TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Martin Abel 175595IDAR

WINDOWS ACTIVE DIRECTORY KASUTAJAGA SISSELOGIMINE LINUX KLIENTARVUTISSE EESTI ID-KAARDIGA

Diplomitöö

Juhendaja
Edmund Laugasson
MSc

Tallinn 2021

Autorideklaratsioon

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

Autor: Martin Abel
17.05.2021

Annotatsioon

Käesoleva diplomitöö eesmärgiks oli luua kiipkaardiga sisselogimise lahendus Ubuntu Linuxi arvutis, mis asub Microsoft Windowsi domeenis. Lahendus peab töötama viimase *Ubuntu Linuxi LTS* versiooniga. Kiipkaardiks on Eesti ID-kaart.

Töö teoreetilises osas uuriti Tallinna Tehnikaülikooli Windowsi domeeni sisselogimist Windowsi arvutitest kasutades ID-kaarti. Uuriti ka Ubuntu ja Windowsi domeeni vahelisi seoseid ning kitsaskohti ID-kaardiga sisselogimiseks. Lisaks viidi läbi küsitlus Tallinna Tehnikaülikooli IT Kolledži tudengite seas, selgitamaks välja huvi loodava lahenduse vastu.

Töö praktilises osas loodi testkeskkond vastavalt lähtetingimustele. Testkeskkonnas loodi prototüüp võimaldamaks Windowsi domeeni kasutajaga sisselogimist Ubuntu arvutis, kasutades Eesti ID-kaarti.

Diplomitöö tulemuseks oli töötav prototüüp vastavalt lähtetingimustele.

Diplomitöö on kirjutatud eesti keeles ning sisaldab teksti 24 leheküljel, 9 peatükki, 8 joonist.

Abstract

The aim of this thesis was to create a smart card login solution on an Ubuntu Linux Computer connected to a Microsoft Windows domain. The solution must work with the latest version of Ubuntu Linux LTS. The smart card is an Estonian ID card.

In the theoretical part of the diploma thesis, the login to the Windows domain of Tallinn University of Technology from Windows computers using an ID card was studied. The connections between Ubuntu and the Windows domain and the bottlenecks for logging in with an ID card were also examined. In addition, a survey was conducted among the students of Tallinn University of Technology IT College to find out their interest in the solution to be created.

In the practical part of the diploma thesis, a test environment was created according to the initial conditions. A prototype was created in the test environment to enable a user with a Windows domain account to log in to an Ubuntu computer using an Estonian ID card.

The result of the diploma thesis was a working prototype according to the initial conditions.

The diploma thesis is written in Estonian and contains text on 24 pages, 9 chapters, 8 figures.

Mõisted

Active Directory	Aktiivkaust - loob ühise liidese ja andmebaasi võrgustatud kataloogide ja ressursside korraldamiseks ja hoolduseks
Autoriseerimise-sertifikaat	Sertifikaat isikustamiseks, avalik võti.
DNS	Nimelahenduse teenus.
Domeenikontroller	Windowsi domeeni turvalisuse, autoriseerimise ja halduse eest vastutav server.
Domeeni arvuti	Windowsi domeeni, domeenikontrolli haldusesse kuuluv arvuti.
Domeeni kasutaja	Kasutaja Windowsi domeenis, domeenikontrolleri halduses.
Dual boot	Samas füüsilises arvutis kasutusolevad kaks operatsioonisüsteemi. Arvuti käivitamisel antakse kasutajale valik, millist operatsioonisüsteemi käivitada.
FQDN	Domeeninimi, mis sisaldab kõiki nimetatava üksuse kõrgemaid domeene.
Group Policy	Rühmareeglistik, domeeni liikmete haldamiseks
Group Policy Management	Windowsi operatsioonisüsteemis kasutatav tööriist rühmareeglistiku haldamiseks.
Juurtaseme sertifikaat	Sertifikaat mis on enda poolt signeeritud, kasutatakse kesktaseme sertifikaatide signeerimiseks.
KDC	Võtmeväljastuskeskus krüptograafias.
Kerberos	Vastastiku autentimise protokoll.
Kerberos realm	Haldusala vastastikuse autentimise protokolli kasutamiseks.
Kesktaseme sertifikaat	Sertifikaat mis on allkirjastatud juursertifikaadi pool, ID-kaardi puhul kasutatakse kasutajate sertifikaatide väljastamiseks.
LDAP	Lihtsustatud kataloogisirvimise protokoll. Komplekt protokolle, mis võimaldavad ligipääsu infokataloogidele.
MFA	Autentimismeetod, kus arvutikasutajale võimaldatakse ligipääs ainult siis, kui ta esitab autentimismehhanismile korrektselt kaks või enam tõendit.

Moodul	Rakenduse osa.
NTP server	Server, mis tagab internetis asuval raadio-, aatom- või muul kellal põhinevat täpset kohalikku ajaarvestust.
PKI	Inimeste, reeglite ja protseduuride süsteem avalike võtmete sidumiseks kasutajate identiteetidega, tavaliselt sertifikaatide abil.
PKNIT	Võtmeväljastusekeskusega autoriseerimiseks kasutatav mehanism Kerberos 5 protokollis.
Skel	Linuxi operatsioonisüsteemides kirjeldatud vaikimisi kasutajaprofiil.
UNI-ID	Tallinna Tehnikaülikoolis kasutusel olev digitaalne identinteet.

Sisukord

Jooniste loetelu

1. Sissejuhatus

Tänapäeval pööratakse eraldi rõhku turvalisusele erinevate e-teenuste kasutamisel. Mitmeastmelist autentimist *(inglise k. lühend MFA)* on rakendatud nii riiklike, finants kui ka meditsiini teenustes. Tihtipeale on tegemist ka turvalise mugavusteenusega, pikkade paroolide asemel piisab erinevate PIN koodide meelespidamisest. Üks paljudest võimalikest *MFA-dest* on kiipkaart. Eesti kõige populaarsem kiipkaart (*inglise k. lühend Smart Card*) on ID-kaart.

ID-kaart kui isikutunnistus on Eestis kohustuslik isikut tõendav dokument. ID-kaarti saab lisaks tavapärasele isiku tõendamisele kasutada ka enda isiku tuvastamiseks elektroonilises keskkonnas.[1] Microsoft Windowsi (edaspidi Windows) operatsioonisüsteemides on kiipkaardiga kasutajasse sisselogimine sisseehitatud. Antud lahendus on ka rakendatud Tallinna Tehnikaülikoolis.

Lisaks Windowsi operatsioonisüsteemile on Tallinna Tehnikaülikooli IT Kolledžis (edaspidi IT Kolledž) kasutusel Ubuntu Linuxi operatsioonisüsteem, milles kiipkaardiga kasutajasse sisselogimist ei võimaldata. Küll on Ubuntu klassiarvutid seotud ülikooli Windowsi domeeniga. Diplomitöö eesmärgiks on luua prototüüp, mis võimaldaks kiipkaardiga sisselogimist Windowsi domeeni kuuluvates kolledži Ubuntu arvutites.

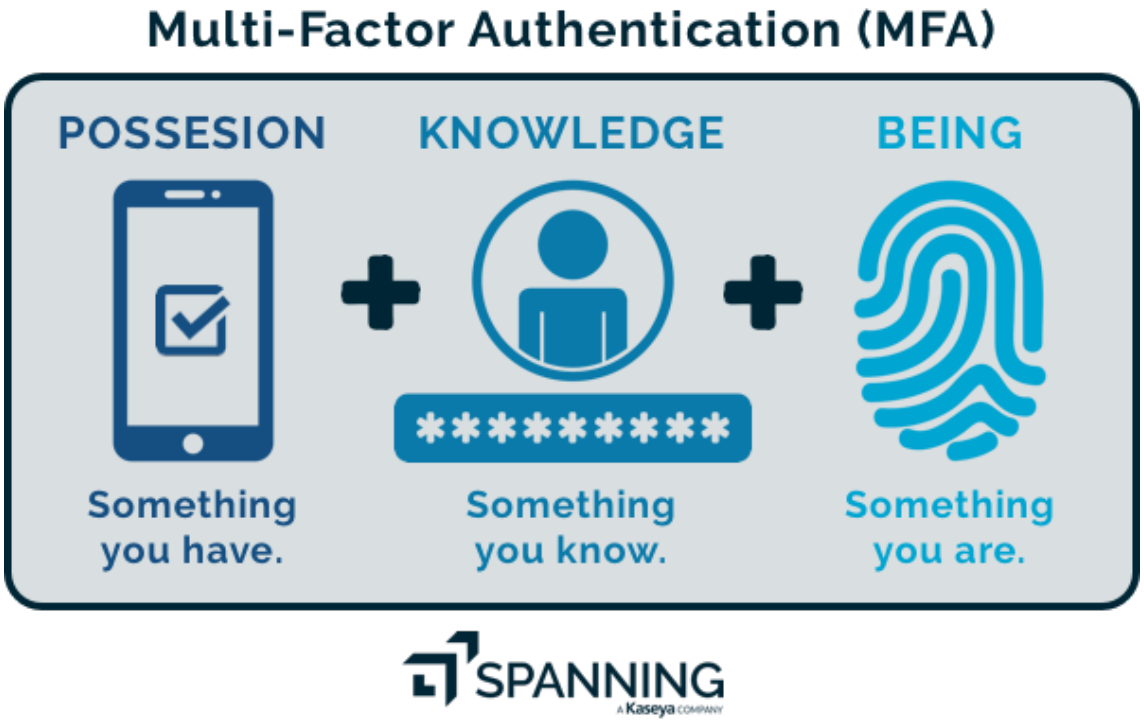
Diplomitöö teoreetilises osas uuriti IT Kolledžis kasutusel olevat ID-kaardiga sisselogimise lahendust Windowsi arvutites. Uuriti Ubuntu arvutite puhul Windowsi domeeniga siduvust ning millised on olnud kitsaskohad kiipkaardiga sisselogimise võimaldamiseks Ubuntu klassiarvutites. Lisaks viidi läbi küsitlus IT Kolledži tudengite seas eesmärgiga hinnata huvi loodava lahenduse vastu ning anti hinnang tudengite teadlikkusest kiipkaardiga sisselogimise võimalusest Windowsi operatsioonisüsteemis.

Diplomitöö praktilises osas kirjeldati testkeskkonna ja prototüübi loomist. Lisaks andis autor hinnangu loodud prototüübile.

Diplomitöö teema valik tuleneb IT Kolledži süsteemiadministraatori ja IT juhi soovist Ubuntu ja Windowsi sisselogimise võimalusi ühtlustada ning pakkuda *MFA* sisselogimise võimalust tudengitele. Lisaks tunneb diplomitöö autor huvi *MFA* lahenduste vastu.

2. Hetkeolukord

Tänapäeval kui rääkida turvalisest sisselogimisest, räägitakse enamasti *MFA-st*. *MFA* on kahe või rohkema astmeline isikustamise viis. Enamasti on see kombinatsioon paroolist või PIN koodist, see mida kasutaja teab ning midagi mis tal on, näiteks kiipkaart. Lisaks võib mingis isikustamise etapis kasutada ka biomeetriat, näiteks sõrmejälge. Seega kinnitatakse isikustamine vähemalt kahe erineva meetodiga, mis tõstab oluliselt turvalisust, võrreldes tavapärase parooliga. *MFA* eesmärk on tõsta kasutaja andmete ning süsteemi turvalisust. Paroolid võivad lekkida kasutaja teadmata, kuid füüsilise objekti nagu kiipkaart või telefoni kadumist märkab kasutaja varem või hiljem.[2]



Joonis 1. Näide *MFA-st*[3]

Eestis kõige populaarsem *MFA* on Eesti ID-kaart. ID-kaardiga saab Tallinna Tehnikaülikoolis logida sisse erinevatesse õppekeskkondadesse. Lisaks erinevatele õppekeskkondale on võimalik ülikoolis kasutada ID-kaarti sisselogimiseks Windowsi operatsioonisüsteemiga arvutisse. Windowsi operatsioonisüsteemis on vaikimisi sisse kirjutatud kiipkaardiga sisselogimise funktsioon. Eeldus on kehtivate Eesti ID-kaardi juur-

ja kesktaseme sertifikaatide olemasolu domeeni kontrolleris ja domeeni arvutites. [4]

Peale Windowsi operatsioonisüsteemi on ülikoolis kasutusel ka Ubuntu Linuxi operatsioonisüsteemiga arvutid. Ubuntu klassiarvutid kuuluvad küll Windowsi domeeni, kuid erinevalt Windowsi arvutitest, on võimalik Ubuntu arvutitesse sisse logida ainult kasutades domeeni kasutajat.

IT Kolledž, kui juhtiv kolledž IT maastikul, võiks lisaks Windowsi operatsioonisüsteemile võimaldada turvalist ning kiiret sisselogimist ka Linuxi operatsionisüsteemiga Windowsi domeeni arvutitesse. Domeeni kasutajasse sisselogimine Eesti ID-kaardiga tõstaks sisselogimise kiirust ning turvalisust. Enda isikustamiseks vastu domeenikontrollerit vajab tudeng lisaks PIN koodile ka kehtivate sertifikaatidega ID-kaarti. Diplomitöös loodava lahenduse vastu tunneb suurt huvi kolledži Linuxi süsteemiadministraator ning IT juht. Autorile teadaolevalt on loodavast lahendusest samuti huvitatud avalik sektor.

3. Ülesande püstitus

Diplomitöös püstitatud eesmärk oli luua prototüüp, võimaldamaks Linuxi arvutiga domeeni kasutajasse sisselogimist kasutades kiipkaarti.

Kuna diplomitöös loodud lahendust soovitakse rakendada IT Kolledži Ubuntu klassiarvutites, pidi vastama prototüüp järgnevatele tingimustele:

- Kasutatakse viimast *LTS* versiooni Ubuntu operatsioonisüsteemist: *Ubuntu 20.04.2 LTS*
- Ubuntu arvutid on lisatud *Microsoft Windowsi Active Directory* domeeni.
- Domeenikontrolleril kasutatakse viimast *Microsoft Windows Server 2019* operatsioonisüsteemi.
- Sisselogimine on võimaldatud kehtivate Eesti ID-kaartidega.

4. Metoodika valik

Diplomitöös kasutatud metoodikad on intervjuu ekspertidega, eksperimendid ning küsitlus.

IT Kolledži tudengitega viidi läbi küsitlus selgitamaks välja huvi diplomitöös loodud lahenduse vastu.

Diplomitöös viidi läbi intervjuu eksperdiga uurimaks Windowsi domeeni tehnilisi seadistusi võimaldamaks sisselogimist ID-kaardiga. Lisaks uuriti Ubuntu arvutite tehnilisi seadistusi Windowsi domeeniga liitmiseks. Selgitati välja, miks ei ole õnnestunud Ubuntu arvutites rakendada ID-kaardiga sisselogimist Windowsi domeeni kasutajasse.

Prototüüp loodi eksperimendi käigus. Esmalt seadistas diplomitöö autor testkeskkonna, mis koosnes kolmest virtuaalmasinast: domeenikontroller ja kaks klientarvutit - Windows ning Ubuntu. Testkeskkond vastas töös esitatud lähtetingimustele. Klientarvutid liideti domeeniga. Ubuntu klientarvuti liideti Windowsi domeeni analoogselt IT Kolledži Ubuntu arvutites kasutatud seadistustega. Windowsi klientarvuti eesmärgiks oli testida domeenikontrolleri seadistusi võimaldamaks sisselogimist ID-kaardiga.

Prototüübi loomisele läheneti Windowsis toimivat lahendust silmas pidades. Lisaks kasutas autor lahenduse loomisel tehnilist juhendit sisselogimaks Windowsi domeeni kasutajasse Ubuntu arvutis, kasutades Yubikey-d kui kiipkaarti.

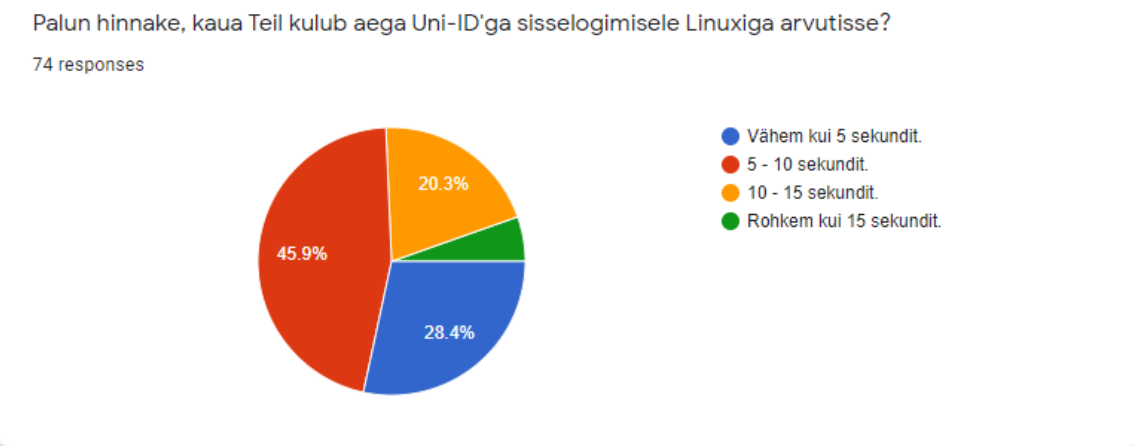
Loodud prototüüpi testiti testkeskkonnas, mis vastas lähtetingimustele. Loodud prototüüp võimaldas Windowsi domeeni kasutajaga sisse logida Ubuntu arvutisse, kasutades Eesti ID-kaarti.

5. Küsimustiku analüüs

Küsitluse valimiks on IT Kolledži üliõpilased. Küsimustikus on 4 küsimust selgitamaks välja kasutaja harjumused domeeni arvutitesse sisselogimiseks ning huvi loodava lahenduse vastu. Lisaks on küsitluse eesmärk lasta tudengitel mõõta orienteeruvalt sisselogimise kiirust domeeni arvutisse ning saada tudengitelt hinnang IT Kolledžis täna kasutusel oleva lahenduse turvalisuse kohta. Küsimustiku vastustest loeb diplomitöö autor välja IT Kolledži tudengite domeeni kasutajasse sisselogimise harjumused ning nende huvi loodava lahenduse kasutuselevõtuks kolledžis.

Küsitlus viidi läbi elektrooniliselt kasutades Google Forms keskkonda. Küsitlus oli eesti keeles ning saadeti välja õppeosakonna poolt IT Kolledži tudengitele. Küsitlusele oli aega vastata 4 nädalat. Küsitlusele vastas kokku 74 tudengit.

"Palun hinnake, kaua Teil kulub aega Uni-ID'ga sisselogimisele Linuxiga arvutisse?"



Joonis 2. Küsimustik: UNI-ID'ga Linux arvutisse logimise ajaline hinnang

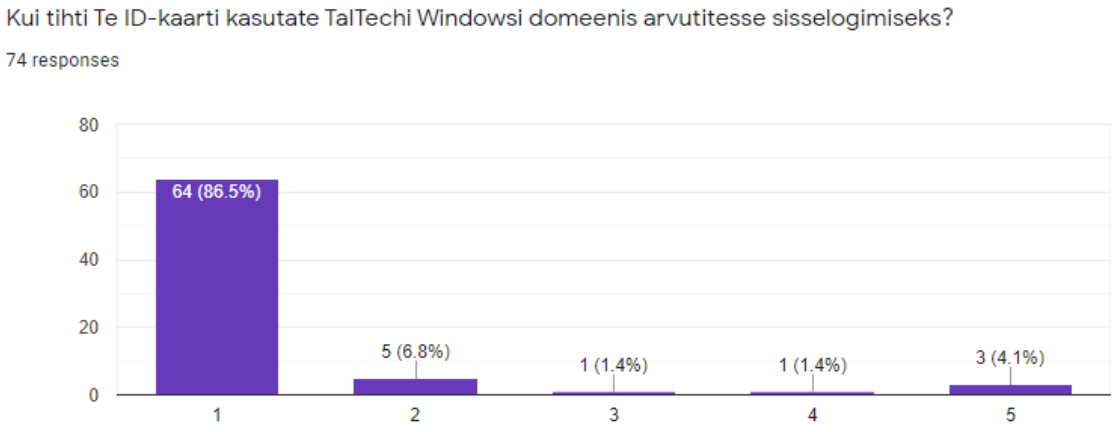
Küsimuse eesmärgiks oli lasta tudengitel mõõta orienteeruvat aega kaua neil kulub täna domeeni kasutajaga sisselogimiseks IT Kolledži arvutitesse, mis kasutavad Linuxi operatsioonisüsteemi. Küsimuse vastusevariantides mõõdeti aega 5 sekundilise intervalliga. 5, 5-10, 10-15 ja rohkem kui 15 sekundit.

Enim vastanutest, 45.9% ehk 34 vastajat, arvas et neil kulub domeeni kasutajasse

sisselogimiseks aega 5 kuni 10 sekundit. 28.4% ehk 21 vastajat hindas orienteeruvaks sisselogimise ajaks vähem kui 5 sekundit. 20.3% ehk 15 vastajat hindas orienteeruvaks sisselogimise ajaks 10 kuni 15 sekundit. Kõige vähem vastajatest, 5.4% ehk 4 tudengit, hindas orienteeruvaks sisselogimise ajaks rohkem kui 15 sekundit.

IT Kolledžis on domeeni kasutajanimi minimaalselt 6 tähemärki ning parool 8 tähemärki pikk. Domeeni kasutaja puhul *UPN-i* kirjutama ei pea, piisab kasutajanimest. Populaarseima vastuse puhul (45.9%), hinnati orienteeruvaks sisselogimise ajaks 5-10 sekundit. ID-kaardi kasutamine kasutajasse sisselogimisel annaks ajalise võidu. Teisel kohal (28.4%) populaarseim vastus, et sisselogimine domeeni kasutajaga võtab aega vähem kui 5 sekundit, ei tundu domeeni kasutajanime ning parooli nõudeid arvestades reaalne. Pigem on vastaja olnud optimistlik. Antud olukorras ID-kaardiga sisselogimisel ajavõitu ei teki, või on see minimaalne. Vastajad, kes hindasid orienteeruvaks sisselogimise ajaks 10 kuni 15 sekundit (20.3%), on ID-kaardiga sisselogimine autori hinnangul kiirem kui kasutades domeeni kasutajat ja parooli. 5.4% vastanutest, kes hindas orienteeruvaks sisselogimise ajaks 15 sekundit, kasutavad autori hinnangul keerulisemat parooli kui tavapärane domeeni parooli nõue ning nende puhul oleks ID-kaardiga sisselogimisel ajavõit märgatav.

"Kui tihti Te ID-kaarti kasutate TalTechi Windowsi domeenis arvutitesse sisselogimiseks?"



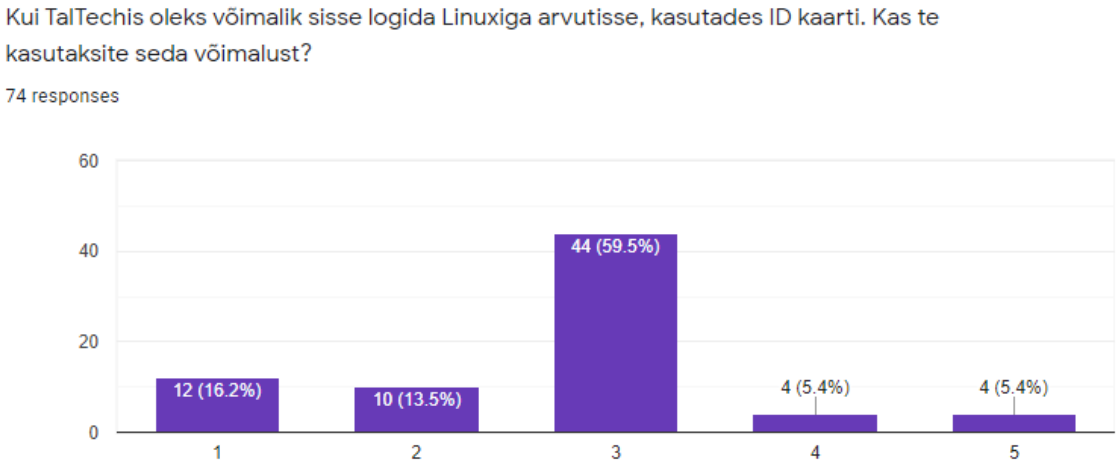
Joonis 3. ID-kaardiga Windowsi ID-kaardiga Windowsi sisselogimise populaarus

Küsimuse puhul kasutas autor Likerti skaalat, kus lasti vastajatel hinnata kui tihti nad kasutavad võimalust ID-kaardiga Windowsi domeeni arvutisse sisse logida. Küsimust hinnati viie palli süsteemis: 1 (pigem ei kasuta) kuni 5 (väga tihti kasutan). Täna on IT Kolledžis ID-kaardiga sisselogimise võimalus ainult Windows operatsioonisüsteemiga domeeni arvutites. Küsimuse eesmärgiks oli hinnata tudengite harjumust kasutada ID-

kaarti kui sisselogimise vahendit.

Enim vastanutest, 86.5%, kes on 64 vastanut, pigem ei kasuta (1 pall) täna võimalust Windows domeeni arvutisse sisselogimiseks ID-kaardiga autentimise võimalust. Autor järeldab vastusest, et kasutajad kas ei tea võimalust ID-kaarti kasutada alternatiivse sisselogimise meetodina või on kasutajatel harjumus kasutada tavapärast sisselogimise meetodit. Põhjuseks võib pidada, et ID-kaardiga on võimalik sisse logida ainult Windowsi operatsioonisüsteemiga domeeni arvutites. Seega võib väita, et kasutajatel puudub harjumus antud võimalust kasutada. Kõige vähem vastanutest, 5.5%, kes on 4 vastanut (vastavalt 4 ja 5 palli) kasutavad ID-kaarti Windowsi domeeni arvutisse sisselogimiseks väga tihti. Autor arvab, et antud vastajate jaoks oleks väga mugav kui ka Linuxi operatsioonisüsteemi saaks ID-kaardiga sisse logida. Lisaks arvutisse sisselogimisele on täna ülikoolis sisselogimise võimalus ID-kaardiga õpikeskkondadesse. Vastanutest 6.8% ja 1.4% hindas harjumust ID-kaardiga sisselogimist Windows domeeni arvutisse vastavalt 2 (5 vastanut) ja 3 (1 vastanu) palli skaalal 5-st. Kasutajad küll teavad võimalusest kasutada ID-kaarti sisselogimiseks Windows domeeni arvutisse, kuid ei kasuta seda, sest see on ainus kasutusel olev operatsioonisüsteem, mis võimaldab sisselogimist ID-kaardiga domeeni kasutajasse ning kasutajatel puudub harjumus.

"Kui TalTechis oleks võimalik sisse logida Linuxiga arvutisse, kasutades ID kaarti. Kas te kasutaksite seda võimalust?"



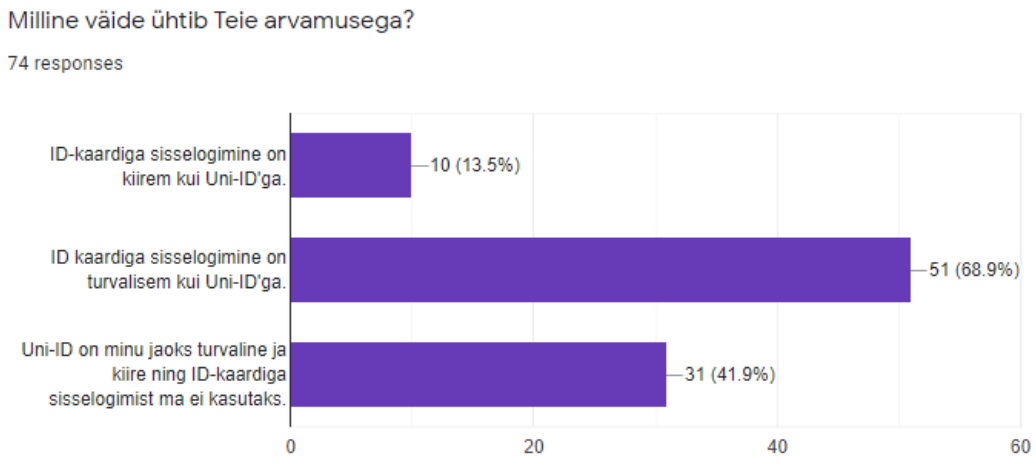
Joonis 4. Huvi kasutamaks ID-kaarti Linux arvutisse sisselogimiseks

Küsimuse puhul kasutas autor Likeri skaalat, kus lasti vastajatel hinnata kui tihti nad kasutaks võimalust logida sisse ID-kaardiga Linuxi operatsioonissüsteemiga ülikooli domeeni arvutisse. Küsimust hinnati viie palli süsteemis: 1 (pigem ei kasuta) kuni 5 (väga tihti kasutan). Täna IT Kolledžis antud võimalus Linux operatsioonisüsteemiga arvutites

veel puudub. Küsimuse eesmärgiks oli hinnata tudengite huvi loodava lahenduse vastu.

Populaarseim hinnang, 59.5% (44 vastajat) oli 3 viie palli skaalal, et vastajad kasutaks ID-kaardiga sisselogimist Linuxi operatsioonisüsteemis. Autor võib antud vastusest järeldada, et tudengid oleksid nõus kasutama võimalust nii Windowsi kui ka Linux operatsioonisüsteemis ID-kaardiga domeeni kasutajasse sisselogimiseks. Tudengid pole täna harjunud antud võimalust kasutama, sest see on kasutusel ainult Windowsi domeeni arvutites. Teisel kohal, 16.2% (12 vastajat) pigem ei kasutaks ID-kaardiga sisselogimise võimalust Linuxi operatsioonisüsteemis. Autor võib antud vastusest järeldada, et kuna täna on antud võimalus ainult Windows domeeni arvutites, pole tudengid antud võimalusega harjunud ning ei näe võimalikku mugavust ning turvalisust loodavas lahenduses. Kolmandal positsioonil vastanutest valis 2 palli viie palli skaalal, et nad ei kasutaks ID-kaardiga sisselogimise võimalust domeeni kasutajatesse. Nagu ka 1 palli (pigem ei kasuta) valinud vastajatest, võib autor üldistada, et ID-kaardiga sisselogimisega domeeni kasutajasse pole tudengid harjunud ning ei tunne loodava lahenduse vastu vajadust. Kokku 10.8% (4+4) vastajatest valis kas 4 või 5 palli viiest, mis näitab, et nad pigem kasutaksid loodavat lahendust sisse logimaks domeeni kasutajaga Linuxi operatsioonisüsteemiga arvutisse. Autor võib järeldada, et antud valiku teinud vastajad tunnevad suurt huvi loodava lahenduse vastu ja näevad lahenduses lisa turvalisuse ning mugavuse aspekti. Eriti kui mõlemas operatsioonisüsteemis oleks võimalik sisse logida domeeni kasutajaga kasutades ID-kaarti.

"Milline väide ühtib Teie arvamusega?"



Joonis 5. Küsimustik: Hinnang ID-kaardiga domeeni arvutisse sisselogimisele

Autor esitas antud küsimusel 3 väidet, mille vahel lasi vastajal valida. Vastaja sai valida ka mitu väidet korraga, mis tema arvamusega kattub. Väited olid järgmised: "ID-kaardiga

sisselogimine on kiirem kui Uni-ID'ga", "ID-kaardiga sisselogimine on turvalisem kui Uni-ID'ga" ja "Uni-ID on minu jaoks turvaline ja kiire ning ID-kaardiga sisselogimist ma ei kasutaks". Küsimuse eesmärgiks oli hinnata täna kasutusel olevat sisselogimise võimalust domeeni arvutisse (UNI-ID) ehk domeeni kasutaja turvalisust ja kiirust võrreldes loodava lahendusega (ID-kaardiga sisselogimine).

Populaarseim väide, millega vastajad nõustusid oli "ID-kaardiga sisselogimine on turvalisem kui Uni-ID'ga". Antud väitega nõustus 68.9% vastanutest, ehk 51 tudengit. Teisel kohal oli väide "Uni-ID on minu jaoks turvaline ja kiire ning ID-kaardiga sisselogimist ma ei kasutaks". Antud väitega nõustus 41.9% vastanutest, ehk 31 tudengit. Väitega "ID-kaardiga sisselogimine on kiirem kui Uni-ID'ga" nõustus 13.5% vastanutest ehk 10 tudengit. Autor võib antud vastustest järeldada, et vastajate arvates on täna kasutusel olev domeeni kasutajaga sisselogimine piisavalt turvaline, kuid nad nõustuvad, et ID-kaardiga sisselogimine tõstaks turvalisust. Lisaks tunneb osa vastanutest, et kui ID-kaardiga saaks sisse logida mõlema operatsioonisüsteemiga ülikooli domeeni arvutisse, lisaks see kiirust ja mugavust.

6. Tehniline ülevaade

Eesmärk on anda tehniline ülevaade IT Kolledži arvutiklassides kasutavatest operiatsioonisüsteemidest ning kuidas nad on seotud domeenikontrolleriga. Kolledžis on arvutiklassides kasutusel *dual boot* arvutid, seega on võimalik arvutit käivitada nii Windowsi kui ka Ubuntu operatsioonisüsteemiga. Lisaks antakse ülevaade kuidas on võimalik ID-kaardiga sisse logida Windows 10 klassiarvutites domeeni kasutajaga ja millised on olnud kiipkaardiga Ubuntu klassiarvutitesse sisselogimise võimaldamise kitsaskohad.

6.1 Windowsi klassiarvutid ja Windowsi domeen

Diplomitöö autor vestles IT Kolledži IT juhiga, et tutvuda täna kasutusel oleva lahendusega. Lisaks antakse ülevaade seadistustest, mis võimaldab sisselogimist domeeni arvutitesse kasutades ID-kaarti.

Ülikooli domeenikontrollerites on kasutusel Windows Server 2019 operatsioonisüsteem. IT Kolledži arvutiklassi arvutites on kasutusel Windows 10 operatsioonisüsteem.

Domeenikontrollerid vajavad domeenikontrolleri autoriseerimise-sertifikaati *(inglise k. Domain Controller Authentication)*, võimaldamaks kiipkaardiga domeeni arvutitesse sisselogimist.[4] Autoriseerimis-sertifikaat tuleb vaikimisi kaasa kui domeenikontrollerile on paigaldatud ja seadistatud *Active Directory Certificate Services* roll.[5] Nii domeenikontroller kui ka domeeni arvutid peavad usaldama Eesti ID-kaardi juur- ning kesktaseme sertifikaate. Domeenikontrolleritesse on paigaldatud ID-kaardi juursertifikaadid *EE-GovCA2018*, *EE Certification Centre Root CA* ning kestaseme sertifikaadid *ESTEID-SK 2011*, *ESTEID-SK 2015*, *EID-SK 2016* ja *ESTEID2018*.[4] Vajalikud sertifikaadid saab alla laadida Sertifitseerimiskeskuse kodulehelt.[6]. Oluline on juursertifikaadid paigaldada sertifikaadi hoidla *Trusted Root Certification Authorities* kausta. Kesktaseme sertifikaadid paigaldada sertifikaadi hoidla *Intermediate Certification Authorities* kausta.[4]

Sertifikaadid publitseeritakse domeeni arvutitele kasutades rühma reeglistikku *(inglise k. Group Policy)*. *Group Policy Management* utiliidis on soovitav seadistada vaikereeglistik

Default Domain Policy. *Default Domain Policy* rakendab vaikimisi seadistuse igale *Active Directory* objektile. Seadistused tuleb teha rühmareeglistiku kaustas *Computer Configuration/Policies/Windows Settings/Security Setting/Public Key Policies*. Sertifikaadid paigaldada nagu oli kirjeldatud domeenikontrolleri puhul. Lisaks sertifikaatidele kasutatakse rühma reeglistiku kiipkaardiga sisselogimise sätete seadistamiseks domeeni arvutites. Mõistlik on kiipkaardi sisselogimise seadistused teha samas vaikereeglistikus. Seadistused teha reeglistiku kaustas *Computer Configuration/Policies/Administrative Templates/Windows Components/Smart Card*. Reeglistiku kaustas aktiveerida (valida *Enable*) järgnevad seadistused: *Allow certificates with no extended key usage certificate attribute* ja *Allow ECC certificates to be used for logon and authentication*. Kiipkaardiga kasutajatesse sisselogimise võimalus on sisseehitatud Windows 10 operatsioonisüsteemi. Rühmareeglistiku abil lülitame domeeni arvutites vajalikud sätted sisse.[4]

Domeenikontrolleris seotakse domeeni kasutajad *(inglise k. Domain Users)* kasutajale kuuluva ID-kaardi kasutaja sertifikaadiga. Kasutaja sertifikaadi saamiseks on mitmeid erinevaid meetodeid.[4] Näiteks küsitakse kasutaja sertifikaadid Sertifitseerimiskeskuse andmebaasist *LDAP* päringuga kasutades kasutaja isikukoodi.[7] Lisaks *LDAP* päringule on võimalik kasutaja sertifikaate välja eksportida kasutaja arvutist, millega on ID-kaarti juba kasutatud, kasutades Windowsis lokaalset sertifikaatide hoidlat. Kasutaja sertifikaat lisatakse domeeni kasutaja *Security Identity Mapping* alla. Kasutaja sertifikaat võib olla seotud ainult ühe domeeni kasutajaga.[4] Kasutaja sertifikaatide sidumine ja uuendamine käib ülikooli domeenis isikukoodi alusel, kasutades tarkvara, mis teeb päringud Sertifitseerimiskeskuse andmebaasi suunas. Isikukood kasutajatel on kirjeldatud *Active Directory-s* kasutaja objektile *(inglise k. User Object)* loodud atribuudis *hlmTTUFIMISIKUKOOD*. Tarkvara on loodud ettevõtte poolt Number Kuus Konsultatsioonid OÜ.

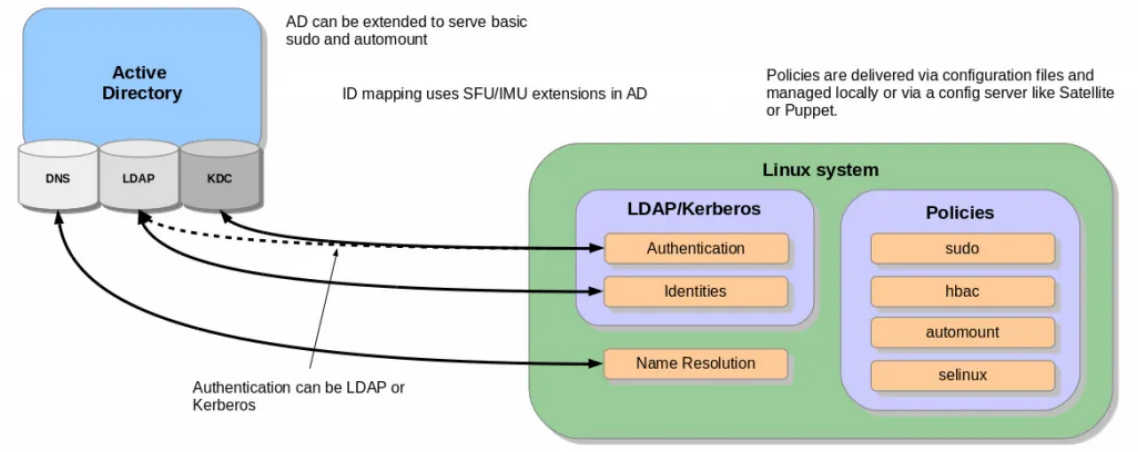
Windowsi tööjaamades peab olema installeeritud ID-kaardi tarkvara, et võimaldada ID-kaardiga sisselogimine domeeni kasutajasse. Tööjaama seadistused on mõistlik seadistada keskselt domeeni rühma reeglistikku kasutades.

6.2 Ubuntu Linuxi klassiarvutid ja Windowsi domeen

Diplomitöö autor vestles IT Kolledži Linuxi süsteemiadministraatoriga, et tutvuda täna kasutusel oleva lahendusega. Lisaks antakse ülevaade seadistustest, mis võimaldavad sisselogimist domeeni arvutitesse kasutades domeeni kasutajat. Kirjeldatakse murekohad, miks ei ole võimalik täna Ubuntus sisse logida domeeni kasutajaga kasutades ID-kaarti.

IT Kolledžis on arvutiklassi arvutites kasutusel Ubuntu 20.04.2.0 LTS operatsioonisüsteem. Täna ei saa vaikimisi Ubuntu operatsioonisüsteemiga arvutit liita Windowsi domeeniga. Selleks, et liita Ubuntu arvutid Windowsi domeeniga, ühtegi seadistust tegema ei pea. Kõik seadistused tuleb teha Ubuntus.

Ubuntu arvuti Windowsi domeeniga liitmise eelduseks on teha arvuti nähtavaks Windowsi domeenikontrollerile. Windowsi domeenikontrollerit tasub kasutada Ubuntu arvuti *DNS-ina*. Ubuntu kasutab Windows domeeniga liitumisel domeeni kontrolleri täispikka nime *(inglise k. lühend FQDN)*. Windows domeeniga liitumiseks peavad Ubuntu tööjaamas olema paigaldatud järgnevad tarkvara paketid: *realmd, libnss-sss, libpam-sss, sssd, sssd-tools, adcli, samba-common-bin, oddjob, oddjob-mkhomedir* ja *packagekit*. IT Kolledžis kasutatakse *SSSD* rakendust liitmaks Ubuntu arvutid Windowsi domeeniga. *Adcli* rakenduse käsku *realmjoin* kasutatakse Windowsi domeeniga liitumiseks. *Realmjoin* käsk seadistab enamik konfiguratsioonifailid automaatselt. Ubuntu ja Windowsi domeeni vahelised seadistused on kirjeldatud */etc/sssd/sssd.conf* failis. Domeeni kasutajate autentimiseks kasutatakse *Kerberost*. *Mkhomedir* moodul tuleb seadistada *PAM* konfiguratsioonifailis peale Ubuntu arvuti liitmist Windowsi domeeniga. *Mkhomedir* moodulit kasutatakse domeeni kasutajasse esmakordsel sisselogimisel arvutisse kodukausta loomiseks. *PAM* konfiguratsioonifailis on kirjeldatud *skel*, mis on domeeni kasutaja vaikeprofiil.[8]



Joonis 6. Ubuntu Windowsi domeenis[8]

Ubuntusse ei ole sisseehitatud kiipkaardiga sisselogimist. Erinevate pakettidega on see aga võimalik. IT Kolledžis on testitud ID-kaardi wikis avaldatud juhendit[9] Linuxi süsteemiadministraatori poolt. Juhend polnud piisav, et võimaldada domeeni kasutajaga ID-kaardiga sisselogimist. Takistuseks osutus seadistuse kirjeldus, kuidas võimaldada sisse logida ID-kaardiga Windows domeeni.

7. Prototüübi loomine

Diplomitöö käigus loodi prototüüp ID-kaardiga sisselogimiseks Ubuntu operatsioonisüsteemiga arvutisse, mis asub Windowsi domeenis. Töö praktiline osa koosnes kahest osast, testkeskkonna loomine ja seadistamine vastavalt lähtetingimustele ning prototüübi loomine.

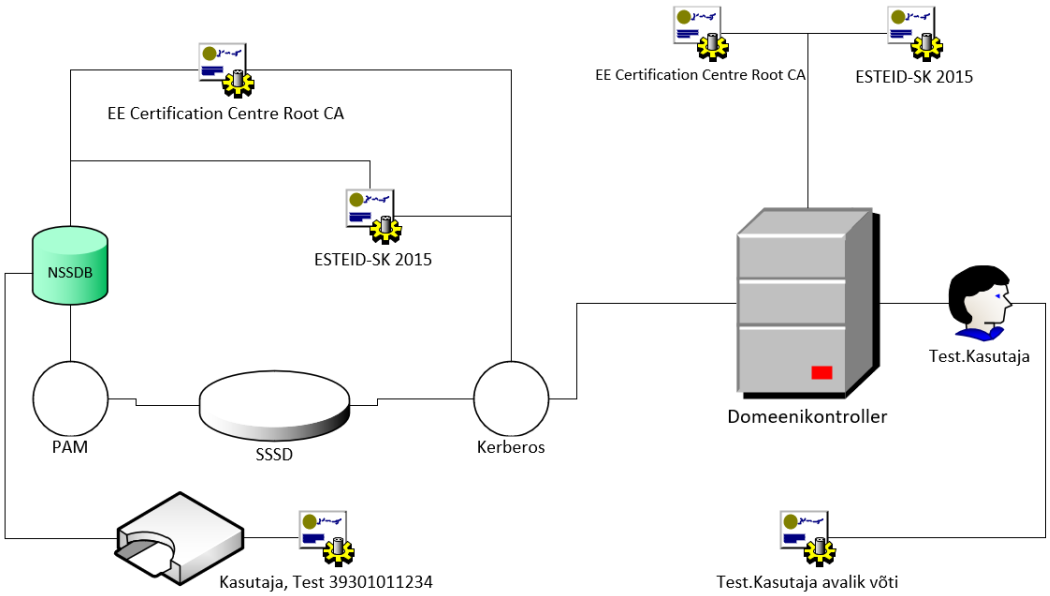
7.1 Testkeskkonna seadistamine

Prototüübi loomine algas testkeskkonna loomisega. Testkeskkond loodi virtuaalne kasutades Oracle VM VirtualBox 6.0.24. USB-kiipkaardi lugeja ühendamiseks virtuaalmasinaga oli vaja paigaldada lisaks VirtualBoxile lisapakett[10]. Testkeskkonda loodi kolm virtuaalmasinat, domeenikontrolleri server ja kaks klientarvutit. Domeenikontrolleri serverina kasutati Windows Server 2019 ja klientarvutitel vastavalt Windows 10 ning Ubuntu 20.04.2 LTS operatsioonisüsteemi. Windows serverile paigaldati rollid *Active Directory Domain Services* ja sellega vaikimisi tulevalt *DNS Server* roll. Lisaks *PKI* korrektseks toimimiseks *Active Directory Certificate Services* roll. Serveris seadistati domeen ning liideti klientarvutite virtuaalmasinad domeeni. Ubuntu virtuaalmasin liideti domeeni kasutades *SSSD-d*. Domeeni liitmise protsess on kirjeldatud diplomitöö peatükis 6.2. Windows 10 virtuaalmasina domeeni liitmisel erisusi ei olnud. Nii domeenikontrolleri seadistamisel kui ka Windows 10 virtuaalmasina liitmisel domeeniga kasutati Microsofti parimaid praktikaid.[11][12] Klientarvuti virtuaalmasinatele paigaldati operatsioonisüsteemile vastav Eesti ID-kaardi tarkvara võimaldamaks ID-kaardi kasutamist. Tarkvara on allalaetav vastavalt operatsioonisüsteemile Eesti ID-kaardi kodulehelt.[13] Ubuntu puhul kasutas diplomitöö autor skripti ID-kaardi tarkvara paigaldamiseks. Tarkvara paigaldamiseks piisas ainult skripti käivitamisest.[14] Nii domeenikontrolleri kui ka klientarvuti seadistati kasutama EENet *NTP* serverit.[**17**]

7.2 Lahenduse loomine

IT Kolledžis on varasemalt proovitud ID-kaardiga sisselogimist Ubuntu arvutites kasutusele võtta, selleks kasutati Eesti ID-kaardi wikis kirjutatud juhendit.[9] Antud juhend on väga vana ning kirjeldab erinevalt diplomitöös loodud lahendusest vaid lokaalse

kasutajaga sisselogimist. Töö käigus loodud lahenduse puhul pole kasutajad kaardistatud ID-kaardi kasutaja sertifikaadiga. Kasutajate sertifikaadid on kaardistatud domeenikontrolleris oleva kasutajaga. Lisaks kasutajad, mida kasutatakse sisselogimiseks, ei ole Ubuntu lokaalsed kasutajad. Kasutajad asuvad Windows domeenis. Loodud lahendus on pigem sarnane Windowsi operatsioonisüsteemiga, kus sertifikaadid, mida sisselogimisel kasutatakse on hoiustatud hierarhia alusel sertifikaadihoidlas, Ubuntu puhul andmebaasis. Diplomitöö autor on lahenduse loomisel keskendunud Windowsi kiipkaardiga sisselogimise loogikale. Lisaks on diplomitöö autor saanud inspiratsiooni Yubico Yubikey kui kiipkaardi lahendusest, millega on seadistatud *Active Directory* domeeni kasutajad sisse logima Ubuntu klientarvutisse. Yubikey-ga kui kiipkaardiga sisselogimiseks on kasutatud *Kerberos 5* protokolli ning rakendust *SSSD-d*.[15]



Joonis 7. Prototüübi tööpõhimõte

Ubuntu arvutis on kasutatud sertifikaatide andmebaasi lisamiseks *libnss3-tools* paketti. *Certutil* käsuga lisatakse ID-kaardi juur- ning kesktaseme sertifikaadid *NSSDB* andmebaasi. Sertifikaatide lisamisel on oluline, et kõik kasutuselolevad juur- ja kesktaseme sertifikaadid saaksid lisatud ning oleks kirjeldatud sertifikaatidepuu. Näide sertifikaadi lisamisest andmebaasi:

```
certutil -d /etc/pki/nssdb -A -n 'EE-Gov2018' -t CT,C,C -a -i
/etc/pki/ca/EE-GovCA2018.pem
```

Kiipkaardi toimimiseks tuleb siduda *NSSDB* mõne Ubuntus kasutuseloleva kiipkaardi teegiga. Linuxi operatsioonisüsteemides on kaks populaarset rakendust, mida kasutada kiipkaartide lugemiseks. *CoolKey*, mis on näiteks kasutusel Ameerika Ühendriikide

Kaitseministeeriumi kiipkaartide lugemiseks Linuxis ja *OpenSC* rakendus, mis näiteks tuleb kaasa Eesti ID-kaardiga kasutades paigaldus skripti.[16][14] Loodud lahenduses kasutati ID-kaardi haldusvahendi poolt kasutatavat teeki *onepin-opensc-pkcs11.so*. Teeki kasutatakse ainult isikutuvastuseks, allkirjastamise sertifikaati see ei loe.

Viite loomine kasutavale teegile[15]:

```
ln -s /usr/lib/x86_64-linux-gnu/onepin-opensc-pkcs11.so
/usr/lib/onepin-opensc-pkcs11.so
```

NSSDB sidumine teegiga:

```
modutil -dbdir /etc/pki/nssdb -add "onepinopensc" -libfile
onepin-opensc-pkcs11.so
```

Kerberos 5 autentimiseks paigaldati Ubuntu klientarvutile *krb5-pkinit* ja *krb5-user* paketid. *krb5-user* on vajalik *Kerberos 5* protokolli puhul tavapäraseks autentimiseks. Kui Ubuntu ei kuulu *Kerberos realmi*, käivitatakse seadistusliides automaatselt. Seadistusliideses tuleb ära tuleb märkida *realm*, ehk domeen kuhu Ubuntu klientarvuti kuulub ning domeenikontrollerid. *PKINIT-it* kasutatakse *Kerberose* protokolli kasutades kiipkaardiga kasutaja autoriseerimiseks. Autoriseerimist võimaldab loodud lahenduses teha *krb5-pkinit* pakett. *Kerberose* seadistused on kirjeldatud */etc/krb5.conf* failis.[15] Kui Ubuntu kuulub juba mõnda *Kerberos realmi*, tuleb *realm* kirjeldada */etc/krb5.conf* failis käsitsi.

Kerberose realm:

```
default_realm = TESTBOX.ZZ
```

Domeenikontroller, *KDC-na* kasutatakse *Active Directory*:

```
pkinit_kdc_hostname = DC.TESTBOX.ZZ
```

ID-kaardi juursertifikaatide kaust.

```
pkinit_anchors = DIR:/etc/pki/ca/
```

ID-kaardi kesktasemesertifikaatide kaust.

```
pkinit_pool = DIR:/etc/pki/ca/sub/
```

PKCS11 liidese kasutamisel määratletud teek ning millist sertifikaati loetakse. Loodud lahenduse juures kasutatakse ID-kaardi tarkvaraga kaasatulevat teeki ning isikustamisesertifikaati, mis on ID-kaardil esimene.

```
pkinit_identities = PKCS11:onepin-opensc-pkcs11.so:
slotid=0:certid=01
```

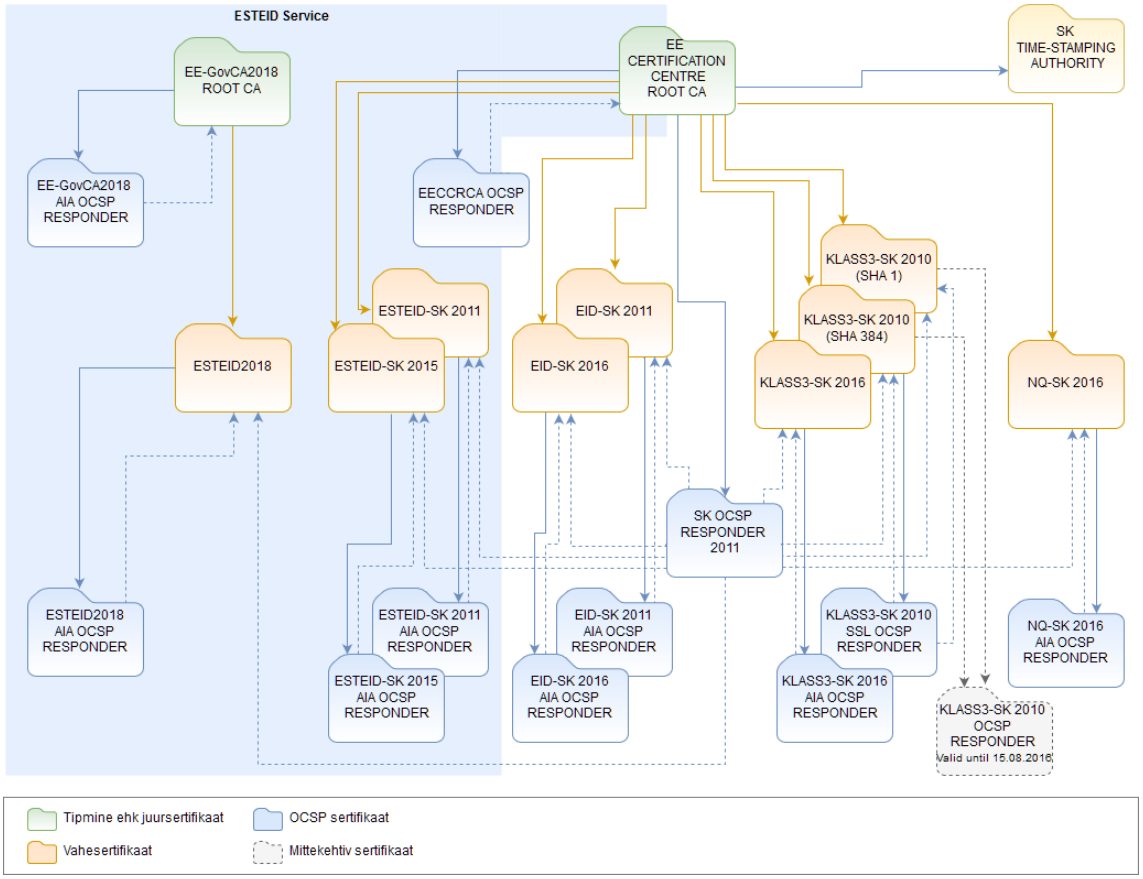
Kerberose puhvri määramine.

```
default_ccache_name = KEYRING:persistent:%{uid}
```

Lisaks tuli domeenikontrolleris lubada kolmandate osapoolte sertifikaatidega *Kerberos* autentimine, mis antud lahenduse puhul olid ID-kaardi juurtaseme sertifikaadid. Vaikimisi kontrollitakse *Kerberos* autentimise puhul domeenikontrolleri autoriseerimis-sertifikaati. Sertifikaatide lisamine domeenikontrolleris käis samuti *certutil* käsuga.[17]

```
certutil -enterprise -addstore NTAuth EE-GovCA2018.der.cer
```

Nii domeenikontrolleri kui ka Ubuntu puhul laeti alla sertifikaadid Sertifitseerimiskeskuse repositooriumist. ID-kaardi sertifikaatidel on aegumise tähtaeg ning sertifikaate tuleb hoida ajakohasena. Domeenikontrolleri puhul oli oluline kasutada *der* ja Ubuntu puhul *pem* faili formaati.[6]



Joonis 8. SK sertifitseerimishierarhia ülevaade[18]

Viimaks oli vaja seadistada *PAM* ja *SSSD*. Lahenduses */etc/sssd/sssd.conf* on lubatud sertifikaatidega kasutaja valideerimine ning autentimine vastu domeenikontrollerit. Muus osas jäid seadistused samaks nagu vaikimisi *sssd.conf* failis Windows domeeni Ubuntu arvutis.[15]

Kiipkaardiga valideerimise ja autentimise lubamine *SSSD-s*:

```
pam_cert_auth = True
```

SSSD paketi teeki *pam_sss* kasutatakse kasutaja sisse logimisel võimalike autentimismeetodite rakendamisel. Selleks kasutab *pam_sss* spetsiaalset faili */var/lib/sss/pubconf/pam_preauth_available*.[19] Faili vaikimisi pole ning see tuli ise luua, piisas tühjast failist. Peale faili loomist seadistas diplomitöö autor üldise sisselogimise konfiguratsioonifailis */etc/pam.d/common-auth*.[15]

/etc/pam.d/common-auth failis tehti muudatused järgnevalt[15]:

```
# here are the per-package modules (the "Primary" block)
auth [success=2 default=ignore] pam_sss.so forward_pass
auth [success=1 default=ignore] pam_unix.so
try_first_pass nullok_secure
# here's the fallback if no module succeeds
```

8. Tulemuste analüüs

ID-kaardi tarkvara arendatakse Linuxi värskematele operatsioonisüsteemidele, kuid ametlikes juhendites rõhutatakse just Linuxi distributsiooni Ubuntut.[13] Loodud lahendus avab Ubuntus uue võimaluse, sisselogimise Eesti ID-kaardiga, mille kohta avalikku juhendit internetis veel ei leidu.

8.1 Testkeskkonna analüüs

Lahenduse loomiseks loodi virtuaalne testkeskkond. Virtuaalne testkeskkond võimaldas autoril muudatuse ebaõnnestumisel taastada eelnev seis. Testkeskkond loodi autori poolt kohalikus masinas, kuna autor vajas kiipkaardi lugemiseks virtuaalmasinaga füüsilisele infrastruktuurile ligipääsu. Kiipkaardi kasutamine kaugelt haldavas virtuaalmasinas oleks olnud raskendatud. Autor ei leidnud sobivat lahendust kiipkaardi sidumiseks kaugelt haldava masinaga, tänu millele poleks olnud võimalik testida loodud lahendust. Lisaks tagab enda loodud keskkond täielikud administratiivsed õigused kasutatavas taristus, mida kooli infrastruktuuri poolt poleks turvalisuse kaalutlustel võimaldatud. Virtualiseerimiseks oli võimalik kasutada mitut erinevat platvormi nii VMware Player kui ka Oracle VM Virtualboxi. Mõlemad platvormid täidavad testkeskkonna loomiseks kõiki nõudeid. Autor otsustas kasutada Oracle VM Virtualboxi kasutusharjumuse tõttu.

Virtuaalmasinate loomisel kasutas autor sama versiooniga operatsioonisüsteeme nagu on kasutusel IT Kolledžis, et vältida võimalikke versioonist tulevaid erisusi. Domeenikontrolleris keskenduti rollide valikul ainult hädavajalikule, mis võimaldaks klientarvutid domeeniga liita ja kasutada *Kerberose* autentimist. Lisaks võeti arvesse diplomitöö peatükis 6.1 kirjeldatud tehnilist käiku. Peatükis 6.1 kirjeldatud tehnilised seadistused on eelduseks, et ID-kaardiga sisselogimine toimiks Windows 10 domeeni arvutis. Kuigi diplomitöö ei keskendu ID-kaardiga sisselogimisele Windows 10 operatsioonisüsteemis, oli antud test vajalik, et kontrollida domeenikontrolleri võimekust lubada ID-kaardiga sisselogimist. Testi käigus selgus, et domeeni kasutaja sidumine kasutaja sertifikaadiga on korrektne ning domeenikontroller on õigesti seadistatud võimaldamaks sisselogimist ID-kaardiga. Lisaks sai autor testides eelduse, millele peaks keskenduma Ubuntu operatsioonisüsteemis võimaldamaks ID-kaardiga sisselogimist domeeni kasutajaga. Eeldus Ubuntus ID-kaarti kasutada, oli paigaldada Eesti ID-kaardi

tarkvara. Testkeskkond tekitas autorile eelduse diplomitöös käsitlevale probleemile lahenduse leidmiseks.

8.2 Lahenduse analüüüs

Diplomitöö autor kasutas kiipkaardiga sisselogimiseks Ubuntus *Kerberos 5* protokolli domeenikontrolleriga autentimiseks. *Kerberos 5* protokollile on ülesse ehitatud ka kiipkaardiga sisselogimine Windowsi operatsioonisüsteemis.[20] Autoril oli kaks valikut millise rakenduse põhjal kiipkaardiga sisselogimine seadistada, kas *CoolKey* või *OpenSC*. Kuna uued kiipkaardid toetavad pigem *OpenSC* rakendust, otsustas autor lahenduse leidmiseks jätkata *OpenSC-d* kasutades.[21] Lisaks on *OpenSC* rakendus kasutusel Eesti ID-kaardi tarkvara poolt Ubuntu operatsioonisüsteemis.[14] Autor võttis inspiratsiooni lahenduse väljatöötamisel mujal maailmas kasutusel olevast populaarsest kiipkaardist Yubikey. Yubikey on üks kiipkaartidest, mille arendusel on pööratud rõhku ka Linuxi operatsioonisüsteemidele. Yubikey kui kiipkaardi (Yubikey PIV) funktsionaalsus on sarnane Eesti ID-kaardile. Mõlemad kaardid toetavad *PKCS#11* standardit ja *ECC p-384bit* krüpteeringut. Lisaks on mõlemad kiipkaardid toetatud *OpenSC* rakenduse poolt.

Kasutatav juhend võttis kiipkaardiga sisselogimise loogika vastu domeenikontrollerit kokku, juhendis kirjeldatud juhised tuli muuta vastavalt ID-kaardi eripäradele.[15] Oluline erinevus ID-kaardi ja juhendis kasutatava Yubikey vahel olid sertifikaadid. Yubikey puhul, olid sertifikaadid seotud domeenikontrolleriga, ID-kaardi puhul on sertifikaadid väljastatud Sertifitseerimiskeskuse poolt. Võrreldes Windowsi ja Ubuntu domeeni arvutit, siis Ubuntu puhul *Kerberose* autentimine ilma ID-kaardi juursertifikaadi lisamiseta *NTAuthStore* ei õnnestunud. Windowsi domeeni arvutid kasutavad *Kerberose Ticketi* küsimisel domeeni autoriseerimise-sertifikaati, mida usaldab iga Windowsi domeeni masin. Windowsi domeenikontrolleriga pole Ubuntu operatsioonisüsteemis veel vaikimisi domeeniga sidumist ja kiipkaardiga autentimist sisse ehitatud. Ubuntu 21.04 versioonis on juba Windows domeeniga sidumine ilma eripakette kasutamata võimaldatud. Loodame, et sellele lisanduvad kõikvõimalikud Windowsis vaikimisi võimaldatud sisselogimise võimalused.[22]

Diplomitöö autori arvates ühtlustas loodud lahendus Windowsi ja Ubuntu domeeni arvuteid, andes kasutajale mõlema operatsioonisüsteemi puhul võimaluse kasutada turvalist sisselogimise võimalust. Kuna peale sisselogimist on ID-kaart juba kiipkaardi lugejas, muutuvad erinevate finants, tervishoiu või riiklike e-teenuste kasutamine samuti mugavamaks. Kui varem pidi kasutaja Ubuntu arvutis otsima välja ID-kaardi või kasutama mõnda mugavusteenust nagu Mobiil-ID või Smart-ID, siis nüüd on kõik turvaliselt ainult PIN koodi kaugusel.

9. Kokkuvõte

Käesoleva diplomitöö eesmärk oli luua prototüüp võimaldamaks domeeni kasutajaga sisse logida Windows domeeni kuuluvatesse Ubuntu arvutitesse kasutades Eesti ID-kaarti.

Diplomitöös lahendatavaks probleemiks oli lahenduse puudumine, mis võimaldaks sisse logida Windows domeenis olevasse Ubuntu arvutisse domeeni kasutajaga kasutades Eesti ID-kaarti.

Prototüübi loomisel oli seatud nõue, et loodud lahendus oleks rakendatav IT Kolledžis. Autor uuris ning analüüsis prototüübi loomiseks kolledžis kasutuselolevate operatsioonisüsteemide seoseid Windows domeeni ja ID-kaardiga. Lisaks viidi läbi küsitlus IT Kolledži tudengite seas, selgitamaks välja huvi loodud lahenduse vastu.

Diplomitöös kirjeldati prototüübi loomise ja seadistamise etappe. Diplomitöö praktiline osa on dokumentatsiooniks IT Kolledžis diplomitöös loodud lahenduse rakendamiseks.

Diplomitöö tulemusena loodi lahendus, mis võimaldab domeeni kasutajaga sisse logida Windows domeeni kuuluvasse Ubuntu arvutisse kasutades Eesti ID-kaarti.

Kasutatud kirjandus

[1] Politsei- ja piirivalveamet *Isikut tõendavad dokumendid*. [WWW] https://www2.politsei.ee/et/teenused/isikut-toendavad-dokumendid/ (08.05.2021).

[2] NIST *Back to basics: Multi-factor authentication (MFA)*. [WWW] https://www.nist.gov/itl/applied-cybersecurity/tig/back-basics-multi-factor-authentication
(06.05.2021).

[3] McDermott, M. *Why Multi-Factor Authentication (MFA) Is a Must-Have in the Microsoft World and Beyond*. [WWW] https://spanning.com/blog/why-multi-factor-authentication-is-a-must-have/ (07.05.2021).

[4] Vanem, U. *EID kaardiga Windows domeeni logimine*. [WWW] https://www.id.ee/wpcontent/uploads/2020
/01/1901__ID$_k aardi_login_Windows_domeenis.pdf(20.04.2021)$.

[5] Micrsoft Docs *Validate and Configure Public Key Infrastructure*. [WWW] https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-cert-trust-validate-pki
(24.04.2021).

[6] SK ID Solutions AS *SK sertifikaadid*. [WWW] https://www.skidsolutions.eu/repositoorium/sk-sertifikaadid/ (20.04.2021).

[7] SK ID Solutions AS *ESTEID LDAP kataloogi kasutamine*. [WWW] https://www.skidsolutions.eu/repositoorium/ldap/esteid-ldap-kataloogi-kasutamine
(20.04.2021).

[8] Mutaj J. *Join Ubuntu 20.04\18.04 / Debian 10 To Active Directory (AD) domain*. [WWW] https://computingforgeeks.com/join-ubuntu-debian-to-active-directory-ad-domain/ (23.04.2021).

[9] eID rakendusjuhend *eID kasutamine olemasolevate rakendustega*. [WWW] https://eid.eesti.ee/index.php/EID$_k asutamine_olemasolevate_rakendustega\#ID-kaardiga_sisselogimine_Linuxisse(30.04.2021)$.

[10] Oracle *Download VirtualBox (Old Builds): VirtualBox 6.0*. [WWW] https://www.virtualbox.org/wiki/Download$_O ld_B uilds_{60}(20.04.2021)$.

[11] Microsoft Docs *Install Active Directory Domain Services (Level 100)*. [WWW] https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/deploy/install-active-directory-domain-services–level-100-
(24.04.2021).

[12] Microsoft Docs *Add-Computer*. [WWW] https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.management/add-computer?view=powershell-5.1
(23.04.2021).

[13] RIA *ID-tarkvara toetatud operatsioonisüsteemid*. [WWW] https://www.id.ee/artikkel/id-tarkvara-toetatud-operatsioonisusteemid/
(25.04.2021).

[14] RIA *Ubuntu: ID-tarkvara paigaldamine, uuendamine ja eemaldamine*. [WWW] https://www.id.ee/artikkel/ubuntu-id-tarkvara-paigaldamine-uuendamine-ja-eemaldamine/
(25.04.2021).

[15] Tim *Linux – Enable Smartcard Authentication Against Active Directory and generate TGT using PKINIT*. [WWW] https://scriptech.io/linux-enable-smartcard-authentication-against-active-directory-and-generate-tgt-using-pkinit/
(2.05.2021).

[16] Debian wiki *Common Access Card (CAC)*. [WWW] https://wiki.debian.org/Common%20Access%20Card%20%28CAC%29
(07.05.2021).

[17] Microsoft Docs *How to import third-party certification authority (CA) certificates into the Enterprise NTAuth store*. [WWW] https://docs.microsoft.com/en-us/troubleshoot/windows-server/windows-security/import-third-party-ca-to-enterprise-ntauth-store
(03.05.2021).

[18] SK ID Solutions AS *SK sertifitseerimishierarhia ülevaade*. [WWW] https://www.skidsolutions.eu/repositoorium/ (07.05.2021).

[19] Soualem N. *Sssd.conf - the configuration file for SSSD*. [WWW] https://www.math-linux.com/man/man5/sssd.conf.5.html (05.05.2021).

[20] Microsoft Docs *Windows Authentication Overview*. [WWW] https://docs.microsoft.com/en-us/windows-server/security/windows-authentication/windows-authentication-overview
(01.05.2021).

[21] Red Hat. *Smart Card support in RHEL8*. [WWW] https://access.redhat.com/articles/4253861 (03.05.2021).

[22] Canonical Ltd. *Ubuntu 21.04 is here*. [WWW] https://ubuntu.com/blog/ubuntu-21-04-is-here (07.05.2021).

Lisa 1. Lihtlitsents

Mina, Martin Abel

1. Annan Tallinna Tehnikaülikoolile tasuta loa (lihtlitsentsi) enda loodud teose "WINDOWS ACTIVE DIRECTORY KASUTAJAGA SISSELOGIMINE LINUX KLIENTARVUTISSE EESTI ID-KAARDIGA" , mille juhendaja on Edmund Laugasson,
   1.1. reprodutseerimiseks lõputöö säilitamise ja elektroonse avaldamise eesmärgil, sh Tallinna Tehnikaülikooli raamatukogu digikogusse lisamise eesmärgil kuni autoriõiguse kehtivuse tähtaja lõppemiseni;
   1.2. üldsusele kättesaadavaks tegemiseks Tallinna Tehnikaülikooli veebikeskkonna kaudu, sealhulgas Tallinna Tehnikaülikooli raamatukogu digikogu kaudu kuni autoriõiguse kehtivuse tähtaja lõppemiseni.
2. Olen teadlik, et käesoleva lihtlitsentsi punktis 1 nimetatud õigused jäävad alles ka autorile.
3. Kinnitan, et lihtlitsentsi andmisega ei rikuta teiste isikute intellektuaalomandi ega isikuandmete kaitse seadusest ning muudest õigusaktidest tulenevaid õigusi.

17.05.2021