähtuvalt loodi analüüsi käigus demo eesti.ee Facebook Leht (Pikseldus), Whatsapp demo kontod ja taotleti juurdepääsu API-le. Projekti perioodi vältel ei saadud vastust WhatsApp konto osas, kuna antud protsess on võrdlemisi pikk ja 6 nädala jooksul juurepääse, kuid ka eitavat vastust ei saadud.

Analüüsi käigus uuriti nii digitaalse allkirjastamise kui ka tugeva autentimise meetodeid, millest mobiilsetes suhtluskanalites kasutatavaks osutusid Mobiil-ID ja Smart-ID. Projekti lõppfaasis selgusid täiendavad õiguslikud piirangud, mis rakenduvad kanalite kasutamisele. Nimelt on kanalite ja terviklahenduse turvalisuse tase ISKE K2S1T1, mis vastab avalikele teenustele esitatavatele miinimumnõuetele. Riskiks on aga täiendavad nõuded, mida asutused peavad silmas pidama. Näiteks Facebooki puhul peab AKI hinnangul arvestama, et toimub andmete kolmandasse riiki edastamine, mis ei ole GDPR järgi keelatud, kuid tuleb kirjeldada kuidas asutused tagavad need täiendavad kaitsemeetmed (kirjeldatud detailsemalt andmekaitse mõjuhinnangu peatükis). Riski maandamiseks saaks Facebooki kaudu liigutada ainult näiteks üldistatud teavitusi või muud sisu, mis ei ole detailselt isikustatud. See omakorda tähendab, et Facebook Lehe kaudu vestlusteenust pakkuval asutusel lasub andmete töötlemisel kaasvastutaja roll ning andmete eksportijana vastutab asutus kõigi klientidele põhjustatud andmekahjude tekitamise eest. Ehk kokkuvõtlikult võib öelda, et tehniliselt on turvalisus süsteemis tagatud, kuid kasutusel olevad tüüplepingud suurkorporatsioonide ja asutuse vahel (nt Facebook *Terms of Service*) ei taga kaitset koostööpartneri poolt teostatud andmekahjude osas, mis muudab nii tugeva autentimise kui allkirjastamise alternatiivses kanalis veel täna tarbetuks. Lahenduseks oleks EU tasemel õigusselguse saavutamine läbi uue EU-USA koostööd kirjeldava raamistiku või läbi teenusepakkuja teenustaseme lepingu täienduste, mis tagaksid läbipaistvuse ja andmekaitse tingimustele vastavuse.

5 https://www.similarweb.com/apps/top/apple/store-rank/ee/all/top-free/iphone/

Süsteemi arhitektuuri loomisel oli üheks ärinõudeks analüüsis kodanikuga toimunud vestluse salvestamine riiklikus postkastis, kuid lähtuvalt alternatiivsete kanalite kasutamisest ei pruugi lahendus alati liidestuda läbi riigiportaali eesti.ee keskkonna. Liidestamine alternatiivsete kanalite vaates on mõistlik mõningatel juhtudel otse vastu asutuste juturoboteid ja nende taga olevaid süsteeme, mis haldavad sessiooni infot ning selle jooksul toimunud vestluste kokkuvõtteid. Seetõttu käsitleti sessiooni kokkuvõtteid vaid tehnilisel tasemel logidena, mida on võimalik hiljem auditeerimisel kasutada.

Äriprotsessid

Alternatiivsete kanalite kasutamine asutustes

Analüüsi raames kaardistati kaasatud asutustes (RIA, MKM, PRIA, PPA, Häirekeskus, Sotsiaalkindlustusamet ja Maanteeamet) tänased teadete edastamise ja klientidega suhtlemise meetodid. Protsessis kasutati intervjueerimise küsimustikku. Küsimustiku vastuste põhjal koostati näidis kasutusjuhud ning leiti ühtselt kirjeldatud tehnilised lahendused äriprotsessidele. Intervjueerimise käigus keskenduti kahele peamisele kanalite kasutamise juhule: klientidele teadete saatmine (asutuse poolt vestluse alustamine) ja nendega suhtlus (kliendi poolt algatatud vestlused).

Teadete all mõtleme siinkohal erinevaid otsuseid, kutseid ja meeldetuletusi, millele asutused üldjuhul vastust ei oota. Need jaotuvad omakorda veel manustega ning informatiivseteks teadeteks. Manusega kirjad edastatakse kohalejõudmise kontrolliga ning tüüpilised teated suunavad kliendi kirjas oleva lingi kaudu mõnda e-teenusesse jätkutoiminguid tegema (nt. juhilubade uuendamine). Asutused saavad saata isikukood või isikukood@eesti.ee peale teavitusi – peamine probleem on klientide postkasti suunamine igapäevaselt kasutatavale e-posti aadressile mõneti madal (ca 400k suunamist). See on asutuste jaoks mure koht kodanikeni jõudmisel kasutades selleks riikliku postkasti saatmise võimalust. Mõnedes asutustes eelistati teateid edastada asutuse enda süsteemidest, kuna riigiportaali eesti.ee riiklikus postkastis pole paljud süsteemi kasutavate kodanike kontaktid ajakohased või puuduvad üldse. Mitmed asutused on loonud menetlussüsteeme, e-teenuseid ja kirjade edastamise lahendusi, mis saadavad teateid otse klientidele ilma riikliku postkasti funktsionaalsuseta. Samuti kasutatakse osade teadete edastamiseks paberkandjal kirju koos kohaletoimetamise kontrolliga, näiteks tähitud kirjad, mis edastatakse isikule allkirja vastu. Paberkandjal kirju kasutatakse näiteks seadusest tuleneva kohustuse või puuduliku kontaktinfo tõttu, peamiselt saadetakse esimesed teavitused digitaalsetes kanalites ja kui nende kohaletoimetamine ei õnnestu, siis kasutatakse paberkandjal kirja.

Suhtluse alla kvalifitseerime need teated, millele oodatakse kliente samas kanalis ka vastama. Laiemalt saab suhtlust vaadelda ka keskse kliendihaldustarkvara põhiselt, mis võimaldaks klientidega suhelda kanalite üleselt ja hallata toimunud vestluste ajalugu. Sellisteks teenusteks on näiteks kliendi poolt algatatud küsimused telefoni või e-maili teel ning asutuse järelepärimised erinevate toimingute raames. Kasutajatoe teenuste osas üldiselt isikustatud infot ei edastata ega klientide autentimist ei teostata, kuid analüüsi käigus toodi välja soovi selliseid teenuseid pakkuda PRIA, EMTA, SKA ja KOV'ide juturoboti teenustes. Järelepärimiste osas kasutatakse enamasti asutuse e-teenuste automaatseid teateid, mis suunavad kliendi vastavasse teenusesse. Samuti kasutatakse krüpteeritud dokumentidega e-kirjade saatmist.

Teadete vahendamisel on oluline välja tuua autentimise tasemed vastavalt RIA autentimise nõuetele[6] jaotuvad need:

- Kõrge - isik omab ja teab midagi (nt ID-kaart, mID või ELi liikmesriigi eID ja PINkood vms). Selle tasemega on võimalik kindlalt tuvastada, et isik on see kes ta väidab ennast olevat ja saab kinnitada toiminguid (nt ID-kaartdiga pin 1 ja pin2).
- Märkimisväärne - isikul on mõni enamasti turvaline identimise vahend (nt *soft certificate* ja PIN-kood, kasutajanimi ja kordumatud paroolid või koodikalkulaator jms)
- Madal - isikul on nõrk identimisvahend (nt kasutajanimi ja püsiparooli või korduvate paroolidega paroolikaart; kasutajanimi ja e-kirja või SMSiga saadetav parool vms).
- määratlemata - määratlemata (nt e-kirjaga saadetav parool, Facebook Connect, Twitter Login vms)

Lähtuvalt Eestis tavaks saanud autentimise meetoditele loeme antud analüüsis tugevaks autentimiseks kõrge autentimise taseme ja ülejäänud 3 välja toodud meetodit rakenduse loomisel vaadeldakse nõrgemate autentimise tasemetena. Samuti on kasutusel autentimata süsteemi kasutamine, kus klient ei pea ennast tuvastama teadete edastamiseks (nt anonüümsete päringute korral).

Alternatiivsete kanalite kasutamiseks leidsime mitmeid kasutuslugusid, mis jaotusid peamiselt kolme kategooriasse:

- Teadete edastamine kiirematesse kanalitesse (nt SMS);
- Kodulehe juturobot/vestlus;
- Sotsiaalmeedia kanalid (peamiselt Facebook, WhatsApp).

Peamise teemana oli analüüsiskoobis teadete saatmine alternatiivsete kanalitesse, mis toimiksid sarnaselt e-kirjale ja SMS teenustele. Alternatiivsed kanalid oma olemuselt ei suuda veel täna asendada e-kirja või SMS teenust, kuna enamasti ei võimalda need vestluse alustamist asutuse poolt (nt. Facebook, Apple Business Chat jt). Samas näiteks WhatsApp ja Viber pakuvad oma platvormidel teate edastamise võimalusi kuid need on mõningate piirangutega (kirja mallidel põhinevate teadete edastamine, kus kirja mall/sisu on vajalik kooskõlastada teenusepakkujaga) ning tasu eest. Piirangud ei võimalda klientidega alustada vabatekstilist vestlust, mis võiks suhtluskanalis olla ka eelistatud variant. Samas seab WhatsApp riigiasutustele piiranguid platvormiga liitumiseks, kuna üsna rangelt kontrollitakse poliitilise sisuga teksti edastamist platvormil. Analüüsi käigus alustati RIA taotlusega platvormile juurdepääsude saamiseks, kuid 6 nädalat kestnud protsessi jooksul ei ole veel vastust saadud. Samas MSP teenusepakkujaga suheldes tähendasid nad, et tehakse erandeid ja teise EU riikide mõned asutused on vastava juurdepääsu saanud. Näiteks:

Tere, eesnimi perenimi

Seoses teie taotlusega tekkisid järgmised küsimused:

1. *...*
2. *...*

Detailsem kanalite võrdlus on tehtud peatükis Tehniline alternatiivsete kanalite võrdlus.

Teadete edastamise osas tõid kaasatud asutused välja soovi parandada tänast e-kirja teel info edastamise kiirust. Selleks kaaluvad ja rakendavad juba mitmed asutused SMS teenust. Intervjueerimise käigus tutvustati ka WhatsApp Business Templates võimalus, mille osas oli

6 https://www.ria.ee/sites/default/files/content-editors/EID/autentimislahendustele-kehtivad-nouded.pdf

tagasiside võrdlemisi erinev. Asutuses puudub info klientide tänaste eelistatud suhtluskanalite osas kuigi mõned, näiteks PRIA, plaanivad klientide eelistuste kaardistamist. Samuti tekitas küsimusi teenuse tasuline pool ning valmidus asutuse poolt hallata teatele vastamist nendes kanalistes (sh SMS), kuna puuduvad tööriistad interaktiivseks vestluseks. Ühe takistusena toodi välja ka eelnevalt kirjeldatud riikliku postkasti vähene kasutamine, mis tingib täna dubleeriva süsteemi loomist asutusse. Asutuste poolne lähenemine viitab tänase riikliku postkasti teenuse kehvale teenuse disainile ja parema lahenduse olemasolul kaaluksid asutused selle integreerimist. Täna käivad tööd riikliku postikasti teenuse paremaks disainimiseks ning ka käesolev projekt toetab klientide kesksema teenuse loomist.

Teine kasutuslugu, mille osas oli asutustes ka kõige suurem huvi, on kasutajatoe ja teenuste pakkumine läbi vestlusakna. Seda nii e-teenuse sees kui asutuse kodulehel, tagamaks kliendi tugeva autentimise, tarkvara haldamine asutuses ning samaaegselt e-teenuses toimuva toetamiseks. PRIA pakub näiteks toetuse avalduste täitmisel telefoni teel tuge, mis võimaldab spetsialistil näha, mida klient taotlusega teeb. Lisaks toodi veel välja erinevate teenuste leidmine ja juhenditele viitamine asutuse kodulehel.

Viimane kasutuslugu on kasutajatoe ja teenuste pakkumine sotsiaalmeedias. Teenuse kasutamise eesmärgiks on toetada tänast kasutajatoe funktsionaalsust ja pakkuda anonüümseks jääda soovivate klientide nõustamist nt ohvriabi või PPA-lt erinevate juhtumite osas nõu küsimisel. Sotsiaalmeedia kanalite kasutamises ei tulnud analüüsi käigus välja klientide tugevalt autenditud sessioonide kasutamise vajadust alternatiivsetes kanalites. Isikustatud info edastamiseks eelistati e-teenuseid ja kodulehe akna vahendusel, kuid arvati, et sotsiaalmeedia kanalid ei ole parim lahendus sellise info edastamiseks. Samuti kaaluti tugevalt autenditud telefoni teenuseid, kuid hetkel pole seda teenust kasutusele võetud.

Analüüsi üheks peamiseks küsimuseks on kas alternatiivsete kanalitega liidestamine on mõistlik ja vajalik ning millist väärtust see klientidele looks? Alternatiivsete kanalite laiemal vaatlemisel näeme, et enamik suurettevõtteid rakendavad selliseid lahendusi enda klienditeeninduse ja äriprotsessides ning tehnoloogia areng suundub üha rohkem automatiseeritud vestluste haldusele. Samuti on selge trend järjest rohkem kasutada kiireid vestluspõhiseid tehnoloogiaid teenuste tarbimisel. Alternatiivsete kanalite kasutuselevõtt parandaks teenuste kättesaadavust klientidele. Vaatleme esimeseks liidestumise mõistlikkust asutuse seisukohalt, kus näeme et läbi alternatiivsete kanalite on võimalik lahendustesse tuua automatiseerimist (juturobotid) ja teenustes kiirema infovahetuse pidamiseks läbi sõnumivahetus lahenduste. Samuti on võimalik asutuste kodulehtede kaudu pakutavates vestlusakendes kliente efektiivsemalt toetada erinevate avalduste, taotluste jt vormide täitmisel, kuna on võimalik arendada tugevalt autenditud kasutajatoe funktsionaalsus koos e-teenuse keskkonnaga. Teiseks on klientidele, kes eelistavad teksti põhiseid suhtluskanaleid, võimalik täiendada teenuse kättesaadavust ja toimingute kiirust. Lisaks on teksti põhised lahendused olulised erivajadustega klientidele, kes suhtlevad teksti põhiselt (nt Häirekeskusel on süsteem erivajadustega klientide teenindamiseks SMS vahendusel). Siinkohal tuleb juurde tuua veel uute alternatiivsete kanalite osas tehnoloogia vaade lähtuvalt platvormidest ja nende võimalustest, mida käsitleti detailsemat Tehniliste alternatiivide võrdluse peatükis ja leiti, et eelistatud on Whatsapp, Facebook ning kodulehele integreeritavad vestluse lahendused.

Kokkuvõttes võib välja tuua laialdase huvi alternatiivsete kanalite kasutamise osas, eriti pidades silmas nooremat generatsiooni, kes eelistavad suhtlemisel kasutada just sõnumite vahetust. Kasutust nähakse pigem kasutajatoe ja teenuste pakkumisel kanalites ning vähem tugevalt autenditud teenuste osas. Intervjueerimise käigus toodi välja eelistatud kanalitena Facebook ja nooremate hulgas WhatsApp rakendused. Uuritud on kasutajate eelistusi

riigiportaali kasutajate rahulolu uuringus[7] kus on leitud, et sotsiaalmeedia kanaleid eelistavad 15% vastanud e-residentidest ja 5% kogu valimist. Lahenduse rakendamisel soovitakse integreerimist otse asutuses kasutatavate teenuste ja süsteemide vastu, mis ei oleks sõltuvusest riiklikust postkastist. Otse integreerimiseks on eelduseks lihtsalt taaskasutatav komponent sarnaselt TARA lahendusele, mis võimaldaks asutusel endiselt hallata oma süsteemi tervikuna ja kasutada lahendust asutuse kliendi baasiga. Samas võib teenus muutuda klientidele ebamugavamaks, kuna nad peavad enda eelistusi haldama kõigi teenuste juures eraldi. Samuti on eeliseks keskse süsteemi teadete hinnastamise, haldamise ja uuendamisega vähenevad kulud. Siin saab võrdluseks tuua alternatiivsetest kanalites sõnumivahetus platvormi kasutamise, kus teenuse ostmisel saadakse mahu soodustust, näiteks analüüsitavate mahtudega WhatsApp teenuse otse ostmisel on teate hinnaks 0.054€, aga vahendaja kaudu 0.034€. Erinevus tuleneb sellest, et vahendaja ostab teenust miljardite teadete edastamiseks, kuid Eestis on analüüsist lähtuv vajadus vaid 300 000 teadet, mis ei anna sellist mahu soodustust.

Eesti.ee riiklik postkast

Riikliku postkasti kasutamine asutustes on hetkel pigem madal, kuna süsteemis puuduvad paljud asutuse klientide kontaktandmed, mis ei võimalda suhtlust kogu kliendibaasiga. Samuti on tänane lahendus orienteeritud teadete väljasaatmisele, kuid kliendil puudub mõistlik lahendus samas kanalis vastamiseks. See on põhjustanud olukorra, kus asutused on loonud enda sisemised posti- ja suhtlussüsteemid. Alternatiivsete kanalite lahenduse kasutuselevõtuks peaks loodav süsteem liidestuma universaalselt asutuse süsteemidega ja toimima koos juturoboti lahendusega. Seda juba planeeritud arenduste vaates, mis ei näe ette täiendavat riikliku postkastiga integreerimist aga ka asutuse kontaktide erisuse tõttu. Täna käivad tööd riikliku postikasti teenuse paremaks disainimiseks ning ka käesolev projekt toetab klientide kesksema teenuse loomist, mis võiks tuleviks muuta riikliku postkasti kasutamist atraktiivsemaks.

Kasutuslood

Kasutuslugude kirjeldamisel lähtuti hetkel kasutusel olevast eesti.ee riikliku postkasti funktsionaalsusest ning intervjueerimisel kogutud huvitatud asutuste kasutuslugudest. Analüüsis toome välja kolm peamist kasutusjuhtu:

- Esimene sarnaneb tänasele riiklikule postkastile, ehk võimaldab saata teateid kliendile ja ei oota kliendilt mingit vastust.
- Teine on täielikult alternatiivses kanalis realiseeritud tugevalt autenditud sessiooniga vestlus, mis võimaldab edastada klientidele kanalis ka isikustatud infot.
- Kolmandal juhul saadetakse klientidele teade alternatiivses kanalis ja suunatakse seejärel manusega kirja lugemiseks riikliku postkasti või asutuse e-teenindusse.

Kasutuslugude kirjeldamisel oleme leidnud, et asutused suhtlevad klientidega peamiselt kolme kanalit kasutades: telefoni teel, e-maili/SMS teel ning kohaletoimetamise kontrolliga kanaleid kasutades. Neid kasutatakse vastavalt kasutajatoe pakkumiseks, teavitusteks (ei oodata samas kanalis vastamist) ja tundliku info edastamiseks, mis nõuab näiteks taotluste/avalduste esitamist. Alternatiivseid kanaleid kasutusele võttes tähendab see, et lahenduselt ei oodata alati kahepoolset suhtlust.

7 https://www.ria.ee/sites/default/files/kantar_emor_riigiportaali_eesti.ee_rahuloluanaluus_koondaruanne.pdf

Alternatiivne kanal e-mailile ja SMS teadetele

Kasutusloo oleme loonud võrdlemisi tüüpilisele asutuse poolt välja saadetavale teavitusele, mis põhineb tüüpkirja põhjal ning asendatakse vaid osa isikustatud välju. Näitena Maanteeameti poolt edastatav juhilubade aegumise teade:

Tere, eesnimi perekonnanimi

Teie juhiloa kehtivusaeg lõppeb 30.07.2020. Juhiloa vahetamise eelduseks on uus kehtiv tervisetõend.

Uue tervisetõendi saamiseks palume pöörduda perearsti poole ning taotleda e-tervisetõendit. Selleks palume eelnevalt täita tervisedeklaratsioon aadressil www.digilugu.ee .

Kui perearst on edastanud e-tervisetõendi läbi e-tervise infosüsteemi Maanteeametile, saate uue juhiloa taotleda meie e-teeninduses.

Juhiloa vahetus on Maanteeameti e-teeninduses kiirem ja 20% soodsam kui teenindusbüroos. Juhiloa vahetuse riigilõiv e-teeninduses on 20 eurot, teenindusbüroos 26 eurot.

Soovitame Teil tellida juhiloa oma postkasti, vältimaks ootejärjekordi meie teenindusbüroodes.

Juba 70% juhiloa vahetajatest eelistab e–teenindust ja posti teel kättetoimetamist.

Juhiloa vahetamiseks on vajalik kehtiv elektrooniline foto ja allkiri ning alaline elukoht Eestis. Alaline elukoht on koht, kus isik elab iga kalendriaasta jooksul vähemalt 185 päeva isiklike või tööalaste sidemete tõttu. Alalist elukohta tõendavad rahvastikuregistri andmed.

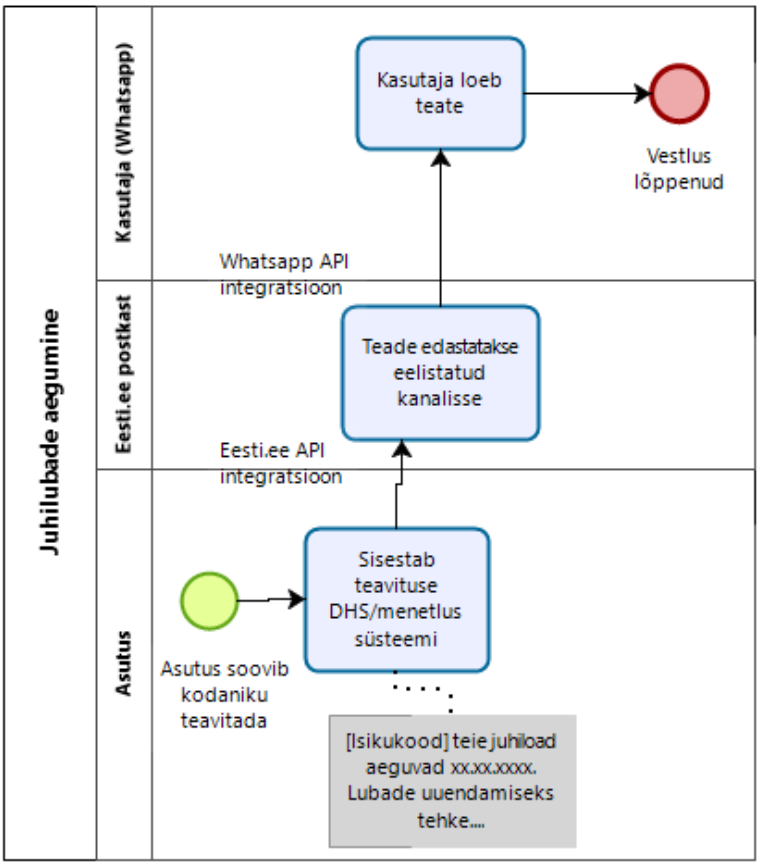
Juhul, kui olete jõudnud oma juhiloa juba ära vahetada, palun eirake seda pöördumist.

Liiklusreeglid on aja jooksul muutunud. Kasutage võimalust ja kontrollige oma teadmisi liiklusreeglitest Maanteeameti proovieksami küsimustega.

Turvalist liiklemist soovides

Maanteeamet

Kasutusloos (Joonis 1) liigub teade asutusest üle kirjeldatud x-tee teenuse või postkasti teenuse valitud isikukoodiga kliendile. Kiri väljastatakse üldjuhul asutuse DHS või menetluse süsteemist, seejärel jõuab see riiklikku postkasti ning edastatakse ka kliendi eelistatud alternatiivsesse kanalisse, nt. WhatsApp rakenduse kontole. Sellistele teadetele ei oodata üldiselt vastust vaid need on mõeldud kliendile informatiivse sisu edastamiseks või suunamiseks näiteks asutuse e-teenindusse edasisteks toiminguteks. Lahenduse toimimise eelduseks on kliendi eelnev alternatiivse kanali konto sidumine riiklikus postkastis enda eelistatud suhtluskanaliga.

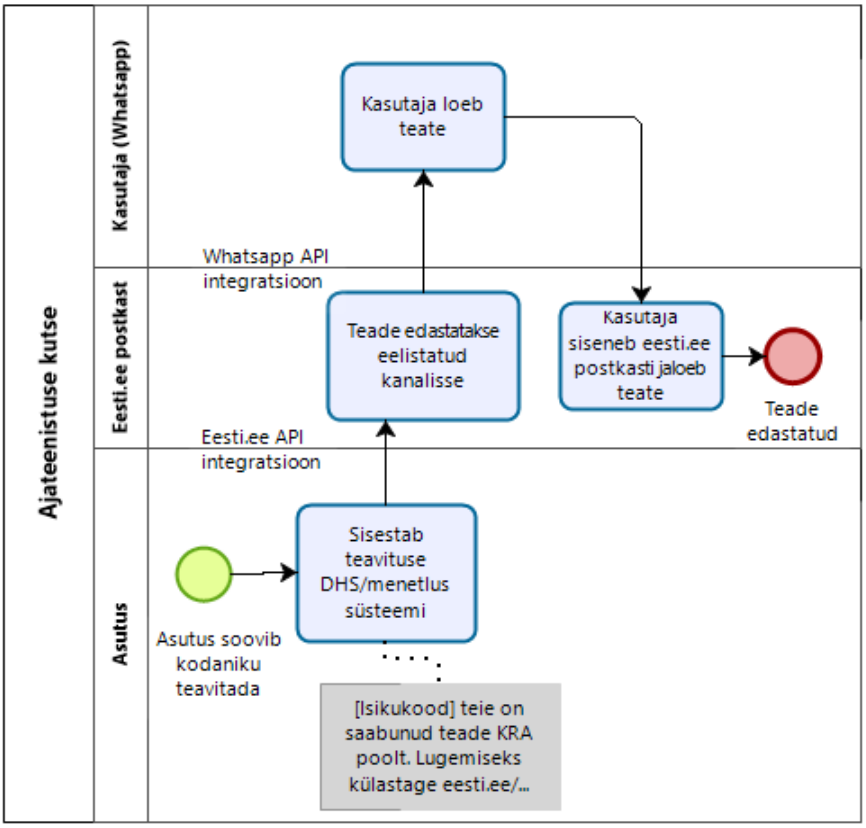


Joonis 1 Teate edastamine kliendi poolt eelistatud kanalisse

Manusega või tundlike isikuandmetega teate edastamine

Asutustes edastatakse tihti kohaletoimetamise kontrolliga konfidentsiaalseid dokumente. Selliste teadete lugemiseks saadetakse tavaliselt kliendile e-postile sõnum, et nende riiklikku postkasti on saabunud teade. Lahenduse eeliseks on see, et klient saab tutvuda dokumentidega tugevalt autenditud kanalis ning asutus saab olla veendunud, et klient on kirja kätte saanud. Lisaks riigiportaali eesti.ee riiklikule postkastile on kasutusel ka erinevaid e-teeninduse keskkondasid, mille kaudu asutused dokumente edastavad. Täiendavate keskkondade kasutamine on tingitud peamiselt madalast riigiportaali eesti.ee riikliku postkasti kasutamisest (~59% klientidest on postkasti suunanud[8]) ja kontaktide ajakohasus platvormil on madal, kuna osaliselt on klientide kontaktandmed muutunud või on need valesti sisestatud. Asutuste e-teenindustes on seetõttu rohkem ajakohaseid kliendikontakte, mis tingib enda kanalite loomise vajaduse.

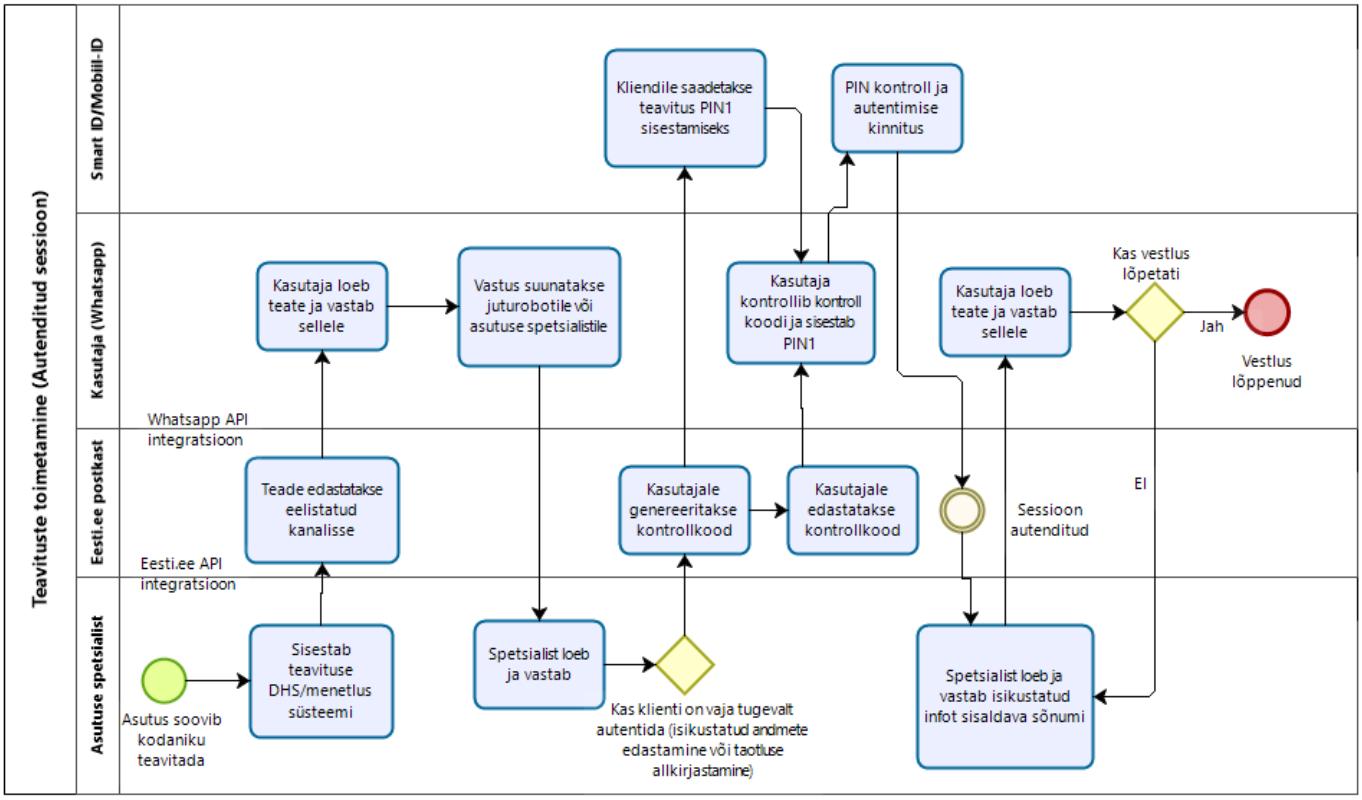
Analüüsi käigus kirjeldasime kahte võrdlemisi sarnase turvatasemega, kuid kliendi vaates erinevat võimalust eelnevalt kirjeldatud teadete edastamiseks. Esiteks toome välja protsessi, kus on e-kiri asendatud alternatiivse kanaliga WhatsApp (Joonis 2). Kliendile liikuv teade on informatiivne ja ütleb vaid, et kliendile on saabunud teade riiklikku postkasti, kus ta saab sellega tutvuda. Lahendus võiks olla eelistatud, kuna sarnaneb olemasolevale funktsionaalsusele ning garanteerib andmekaitse vaates minimaalse riskide tekke (st. välistele teenusepakkujatele edastatakse minimaalselt klientide infot). Alternatiivsete kanalite lahenduses saab klient teate valitud alternatiivses kanalis ja suundub kirjas oleva lingi kaudu asutuse e-teenusesse või riiklikku postkasti detailsemat teadet lugema.



Joonis 2 Manusega teate edastamine kliendi poolt eelistatud kanalisse

8 https://www.ria.ee/sites/default/files/kantar_emor_riigiportaali_eesti.ee_rahuloluanaluus_koondaruanne.pdf

Teiseks võimaluseks on kliendi autentimine alternatiivses kanalis (Joonis 3) kasutades selleks Smart-ID või Mobiil-ID lahendust sarnaselt näiteks täna pankade telefonitoes pakutavatele, kus klient autenditakse vestluse jooksul. Selleks küsitakse kliendilt vestluse jooksul eelistatud autentimise viisi ja tuvastamiseks vajalikku isikukoodi/telefoni numbrit, misjärel vastatakse kliendile kontrollkoodiga. Selle põhjal saab klient autentimisteate valitud meetodis ning sisestab enda PIN koodi. Autentimise lahenduse osas tuleb tähele panna, et klient kontrollkoode ja eelistatud meetodi valikut asutuse spetsialist ei näe, vaid päringud teostatakse automaatselt süsteemi poolt. Edasine vestlus toimub sessioonipõhiselt ja klient logitakse automaatselt välja peale vestluse lõppu. Alternatiiv on küll tehniliselt piisavalt turvaliselt lahendatud, kuid selle rakendamise riskid tulenevad tänastest õiguslikest nõuetest, mida käsitleme Õigusanalüüsi peatükis.



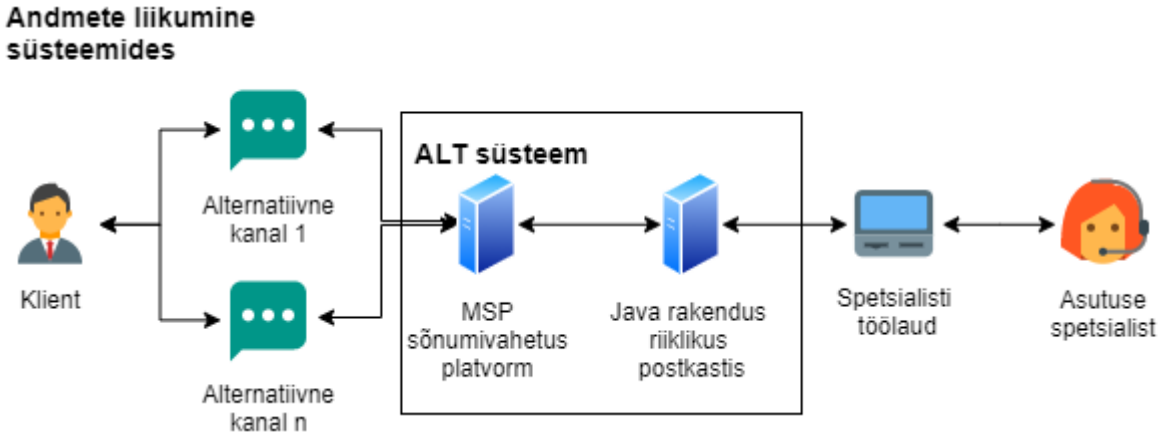
Joonis 3 Kliendi autentimine alternatiivses kanalis ja isikustatud info edastamine

Tehniline alternatiivsete kanalite võrdlus

Tehniliste lahenduste võrdluseks kirjeldame esmalt süsteemi komponendid (**Error! Reference source not found.**), milleks on alternatiivsed kanalid (nt Facebook, WhatsApp), sõnumivahetusplatvorm (MSP), riikliku postkasti juurde loodud rakendus, spetsialisti töölaua tööriist (võib olla osa juturoboti lahendusest). Süsteemi klientideks on kliendid ja asutuse spetsialistid.

ALT süsteem on liidestujaks suurele hulgale erinevatele alternatiivsetele kanalitele, mille erinevad andmeformaadid viiakse süsteemis ühtsele kujule ja edastatakse läbi API asutuses kasutusel olevale töölauale või juturobotile. Analüüsis ei käsitletud asutuse poolseid

integreeritavaid komponente täpsemalt, kuna hetkel pole vestluste halduseks sobivaid tööriistu. Lähim võimalik lahendus on DHS süsteemid ja Jira Service Desk lahendused, mis on mõeldud kirjade vahetuseks. Paralleelselt ALT süsteemi analüüsiga teostati ka juturoboti analüüs, mille raames uuriti sobivaid tööriistu asutuses operatiivselt teadetele vastamiseks.



Joonis 4 Süsteemi komponendid

Alternatiivsete kanalite võrdlemisel vaatasime tehnilisi võimalusi lähtuvalt kirjeldatud kasutusjuhtudest, milleks on klientidele teadete saatmine ja nendega aktiivne suhtlus vastavas kanalis. Kanalite võrdluses vaadeldi esmalt laiemat tehniliste sõnumivahetuse platvormide ringi:

- Facebook Messenger
- Twitter
- Telegram
- WeChat
- iMessage
- Viber
- Skype
- Slack
- WhatsApp
- Signal

Kanalite esialgne analüüs näitas, et mitmed kanalid ei sobi nende madala populaarsuse või riiklike mõjutuste tõttu (nt WeChat). Detailsemas analüüsis käsitleti 5 kanalit, mida võrdleme valitud parameetrite alusel (Tabel 1). Võrdluse koostamisel lähtusime analüüsi eesmärkidest tulenevalt sõnumitehnilisi platvormi piiranguid ja võimalusi, turvalisuse ja andmekaitse aspekte ning platvormi kasutamisega seotud kulusid arvestades.

Tabel 1 Alternatiivsete kanalite võrdlus

	WhatsApp	Facebook Messenger	Apple Business Chat	Signal
Sõnumi saatmine klient -> asutus	Jah.	Jah, kui asutusel on Facebook Leht.	Jah, kui asutus on registreeritud Apple Business konto.	Jah
Sõnumi saatmine asutus-> klient	Jah. Kui klient on algataja, siis tasuta. Lisaks tasulised Template sõnumid	Lehe kaudu - ainult juhul, kui klient algatab vestluse. (vastata saab 1-7 päeva jooksul)	Ainult juhul, kui klient algatab vestluse. Vastata saab seni kuni klient vestlust sulgenud ei ole	Jah
Konto sidumine Eesti.ee postkastiga	Klient peab saatma kinnituseks sõnumi oma WA kontolt vastuvõtvale kontole.	API lahendust ei võimalda. Võimalik läbi kliendi tugeva autentimise kanalis.	Ei. Suhtlus on sessioonipõhine.	Võimalik, läbi klient telefoni numbri
Massteavitused	Jah (piiratud saajate arvuga[9]).	Ei	Ei.	Jah
Suhtlusviis	REST API läbi sõnumiplatvormi.	REST API	Ainult läbi Apple toetatud sõnumiplatvormi (REST API).	Signal Library
API versioonid/ muudatused arendamiseks	8 minor versiooni aastal 2020.	8 major versiooni 4 aastaga.	Sõltub sõnumiplatvormist (vahendajast).	Avatud lähtekood, pidevalt arendatav
API turvalisus	HTTPS + AccessKey (sõnumiplatvormi REST API)	HTTPS + AccessKey (nii otse Graph API kui sõnumiplatvormi REST API)	HTTPS + AccessKey (sõnumiplatvormi REST API)	Lokaalne
Andmete salvestamine	Tõenäoliselt Facebooki datacenterites: EU territooriumil: Lulea (Rootsi) / Clonee (Iirimaa) - selle hetkeni, kui andmed on edastatud adressaadile.[10] Tuleb arvestada, et andmed liiguvad ka EL-st välja.	Tõenäoliselt EU territooriumil: Lulea (Rootsi) / Clonee (Iirimaa). Tuleb arvestada, et andmed liiguvad ka EL-st välja.	Apple serverites üle maailma.	Serverites ei salvestata muid kliendi andmeid kui kasutamise algusaeg ja viimase kasutuse aeg.
Klientide autentimise tase[11]	K0-1, S0-1, T0-1	K0-1, S0-1, T0-1	K0-1, S0-1, T0-1	K0-1, S0-1, T0-1
Allkirjastamise võimalused	Ainult teenusepakkuja juures.	Ainult teenusepakkuja juures.	Ainult teenusepakkuja juures.	Lisaarendus
Tasud	Väljasaadetavatele sõnumitele rakenduv tasu alates €0.0427/sõnum.	-	-	-
Sõnumi piirangud	Template teade kuni 950 tähemärki.	Kuni 20000 tähemärki.	Kui sõnum saadetakse mitte-iOS seadmele, muutub see tavaliseks SMSiks	Puuduvad

9 https://developers.facebook.com/docs/whatsapp/api/rate-limits/#messaging

10 https://www.whatsapp.com/legal/client

11 https://www.ria.ee/sites/default/files/content-editors/EID/autentimislahendustele-kehtivad-nouded.pdf

Üldiselt on asutustele ja ettevõtetele mõeldud alternatiivsete kanalite võimalused suunatud kasutajatoe funktsiooni pakkumiseks, mis aga seab mitmeid piiranguid klientidega suhtlemisel. Peamiseks takistuseks on klientidele teadete saatmine ehk enamasti ei võimaldata asutuse poolt vestluse algatamist. Rakendused võimaldavad suhtlust kui klient saadab esimese päringu teenusesse, millele saab seejärel vastata. Selline nõue välistab või vähendab platvormide riske vestluskanalites reklaami edastamiseks ja võimaldab klienttele just kasutajatoe funktsionaalsust pakkuda. Kanalis küsimustele vastamiseks on samuti seatud ajalised piirangud vahemikus 1-7 päeva, mis võimaldavad info edastada vaid kliendi algatatud teemal. Detailsemas analüüsis käsitleme viit alternatiivset kanalit, millest vaid üks võimaldab alustada teadete edastamisega platvormil, WhatsApp. Antud platvorm võimaldab oluliste piirangutega klientidele teade edastamist (Template Messages abil), mis on platvormil tasuline (~0.05€/sõnum), peab vastama eelnevalt kontrollitud mallile ning tohib sisaldada maksimaalselt 950 tähemärki.

Näitena saaks muudetud kujul (näide 1700 tähemärki) edastada hetkel aktuaalset teadet Terviseametilt:

Hea Eesti inimene!

Edastame Terviseameti kõige olulisema info koroonaviiruse (COVID-19) kohta.

Kui oled tulnud riskipiirkonnast või kokku puutunud koroonaviirusesse haigestunuga, jää kaheks nädalaks koju ja jälgi sel ajal oma tervist. Riskipiirkondade kohta saad infot: www.terviseamet.ee/riskipiirkonnad

Pea meeles! Praegu on gripihooaeg ja liikvel on erinevad nakkushaigused, mille sümptomid on koroonaviirusega sarnased.
Palaviku, köha või hingamisraskuste korral küsi nõu perearstilt või perearsti nõuandeliinilt 1220 (välismaalt helistades +372 634 6630) ja maini, kui oled saabunud viimase 14 päeva jooksul riskipiirkonnast või oled kokku puutunud koroonaviirusesse haigestunuga.
Tavapäraselt kaasneb koroonaviirusega palavik, köha ja/või hingamisraskused ning see levib inimeselt inimesele piisknakkuse (köhimise ja aevastamise), samuti saastunud pindadel olevate pritsmete ja käte kaudu.
Üldjuhul kulgeb haigus kergete haigusnähtudega. Koroonaviirus ohustab kõige enam vanemaealisi ja nõrgenenud immuunsüsteemiga inimesi.

Soovitused:
- *Kõige paremini saad end ja oma lähedasi haigestumise eest kaitsta, kui pesed hoolikalt ja regulaarselt käsi!*
- *Kui tunned end haigena, püsi kodus ja ravi end, nii tervened kiiremini ja kaitsed haigestumise eest ka teisi.*
- *Haigestunud inimesest hoia vähemalt ühe meetri kaugusele.*
- *Viiruse kahtluse korral ära mine erakorralise meditsiini osakonda (EMO) – sellega võid ohustada teisi. Helista perearstile või perearsti nõuandeliinile 1220 (välismaalt helistades +372 634 6630).*

Korrektse ja ajakohase info koroonaviiruse kohta leiad aadressilt: www.koroonaviirus.ee

Lisainfo haiguslehtede kohta Haigekassa koduleheküljelt: VAJUTA SIIA

Täname mõistva suhtumise ja koostöö eest!
Terviseamet
www.terviseamet.ee

Platvormide turvalisuse ja andmekaitse alased lahendused on võrdlemisi sarnased. Kirjavahetust hoitakse üldjuhul EU serverites (kuid võib toimuda andmete hoidmine ehk töötlemine ka EL välistes serverites sh. kolmandad riigid), kliendi andmeid võimaldatakse kustutada ning andmevahetus API kaudu käib üle turvatud liidese. Samas on platvormidel klientide sisselogimine lahendatud sarnaselt e-kirjadele ehk kasutajanime/parooli sisestamisega, mis ei võimalda klientidele baaslahenduses tundlikku ja eriliigilist isikustatud infot edastada. Samuti võib piiravaks teguriks saada ettevõtete poliitika töödelda mõningaid andmeid emaettevõtetes (peamiselt Ameerika Ühendriigi), mis seab lahenduse kasutamisel teatavad piirangud andmete säilitamiseks kanalis. Täpsemalt peatükis Õigusanalüüs.

Täiendava alternatiivina vaatleme kodulehele või e-teenusesse paigaldatavat vestlustööriista, mida hanke raames tehnilise poole pealt detailsemalt ei hinnata, kuna seda tehakse juba MKM-i paralleelses Juturoboti analüüsis. Alternatiivkanalina on selline lahendus aga andmekaitse ja klientide tugeva autentimise vaatest parim lahendus mille tõttu planeerime seda alternatiivkanalite arhitektuuri planeerimisel loodavas süsteemis liidestada.

WhatsApp

WhatsApp platvorm pakub teadete saatmise ja suhtluse võimalusi. Platvormi kasutamiseks asutuse poolt kasutatakse WhatsApp Business ja klientide poolt WhatsApp rakendust (edaspidi käsitleme mõlemat WhatsApp nime all). Teadete saatmiseks on vaja eelnevalt kliendi telefoninumber siduda riiklikus postkastis, mis võimaldab seejärel klientidele teadete edastamist läbi Templates funktsiooni. See tähendab, et asutusel on võimalik edastada eelnevalt platvormil kinnitatud malli põhjal kuni 950 tähemärki pikka teadet. Teadete edastamise funktsionaalsus on tasuline ja maksab alates 0.0427€/sõnum [12](sõltuvalt saadetud sõnumite hulgast; väiksemate mahtude puhul on hind suurem nt sõnumi hind kuni 250k - 0.053€, 3M - 0.05€, 5M - 0.0427€ . Suhtlus platvormil on aga tasuta ja ilma piiranguteta, kui selle alustab klient ise. WhatsApp piirab platvormi kasutamist riigiasutustele, kuna nähakse ohtu selle kasutamist poliitiliste reklaamide edastamiseks, kuid analüüsi käigus on selgunud, et paljudes teistes riikides on asutustele ligipääs platvormile antud (info on saadud MSP intervjuudest nii MessageBird, Zendesk Sushine, kui Twilio esindajatega rääkides, kuid kuna info on konfidentsiaalne siis detailsemalt seda avada ei saa). Liitumise valideerimiseks tuleb asutusel taotleda vastavat juurdepääsu.

Facebook Messenger

Platvorm on loodud eesmärgiga toetada kliente ja vahendada teenuseid. Alternatiivsete kanalite vaates võimaldab platvorm vastata klientide päringutele, kuid ei võimalda asutusel vestlust alustada, mis elimineerib kanali teadete saatmiseks. Samuti ei väljasta Facebook kliendi identifikaatorit vaid see edastatakse Facebook Lehe (*Page Scoped Identificator*) põhiselt kliendi kohta. See tähendab, et ühel kliendil võib olla süsteemis mitmeid identifikaatoreid. Suheldes teenustega näiteks PPA ja Eesti.ee Facebooki lehtedelt on kliendil mõlemal Lehel oma identifikaator. See omakorda piirab võimalust kasutajat identifitseerida API põhiselt riikliku postkastiga. Facebook'i puhul on täiendavaks piiranguks päringutele vastamise ajaaken 1-7 päeva, mis on platvormi üldine poliitika välistamaks reklaamide edastamist antud kanalis. Erandiks on lehekülgede kaudu teostatavad müügid ja üritused, kus on võimalik edastada teated sündmuse toimumise või kauba saatmise kohta peale selle aja möödumist. Täiendavalt on piiratud testimise faasis *News Feed*[13] funktsioon, mille kaudu saavad ettevõtted, MTÜ'd ja tervisega seotud asutused saata kasutajatele

12 https://developers.facebook.com/docs/whatsapp/pricing/

13 https://developers.facebook.com/docs/messenger-platform/policy/policy-overview

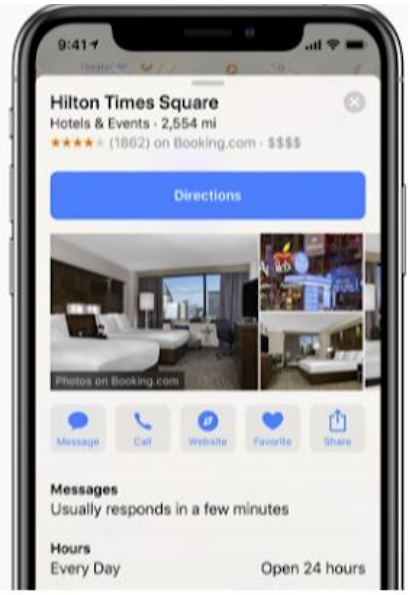
perioodilisi uudiseid. Funktsiooni piiratud juurdepääs asutustes kasutamiseks võimaldaks seda analüüsi raames vaadelda Terviseameti ja Häirekeskuse teenuste osas, kus oleks võimalik edastada näiteks informatsioon seoses COVID-19 muudatustega. Facebooki täiendavaks piiranguks on kasutajakonto sidumine, kuna antud funktsionaalsust platvorm ei paku. Facebook'i kaudu suhtluses on alternatiiviks klienditugev autentimine kanalis, kuid see on hetkel piiratud võrdlemisi suurte riskide võtmisega, mida käsitleme täpsemalt andmekaitsealase mõjuhinnangu peatükis.

Apple Business Chat ja Google Chat

Mõlemad lahendused on mõeldud toimima otsingumootorites ja võimaldavad ettevõtetega suhtlust ning teenuste pakkumist. Nende eeliseks on otsingus leitavate vastuste osas kohesel olemas olevad nupud, millele vajutades saab vestlust alustada (vt Joonis 5). Lahenduse kasutamisel on need head alternatiivsed kanalid kasutajatoe funktsionaalsuse pakkumisel sarnaselt Facebook'ile. Lahendused võimaldavad kasutajal asutuse poole pöörduda vestlust alustades ning neis on võimalik luua automatiseeritud vastuseid vastavalt kliendisisendile. Samuti on toetatud *intent*-funktsionaalsus, mis annab klientidele teatud valikvastused vastavalt esitatavale küsimusele ja võimaldavad vähendada asutuse spetsialistide töömahtu.

Olemuselt on Apple Business Chat rohkem toodete/teenuste müügile ja klienditoele orienteeritud lahendus, võimaldades kergesti saata kliendile interaktiivset sisu (pildid, videod, valikud) ning kohest Apple Pay abil maksmist. Apple Business Chat suhtlus toimub kasutades Apple rakendust iMessages ja kogu kliendi-asutuse vaheline suhtlus toimub selle abil. Sõnumid jäävad nähtavaks ning asutus saab kliendile saata uusi teateid kuni klient sõnumivahetuse eraldi sulgeb.

Google Chat on rohkem suhtlusrakendus, sarnane Slackile, võimaldades luua erinevaid kanaleid ja suhtlusgruppe. Siiski saab seda ka üks-ühele suhtlusel kasutada, suhelda asutuste kasutajatoega ning automatiseerida suhtlust erinevate juturobotite abil. Mobiiltelefonides kasutatakse suhtluseks Google Chat rakendust, arvutites on olemas veebipõhine klient. Kui kord on vestlus osapoolte vahel avatud, siis saab seda ajalise piiranguta jätkata kuni üks osapool vestlusest lahkub või teise osapoole blokeerib.



Joonis 5 Apple Business Chat kasutajaliides avatakse vajutades Message ikooni

Signal

Signal on vabavaraline ja avatud lähtekoodiga sõnumivahetusplatvorm mis on viimastel aastatel kogunud populaarsust turvalist sõnumivahetust hindavate inimeste seas. Signali eripära võrreldes teiste levinud platvormidega on see, et sõnumeid vahetatakse otse klientide vahel ning krüpteerituna. Serverid ei hoia klientide kohta mingit personaalset infot ega ülevaadet kontaktidest, kellega suheldakse. Platvorm vastab täielikult GDPR nõuetele.

Signali kasutamise teeb antud analüüsis raskeks tema integreerimise tehniline keerukus. Signali puhul pole loodud API-t vaid on saadaval erinevatele platvormidele kirjutatud teegid, mille abil saab sõnumivahetuse loogika luua enda süsteemi osaks. Selle plussiks on erinevate funktsioonide kasutamise ja integreerimise võimalus, kuid see nõuab funktsionaalsuse detailsemat analüüsi ja mahukat arendustööd.

Signali klientide hulk Eestis ei ole väga suur ja nende teenuse kasutamiseks ei ole võimalik kasutada sõnumivahetuse platvormi (MSP-d). Samuti oleks integreerimine asutuse süsteemidega üsnagi ajamahukas.

Sõnumiplatvormid

Platvormide kasutamiseks on lahenduste tootjad (Apple, WhatsApp, Facebook jt) seadnud veel täiendavalt piiranguid liidestuvale osapoolele, mille tõttu kasutatakse selleks peamiselt kahte tehnilist lahendust.

Esimese ja soovitatud lahendusena ei integreerita nende API-t otse asutuse tehniliste liideste vastu vaid kasutatakse sõnumivahetuse platvormi (MSP). Selline lahendus garanteerib lahenduse tervikliku toimimise API uuendamisel, mida tehakse võrdlemisi regulaarselt kuid omakorda seab täiendavad halduskulud asutusele. Samuti läbitakse MSP kasutamise puhul iga platvormi uuenduse korral täiendav valideerimise ning hindamise protsess sarnaselt mobiilirakenduste uuendamisele App Store või Google Play keskkondades.

Teise lahendusena on asutusel võimalik MSP roll ise võtta ja valideerida regulaarselt teenuse uuenduste järel lahenduse toimimist ning uuendada asutuses toimivaid tehnilisi protsesse ise. Lahendus tähendab täiendavaid haldus ja arendus kulusid. Samuti on platvormide vahendusel ostetud teate hind odavam kui otse integreerides, kuna platvormid vahendavad miljardeid teateid. Siin võib näitena tuua MessageBird ja ise arendatud MSP kulud teadete edastamisel. Võrdluse aluseks oleme võtnud analüüsis kaardistatud asutuste sõnumivahetuse mahuna ligikaudu 3 000 000 sõnumit aastas, millest optimistliku hinnanguna 30% võiks liikuda alternatiivsetes kanalites (jaotub omakorda Whatsapp 300 000, Facebook 300 00 ja juturobot 300 000). Sõnumivahetuse ühiku hinnaks MessageBird platvormil on 0.0045€[14] ehk 2700€ aastas (juturoboti teated ei liigu MSP vahendusel), millele lisandub 0.034€ Whatsapp Template teadete tasu, ehk kokku 13 900€ aastas. Samas ise arendades pole küll teate edastamise tasu kuid WhatsApp teate tasu on väikese mahu tõttu kallim - 0.0541€ ehk samade mahtude juures tuleb aastaseks kuluks 16 230€. Seega ei ole mõistlik otse integreerimist teha vaid kasutada selleks sobivaimat teenusepakkujat.

Sõnumivahetus platvormi valimisel vaatleme toetatud kliendipoolsed suhtluskanaleid (peaks toetama minimaalselt Facebook Messenger ja Whatsapp APIt), andmete salvestamine ja turvapoliitikat, kanalite vahel vahetamise funktsionaalsust ehk omni-channel lahenduse olemasolu, integreerimise-, püsi- ja jooksevkulusid.

Järgnevalt on kirjeldatud analüüsi raames analüüsitud sõnumivahetus platvormide alternatiive:

- Zendesk Sunshine
- MessageBird
- Twilio
- Ise arendatud lahendus

Tabel 2 MSP võrdlus

	Zendesk Sunshine	**MessageBird**	**Twilio**	**Eraldi arendatav lahendus (PoC tasemel)**
Toetatud kliendipoolsed suhtluskanalid	WhatsApp, Viber, FB Messenger, Apple Business Chat, Twilio (SMS), WeChat, Alexa (preview), Google Assistant (preview).	WhatsApp, Apple Business Chat, FB Messenger, Instagram.	WhatsApp, SMS, e-post	1 toetatud kanal (nt WhatsApp) Tulevikus täiendavate kanalite haldus/arendus[15]
MSP verifitseerimine	Ei	Ei	Ei	Jah
Andmete salvestamine	US/EU (Premium/Enterprise)	Google pilveplatvormi	US	Kliendi valitud asukohas.

14 https://messagebird.com/en/pricing/api

15 sõltub saadetud sõnumite hulgast. Tabelis väljatoodud hind kajastab esimese 250 000 sõnumi puhul kehtivat hinda per sõnum. Mida suurem kogus, seda odavam tuleb sõnumihind, näiteks 250 000.-1 000 000. sõnumi saatmiskulu Eestis on €0.0541/sõnum. Täpsem info https://www.twilio.com/whatsapp/pricing/

		serverites Belgias ja Madalmaades.		
Kanalivahetus	Jah	Jah	Ei	Lisaarendus
Kuutasu	2000€	-	-	Majutuskulud.
Teadete saatmise tasu	Fikseeritud kuutasu 1000€/kuu kuni 50k vestluse kohta WhatsApp Business Templates kasutamine 500€/kuu kuni 50k teavituse saatmiseks	WhatsApp: €0.0045/sõnum kliendi algatatud sessioonis; €0.034 (WA fee) + €0.0045 (Messagebird fee) / template sõnum.	Twilio vahendustasu $0.005/sõnum + WhatsAppi sõnumi hind €0.0553/template sõnum*	Platvormi sõnumisaatmistasu (WhatsApp €0.0541/template sõnum)
Integreerimise, haldus ja arenduskulu	Madal	Madal	Madal	Kõrgem

Tabel 3 MSP võrdlus

Zendesk Sunshine

Antud platvorm on üks populaarsemaid valikuid suurkorporatsioonide kliendihaldus lahenduste loomisel, kuna on tugevalt integreeritud Zendesk CRM tarkvaraga ning võimaldab teenindada suurt hulka alternatiivseid kanaleid. Lahenduse puuduseks on peamiselt suur seotus nende CRM-ga, mis piirab integreerimise võimalusi kolmandate osapoolte lahendustega nagu analüüsi raames vaadeldav ALT süsteem. Samuti on teenuse kasutamine kõige kallim (alates fikseeritud tasuga 3000€ kuus), kuna hinnastamise osas rakendatakse võrdlemisi suuri kuutasusid olenemata kasutatavast andmemahust. Teise võrreldavate teenusepakkujate lahendused hinnastavad teadete põhiselt, mis muudab lahenduse paindlikumaks. Samas on lahenduse eeliseks parem kasutajatugi, võimalus andmete hoiustamiseks EU territooriumil ja omni-channel funktsionaalsuse tugi, mis võimaldab kliendiga toimunud vestlusi hallata mitmes alternatiivses kanalis, kui edastada neid teistesse kanalitesse. Omnichannel lahendus on oluline Bürokratt visiooni vaates, kus kasutajaga peetud vestlust peab saama edastada teistele asutustele edasi vestluse jätkamiseks.

MessageBird

Platvormi integratsioonid eelkõige Facebook-i ja Whatsapp-i osas katavad soovitud nõuded MSP-le seatud ärinõuetest. Samuti on tagatud paindlik hinnastusmudel, mis on teate põhine ja välistab suured püsikulud. Sarnaselt Zendesk lahendusele hoitakse andmeid rangelt EU territooriumil ning pakutakse kõrgkäideldavuse ja andmekaitse nõuetele vastavaid tehnilisi lahendusi. Samuti on toetatud omni-channel funktsioonid klientide vaates ja MSP teenusele keskendudes pakub parimat API’t süsteemide liidestumiseks. Analüüsitavatest platvormidest eelistatud lahendus, kuna vastab esitatud nõuetele kõige täpsemalt.

Twilio

Platvormil on mitmeid piiranguid, millest määravaimaks on andmete hoiustamine Ameerika Ühendriikide territooriumil, mis ei taga piisavat isikuandmete kaitset ning läbipaistvust

andmete turvalisuse osas. Samuti puudub integratsioon näiteks Facebook API'ga ja omni-channel tugi. Lahendust kasutades võtaks asutus asjatuid riske ja piiraks võimalikku funktsionaalsust teenuse kasutamisel.

Otse integreerimine

MSP funktsionaalsuse loomine asutuse haldusalasse ja selle majutamine riigipilves või asutuse serverites tagaks täieliku ülevaate andmete liikumisest, kuid loob olulisi kulutusi süsteemi halduse ja API-de uuendamisega seotud toimingute läbiviimisel. Detailsemalt vaatleme süsteemi loomisel tekkivaid kulutusi Kulumudeli peatükis, kus toome välja detailsemalt kulukomponendid lähtuvalt lahenduse loomisest riikliku postkasti juurde. Ise arendatud süsteemi piiranguks võib saada WhatsApp API integreerimine, kuna ettevõtte eesmärgiks on garanteerida teenuse API uuendamisel selle toimimine, aga väikeste klientidega (mida Eesti kõikide teenuste vaates tervikuna mõne miljoni teatega on) tekiks üleliigne koormus teenuse haldamisel ja igakordsel sertifitseerimisel. See ei tähenda, et Whatsapp APIga poleks otseliideseid ettevõtetega tehtud ja see poleks võimalik. Arenduse vaates on MSP funktsionaalsuse realiseerimine võrdlemisi lihtne kasutades soovitud kanalite Java teeke ning lisada sessioonihaldus lahendused vastavalt nõuetele, kuid kulukaks lähevad kontode halduslahendused ja pidev APIde uuendamine (FB 2 versiooni ja WA 8 versiooni 2020 aastal). Analüüsitavate nõuete hindamisel ei saa seega antud alternatiivi lugeda eelistatuks, kuid vaatleme seda alternatiivina MSP lahenduse loomisel.

Klientide rahulolu mõõtmine

Klientide rahulolu mõõtmiseks on mitmeid alternatiive: e-maili teel küsitlused peale teenuse kasutamist (*Customer Satisfaction Surveys*); rahulolu hindamine vestluse lõpus (*Customer Satisfaction Score)*; tuttavatele soovitamise hindamine (*Net Promoter Score*); klientide vestluste analüüs; jne. Analüüsi raames soovitame klientide rahulolu hindamiseks kasutada *Customer Satisfaction Score* metoodikat, mis tähendab kasutajatelt tagasiside küsimist kohe peale teenuse kasutamist vestluseaknas. Klient annab hinnangu 5 palli süsteemis ja tulemus arvutatakse vastuste keskmisest lähtuvalt. Meetodi eeliseks on minimaalne ajakulu vastamiseks kuna võtab vähe aega, siis ongi eelistatud mobiilsetes seadmetes ning reaalajas jälgitav rahulolu skoor.

Teiste metoodikate kasutamine võib olla vajalik juhul, kui teenuse pakkumisel on regulaarselt rahulolematust. Sellisel juhul võib näiteks kaaluda kehva tulemuse saanud vestluste analüüsi, mis võimaldaks paremini mõista klientide rahulolematuse põhjuseid. Antud variandi eelduseks on see, et analüütikul on juurdepääs varasematele vestlustele, mis mõningatel juhtudel pole võimalik, näiteks terviseandmeid sisaldavate vestluste puhul. Teise meetodina võib rakendada e-maili teel edastatavat ca 3-5 minutit täidetavat küsimustikku koos vaba teksti väljadega, mis võimaldaks saada detailsemat ülevaadet võimalikest probleemidest. Kaaluda võiks ka tagasiside põhjal klientidelt telefoni teel tagasiside küsimist, kui teenuse osutamise kirjeldusest selgub, et teenust pakuti adekvaatselt, kuid hinnang tuli oluliselt madalam.

Klientide autentimine ja allkirjastamise võimalused

Hetkel kehtiva Eesti Vabariigi infosüsteemide autentimislahendustele rakenduvate nõuete[16] kohaselt ei kvalifitseeru väliste teenusepakkujate alternatiivsete kanalite lahendused tugevalt autenditud teenusteks, vaid on tasemel "määratlemata". Määratlemata tasemega autentimisvahendite kasutamist määrus EU tasemel ei reglementeeri ja nende kasutamise

16 https://www.ria.ee/sites/default/files/content-editors/EID/autentimislahendustele-kehtivad-nouded.pdf

otsustamine on jäetud iga liikmesriigi pädevusse. Lähtuvalt piirangust tuleb teenuste osutamine, mis nõuab autentimise taset “kõrge”, suunata näiteks asutuse kodulehele/juturobotile autenditud sessioonis suhtlemiseks.

Alternatiivina on kanalite autentimise võimaluseks mobiilsetel seadmetel toetatud Smart-ID ja Mobiil-ID lahendused. Seda just selle tõttu, et mobiilirakendused on peamised alternatiivkanalite lahendused ja ei võimalda rakendada ID kaardiga autentimist sessiooni sees (rakenduse tehniliste piirangute tõttu). Autentimine toimuks sarnaselt telefoni teel teostatavate autentimise päringutele, kus asutuse töötaja saaks suhtluskanalis algatada kliendi autentimise. Näiteks võib siin tuua Swedbank telefonitoe funktsionaalsuse, kus klient saab kõne kestel valida eelistatud autentimise viisi mille peale öeldakse kõnes kontrollsõna ja mille peale klient sisestab vastava autentimismeetodi PIN koodi oma telefoni. Lahendus tähendab aga täiendavat kuluallikat süsteemi kasutamisel.

Kampaania info edastamine alternatiivsetes kanalites

Kampaaniainfona vaatleme siin riiklike või piirkondlikke teateid, mida on tarvis operatiivselt edastada. Sellisteks teadeteks võivad olla COVID vaates olukorra uuendused, Maksuameti perioodilised teated või näiteks tormioht mõnes piirkonnas.

Tänased teenusepakkujad kaitsevad kliente autenditud kanalites reklaami saatmise eest, mistõttu pole platvormidel võimalik kampaaniaformaadis infot lihtsalt edastada. Piirang on tõenäoliselt loodud platvormide peamise tuluallika kindlustamiseks nende eelistatud meetodil. Samuti on piiratud riigiasutuste juurdepääs platvormile, kuna ei soovita poliitilise sisuga sõnumite saatmist. Lähtuvalt seatud piirangutest on lähim võimalik funktsionaalsus klientide massiliseks teavitamiseks Whatsapp Business Template lahendus, mis eeldab süsteemi sõnumimalli (*template*) sisestamist. Seejärel kontrollitakse sõnumi malli sisu teenusepakkuja poolt ning sobivuse korral saab vastavaid teateid edastada lõppkasutajatele.

Kampaaniainfo edastamiseks on eelistatud kanalid e-mail, SMS teenused ja WhatsApp, mille kaudu sõnumite saamiseks peab klient andma enda kinnituse kampaaniainfo saamiseks.

Statistika kogumine ja avaandmete avalikustamine

Alternatiivsete kanalite kasutamisega tekib erinevat liiki statistikat teostatud vestluste ning klientide osas. Osa sellest on lihtsad ülevaated nagu näiteks kontaktide arv, klientide demograafilised andmed, kontakti eesmärk, jne. Samas on võimalik kogutud andmete pealt teha ka sügavamaid järeldusi ja nende abil kasutusele võtta meetmeid, millega oluliselt parandada teenuse kvaliteeti ja kättesaadavust.

Näiteks võib tuua mõõdiku, mis näitab, mitme dialoogiga (täpsustamisega) ja ajaga klient soovitud info kätte sai ning kas keerulisemate juhtumite puhul saab juba ennetavalt täpsustavad küsimused ära küsida, mille vastuseid asutuse töötaja näeks suhtluse juures. Teine variant on uute teenuste või seadusemuudatuste mõjul tekkivad küsimused, mille puhul saaks näiteks ajutiselt tuua vastava teema esile ja suunata sellest huvitatud kliendid otse vastava info või spetsialistide juurde. Kuna klientide ja asutuste omavaheline suhtlus sisaldab tihti eri liiki isikuandmeid, siis statistika kogumise ja nende avaldamisega väga detailseks minna ei saa. Isikuandmeid sisaldavate vestluste põhjal saavad asutused (või ametid, kellele on see õigus antud) teenuse kvaliteeti monitoorida ja parandada.

Avaandmetena saaks kindlasti avalikustada alternatiivsete kanalite isikustamata statistikat, nagu näiteks pöördumiste arv, liik ja klientide demograafilised näitajad. Võimalusel ka

teenuste n.ö. kvaliteedinäitajad ja miks ka mitte automaatvastuste/juturobotite poolt lahendatud küsimuste osakaal ning sellega seotud ajaline kokkuhoid. Neid võimalusi tuleks teenuseid arendades kindlasti detailsemalt analüüsida ja planeerida.

Paberkandjatel kirjade edastamine

Kogu teabevahetuse üldine suund on elektrooniline suhtlus. Paberkandjal kirju edastatakse vaid järgnevates olukordades:

- inimene ei saa elektroonilisi vahendeid kasutada – need kas puuduvad või ei saa ta neid kasutada tervislikel vm põhjustel – näide: insuldijärgne seisund;
- elektroonilist teadet/dokumenti ei saa väljastada, näiteks tehnilistel põhjustel;
- rakendatakse erijuhtudel, näiteks välisriigi jaoks;
- paberil saatmist nõuab seadus või selle alusel antud määrus;
- harva väljastatakse dokumente ka siis, kui see koostatakse järelevalve käigus kohapeal ja antakse käest-kätte.

Reaalselt ei saa paberkandjal andmete väljastamist lõpetada, kuid vaikimisi valikuna peaks alati pakkuma elektroonilist esitamist. Õigusaktid tuleks üle vaadata, et poleks ainult paberi nõuet. Näiteks Maaeluministeerium muutis kõik sellised õigusaktid ära haldusmenetluse seaduse muutmise ajal. Eelistatud oleks selline seadusesäte, et kõik dokumendid lähevad alati eesti.ee postkasti ja vaid vajadusel väljastatakse neid paberil.

Paberkandjal kirjade saatmise osas on koostatud konsolideerimise analüüs, kus on pakutud varianti, et dokumendid tehakse elektrooniliselt ja kui vaja saata paberil ja siis edastatakse need postiteenuse pakkujale (Omniva vm). Teenusepakkuja rolliks on printida ja vajadusel lisada kinnitus koopia õigsuse kohta, panna ümbrikusse ning saata välja. Sellise lahenduse eeldusteks on

- üks keskne leping koos konfidentsiaalsusnõuetega (sh. nõuded postiteenuse pakkuja töötajatele);
- allkirja nõudest loobumine seal, kus võimalik (saab asendada kooskõlastuse/kinnitamisega süsteemis, digitempliga, ajatempliga);
- seal kus on vaja allkirja, kasutatakse digiallkirja ja koopial on automaatne märge allkirja andmise aja kohta.

Üheks probleemiks sellise lahenduse loomisel on koostöö postiteenuse pakkujaga, kus teenusepakkuja ei pruugi olla ühest lepingust huvitatud. Tulemuseks on see, et ei saada soodsamat lepingut suuremahulisema kirjade arvu tõttu, vaid rakendatakse väiksema mahulisi eraldi lepinguid asutustega, kus teenuse hinnad on kõrgemad.

Teise teemana tuleb käsitleda kirjade kohaletoimetamist, kus neid saab lugeda kätte toimetatuks:

- elektroonilises keskkonnas on dokument avatud või alla laetud;
- paber on saadetud rahvastikuregistris märgitud elukoha aadressile.

Osa dokumentide kättetoimetamist peab aga isik selgesõnaliselt kinnitama väljastusteatel või eraldi teatega.

Probleemiks on see kui inimene teab või eeldab, et dokumendi sisu talle ei meeldi (nt trahv, kohtukutse) ning ta ei soovi seda vastu võtta. Kui ta jätab sellise elektrooniliselt saadetud dokumendi vastu võtmata, saadetakse see paberil. Siin võiks kaaluda alternatiivina õigusaktide (nt Maksuhaldurile elektroonilisel teel esitatavate dokumentide formaadi- ja allkirjanõuded ning muud elektroonilisele teabevahetusele esitatavad nõuded maksumenetluses ja riigi-, valla- ning linnaasutuste poolt elektroonilisel teel esitatavate deklaratsioonide ja muude dokumentide nimekiri[17], sarnaselt on lahendatud ka teistes dokumentide elektroonilisel kättetoimetamist kirjeldavad õigusaktid, kus klient peab kirja vastuvõtmiseks sellekohase kinnituse andma) muutmist selliselt, et kiri loetakse kohale toimetatuks, kui kirja pole määratud perioodi jooksul kliendi poolt avatud.

Sisuliselt on temaatika seaduses kirjeldatud ja alternatiivsete kanalite loomise lahendusel arvestatakse kirjade edastamise ning kättetoimetamise nõudeid, kuid olemuslikult ei saa muuta isikute käitumist selliste teadete paberkandjal kasutamiseks või soovi neid olenemata kanalist vastu võtta.

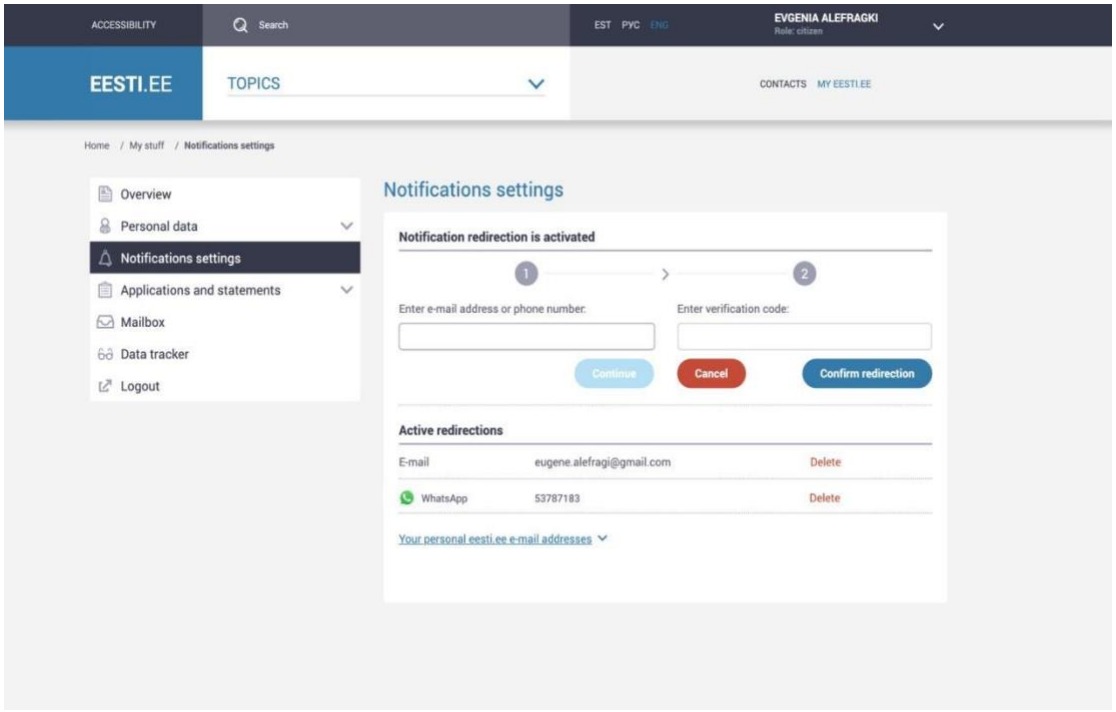
Kasutajaliides

Kasutajaliidese osas on muudatused seotud alternatiivse kanali lisamisega, et saaks teavitusi edastada ning kliendi poolt läbiviidud vestlusi kuvada riiklikus postkastis. Liidese täiendamisel (konto lisamiseks) on võimalus kasutada WhatsApp vaadet, kus kliendi konto lisatakse sarnaselt tänasele telefoninumbri lisamisele. Kasutajale saadetakse süsteemist kanalisse kontrollkood ja klient sisestab selle riigiportaalis. Sarnaselt saab lisada ka teisi kontosid, kus kasutajal on olemas unikaalne konto identifikaator või telefoni number laiendades vaates valitavate kontode hulka. Samas näiteks Facebooki lahenduse puhul pole sellist konto lisamist võimalik teha, kuna rakenduse API ei näe sellist funktsionaalsust ette ja kasutajaga pole võimalik vestlust asutuse poolt alustada. Lahendusena kasutatakse Facebooki puhul kliendi tugevat autentimist, mis võimaldab valideerida kasutajat vastu tema isikukoodi. Nii autenditud Facebooki kui WhatsApp teated salvestatakse postkasti sessioonipõhiselt ehk ühe kirjana, milles on kasutajaga sessiooni jooksul toimunud vestlus. Sessiooni pikkuseks on seejuures 24 tundi, riiklikus postkastis hoitakse seda kirjavahetust vastavalt kehtivale määrusele ja klient saab seal vaadata endaga toimunud vestluste ajalugu.

Järgnevalt on kujutatud Figma joonistena (Joonis 6, Joonis 7, Joonis 8) kasutajaliidese visandid, mille alusel on võimalik kasutajaliidese jätkuarendusi teostada. Disaini loomisel lähtuti tänasest kujundusest ning lisati kujundus telefoninumbri abil täiendava alternatiivkanali kasutuselevõtu funktsionaalsus.

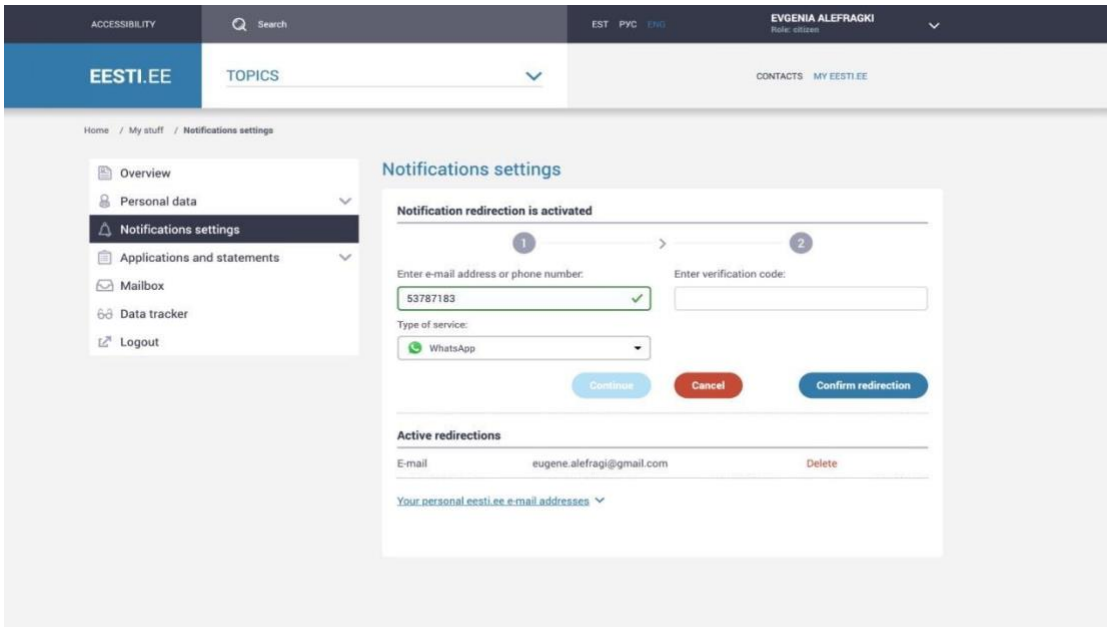
Joonisel 5 on kujutatud lisatud kontode kuvamise vaade, mis sarnaneb tänases kasutajaliideses eksisteerivale kontode nimekirjale, kuhu lisanduvad täiendavalt alternatiivsed kanalid.

17 https://www.riigiteataja.ee/akt/12830461?dbNotReadOnly=true



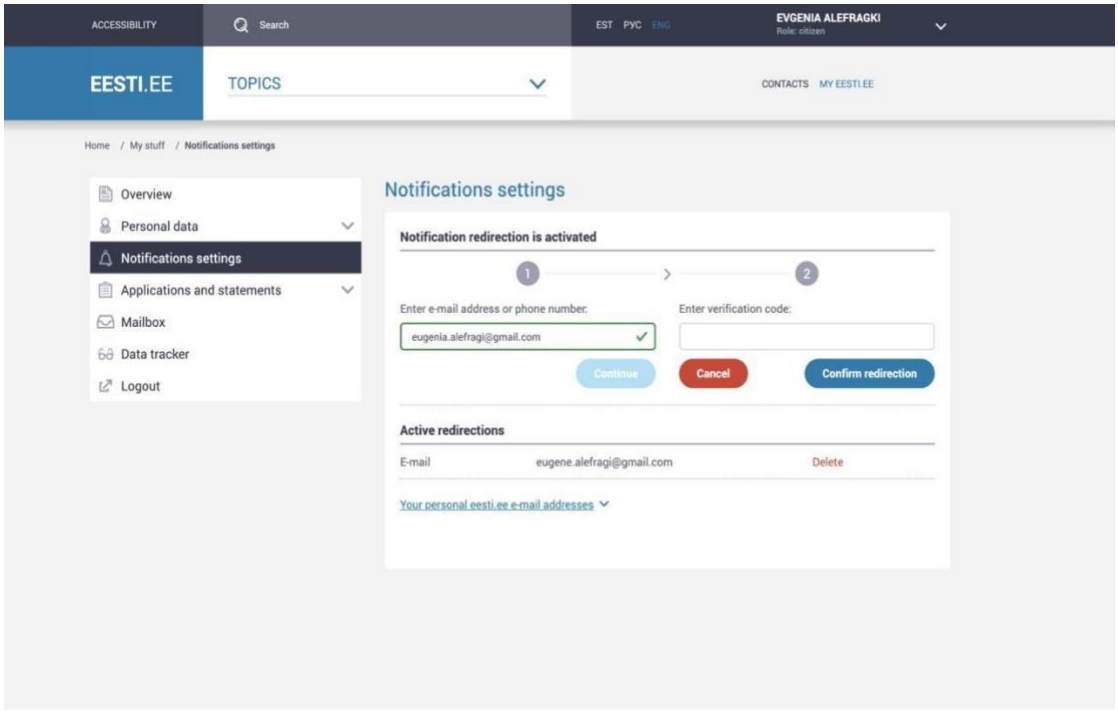
Joonis 6 Kliendi WhatsApp konto seotud

Joonis 7on kuvatud uue konto lisamine, mis muudab tänase kasutajaliidese vaadet lisades täiendava valikmenüü telefoninumbrit kirjutades. Valik menüüst saab valida näidisel telefoni kontakti ja Whatsappi platvormide vahel. Muudatus on vajalik, kuna senises kasutajaliideses seostati kliendi telefoninumbrit otseselt telefoniga, kuid lisanduva Whatsapp lahenduse korral tähendab see konto identifikaatorit ja avab täiendava dialoogi valik vastusena.



Joonis 7 Kliendi telefoni numbri sisestamisel alternatiivse kanali valiku dialoog

Joonis 8 Joonis 7on kirjeldatud tänast e-maili lisamise loogikat, mis ei ava Joonis 7 kirjeldatud lisa valikute lahtrit, kuna pole kirjeldatud ühtegi alternatiivset kanalit, mis kasutaks konto identifikaatorina e-maili.



Joonis 8 Kliendi e-maili sidumisel kasutajaliidese kujundus

Õigusanalüüs

Alternatiivsete kanalite vaates keskendub õigusanalüüs peamiselt avaliku teabe ja isikuandmete haldamisele valitud platvormidel Facebook Messenger ja WhatsApp. Analüüsi käigus toome välja erinevad piirangud GDPR-i ja valitud teenusepakkuja vaates ning laiendame piirangute tähendust teistele alternatiivsetele kanalitele.

Kanalites hallatavate andmete mõistmiseks oleme need jaotunud kolme kategooriasse lähtuvalt eelnevalt kirjeldatud kasutuslugudest.

Esimesena vaatleme avalikku teavet, milleks analüüsi kontekstis on kasutajatoe pakkumisel edastatav isikustamata info teenuste kättesaadavuse ja kasutamise osas. Nende puhul tuleks vaatamata juurdepääsupiiranguta teabe olemusele seadusandjal kehtestada vastavate teabeliikide puhul volitatud töötlejate (alternatiivsete kanalite teenuse pakkujad) kaasamiseks selge õiguslik alus. Kuna põhiseadusest tulenev seadusliku aluse põhimõte nõuab avaliku võimu igasugusele tegevusele, sealhulgas avalike alternatiivsete kanalite poolt pakutavate teenuste vahendusel toimuvale andmetöötlusele, õiguslikku alust ja seadusandjal tuleb tekitada juurdepääsupiiranguta teabe töötlemiseks avalike alternatiivsete kanalite vahendusel selge õiguslik alus. See ei tähenda siiski tingimata, et selline andmetöötlus kehtiva õiguse alusel keelatud oleks.

Teise andmeliigina vaatleme tavalisi isikuandmeid. Kolmandasse gruppi oleme liigitanud tundlikud- ja eriliigulased isikuandmeid, mille käsitlemine antud analüüsis toob täiendavad riskid kolmandate osapoolte lahenduste kasutamisel. Tavalised isikuandmed on teave inimese ehk füüsilise isiku (andmesubjekti) kohta, millega saab teda otseselt või kaudselt tuvastada. Tundlikud ja eriliiki isikuandmed on määratletavad isiku privaatelule suuremat ohtu valmistavate andmetena. Näiteks võib siin tuua sotsiaalabi saamise või kriminaal- ja väärteomenetlusega kogu toimumise protsessi jooksul kogutud andmed.

Tavaliste isikuandmete puhul näeme nende tekkimist peamiselt asutuse poolt edastatavate teadete osas, kus teade suunab kliendi tundlikke isikuandmeid lugema teenusepakkuja poolsesse tugevalt autenditud keskkonda (nt riiklik postkast). Tundlikud andmed tekivad peamiselt erinevates menetlus-, taotlus- või toiminguprotsessides ning neid ei saa ilma riskideta kolmandate osapoolte poolt pakutavates teenustes üldjuhul edastada. Täpsemalt oleme seda käsitlenud Vastutava ja volitatud töötleja peatükis. Vastutav ja volitatud töötleja

GDPR-i kohaselt jaotuvad isikuandmete töötlejad vastutavateks töötlejateks ja volitatud töötlejateks. Vastutav töötleja on GDPR artikli 4 punktist 7 lähtuvalt antud analüüsis asutus, kes pakub alternatiivse kanali kaudu teenust. Kusjuures alternatiivse kanali teenust pakkuv ettevõte (nt Facebook) on kaasvastutav töötleja, kuna osaliselt töödeldakse andmeid teenusepakkuja juures. Volitatud töötleja[18] on GDPR artikli 4 punktist 8 lähtuvalt teenusepakkuja, kes töötleb isikuandmeid riigi- või kohaliku omavalitsuse asutuse poolt etteantud eesmärkidel. . Kusjuures alternatiivse kanali teenust pakkuv ettevõte (nt Facebook) on volitatud töötleja, kuna osaliselt töödeldakse andmeid teenusepakkuja juures. Antud analüüsi käigus võib volitatud teise taseme töötlejaks olla ka näiteks Facebooki koostööpartner, kes pakub andmete analüüsi või töötlemise teenust vastavalt standardlepingu tingimustele.

Vastutava töötlejana on asutusel kaks peamist kohustust kaasvastutava ja volitatud töötleja kaasamisel (nt Facebook). Esimene neist on GDPR artikli 28 lõikest 1 tulenev usaldusväärse

18 https://www.riigiteataja.ee/akt/104012019011

teenusepakkuja valimise kohustus ehk kohustus veenduda, et volitatud töötleja annaks piisava tagatise asjakohaste tehniliste ja korralduslike meetmete rakendamise kohta, tagades seeläbi vastavuse GDPR nõuetele ja andmesubjekti õiguste kaitse. Teine oluline vastutava töötleja kohustus on GDPR artikli 28 lõikest 3 tulenev andmetöötluslepingu sõlmimise kohustus. Sisuliselt on tarvis veenduda teenusepakkuja poolt esitatavas standardlepingus kirjeldatud tingimuste vastavuses seatud andmehalduse eesmärkidele ning lepingus seatud tagatiste osas. See on oluline, kuna vastutava töötlejana ja andmete platvormile edastajana lasub asutusel vastutus isikuandmetega tehtavate kahjude korvamisel.

Teenusepakkujaga sõlmitav leping on üldjuhul teenusepakkuja määratud tüüptingimustega ning üldjuhul pole tingimused läbiräägitavad. Seetõttu lasub asutusel kohustus hinnata GDPR artikli 28 lõike 3 sätestavaid asjaolusid ja tingimusi. Sellisteks tingimusteks on eelkõige:

- vastutava töötleja dokumenteeritud juhiste järgimise nõue;
- konfidentsiaalsuskohustuse seadmise nõue;
- GDPR artikli 32 kohaste turvalisuse meetmete rakendamise nõue;
- GDPR artikli 28 lõigetes 2 ja 4 sätestatud, täiendavate volitatud töötlejate kaasamisel kohalduvad nõuded;
- andmesubjekti õiguste teostamist puudutavatele taotlustele vastamise osas vastutava töötleja abistamise nõue;
- GDPR artiklitest 32-36 tulenevate kohustuste täitmisel vastutava töötleja abistamise nõue;
- isikuandmete õigeaegse kustutamise nõue;
- vastutavale töötlejale teabe kättesaadavuse tagamise nõue.

Kuna GDPR seab asutuse antud lahenduses vastutavaks töötlejaks ja alternatiivse kanali teenusepakkuja lepingu alusel andmete volitatud töötlejaks, kuid asutustel puudub üldjuhul võimalus lepingu sisu mõjutada, siis tuleb täpsemalt käsitleda lepingust tulenevaid riske ning piiranguid teenuse kasutamisel.

Kolmandates riikides andmete töötlemine

Enamik alternatiivseid kanaleid pakkuvaid teenuseid on peakorteriga Ameerika Ühendriikide territooriumil ja olenemata osade andmekeskuste paiknemisele EU territooriumil näevad lepingutingimused ette, et näiteks Facebookil (sarnased tingimused nii nende Facebook Messenger, kui WhatsApp teenuste lepingutes) on õigus andmeid töödelda ka Ameerika Ühendriikide territooriumil ja täiendavalt nende volitatud teenusepakkujate juures. GDPR artikli 44 kohaselt on lubatud isikuandmete edastamine kolmandale riigile üksnes juhul, kui vastutav töötleja ja volitatud töötleja on täitnud kooskõlas GDPR teiste sätetega käesolevas peatükis sätestatud tingimused, sealhulgas juhul, kui kolmas riik saadab isikuandmed omakorda edasi muule kolmandale riigile. GDPR artikkel 45 sätestab isikuandmete edastamise tingimused kolmandatesse riikidesse kaitse piisavuse otsuse alusel. Isikuandmeid võib kolmandale riigile sellel alusel edastada siis, kui Euroopa komisjon (edaspidi Komisjon) on teinud GDPR artikli 45 lõike 3 kohase otsuse, mille kohaselt asjaomane kolmas riik, kolmanda riigi territoorium või kolmanda riigi üks või mitu kindlaksmääratud sektorit tagavad isikuandmete kaitse piisava taseme. Kui Komisjon on

konkreetse kolmanda riigi osas langetanud vastava kaitse piisavuse otsuse, ei ole GDPR artikli 45 lõike 1 kohaselt isikuandmete edastamiseks vaja eriluba.

Tulenevalt sellest, et Ameerika Ühendriikide osas ei ole käesoleva analüüsi koostamise ajal Komisjon kaitse piisavuse otsust langetanud ja pilvandmetöötlusel põhinevate töökohateenuste kasutuselevõtu kontekstis riigi ja kohaliku omavalitsuse üksuse asutuste poolt on oluline isikuandmete edastamise võimalikkus eeskätt just Ameerika Ühendriikidele, ei ole kaitse piisavuse otsuse alusel isikuandmete edastamise võimaluse edasine analüüsimine käesolevas analüüsis otstarbekas. Konkreetsemalt Ameerika Ühendriike puudutava isikuandmete edastamise osas on AKI eraldi rõhutanud, et ka USA-d loetakse mittepiisava andmekaitsetasemega riigiks. Kuni 16. juulini 2020 oli isikuandmete vastutavatel ja volitatud töötlejatel võimalik edastada isikuandmeid Ameerika Ühendriikidesse Euroopa Komisjoni rakendusotsuse 2016/1250 (edaspidi ka Privacy Shield) alusel, mis reguleeris isikuandmete kaitse piisavust andmete edastamisel Euroopa Liidu ja Ameerika Ühendriikide vahel.[19] Privacy Shield raamistiku kehtivuse lõpetas Euroopa Kohtu 16.07.2020 otsus kohtuasjas C-311/18 (edaspidi Schrems II).[20]

Teised alternatiivsed kanalid

Kuna eelnevalt välja toodud andmekaitse riskid sisuliselt välistavad e-teenustes pakutava info (enamasti tavalised ja tundlikud isikuandmed) edastamist PoC raames realiseeritava lahenduse osas, siis vaatlesime ka teisi alternatiive lähemalt. Antud juhul lugesime peamisteks andmekanaliteks e-maili, kodulehel olevad vestlusrobotid ja teised teenusepakkujad (nt WhatsApp, iMessages).

E-maili osas on lahendus lihtsam, kuna teenusepakkujaga (nt Gmail) lepingu teeb isikuandmete omanik ning asutus ei hoia andmeid kellegi teise juures vaid asutuse hallatavas keskkonnas (nt DHS). Näiteks Facebooki puhul on samuti süsteemis sisuliselt 2 postkasti, millest üks on seotud asutuse Lehega ja teine kliendi kontoga, ehk klient teeb lepingu enda chat “postkasti” andmete säilitamise osas ja asutus enda poolsete andmete hoidmiseks. Kuna asutusel lasub endiselt kohustus andmete turvalisuse ja töötluse osas ning ta on sellises olukorras kasutusele võtnud Facebook’i kui volitatud töötleja, siis ei ole andmete haldus piiratud vaid asutuse poolse andmete töötlemisega. Parimaks alternatiivseks kanaliks andmekaitse vaates on asutuse domeenis asuv juturobot/vestlus kanal. Seda nii kasutajatoe funktsionaalse, kui isikuandmete edastamisel (eeldab kliendi tugevat autentimist), kuna selliselt on võimalik tagada andmete sihipärane töötlus ning turvatingimused.

Kokkuvõtvalt saab öelda, et tänases õigusruumis ja teenusepakkujatega tehtavate standardlepingute põhjal pole väliste teenusepakkujatega võimalik isikuandmeid valitud platvormidel töödelda ilma selleks põhjalikku andmekaitse mõjuhinnangut koostamata.

19 Komisjoni rakendusotsus (EL) 2016/1250, 12. juuli 2016, isikuandmete kaitse piisavuse kohta ELi-USA andmekaitseraamistikus Privacy Shield vastavalt Euroopa Parlamendi ja nõukogu direktiivile 95/46/EÜ (teatavaks tehtud numbri C(2016) 4176 all) (EMPs kohaldatav tekst). C/2016/4176. Kättesaadav: https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX:32016D1250 (08.10.2020)

20 Euroopa Kohtu otsus 16. juuli 2020. C-311/18, Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems. Kättesaadav: http://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=ET&mode=lst&dir=&occ=first&part=1&cid=9711043&fbclid=IwAR3vZLGf4enWc03KbDK3DOfEDhgPqK6MWFMWGv1BH2Qz_eCF3HWwnCg8kJU (08.10.2020)

Andmekaitsealane mõjuhinnang

Sissejuhatus

Mõjuhinnangu loomisel võtame aluseks AKI Andmekaitsealase mõjuhinnangu põhja[21] ja kaasatud asutuste sisendi tänastes teenustes edastatava teabe osas. Kuna mõjuhinnang koostatakse üldjuhul spetsiifiliselt asutuse kohta, siis on analüüsis mõjuhinnangu põhja mõneti muudetud, et võimaldada hinnata andmete töötlemisega seonduvaid riske alternatiivsetes kanalites.

Mõjuhinnangu ulatus

Mõjuhinnang keskendub potentsiaalselt kasutusele võetavate alternatiivsete kanalite funktsionaalsusele ning seal liikuvatele andmetele. Mõjuhinnangul vaadeldakse eraldi kolme kasutusjuhtu koos nende juurde kuuluva andmekoosseisuga.

Metoodika

Metoodikana kasutame andmekoosseisu, klientide hulga, riskide ja mõju hindamise maatrikseid leidmaks suurimaid ohu allikaid süsteemi realiseerimisel ning kõige sobivamaid kasutusprotsesse.

Infosüsteemi kirjeldus

Süsteemi kasutusotstarve

Alternatiivsete kanalite all hindame siin peamiselt kolmandate osapoolte poolt pakutavaid pilvepõhiseid (SaaS) vestluslahendusi, mida saab kasutada klientide teavitamisel ja suhtluses (nt Facebook Messenger). Süsteemi andmehaldus ja logimise funktsionaalsused realiseeritakse RIA riikliku postkasti juures (vt PoC arhitektuur ja tehnilised valikud).

Tugisüsteemid (support tiers)

Tugisüsteemina rakendatakse lahendust kasutama asutuse tehnoloogilise toe osakonda, kuna süsteem paigaldatakse asutuse poolt hallatavasse keskkonda. Kui kasutatakse tsentraalset RIA riikliku postkasti juurde loodavat alternatiivset kanalit siis tuge pakub RIA.

Informatsiooni elutsükkel (lifecycle)

Loodavas lahenduses on seatud informatsiooni säilitamisele nõudeks 5 aastat[22], mille vältel tuleb nii kasutajale kui süsteemi pidajale tagada juurdepääs toimunud vestlustele. Uues Eesti.ee määruse muutmise kavandis on sees, et § 21 lg 6 senisel kujul tunnistatakse kehtetuks ja uue sõnastuse kohaselt säilitatakse samu andmeid 3 aastat arvates nende kogumisest ja seejärel andmed anonüümitakse. Täiendavalt tuleks vaadata üle isikuandemete käsitlemise nõuded[23] ja vajadusel neid Eesti.ee määruses täiendada.

Vaadeldes süsteemi eri komponente, siis andmed kustutatakse välise teenusepakkuja süsteemist regulaarselt. Nii tehniline kui vestluse logimine hallatakse loodavast ALT süsteemis (5 aastat), mis on valdava asutuse keskkondades.

21 https://www.aki.ee/sites/default/files/inspektsioon/naidis/andmekaitsealane_mojuhinnang_naidis_1.pdf

22 https://www.riigiteataja.ee/akt/112112015004?leiaKehtiv § 21 lg-s 5

23 https://www.riigiteataja.ee/akt/104012019011

Kasutajad ja nende rollid

Süsteemis on kirjeldatud kasutajatena:

- klient, kelleks võib olla Eesti riigiasutuste poolt pakutavaid teenuseid tarbiv klient (sh e-residendi) või ettevõtte esindaja;
- spetsialist, kelleks võib olla kasutajatoe või teenuse spetsialist, kes vastab tehtud päringutele või saadab teateid kliendile alternatiivsetes kanalites.

Isikuandmete töötlemise toimingud

Isikuandmete kogumine

Kogu süsteemi põhimõte on olla andmete vahendaja ja olenevalt süsteemi lõplikust lahendusest võib isikuandmeid koguneda kahel viisil: turvalogid ja vestluste ajalugu. Isikuandmete teke süsteemis piirdub maksimaalselt tavaliste isikuandmetega olenevalt, kuidas asutused süsteemi enda jaoks kasutusele võtavad.

Isikuandmete säilitamine

Loodavas lahenduses on seatud informatsiooni säilitamisele nõudeks 2 aastat, mille vältel tuleb nii kasutajale kui süsteemi pidajale tagada juurdepääs toimunud vestlustele. Süsteemi ISKE turvaklassiks on K2S1T1 (vt Turvaanalüüs), mis võimaldab kasutada avalikke pilveteenuseid.

Vaadeldes süsteemi eri komponente siis andmeid ei säilitata välise teenusepakkuja süsteemis vaid kustutatakse need regulaarselt. See lahendab riski asutuse poolt hallatavate andmete kontrolli ja halduse osas, kuid andmed säilivad kliendi poolses Facebook sõnumite haldus süsteemis (sarnaselt e-kirjadele on Facebooki Messenger lahenduses 2 andmehoidlat, millest ühes olevat sisu haldab klient – Facebook account ja teist asutus - Facebook Leht). Nii tehniline kui vestluse logimine hallatakse loodavast ALT süsteemis, mis on valdava asutuse keskkondades.

Isikuandmete kasutamine

Vestluste ajalugu on kättesaadav kasutajaga vestelnud asutuse spetsialistile ja kasutajale endale. Isikuandmeid säilitatakse antud süsteemis 5 aastat peale seda, peale mida need kustutatakse.

Isikuandmete edastamine

Antud süsteemist on kasutajal võimalik teha päringud enda isikuandmete ja vestluste osas. Selleks saab klient siseneda riiklikku postkasti, kuhu lisatakse sessiooni kokkuvõte temaga tehtud vestlustest. Juhul kui vestlus oli autentimata ja puudusid isikustatud andmed, siis vestluseid saab vaadata vaid asutuse töötaja (või vastavate volitustega töötajad), kes vestluses osales.

Isikuandmete kustutamine

Andmed kustutatakse asutuse hallatavalt Facebook Lehe süsteemist regulaarselt ja peale viie aastast andmete säilitamist ALT süsteemis. Samas jääb vestluse ajalugu, mis on

salvestatud kliendi Facebook Messenger postkasti tema enda hallata. Isik ei saa nõuda vestluste ennetähtaegset kustutamist, lähtuvalt riikliku postkasti kasutamise korrast[24]

Isikuandmete töötlemise eesmärgid

Töötlemise eesmärgid

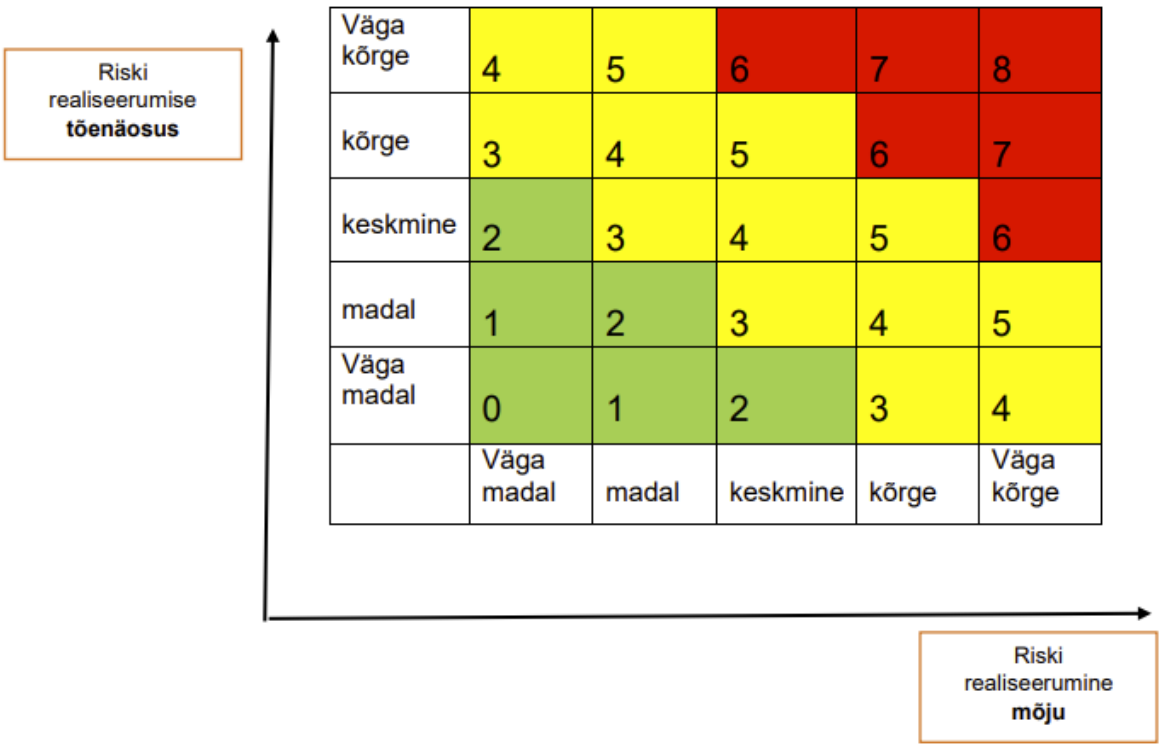
Kuna antud analüüsisvaatleme süsteemi eraldiseisvalt, siis pole võimalik välja tuua andmete töötlemise eesmärki. See tuleb täiendavalt koostada asutusespetsiifiliselt süsteemi kasutusele võttes.

Riskid ja nende maandamine

Riski hindamisel hinnatakse kahte tegurit skaalal 0-4:

- Riski realiseerumise tõenäosus
- Riski realiseerumise mõju

Üldine riski tase leitakse kahe skaala ristumispunktis. Kui üldine riskitase on konkreetse riski/asjaolu kohta määratud, siis tuleb otsustada, mida riskiga ette võtta. Riski võib vältida, delegeerida/üle anda (transferred), vähendada või aktsepteerida.



Riski tase	
Tulemus	**Kirjeldus**
6-8	Kõrge
3-5	Keskmine
0-2	Madal

Joonis 9 Riskide taseme määramine

24 https://www.riigiteataja.ee/akt/112112015004

Tabel 4 Andmekaitse riskid

Risk nr	Riski nimetus	Riski tõenäosus	Riski mõju	Riski tase	Lisamärkused	Ettepanek maandamiseks
1	Andmete töötlemine vaid volitatud töötleja poolt	3	3	kõrge	Riski tõenäosus on märgitud kõrgeks, kuna Facebook on viimase viie aasta jooksul mitmel korral nõude vastu eksinud	Andmed kustutatakse alternatiivsest kanalist regulaarselt. Vastavalt lepingutingimustele kustutatakse andmed kõigist alternatiivse kanali teenust pakkuva ettevõtte süsteemidest.
2	Andmete liikumine volitatud töötleja süsteemidest EU territooriumilt kolmandatesse riikidesse	2	4	kõrge	Hetkel puudub vastutavale töötlejale piisav läbipaistvus volitatud töötleja poolt andmetega teostatavate toimingute üle. Seda peamiselt kolmandatesse riikidesse andmete liigutamise eest.	Andmed kustutatakse alternatiivsest kanalist regulaarselt. Vastavalt lepingutingimustele kustutatakse andmed kõigist alternatiivse kanali teenust pakkuva ettevõtte süsteemidest.
3	Andmete leke volitatud töötlejate süsteemidest	1	4	keskmine	Kõigi andmekahjude eest vastutab vastutav töötleja ehk asutus, kes kasutab alternatiivset kanalit.	Andmed kustutatakse alternatiivsest kanalist regulaarselt.
4	Tundlike isikuandmete esitamine kliendi poolt	2	3	keskmine		Andmed kustutatakse alternatiivsest kanalist regulaarselt. Samuti märgitakse vestluse juurde täiendav juurdepääsupiirang ALT süsteemis
5	Andmete töötlus MSP juures	0	3	keskmine		Andmed kustutatakse MSP kanalist kohe peale vestlus sessiooni lõppemist. Lisaks kasutatakse EU territooriumil olevaid andmekeskusi.
6	Andmete leke ALT süsteemist	0	4	keskmine		Süsteem luuakse vastavalt ISKE K2S1T1 nõuetele ning rakendatakse vastavad turvalahendused.
7	Isikuandmete säilitamise nõuetele mittevastavus (ennetähtaegne kustutamine ja peale tähtaega säilitamine)	2	2	keskmine		Süsteemis rakendatakse dubleerivat andmete säilitamist, automaatseid säilitamise/kustutamise mooduleid ja auditeeritakse andmete säilitamise nõudeid regulaarselt.

Risk nr	Riski nimetus	Riski tõenäosus	Riski mõju	Riski tase	Lisamärkused	Ettepanek maandamiseks
8	Juurdepääsu piiranguga andmetele juurdepääs asutusesiseselt ALT süsteemis	0	1	madal		Süsteemi rakendatavad juurdepääsupiirangud tagavad juurdepääsu vastavalt rollile.

Tabel 5 Andmekaitse riskid

Kasutusel olevad riskide vältimise meetmed

Kuna süsteemi loomisel saame vaadelda vaid arhitektuurseid ja tehnoloogilisi riskide maandamise meetmeid, siis ei kaardistata analüüsis asutuse spetsiifilisi nõudeid.

Infotehnoloogilised turvameetmed

Kogu süsteemi detailsem turvaanalüüs on kajastatud peatükis Turvaanalüüs. Andmekaitse eesmärkidest lähtuvalt on süsteemi ISKE turvaklass K2S1T1, mis tagab süsteemi piisavalt turvalise toimimise. Lisaks on rakendatud minimaalne andmete säilitamise printsiip ehk andmeid hoiustatakse asutuse keskkondadest väljaspool vaid kliendiga suhtluse perioodil, peale mida need alternatiivsetest kanalitest kustutatakse.

Turvaanalüüs

Analüüsis kujunes alternatiivsete kanalite täislahenduse ISKE klassiks K2T1S1. Allpool selgitused iga alamklassi kohta, võttes aluseks RIA ISKE rakendusjuhendi[25] ja Riigiportaali riskianalüüsi[26].

K2

Lahendusel on kolm otsest välist sõltuvust, mis mõjutab käideldavusklassi:

- RIA Riigiportaal, mille klass on K2S1T1 (riskianalüüsi põhjal)
- Sõnumite vahendaja MessageBird, mille SLA järgi on teenus püsti 99.95% ajast (https://messagebird.com/legal/sla/)
- sk.ee (SmartID / mobiilID autentimispäringud) (SLA järgi teenus püsti 99.9% ajast ja maksimaalne katkestuse pikkus 3 tundi)

Alternatiivsete kanalite lahendus on mõeldud töötama kõrgkäideldava arhitektuuriga infrastruktuuris ja Javas arendatud mikroteenuseid on võimalik skaleerida, kuna tegemist on valdavalt stateless minirakendustega (täpsemalt - nad ei hoia state'i oma mälus/kontekstis, vaid kasutavad selleks välist andmebaasi) ja nende ette saab paigaldada koormusjaotureid. Lahendust on võimalik paigaldada ka Kubernetese klastrisse, kus mikroteenustest saab samuti olla mitu iseseisvalt töötavat koopiat; nagu ka Tomcati rakendusserveritele (v.a. lahenduses kasutatavad andmebaasid). Lahenduse back-end-is olevale MongoDB baasile

25 https://www.ria.ee/sites/default/files/content-editors/ISKE/iske_rakendusjuhend.pdf

26 https://confluence.ria.ee/pages/viewpage.action?pageId=124290155

(sessioonihoidla) on võimalik tekitada replica set, mis võimaldab päringuid teha ka juhul, kui üks andmebaasi instants peaks tõrkuma.

T1

Kõik MessageBirdi ja sihtpunkti vahel liikuvad sõnumid salvestatakse back-end andmebaasi ja logitakse turvalogisse - välja arvatud autentimispäringud ja nendega seotud sõnumite (autentimismeetodi ja isikukoodi küsimine, kontrollkood) liiklus, mis salvestatakse ainult turvalogisse. MessageBirdis hoitakse kõiki sõnumeid - otseselt sõnumeid ei kustutata, vaid on võimalik määrata vestlusele staatus “archived” ja sõnumile staatus “deleted”. WhatsApp kui platvorm hoiab sõnumeid selle hetkeni, kuni see adressaadini toimetatakse, pärast seda kustutatakse. Facebookis on olemas funktsionaalsus sõnumi kustutamiseks, kuid see on kasutatav ainult otseliidestuse, mitte MessageBirdi kaudu.

MessageBirdi salvestuspoliitika on selline, et andmeid salvestatakse kasutades GPG AES-256 krüpteeringut ja krüpteeritud varukoopiad asuvad mitmes regioonis korraga. Varundamine toimub kord päevas.

S1

AKI isikuandmete liigituse[27] alusel eriliiki (delikaatseid) isikuandmeid lahenduse kaudu ei edastata. Alternatiivsetes kanalites liikuv info on mõeldud asutusesiseseks kasutamiseks ja neile, s.t. vestlustele, pääseb ligi klient, kellega käib autenditud või autentimata vestlus (platvormi, s.t. Facebooki/Whatsappi kaudu) ning asutuse töötaja, kelle roll on sellele vestlusele reageerida. MessageBird kasutab ISO/IEC 27001:2013 standardit, andmed liiguvad lahenduse, MessageBirdi ja kanali vahel turvatud (HTTPS) kanaleid pidi. MessageBirdis pääsevad sõnumitele ligi administraatorid, kellele on tehtud taustakontroll ning ligipääsu jagatakse vähima ligipääsu põhimõttel (least-privilege model) (kas GDPR alusel iga individuaalse isiku kohta, või MessageBirdi konto omaniku loal) ja four-eyes (s.t. üks administraator iseseisvalt andmetele juurdepääsu ei saa) (allikas: https://www.messagebird.com/security/). Andmeid hoitakse Euroopa Liidu piires Madalmaades ja Belgias asuvates Google Cloud serverites.

MessageBirdi sõnumite/vestluste API on kasutatav API võtmega HTTP päises, mida konto omanik saab vajadusel korduvalt genereerida. Kui klient algatab vestluse mitme Facebook Lehe kaudu, genereerib Facebook talle iga Lehe kohta individuaalse tunnuse - sama kliendi mitut vestlust ei saa Facebook ega MessageBird automaatselt siduda. Tugeva autentimise korral saab sidumine toimuda ainult lahenduse poolel.

Kulumudel

Alternatiivsete kanalite süsteemi loomine hõlmab mitmeid kulusid, millest osad tuleb teha alginvesteeringuna süsteemi rajades, osad aga saavad olema vajalikud süsteemi käigus ja kaasaegsena hoidmiseks. Süsteemi kulude katmiseks on võimalik luua tasusüsteem, mis näiteks turuosaliste poolt makstavate teadete edastamise kaudu katab süsteemi kulud kas täielikult või osaliselt.

Allpool on täpsemalt käsitletud süsteemi kulude tekkemehhanisme ning esitatud esialgsed arvutused. Süsteemi kulusid on hetkel võimalik hinnata ligikaudselt, sest sarnaste süsteemide täpsete arenduskulude prognoosimine ilma terviklahenduseta (st teadmata, mis

27 https://www.aki.ee/et/eraelu-kaitse/isikuandmed-ja-tootlemine/isikuandmete-liigitus

saab olema täpne *back-office* tööriist ja mitu alternatiivset kanalit integreeritakse) on ebatäpne.

Järgnevalt vaatleme kahte alternatiivi süsteemide loomise lõikes, kus peamiseks erisuseks kulukomponentide seas on sõnumivahetusplatvormi realiseerimine. Esimese alternatiivina vaatleme analüüsi esimese pooles välja toodud MSP integreerimist ja teisena MSP funktsiooni võtmist asutuse poolt.

Alternatiiv 1: MSP teenuse vahendusel pakkuda ALT lahendust

Arendusprotsessis näeme analüüsi käigus loodud prototüübi edasiarendusi ja integratsiooni paralleelselt loodavate süsteemidega (nt. juturobot). Nende maht on detailsemalt välja toodud projektiplaani osas. Arenduskulude maht muudatuste tegemiseks on hinnatud projekti kaasatud ekspertide poolt ja selleks on eeldatavasti 850 tundi. Sellest 350 tundi kulub liideste loomisele uute alternatiivsete kanalitega, milleks on WhatsApp API ja kodulehele paigaldatav juturobot. Teise komponendina on infrastruktuuri arendused, mille hulka kuulub Kubernetese klastri seadistamine, Elastic baasi vahetus MongoDB vastu ja andmebaasi klastri seadistamisele, mille kuluhinnanguks on 232 tundi. Kolmanda komponendina on CRM ja riikliku postkasti arendused, mis haldavad kasutajaga peetud vestluste ajalugu ja on hinnatud mahuks 264 tundi. Süsteemi maksumus sõltub muuhulgas ka sellest, kas süsteem kasutab juturobotit ja selle juurde kuuluvat back-office tööriista. Arenduse maksumuse arvutamisel oleme võtnud arendaja tunnihinna väärtuseks 65 eurot/tund (KM-ta).

MSP platvormi kasutamise kulude aluseks oleme võtnud analüüsis kaardistatud asutuste sõnumivahetuse mahuna ligikaudu 3 000 000 sõnumit aastas, millest optimistliku hinnanguna 30% võiks liikuda alternatiivsetes kanalites (jaotub omakorda Whatsapp 300 000, Facebook 300 00 ja juturobot 300 000). Sõnumivahetuse ühiku hinnaks on 0.0045€[28] ehk 2700€ aastas (siia alla ei kuulu juturoboti kaudu toimunud suhtlus, kuna see toimub otse vastu ALT süsteemi). Süsteemi puhul tuleb arvestada ka WhatsApp sõnumite vahendamise teenustasusid, lähtuvalt MessageBird hinnakirjast 0.034€ Whatsapp Template teade, ehk 10200€ aastas.

Täiendavaks kulu komponendiks on süsteemi haldaja poolne arenduse projektijuhtimine arenduse kestel. Projektijuhi roll on arendustööde ajal tööde kirjeldamine ja korraldamine ning kontrollimine. Peale süsteemi valmimist muutub oluliseks liidestujatega koostöö, mis hõlmab süsteemi kasutamise lepingute, integratsioonide, Facebook/Whatsapp kontode sidumist ja x-tee teenuse liitmist süsteemiga. Projektijuhi töö mahuks on hinnatud ½ FTE arendus projekti perioodi vältel ja 6 kuud peale lahenduse toodangu keskkonda viimist.

Lisaks on oluliseks kulukohaks süsteemi halduskulu. See hõlmab süsteemi tehnilist haldamist, IT-infrastruktuuri haldust, vigade ja probleemide lahendamist jne. Selliste kulude puhul kasutatakse sageli kindlat proportsiooni süsteemi loomise kuludest. Ekspertide hinnangul moodustavad tüüpiliselt sarnaste infosüsteemide süsteemi jooksvad halduskulud 10% süsteemi maksumusest.

Lähtuvalt eelnevalt kirjeldatud kulukomponentidest ja halduskuludest (vt ALT süsteemi majutus ja administreerimise kulud 5 aasta jooksul) kujuneb süsteemi loomisele ja haldusele

28 https://messagebird.com/en/pricing/api

viie aasta jooksul ligikaudu 260 792€ ja arvestada tuleb poole aastase arenduste hankimise ja poole aastase juurutamise protsessiga.

Alternatiiv 2: arendada ise MSP funktsionaalsus

Teise alternatiivi loomisel lisanduvad kulud võrreldes eelnevaga tulenevad mahukamast arendustööde teostamisest, kuid hoiab kokku platvormi teenustasude arvelt.

Lahenduse täiendava funktsionaalsuse arendusmahu hinnang on 1840 tundi. Kõik tegevused, mis muidu oleks MessageBird või mõne muu MSP kanda, tuleb endal teostada:

- API lepingute sõlmimine teenusepakkujatega. Sõltuvalt platvormist (WhatsApp API) võib see tegevus võtta tõenäoliselt kuni kuu aega, seoses erinevate kooskõlastamistega teenusepakkuja poolel. Mõnel lihtsamal juhul - Facebook - ei ole vaja teenusepakkuja poolel inimsekkumist ja APIga saab liidestuda praktiliselt koheselt. Liidestuja poolel tekkiv ajakulu ei tohiks ületada summaarselt 40 tundi.
- API integratsioonide arendamine. Lisaks alternatiivis 1 välja toodud WhatsApp API-le ja kodulehe juturobotile tuleb liidestuda ka Facebooki API-ga. Sealjuures tuleb tekitada võimalus liidestuda mitme Page'iga ja mitme erineva kanaliga, luues unifitseeritud viisi kõikide kanalitega suhtlemiseks - vältimaks koodi dubleerimist rakendustes, mis liidestuvad omakorda MSP funktsionaalsusega. Antud punkt on üks mahukamatest, mis käesoleva alternatiivi raames luua tuleb ja selle mahuks on orienteeruvalt 1300 tundi.

Analoogselt eelneva alternatiiviga tuleb samuti ka Elastic baas vahetada MongoDB vastu ja seadistada andmebaasiklaster (236 tundi), ning CRM/riikliku postkasti arendused vestluste ajaloo haldamisteks (264 tundi). Samuti mõjutab süsteemi maksumust juturoboti ja *back-office* tööriista kasutuselevõtt. Lisaks on oluliseks kulukohaks süsteemi halduskulu. See hõlmab süsteemi tehnilist haldamist, IT-infrastruktuuri haldust, täiendavate arenduste tegemist, vigade ja probleemide lahendamist, liidestustööde maksumust jne. Alternatiiv 2 puhul tuleb arvestada suurema halduskuluga, kuna siin tuleb vaadelda ka API uuenduste teostamist süsteemi ja nende valideerimist teenusepakkujaga. Arvestades, et 2020 aastal on Facebook ja WhatsApp andnud välja kokku 10 API muudatust siis oleme hinnanud iga uuenduse arendusmahuks 32-40 töötundi, millel lisandub 20-32 tundi testimiseks ning paigalduseks ja 40-60 tundi volitatud töötlejaga lahenduse valideerimiseks. Kokku eelnevalt kirjeldatud süsteemi halduse tasuna 10% soetusmaksumusest ning lisaks 920 - 1320 tundi aastas APIde uuenduste halduseks. Kalkulatsioonis arvestame optimistlikuma hinnangune täiendavate arenduste tegemise osas 920 tunniga aastas.

Süsteemi puhul tuleb arvestada ka WhatsApp sõnumite vahendamise teenustasusid (arvestame 300 000 teatega nagu alternatiiv 1 puhul), lähtuvalt Whatsapp API hinnakirjast[29] 0.0541€ Whatsapp Template teade, ehk 16 230€ aastas. Sisuliselt tähendab see, et MSP poolt pakutav sõnumivahetus koos nende teenuse tasuga on kokkuvõttes odavam kui otseliidestus. Erinevus tuleneb sellest, et MessageBird'i kaudu ostavad Whatsapp teenust rohkem kui 15 000 ettevõtet, tänu millele saadakse olulisi mahu soodustusi.

Lähtuvalt eelnevalt kirjeldatud kulukomponentidest (vt ALT süsteemi majutus ja administreerimise kulud 5 aasta jooksul) kujuneb süsteemi loomisele ja haldusele viie aasta

29 https://developers.facebook.com/docs/whatsapp/pricing/

jooksul ligikaudu 603 402€ ja arvestada tuleb 9 kuulise arenduste hankimise ja poole aastase juurutamise protsessiga.

ALT süsteemi majutus ja administreerimise kulud 5 aasta jooksul

Hetkel on ebaselge kui paljud asutused oleksid üldse valmis oma süsteeme alternatiivsete kanalitega liidestama, sest asutustel on tihti mitmeid Facebook kontosid (näiteks PPA puhul on lehti nii piirkonna politseinikel ja erinevatel allüksustel) ning see võib osutuda tehniliselt liiga keerukaks või kulukaks. Seda seetõttu, et süsteem küll arvestab lihtsa täiendavate alternatiivsete kanalite liidestamise protsessiga, kuid seadistamiseks läheb ikkagi 2-8 tundi olenevalt olukorrast ning hetkel paralleelses analüüsis uuritav lõppkasutaja liides on samuti täpsustamisel. Administreerimine, mis on seotud asutuste liidestuste, arvelduste ja teiste korralduslike toimingutega. Sellise tegevuse mahuks on teisel aastal arvestatud ½ täistöökoht (FTE – full time equivalent), edasi aga 0,2 FTE-d. Arvutustes on võetud aluseks 2500 euro suurune kuupalk (bruto), millele lisanduvad tööjõumaksud ca 34% ja muud töökohaga seotud kulud 10% brutopalgast 2500 × 1,34 × 1,1 × 12 / 2 = 22 110).

Oluline on välja tuua ka asutuste endi kantavad kulutused, mis tuleb teha süsteemiga liidestumiseks. Seda kulu täpsemalt hinnata ei ole võimalik, kuna analüüs ei käsitle terviklahendust, kuid hinnanguliselt võib täiendava x-tee teenuse liidestumise kuluks olla 120-160 tundi, arvestades keskmiseks arendustöö tunni hinnaks 60€ siis võiks see jääda alla 10 000€ (hind ilma KM-ta ja järgnevad välja toodud hinnad on samuti arvestatud ilma KM-ta)

Halduskulusid saab liigitada järgnevalt:

- Riigipilve spetsialisti töö tehnilise toe pakkumisel (80€/tund; väljaspool tööpäeva €120/tund - allikas https://riigipilv.ee/hinnakiri)
- Asutuse süsteemiadministraatori töö (paigaldamine)
- Asutuse rakendusadministraatori töö (lahenduse haldamine)
- Majutuskulud - Riigipilves on vajalikud vähemalt 2 Kubernetes ON PaaS *premium node*'i, et tagada K2 käideldavus. Sellise lahenduse maksumus on 325€/node/kuu, mis teeb aastaseks kuluks 325*2*12 = 7800€. Lahendust on võimalik minimaalselt paigaldada ka kahele 2 vCPU / 4GB RAM / 30GB SSD konfiguratsiooniga masinale + koormusjaotur (*active/active* või *active/passive* + andmete replikatsioon) (aastane kulu 3*365 = 1095€), kuid sellisel juhul kasvab oluliselt asutusepoolsete spetsialistide töö hulk, et hallata rakendusservereid, seadistada võrk, varundus, turvateenused, operatsioonisüsteemid, andmebaasid, integratsioonid, jne.

Riigipilve ja asutuse spetsialistide töömahuks kokku kujuneks keskmiselt 0.1FTE. Võttes aluseks 2500 euro suurune kuupalk (bruto), millele lisanduvad tööjõumaksud ca 34% ja muud töökohaga seotud kulud 10% brutopalgast, on sellise töömahu hind 2500 × 1,34 × 1,1 × 12 / 11 = 4220€ aastas (arvestamata Riigipilve spetsialisti töömahtu, mis ajaliselt sisaldub samuti 0.1FTE sees).

Eeltoodud tingimuste kohaselt kujuneb järgmine finantsmudel:

Tabel 6 Kulukomponendid

Kulukomponent	**Kulud aastate lõikes (€)**					Kokku 5 aastat (€)
Kulud süsteemi pidajale	1. aasta	2. aasta	3. aasta	4. aasta	5. aasta	
Alternatiiv 1	**Süsteemi 5 aasta Halduskulu kokku**					**260792**
Alginvesteering süsteemi loomiseks (arenduskulu)	55250					55250
Süsteemi arenduse projektijuhtimine (1 FTE /1. aasta)	44200					44200
Süsteemi administratiivne korraldamine (1/2 FTE/ 2.- 5.aasta)		22110	8844	8844	8844	48642
MSP teenustasu (900k teadet aastas)		2700	2700	2700	2700	10800
WhatsApp Business Template sõnumite saatmine MSP vahendusel (300k teadet aastas)		10200	10200	10200	10200	40800
Halduskulu		5525	5525	5525	5525	22100
Infrastruktuuri kulud (Kubernetese 2 node'i Riigipilves)	7800	7800	7800	7800	7800	39000
Alternatiiv 2 kulu	**Süsteemi 5 aasta Halduskulu kokku**					**603402**
Alginvesteering süsteemi loomiseks (arenduskulu)	119600					119600
Süsteemi arenduse projektijuhtimine (1 FTE /1. aasta)	44200					44200
Süsteemi administratiivne korraldamine (1/2 FTE/ 2.- 5.aasta)		22110	8844	8844	8844	48642
WhatsApp Business Template sõnumite saatmine (300k teadet aastas)		16230	16230	16230	16230	64920
Halduskulu aastas		71760	71760	71760	71760	287040
Infrastruktuuri kulud (Kubernetese 2 *node*'i Riigipilves)	7800	7800	7800	7800	7800	39000
Süsteemi integreerimise kulu liidestuvale asutusele						8400

Tabel 7 Kulukomponendid

Projektiplaan ja arendajate profiilid

Täispinu (full stack) programmeerija. Töökogemus: vähemalt 2 (kahe) aastane programmeerimise töökogemus. Vähemalt järgmiste tehnoloogiate/platvormidega: Java, Angular, XML, JSON.

IT arhitekt/arendaja. Töökogemus: vähemalt 2 (kahe) aastane töökogemus infosüsteemide arhitektina. Nõutavad kogemused : Vähemalt 1 infosüsteemi loomise või modifitseerimise ja juurutamise projekt, mille raames on realiseeritud funktsionaalsus, mis vastab järgnevale: andmete sisestamine, muutmine, kinnitamine ja tühistamine/kustutamine; XML/JSON failide moodustamine andmetes toimuvate toimingute tagajärjel; genereeritavate ja vastu võetavate XML/JSON failide valideerimine. X-tee teenuste kasutamine ja loomine, mikroteenustel baseeruva arhitektuuri kasutamise ja arendamise kogemus, API-põhiste liideste kasutamine ja loomine.

IT projektijuht. Töökogemus: vähemalt 3 projekti, mille töömaht on vähemalt 600 (kuussada) inimtöötundi projekti kohta. Juhtimiseks loetakse, kui vastavas rollis on teostatud töid vähemalt 100 (ühesaja) inimtöötunni ulatuses.

Tegevus	**nädal 1**	**nädal 2**	**nädal 3**	**nädal 4**	**nädal 5**	**nädal 6**	**nädal 7**	**nädal 8**	**nädal 9**	**nädal 10**	**nädal 11**	**nädal 12**	**IT projektijuht**	**IT arhitekt/ arendaja**	**Full stack arendaja**
I osa - täiendavate alternatiivstere kanalite integratsioon															
Süsteemi integratsiooni täiendamine juturobotiga													8	80	
Analüüs ja integratsioon kodulehele paigaltatava vestluse liidesega													16	120	
Integratsioon Whatsapp Business APIga													6	80	40
2 osa - CRM/riikliku postkastiga integratsioon ja edasised arendused															
Autentimissessiooni info lisamine suhtlusprotokolli													8	40	
Integratsioon riikliku postkastiga ja liidese loomine asutuste CRMidesse vestluste kokkuvõtete esitamiseks													16	80	40
Süsteemis kasutatava Elastic andmebaasi asendamine MongoDB baasiga													8	40	40
Süsteemi paigalduse täiendamine skaleeruva lahendusena Kubernetes, rakendusserverite ja andmebaaside klastri loomine													24	40	80
Tunde kokku													86	480	200

PoC arhitektuur ja tehnilised valikud

ALT süsteem on oma olemuselt liidestuja alternatiivsete kanalite ja spetsialisti töölaua vahel. Liidestuja rolliks on hallata määratud alternatiivsete kanalite APIde sidumist, eemaldamist ja haldust (sh APIde uuendused). Teiseks funktsionaalsuseks on sissetulevatest erinevatest APIdest teadete viimine ühele formaadile, mis edastataks spetsialisti töölauale. Spetsialisti töölaua vahel võib olla veel üks või mitu juturobotit vestluse automatiseerimiseks. Töölauaks endaks aga vestluste haldustarkvara või CRM lahendus. Süsteem haldab ka vestluste ajalugu autenditud klientidega, kus riikliku postkastiga sidudes on kliendil võimalik vaadata enda vestlusi riiklikust postkastist. Lisaks täidab süsteem tulevikus teadete edastus tasude haldamise rolli, jagades teadete edastamise kulud vastavalt liidestatud asutuste lõikes.

Iteratsioon 1

Prototüübi loomisel on aluseks võetud analüüsis leitud eelistatud kanal milleks on Facebook Messenger ja mille MSP lahendus baseerub MessageBird platvormil. Kuna prototüübi loomise skoobis ei ole asutuse spetsialistile mõeldud tööriista, siis see on lahendatud olemasoleva DHS süsteemi põhiselt.

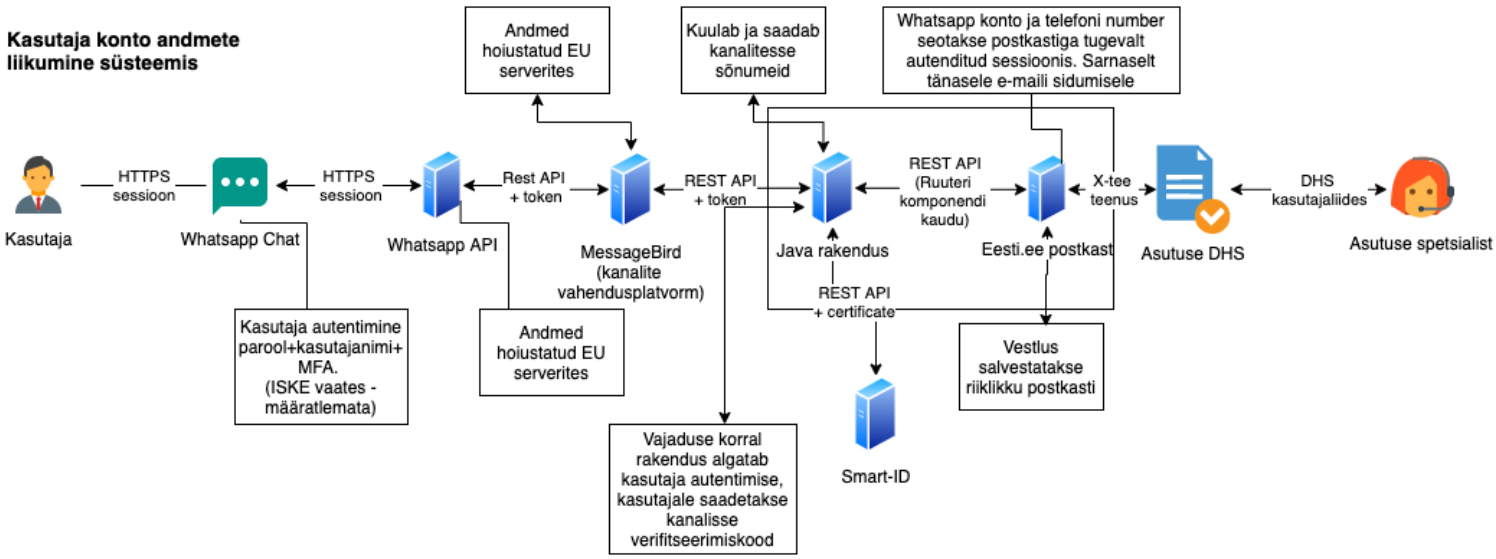
Prototüübi 1. Iteratsiooni funktsioonid on järgnevad:

Funktsioon	Kirjeldus
Spetsialist saab lisada uue alternatiivse kanali (Prototüübi raames Facbooki Lehe)	Spetsialist valib liidestatava kanali tüübi (Facebook Messanger) logib MSP vahendusel liidestatavasse kanalisse ja annab selle integreerimiseks vastava loa. Tulemusena saab lisatud kanalist Facebook Lehele edastatud kliendi teateid edastada ALT süsteemi (tulevikus back-officce töölauale) ja spetsialist saab kliendile sealt vastata.
Spetsialist saab eemaldada alternatiivse kanali (Prototüübi raames Facbooki Lehe)	Spetsialist valib MessageBird töölaualt Facebook Lehe, mida soovib eemaldada ja kinnitab selle eemaldamise.
Klient saab alustada vestlust asutuse Facebook lehel.	Klient kasutab selleks enda Facebook kontot ning kirjutab Eesti.ee Facebook lehel olevase vestluskanalisse. Asutuse spetsialist näeb teadet DHS süsteemis.
Kliendile saab asutuse spetsialist vastata tema päringule.	Asutuse spetsialist näeb päringud testsüsteemi DHS postkastis ning saab neile vastata e-kirja teel.
Klienti saab tugevalt autentida Smart-ID ja Mobiil-ID lahendustega.	Tugeva autentimise algatamiseks saadab spetsialist süsteemi kirja autentimise alustamiseks ja saab vastuseks kliendi isikukoodiga eduka autentimise kinnituse või ebaõnnestumise teate.
Autenditud vestluste ajalugu ja sisu saab vaadata riiklikust postkastist.	Ajalugu salvestatakse peale kliendi sessiooni lõpetamist ning edastatakse riiklikku postkasti.

PoC eesmärk on luua lahendus, mis suhtleb:

- MessageBird sõnumivahendusplatvormiga (sealtkaudu alternatiivkanalid FB Messenger ja WhatsApp)
- sk.ee SmartID Relaying Party API-ga SmartID autentimiseks
- RIG ruuteriga, mille kaudu toimub suhtlus eesti.ee postkasti ja kaugemate komponentidega ahelas.

Lahenduse eesmärk on võimaldada suhtlust lõppkasutaja alternatiivse kanali ja eesti.ee postkasti (ning selle kaudu asutuse spetsialisti) vahel. Alloleval diagrammil (Joonis 10) on ristkülikuga ümbritsetud komponendid RIA haldusalas, sealhulgas loodav lahendus.



Joonis 10 Lahenduse integratsiooni diagramm

PoC arhitektuur (Joonis 11) põhineb sisemiselt mikroteenuste põhisel arhitektuuril ja sisaldab järgnevaid mikroteenuseid :

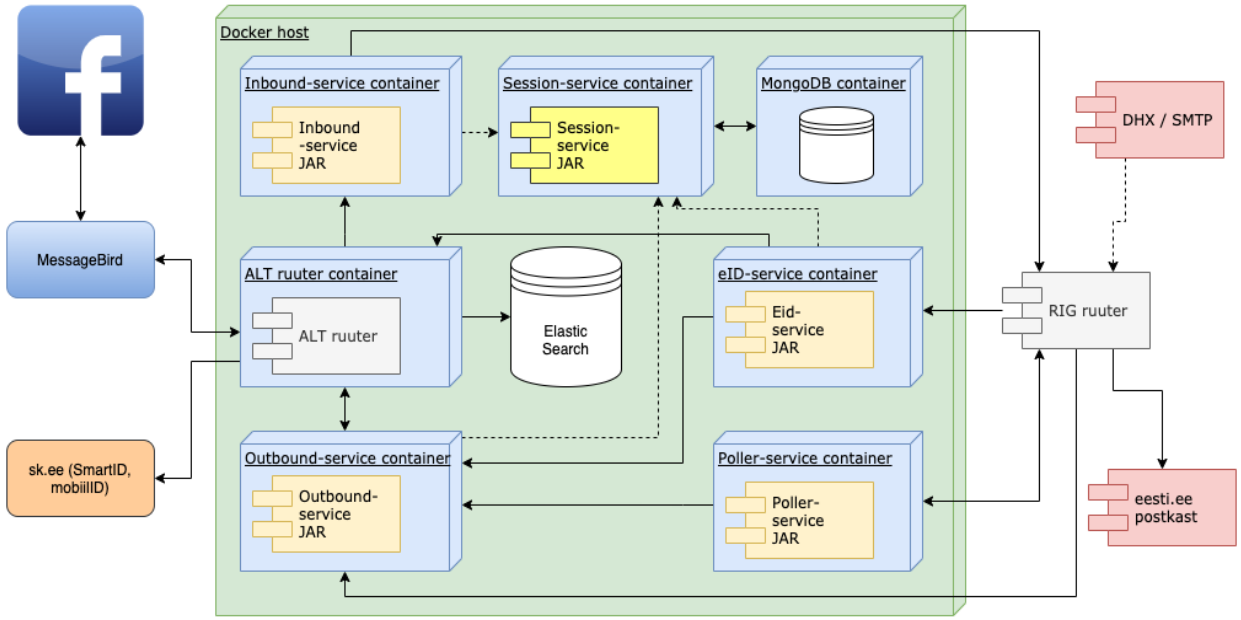
- **session-service**
  - lahenduse sisemine sessioonihalduse komponent
  - sessioon põhineb MessageBirdist tulnud contactID ja channelID väljadel ning lisaväljadena on sinna võimalik lisada ka muid parameetreid, näiteks isikukood kui autentimine on möödunud edukalt
  - talletab sessiooniinfo eraldi skaleeritavasse andmebaasi
- **inbound-service**
  - kuulab MessageBirdist tulnud sõnumeid
  - küsib sessioonihalduselt sessiooni (luues uue või saades juba olemasoleva)
  - tavaliikluse puhul salvestab sõnumi sõnumihoidlasse (PoC raames ElasticSearch)

    - käimasoleva autentimispäringuga seotud info seob sessiooniga ning edastab sessioonivõtme eid-service komponendile

- **outbound-service**
    - küsib sessioonihalduselt sessiooniga seotud kliendi ja kanali ID-d
    - kasutades neid ID-sid, saadab MessageBirdi kaudu kasutajale vestluskanalisse sõnumeid
    - salvestab sõnumi sõnumihoidlasse
    - kui sessiooniID asemel on määratud isikukood, küsib sessioonihalduselt aktiivset sessiooni antud isikukoodiga kasutajale; kui selline puudub, siis salvestab sõnumihoidlasse märkme, et sõnumit ei saanud edastada aktiivse sessiooni puudumise tõttu
- **eid-service**
    - teostab kliendi autentimise, pöördudes SmartID / mobiilID teenuse poole
    - saadab autentimisega seotud vestlussõnumid outbound-service poole
- **poller-service**
    - regulaarsusega käivitatav komponent
    - küsib määratud intervalliga sõnumihoidlast uusi väljaminevaid sõnumeid
    - edastab sõnumid outbound-service teenusele
    - küsib määratud intervalliga lõppenud sessioonide vestlusi ja saadab need kodaniku isiklikku eesti.ee postkasti
- **ALT Ruuter**
    - põhineb Riigiportaali Ruuteri komponendil, kuid sisaldab teistsugust konfiguratsiooni
    - on sõlmpunktiks (*edge location*) lahenduse ja väliste ühenduste (sk.ee, MessageBird) vahel

Rakenduste kogum paigaldatakse PoC raames ühte virtuaalmasinasse, mis luuakse RIA vSpheres, järgnevate parameetritega:

- 2 vCPU või enam
- 4 GB RAM või enam
- 20 GB HDD või enam
- RHEL 8+/Ubuntu 16+/CentOS 7+ või mõni muu OS, mis on võimeline käivitama Dockeri tööriistu
- IP: 10.x.15.y



Joonis 11 Lahenduse arhitektuur Iteratsioonis 1

Iteratsioon 2

Peamine erinevus esimese ja teise iteratsiooni vahel on põhjendatud skoobimuutusega. Kui esimese iteratsiooni üks eesmärkidest oli aidata teostada kliendi eID (SmartID, MobiilID) autentimist suhtluskanali kaudu, siis tulenevalt andmekaitsealasest mõjuhinnangust langevad ära kasutuslood, kus on vajadus tugevaks autentimiseks. Kuna eesti.ee postkasti kasutuseks on vajalik kliendi tugev autentimine, langeb ära ka otsesuhtlus eesti.ee postkastiga, mille algne mõte oli edastada kasutajale vestluslogi. Kuid pool-anonüümse vestluspõhise suhtluse puhul, kus klient end ei autendi, ei saa siduda kasutajat kodaniku postkastiga.

Funktsioon	Kirjeldus
Spetsialist saab lisada uue alternatiivse kanali (Prototüübi raames Facbooki Lehe)	Spetsialist valib liidestatava kanali tüübi (Facebook Messanger) logib MSP vahendusel liidestatavasse kanalisse ja annab selle integreerimiseks vastava loa. Tulemusena saab lisatud kanalist Facebook Lehele edastatud kliendi teateid edastada ALT süsteemi (tulevikus back-officce töölauale) ja spetsialist saab kliendile sealt vastata.
Spetsialist saab eemaldada alternatiivse kanali (Prototüübi raames Facbooki Lehe)	Spetsialist valib MessageBird töölaualt Facebook Lehe, mida soovib eemaldada ja kinnitab selle eemaldamise.
Klient saab alustada vestlust asutuse Facebook lehel.	Klient kasutab selleks enda Facebook kontot ning kirjutab Eesti.ee Facebook lehel olevase vestluskanalisse. Teateid näeb juturobot ja vastab neile automaatselt
Kliendile vastab juturobot.	Juturobot vastab eelseadistusele lähtuvalt.
Klienti saab tugevalt autentida Smart-ID ja	Tugeva autentimise algatamiseks saadab

Mobiil-ID lahendustega.	spetsialist süsteemi kirja autentimise alustamiseks ja saab vastuseks kliendi isikukoodiga eduka autentimise kinnituse või ebaõnnestumise teate.
Autenditud vestluste ajalugu ja sisu saab vaadata riiklikust postkastist.	Ajalugu salvestatakse peale kliendi sessiooni lõpetamist ning edastatakse riiklikku postkasti.

Niisugune olukord lihtsustab PoC lahenduse arhitektuuri ja PoC roll tervikpildis edaspidi on ainult:

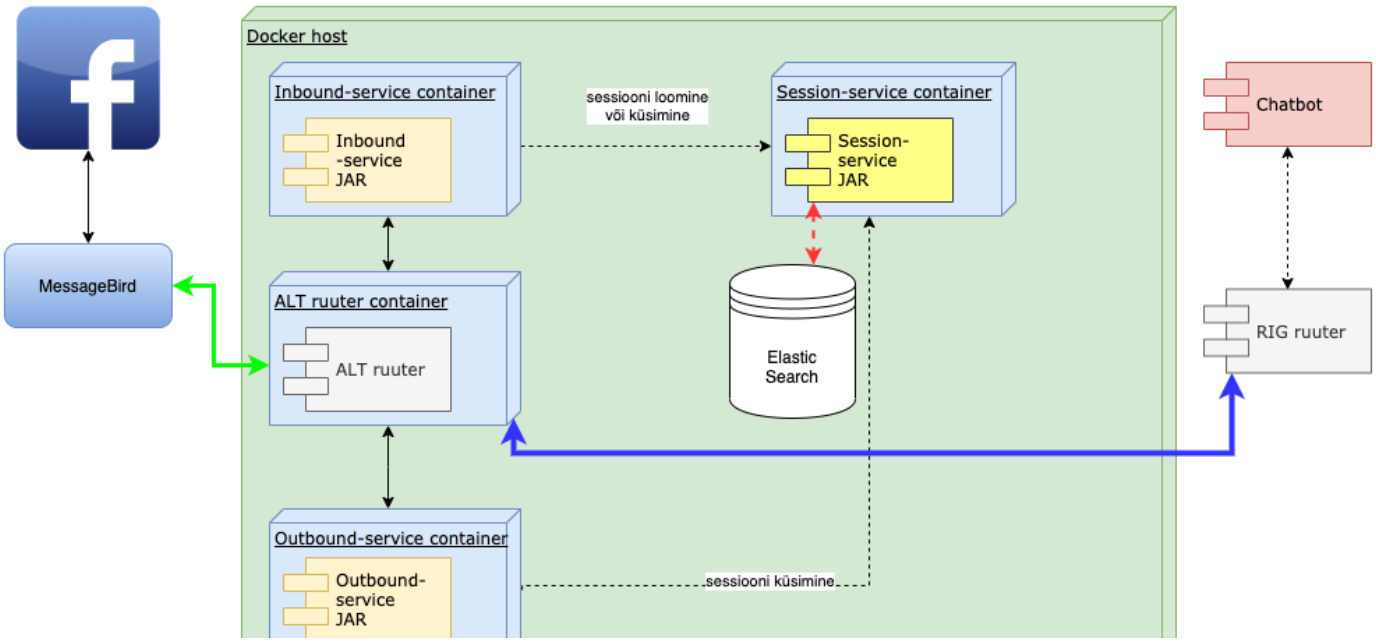
- Genereerida ühtne viis sessioonide halduseks erinevate alternatiivkanalite puhul
- Vahendada – eeskätt MessageBird platvormilt ja sealtkaudu Facebook/WhatsAppist tulevaid sõnumeid - Chatbotilahenduse Chat API suunal
- Võimaldada vastamist Chatbotilahendusest väljamineval suunal – MessageBird platvormi kaudu Facebooki/WhatsAppi kanalisse

Seega algsest pildist langevad ära komponendid:

- eid-service
- poller-service
- sk.ee kui väline autentimiskomponent

Lisaks on PoC teisest iteratsioonist välja jäetud MongoDB kasutamine sõnumihoidlana. Lahenduse parema koostoimimise nimel RIA infrastruktuuriga ja lihtsuse huvides jääb alles ainult Elasticsearch, mida kasutatakse sessioonihoidlana ja mille sisu saab jagada mitme õla vahel, et paraneks käideldavus.

Lahendus on lisaarendusega laiendatav ka muudele suhtluskanalitele lisaks MessageBirdile, kuid PoC kontekstis käib kanalite infovahetus läbi MessageBirdi.



Joonis 12 Lahenduse arhitektuur Iteratsioonis

Iteratsioon 3

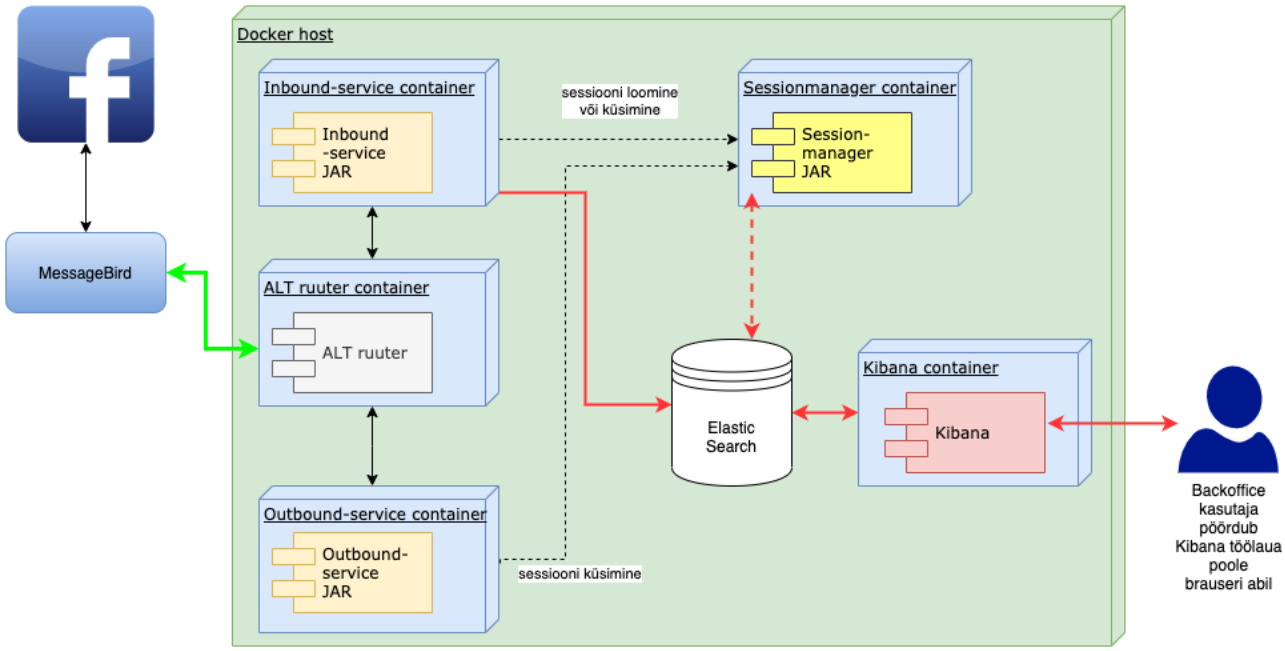
Kolmanda iteratsiooni ajendiks sai asjaolu, et Ruuter, mis on üks keskseid integratsioonikomponente, ei toeta WebSocket kommunikatsiooniprotokolli. WebSocketit kasutab antud juhul Bürokrati Chat API, et sõnumeid tagastada. Tekkis olukord, kus Chat APIsse sai sõnumeid postitada, aga sealt tagasi olemasoleva Ruuteriga (v0.2.0) ei olnud võimalik sõnumeid lugeda ja lisaarendus oleks olnud liigselt mahukas (sealjuures täpne maht teadmata, aga kindlasti kauem, kui tähtajani jäänud nädal aega) ning tagajärjed ebaselged.

Et simuleerida *backoffice* tööriista, tekkis (MKM ja Solita ühine) otsus integreerimise asemel tagastada lahendusest MessageBirdi kaudu fikseeritud sõnumeid, s.o. simuleerida juturoboti. Arhitektuuripildis juba olemasolev ElasticSearch teenus muutus sõnumihoidlaks ja sinna külge tekkis *backoffice* tööriistana Kibana, mida on piisavalt lihtne/kiire paigaldada ja ühildub ElasticSearch teenusega.

Langes ära ka otsene vajadus sessioonihalduse komponendi järele, kuna kolmanda iteratsiooniga muutunud arhitektuuripildis ei omanud see enam väärtust ja suhtlus toimub ainult ühe platvormiga - MessageBird. Tuleviku huvides jäi komponent siiski sisse, et demonstreerida kontseptsiooni, kus suhtlus käiks ühtemoodi olenemata alternatiivkanali allikast.

Sissetuleva sõnumi komponent käivitab selles iteratsioonis automaatse vastuse saatmise outbound-service kaudu.

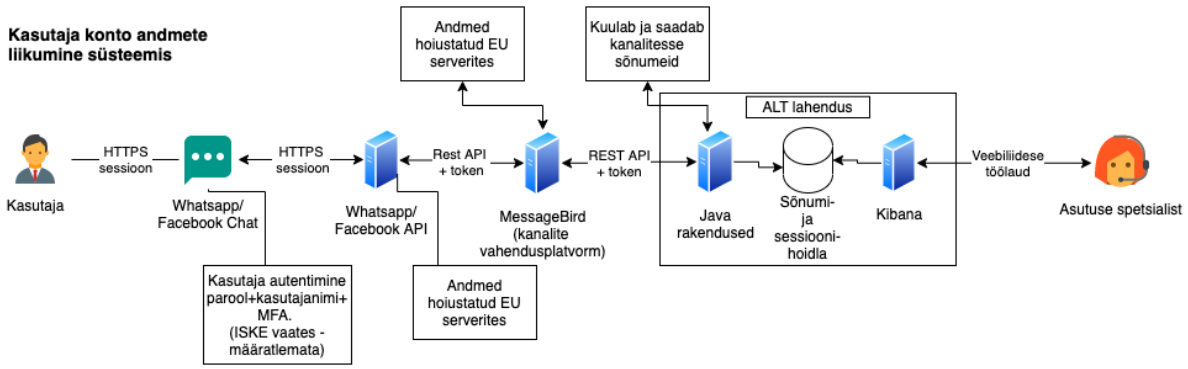
Funktsioon	Kirjeldus
Spetsialist saab lisada uue alternatiivse kanali (Prototüübi raames Facbooki Lehe)	Spetsialist valib liidestatava kanali tüübi (Facebook Messanger) logib MSP vahendusel liidestatavasse kanalisse ja annab selle integreerimiseks vastava loa. Tulemusena saab lisatud kanalist Facebook Lehele edastatud kliendi teateid edastada ALT süsteemi (tulevikus back-officce töölauale) ja spetsialist saab kliendile sealt vastata.
Spetsialist saab eemaldada alternatiivse kanali (Prototüübi raames Facbooki Lehe)	Spetsialist valib MessageBird töölaualt Facebook Lehe, mida soovib eemaldada ja kinnitab selle eemaldamise.
Klient saab alustada vestlust asutuse Facebook lehel.	Klient kasutab selleks enda Facebook kontot ning kirjutab Eesti.ee Facebook lehel olevase vestluskanalisse. Teateid näeb Kibana kasutajaliidesest
Kliendile saab vastata spetsialist.	Spetsialist loeb küsimusi Kibana kasutajaliidesest ja saab neile sealt vastata.
Klienti saab tugevalt autentida Smart-ID ja Mobiil-ID lahendustega.	Tugeva autentimise algatamiseks saadab spetsialist süsteemi kirja autentimise alustamiseks ja saab vastuseks kliendi isikukoodiga eduka autentimise kinnituse või ebaõnnestumise teate.
Autenditud vestluste ajalugu ja sisu saab vaadata riiklikust postkastist.	Ajalugu salvestatakse peale kliendi sessiooni lõpetamist ning edastatakse riiklikku postkasti.



Joonis 13 Arhitektuuri joonis iteratsioonis 3

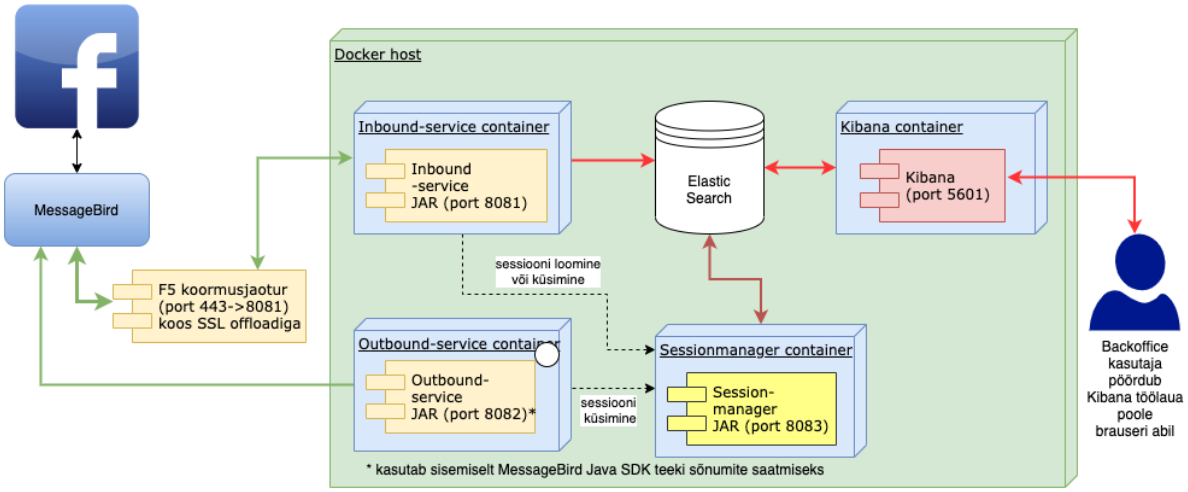
Iteratsioon 4

Iteratsioonis 4 muutus inbound-service selliselt, et nüüd saadab ta fikseeritud sisuga sõnumi outbound-service kaudu kanalisse tagasi. Nii sisse- kui väljaminevad sõnumid on nähtavad sotsiaalmeediaplatvormi vestlusaknas ja Kibanas (Joonis 14).



Joonis 14 Andmete liikumine on iteratsioonis 4

Seoses asjaoluga, et ALT Ruuteril ilmnes lokaalses arvutis ja arenduskeskkonnas mittesoovitav funktsionaalsus (sõnum kärbiti 1381 tähemärgiks), eemaldati ALT Ruuter arhitektuurist, selle asemel liiguvad sõnumid otse inbound-service pihta (Joonis 15).



Joonis 15 Lahenduse arhitektuur

Kasutajate tagasiside

Tagasisideks kaasati analüüsis osalenud asutused ja 10 tavakasutajat. Kokku testis ja andis tagasisidet 18 kasutajat. Kasutajate tagasiside saamiseks kasutati loodud prototüüpi, mille testimiseks kirjeldati testijatele kolm stsenaariumit eesti.ee kasutajatoes. Esimene stsenaarium on eesti.ee lehe kasutamise kohta, teine isikuandmete pärimiseks ja kolmas tehnilisetoega seonduv. Kasutajad küsisid neid ja teisi küsimusi ning kasutajatoe spetsialist vastas neile platvormi vahendusel. Peale seda hindasid kasutajad lähtuvalt küsimustikust lahenduse funktsionaalsust ja kasutatavust vastavalt testitud funktsionaalsusele.

Tagasiside kogumiseks kasutati UEQ - User Experience Questionnaire küsimustikku, mille kohaselt hindasid kasutajad järgnevaid aspekte:

Teema	**Hinnang (1-7)**
arusaamatu - arusaadav	6.1
vastumeelne - rõõmupakkuv	5.7
raske kasutama õppida - kerge kasutama õppida	6.3
väärtusetu - väärtuslik	5.9
igav- põnev	5.4
ennustatav - ootamatu	4.2
aeglane - kiire	4.8
konservatiivne - leidlik	4.9
takistav- abistav	5.6
eemaletõukav- ligitõmbav	4.8
vähemotiveeriv - motiveeriv	4.5
ei vasta ootustele - vastab ootustele	5.4
ebaefektiivne - efektiivne	5.7

Tulemuste põhjal saab järeldada, et kasutajatele meeldis süsteemi lihtsus kasutamiseks ja nähakse väärtust sellise lahenduse loomisel. Positiivselt suhtuti ka lahenduse põnevuse, abistavatus, meeldimise ja efektiivsuse osas. Oluline on siin tuua välja võrdlemisi neutraalne suhtumine lahenduse kiirusesse, kuna vastamise aeg oli alguses aeglasem tänu testimise käigus kirjutatud vastustele. Tulevikus muudab juturoboti rakendamine ja eelnevalt defineeritud tüüpilistele küsimustele ettevalmistud vastuste kasutamine vastamise kiiremaks.

Teenused, mille kasutamist nähakse alternatiivsetes kanalites jaotusid sarnaselt intervjueerimisel leitud tulemustele, kus suurimaks grupiks on kasutajatoe pakkumine.

Populaarsemad teenused	
Klienditugi	90%
Avalduste/taotluste täitmine ja seonduvatele täiendavatele küsimustele vastamine	60%
Teavituste saatmine	60%
E-teenuste pakkumisel vestluse käigus	70%

Erinevused PoC ja terviklahenduse vahel

- PoC paigaldatakse ühte virtuaalmasinasse (active/passive failover teises analoogses virtuaalmasinas), täislahenduse puhul on iga teenus eraldi (sh automaatselt) skaleeritav ja paigaldatav eraldi masinatesse. Võimalikud lahendused on näiteks:
    - Kubernetes klaster
    - Rakendusserverite klaster
    - Andmebaaside klaster andmete replikatsiooniga
- PoC lahenduses on sõnumihoidla samas virtuaalmasinas muude teenustega, täislahenduses on ta väline eraldi skaleeritav teenus.
- PoC lahenduses on kasutusel JAR-id sissepõimitud Tomcat rakendusserveriga, täislahenduses saab kõik mikroteenused realiseerida WAR-dena, et paigaldada vabalt valitud rakendusserverile.
- PoC lahenduses on sõnumihoidlana kasutusel ElasticSearch, täislahenduse puhul on soovitatav MongoDB - põhjenduseks see, et ElasticSearch on mõeldud teistsuguste (täistekstiotsingutele ja logianalüüsile orienteeritud) kasutuslugude jaoks. MongoDB on mõeldud suurema arvu kirjutamiste/uuendamiste jaoks ja täistekstiotsing on samuti võimalik; lisaks on tema mälu ja teiste ressursside kasutus optimaalsem, võimaldades vastu pidada suuremale päringute arvule. Mõlemad on võimalik käivitada mitmes paralleelses *node*-s korraga koos andmete replitseerimisega.
- PoC lahenduses toimub sõnumihoidla poole pöördumine läbi ALT Ruuteri. Sõnumihoidla poole pöörduvad inbound-service ja outbound-service; samuti on võimalik kasutada otse ElasticSearch API-t sõnumite salvestamiseks, pärimiseks, uuendamiseks ja kustutamiseks. Täislahenduses toimub sõnumihoidla poole pöördumine läbi selleks mõeldud eraldi mikroteenuse, mille baasiimplementatsioon oleks muudetav, s.t. ta käiks vastu MongoDB-d. Samuti on teenuse abiga võimalik kontrollida ligipääsusid.