Opinnäytetyö (AMK)

Tieto- ja viestintätekniikka

2022

Eriksson Jesper

TL-III luokiteltu yksittäistyöasema

TURKU AMK
TURKU UNIVERSITY OF
APPLIED SCIENCES

Opinnäytetyö (AMK) | Tiivistelmä

Turun ammattikorkeakoulu

Tieto- ja viestintätekniikka

2022 | 31 sivua

Jesper Eriksson

TL-III luokiteltu yksittäistyöasema

Suomessa liikenne- ja viestintävirasto (Traficom) toimii kansallisena tietoturvaviranomaisena ja vastaa turvaluokitellun tiedon sähköiseen tiedonsiirtoon ja -käsittelyyn liittyvistä turvallisuusasioista, arvioinneista ja hyväksynnöistä. Traficom käyttää auditoinneissa siihen luotua dokumenttia nimeltään Katakri. Katakri on tietoturvallisuuden auditointityökalu viranomaisille.

Combitech Oy tarvitsi TL-III luokitellun yksittäistyöaseman, jolla voidaan käsitellä turvaluokiteltua materiaalia työnteossa. Tavoitteena oli suunnitella ja kehittää TL-III hyväksytty työasema, jota pystytään käyttämään turvaluokitellun materiaalin käsittelemiseen aina tarpeen vaatiessa.

Työasemana toimii Windows 10 käyttöjärjestelmällä varusteltu kannettava tietokone, johon laitettiin Katakrin mukaisesti TL-III vaadittuja kovennuksia fyysisellä ja ohjelmistotasolla. Työasema toimii omassa suljetussa offline-ympäristössä, ja siitä on poistettu kaikki mahdolliset tietoliikenneyhteydet.

Työaseman konfiguroinnissa noudatettiin sekä Katakrin että myös yrityksen tietoturva- ja käyttöpolitiikkaa. Lopputuloksena saatiin luotua työasema, joka täytti TL-III turvaluokituksen vaatimukset.

Asiasanat:

turvaluokitus, turvaluokiteltu, Traficom, Katakri, Windows, järjestelmänhallinta

Bachelor’s Thesis | Abstract

Turku University of Applied Sciences

Information and Communications Technology

2022 | 31 pages

Jesper Eriksson

Designing and developing a classified standalone workstation

In Finland, the Finnish Transport and Communications Agency (Traficom) acts as the national information security authority and is responsible for security issues, assessments and approvals related to the electronic transmission and processing of classified information. For audits, Traficom uses a document created for this purpose called Katakri. Katakri stands for Information Security Auditing Tool for Authorities.

Combitech Ltd needed a classified single workstation that could handle classified material in the workplace. The objective of this thesis was to design and develop a classification-approved workstation that could be used to handle classified material whenever required.

The workstation was a laptop with Windows 10 operating system, on which the classified physical and software hardening required by Katakri was applied. The workstation operates in its own closed offline environment with all possible communication connections removed.

The workstation was configured in accordance with both Katakri and the company's security and access policy. The result was a workstation that met the requirements of classified security classification.

Keywords:

security classification, security classified, Traficom, Katakri, Windows, system management

Sisältö

Sisällys

Kuvat

Taulukot

Käytetyt lyhenteet ja sanasto

2FA	Two-Factor Authentication, kaksivaiheinen todennus
Absolute	Mukautuva päätepisteiden suojausratkaisu
BIOS	Basic Input-Output System, tietokoneen laiteohjelmisto
BIOSConnect	Dellin ohjelmisto, jolla voidaan palauttaa tietokoneen palautusosio hyödyntäen Dellin verkkopohjaisia palautuspalveluita
CHIPSET	Prosessorin piirisarja
Katakri	Tietoturvallisuuden auditointityökalu viranomaisille
MFA	Multi-Factor Authentication, monivaiheinen todennus
NFC	Near-field communication, lähitunnistustekniikkaa hyödyntävä tiedonsiirtotekniikka
TL-III	Turvallisuusluokka III
TL-IV	Turvallisuusluokka IV
Traficom	Liikenne- ja viestintävirasto
U2F	Universal 2nd factor, monivaiheisen todennuksen avoin standardi
USB	Universal Serial Bus, sarjaväyläarkkitehtuuri
Vahti	Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmä
Wi-Fi	Wireless network protocol, langattoman verkon protokolla

1 Johdanto

Turvaluokiteltu materiaali on informaatiota, jota pystyvät käsitteleмään vain siihen valtuutetut henkilöt ja materiaalia voidaan käsitellä vain siihen hyväksytyillä menetelmillä. Suomessa turvaluokitetulle materiaalille voidaan asettaa eri tasoisia turvaluokituksia, jotka määrittelevät salassa pidettävän tiedon vaatimukset ja määräykset. Liikenne- ja viestintävirasto (Traficom) asettaa vaatimukset ja määräykset Suomessa käytettäville turvaluokituksille.

Combitech Oy -yrityksellä oli tarve TL-III luokitellulle yksittäistyöasemalle, jolla pystytään käsittelemään TL-III ja TL-IV luokiteltua materiaalia. Yksittäistyöaseman idea oli tarjota ratkaisua tilanteisiin, joissa työntekijällä tai asiakkaalla on tarve tietokoneelle, jolla pystytään käsittelemään turvaluokiteltua materiaalia, silloin kun heillä ei ole käytössä omaa työasemaa, jolla kyseisen turvaluokituksen materiaaleja pystytään käsittelemään.

Toimeksiantaja antoi projektiin vaatimukset ja ohjeet, joita noudattaen projektia lähdettiin suunnittelemaan ja toteuttamaan. Projekti alkoi suunnitteluvaiheella, jossa suunniteltiin työasemaan tulevat kovennukset sekä muut yksityiskohdat, kuten ohjelmistot. Suunnitteluvaiheessa otettiin selvää erilaisista ratkaisuista, joita projektissa voitaisiin käyttää, ja vertailtiin niitä toisiinsa. Vertailun jälkeen päädyttiin ratkaisuun ja ehdotettiin näitä ratkaisuja toimeksiantajalle.

Toteutusvaiheessa työasemaan asennettiin kaikki tarvittavat kovennukset ja ohjelmistot sekä testattiin kovennuksien toiminnallisuus. Toteutusvaiheessa oli myös mahdollista perehtyä tarkemmin käytettäviin ohjelmiin ja menetelmiin. Projektissa saatiin konsultoida yrityksen tietoturva-asiantuntijoita ja käyttää Katakrin auditointidokumentointia.

Opinnäytetyön tavoite oli saada yritykselle toimiva ratkaisu turvaluokitellun materiaalin käsittelyyn joustavasti sekä tutustua ja oppia tietoturvaluokitellun ympäristön toiminnasta ja rakentamisesta.

2 Työasema

2.1 Valmistelu

Työasemaksi valikoitui yrityksen käytössä oleva kannettava tietokone, joka sopi projektin vaatimuksiin. Tietokoneita tarjolla oli useita erilaisia, joista projektissa käytettävä kone valikoitui sen koon, teknisten ominaisuuksien ja huollettavuuden ansiosta. Tietokone on Microsoftin Windows 10 -käyttöjärjestelmällä toimiva tietokone, johon laitettiin fyysisen ja ohjelmistotason kovennuksia sekä riisutumpi käyttöjärjestelmä.

2.2 BIOS-kovennukset

Ensimmäisenä tietokoneen BIOS -asetuksia kovennettiin Katakrin ja yrityksen oman tietoturvapolitiikan mukaan, jotta ne vastaavat Katakrin [1] mukaista TL-III tason määritelmää alla olevalla lainauksessa.

> Käyttöön on otettu vain käyttövaatimusten ja tietojen käsittelyn kannalta olennaiset toiminnot, laitteet ja palvelut.
>
> Käytössä on menettelytapa, jolla järjestelmät asennetaan järjestelmällisesti siten, että lopputuloksena on kovennettu asennus.
>
> Kovennettu asennus sisältää vain sellaiset komponentit ja palvelut, sekä käyttäjien ja prosessien oikeudet, jotka ovat välttämättömiä toimintavaatimusten täyttämiseksi ja turvallisuuden varmistamiseksi. [1].

BIOS -asetuksista poistettiin käytöstä kaikki epäolennaiset toiminnot ja valmistajan valmiit ohjelmistot, jotka eivät ole tarpeellisia tietokoneen toiminnalle. Tällaisia toimintoja olivat esimerkiksi Absolute, BIOSConnect, Wifi ja Bluetooth. BIOS-asetuksiin myös asetettiin vahva salasana yrityksen salasanapolitiikan mukaan, jotta näitä kovennuksia ei pääse muuttamaan henkilöt, joilla ei näihin ole oikeutta.

2.3 Asentaminen

Tietokoneen käyttöjärjestelmän asennuksessa käytettiin räätälöityä Windows 10 -versiota, josta oli poistettu kaikki tarpeettomat ominaisuudet ja sovellukset. Asennusmedia täytyi erikseen luoda käyttäen Microsoftin omia työkaluja ja tämän jälkeen siitä erikseen siivottiin kaikki turhat ohjelmat ja sovellukset pois, joita työasemassa ei tulla käyttämään. Ohjelmien ja ominaisuuksien poistokriteereinä käytettiin yrityksen ja Katakrin tietoturvapolitiikkaa.

> Ylimääräiset palvelut, sovellukset, yhteydet (myös BIOS-tasolla) ja laitteet on poistettu. [1].

Asennusmedian siivoamisen jälkeen työasemaan asennettiin normaalisti Windows 10 -käyttöjärjestelmä. Asennuksen yhteydessä työasemaan luotiin väliaikainen käyttäjätunnus, jota käytettiin työaseman ohjelmistojen ja laiteajurien asentamisen ajan. Väliaikainen käyttäjä poistettiin siinä vaiheessa, kun käyttöön otettiin järjestelmänvalvojatunnus.

> Kaikkien käyttäjätunnusten osalta on huolehdittava tunnusten elinkaaresta siten, että vain tarpeelliset tunnukset ovat voimassa ja aktiivisia ja tarpeettomat käyttäjätunnukset poistetaan välittömästi. [1].

Myöhemmässä vaiheessa työasemaan luodaan jokaiselle käyttäjälle omat tunnukset ja varmenteet, jotta pystytään toimimaan Katakrin vaatimusten mukaisesti.

> Henkilöiden tunnistaminen:
>
> Käytössä on yksilölliset henkilökohtaiset käyttäjätunnisteet.
>
> Kaikki käyttäjät tunnistetaan ja todennetaan.
>
> Tunnistamisessa ja todennuksessa käytetään tunnettua ja turvallisena pidettyä tekniikkaa tai se on muuten järjestetty luotettavasti. [1].

2.4 Laitteistopäivitykset

Laiteajurit tai laiteohjaimet ovat ohjelmistoja, jotka ohjaavat tietokoneen laitteiden toimintaa. Erilaisia laiteohjaimia on esimerkiksi tietokoneen verkkokorteille, näytönohjaimille, äänikorteille, BIOSille, oheislaitteille sekä monille muille eri komponenteille.

Jotta tietokone pysyy toiminnallisesti parhaassa mahdollisessa kunnossa, siihen haettiin valmistajan sivuilta uusimmat ajuripäivitykset. Tärkeimpinä päivityksinä voidaan mainita BIOS ja CHIPSET -päivitykset, jotka korjaavat mahdollisia haavoittuvuuksia tietokoneen BIOS -tasolla. Myös muita koneen toiminnalle tärkeitä ajureita asennettiin tietokoneeseen. Näin pystytään varmistamaan, että kaikki tarvittavat toiminnot ja oheislaitteet, esimerkiksi telakat, ääni ja USB laitteet toimivat moitteettomasti. Laitteistopäivitysten uusimmat versiot usein myös pitävät sisällään korjauksia vanhojen versioiden tiedossa oleviin haavoittuvuuksiin.

Työasemaan asenettiin myös muutama valikoitu ohjelma, joita katsottiin tarvittavan esimerkiksi dokumenttien käsittelyyn, hallintaan ja muokkaamiseen. Ohjelmissa pyrittiin pysymään mahdollisimman vähässä määrässä, jotta koneessa on asennettuna vain tarvittavat ohjelmat, eikä mitään muuta.

> Ohjelmistot (esim. laiteohjelmistot, sovellukset) pidetään ajantasaisina (vrt. I-19). [1].

2.5 Lokaalit asetukset

2.5.1 Käyttäjätunnukset

Tietokoneeseen asetettiin administrator-käyttäjä, jota voidaan käyttää oikeuksien korottamiseen. Tämän käyttäjän ideana myös on, että sillä pystytään hallinnoimaan muita käyttäjiä tietokoneessa lokaalisti. Administrator-käyttäjälle asetettiin uniikki salasana yrityksen salasanapolitiikan mukaisesti.

> Oletussalasanat on vaihdettu organisaation salasanapolitiikan mukaisiin laadukkaisiin salasanoihin. Salasanoja säilytetään siten, että salasanat ovat suojattuna sekä saatavilla. [1].

Tietokonetta tulee käyttämään useampi käyttäjä kovennetuilla säännöillä, mutta ne täytyy erikseen luoda. Jokaiselle käyttäjälle luodaan omat käyttäjätunnukset ja niihin omat kaksivaiheiset todennukset Katakrin mukaisesti.

> Käytössä on yksilölliset henkilökohtaiset käyttäjätunnisteet.
>
> Kaikki käyttäjät tunnistetaan ja todennetaan.
>
> Tunnistamisessa ja todennuksessa käytetään tunnettua ja turvallisena pidettyä tekniikkaa tai se on muuten järjestetty luotettavasti.
>
> Tunnistuksen epäonnistuminen liian monta kertaa peräkkäin aiheuttaa tunnuksen lukittumisen.
>
> Järjestelmien ja sovellusten ylläpitotunnukset ovat henkilökohtaisia. Mikäli tämä ei kaikissa järjestelmissä tai sovelluksissa ole teknisesti mahdollista, edellytetään sovitut, dokumentoidut ja käyttäjän yksilöinnin mahdollistavat hallintakäytännöt yhteiskäyttöisille tunnuksille (vrt. hallintayhteydet ja erityisesti hyppykonekäytännöt, I-04, sekä jäljitettävyyden toteuttaminen, I-10).
>
> Edellytetään vahvaa, vähintään kahteen tekijään perustuvaa käyttäjätunnistusta. [1].

Koska kyseessä on opinnäytetyö ja tietokone ei tullut vielä aktiiviseen käyttöön, luotiin tietokoneeseen kaksi testikäyttäjää, joille myös myöhemmin asetettiin tunnistautumisvarmenteena YubiKey 2FA-avain. Näitä käyttäjiä käytettiin myöhemmin myös työaseman demoamiseen ja auditointiin.

2.5.2 Verkkoyhteyksien kovennukset

Verkkoliikenteen kovennukset tehtiin ns. kahdella eri tasolla. Kaikki verkkoliikenne estettiin koneeseen tietokoneen omaa palomuuria käyttäen. Windows Defender Firewall-asetuksista pystyttiin luomaan omat säännöt, jotka estävät tietokoneesta kaikki lähtevät ja saapuvat liikenteet. Sääntöjen laittamisen jälkeen niitä myös testattiin Windows PowerShell -ohjelmalla ajamalla komento ”*netstat -abf 5 > activity.txt*”. Kyseinen komento ajaa Netstat-ohjelman parametreilla -a, -b ja -f.

Taulukko 1. Netstatin parametrit [2].

-a	This switch displays active TCP connections, TCP connections with the listening state, as well as UDP ports that are being listened to.
-b	This netstat switch is very similar to the **-o** switch listed below, but instead of displaying the PID, will display the process's actual file name. Using **-b** over **-o** might seem like it's saving you a step or two but using it can sometimes greatly extend the time it takes netstat to fully execute.
-e	Use this switch with the netstat command to show statistics about your network connection. This data includes bytes, unicast packets, non-unicast packets, discards, errors, and unknown protocols received and sent since the connection was established.
-f	The **-f** switch will force the netstat command to display the Fully Qualified Domain Name (FQDN) for each foreign IP addresses when possible.

Testin jälkeen avattiin Netstatin luoma lokitiedosto, josta pystyttiin todentamaan, että tietokone ei pystynyt ottamaan minkäänlaista yhteyttä internetiin.

```
Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            Computer:0             LISTENING
  RpcSs
 [svchost.exe]
  TCP    0.0.0.0:445            Computer:0             LISTENING
 Can not obtain ownership information
  TCP    0.0.0.0:623            Computer:0             LISTENING
 [LMS.exe]
  TCP    0.0.0.0:3389           Computer:0             LISTENING
  TermService
 [svchost.exe]
  TCP    0.0.0.0:5040           Computer:0             LISTENING
  CDPSvc
 [svchost.exe]
  TCP    0.0.0.0:16992          Computer:0             LISTENING
 [LMS.exe]
  TCP    0.0.0.0:49664          Computer:0             LISTENING
 [lsass.exe]
  TCP    0.0.0.0:49665          Computer:0             LISTENING
 Can not obtain ownership information
  TCP    0.0.0.0:49666          Computer:0             LISTENING
  Schedule
 [svchost.exe]
  TCP    0.0.0.0:49667          Computer:0             LISTENING
  EventLog
 [svchost.exe]
  TCP    0.0.0.0:49668          Computer:0             LISTENING
  SessionEnv
 [svchost.exe]
  TCP    0.0.0.0:49669          Computer:0             LISTENING
 [spoolsv.exe]
  TCP    0.0.0.0:49671          Computer:0             LISTENING
 Can not obtain ownership information
  TCP    127.0.0.1:49672        Computer:0             LISTENING
 [LMS.exe]
  TCP    127.0.0.1:49673        Computer:49674         ESTABLISHED
```

Kuva 1. Esimerkkikuva Netstat-komennon lokitiedostosta

Tämän jälkeen tietokoneen verkkoadapterit otettiin kokonaan pois käytöstä muuttamalla koneen verkkoadapteriasetuksia. Tietokoneessa valmistajalta tullessa oli langaton verkkokortti, jossa oli Wi-Fi ja Bluetooth yhteydet. Tämä kortti irrotettiin tietokoneesta pois valmisteluvaiheessa, sillä tietokoneessa ei käytetty ollenkaan langattomia yhteyksiä

2.5.3 Fyysisten porttien kovennukset

Koska tiedonsiirto työasemaan tapahtuu USB-massamuistien kautta, täytyy työasemasta estää kaikki ei-valtuutetut USB-laitteet. Työasemaan ”valtuutetaan” vain hyväksytyt laitteet, jolloin tietokone ei ns. tunnista ei-valtuutettuja laitteita, kun ne kytketään USB-porttiin. USB-porttien koventaminen tapahtui lokaalien ryhmäkäytäntöjen säännöillä. Luotiin sääntö, joka estää kaikki USB-laitteet ja tämän jälkeen vain tarvittavia USB-laitteita hyväksytään. Näin pystytään täyttämään Katakrin asettamat USB-portteja koskevat kriteerit.

> USB-porttien ja vastaavien liityntöjen käytön tapauskohtaisiin ehtoihin voi sisältyä esimerkiksi, että järjestelmään voi kytkeä vain erikseen määritettyjä luotettavaksi todennettuja muistitikkuja (ja vastaavia), joita ei kytketä mihinkään muuhun järjestelmään. [1].

2.5.4 Ryhmäkäytäntö

Group policy eli ryhmäkäytäntö on Microsoft Windowsin ominaisuus, jolla pystytään ohjaamaan käyttäjätilien toiminnallisuutta ja oikeuksia. Koska yrityksellä oli jo käytössä Active Directory-ympäristössä Katakrin mukaisesti kovennettu TL-III hyväksytty ryhmäkäytäntö, pystyttiin sitä myös hyödyntämään tässä työasemassa. Ryhmäkäytäntö pystyttiin hakemaan yrityksen verkosta ja tuomaan työasemalle. Ryhmäkäytännön tuonnissa käytettiin Microsoftin LGPO-ohjelmaa, jolla pystytään ns. ajamaan säännöt suoraan laitteeseen.

> Asetusten tuominen paikalliseen ryhmäkäytäntöön GPO-varmuuskopioista tai yksittäisistä käytäntökomponenttitiedostoista, mukaan lukien rekisterikäytäntö (registry.pol), tietoturvamallit ja laajennetun valvonnan CSV-tiedostot.*(suomennettu.)*. [3]

Ryhmäkäytännön pystyi asentamaan työasemalle yrityksen TL-III ympäristöstä haetusta varmuuskopiosta ajamalla komento: *%PATH%\LGPO\LGPO_30 /v /g %PATH%\tiedostonimi,* komennossa käytettiin parametreja:

/g Import settings from one or more Group Policy backups anywhere

/v Verbose output.

2.5.5 Kaksivaiheinen tunnistautuminen

Työasemaan vaaditaan käyttöön kaksivaiheista tunnistautumista, jotta se tulee olemaan Katakrin TL-III standardien mukainen. Kaksivaiheisen tunnistautumisen ratkaisuna käytettiin YubiKey-turva-avainta, joilla käyttäjät todentavat henkilöllisyytensä työasemaan kirjautuessa. Jokaiselle käyttäjälle ohjelmoidaan henkilökohtainen avain ja avaimia pystytään hallinnoimaan työasemasta administrator-käyttäjällä. Kaksivaiheisessa tunnistautumisessa käytetään Katakrin antamia vaatimuksia.

> Henkilöiden tunnistaminen:
> 1. Käytössä on yksilölliset henkilökohtaiset käyttäjätunnisteet.
> 2. Kaikki käyttäjät tunnistetaan ja todennetaan.
> 3. Tunnistamisessa ja todennuksessa käytetään tunnettua ja turvallisena pidettyä tekniikkaa tai se on muuten järjestetty luotettavasti.
> 4. Tunnistuksen epäonnistuminen liian monta kertaa peräkkäin aiheuttaa tunnuksen lukittumisen.
> 5. Järjestelmien ja sovellusten ylläpitotunnukset ovat henkilökohtaisia. Mikäli tämä ei kaikissa järjestelmissä tai sovelluksissa ole teknisesti mahdollista, edellytetään sovitut, dokumentoidut ja käyttäjän yksilöinnin mahdollistavat hallintakäytännöt yhteiskäyttöisille tunnuksille (vrt. hallintayhteydet ja erityisesti hyppykonekäytännöt, I-04, sekä jäljitettävyyden toteuttaminen, I-10).
> 6. Todennus tehdään vähintään salasanaa käyttäen. Mikäli käytetään salasanatodennusta, a) käyttäjiä on ohjeistettu hyvästä turvallisuuskäytännöstä salasanan valinnassa ja käytössä, b) käyttöä valvova ohjelmisto asettaa salasanalle tietyt turvallisuuden vähimmäisvaatimukset ja pakottaa salasanan vaihdon sopivin

määräajoin. Salasanan vaihdon sopiva määräaika tulee suhteuttaa organisaation toimintaympäristön ja laitteessa käsiteltävän ja säilytettävän turvallisuusluokitellun tiedon luokituksen mukaan, muut turvallisuusratkaisut huomioiden.

Laitteiden tunnistaminen:
7. Turvallisuusluokitellun tiedon käsittelyyn käytetään vain organisaation tarjoamia ja hallinnoimia, kyseiselle turvallisuusluokalle hyväksyttyjä päätelaitteita. Kaikkien muiden laitteiden kytkeminen turvallisuusluokitellun tiedon käsittely-ympäristöön on yksiselitteisesti kielletty. Henkilöstö on ohjeistettu ja velvoitettu toimimaan ohjeistuksen mukaisesti.

Tietojärjestelmien tunnistaminen:
8. Tietoa keskenään vaihtavat tietojärjestelmät tunnistetaan käyttötapaukseen soveltuvalla tekniikalla, kuten salasanoilla, avaimilla (esim. API-avain), tunnistevälineillä (tokeneilla, esim. oAuth) tai vastaavilla menetelmillä. Tunnistautuminen tehdään salattuja yhteyksiä pitkin.

Turvallisuusluokkien III-II käsittely-ympäristöissä vaatimus voidaan täyttää siten, että kohtien 1–5 ja 7–8 lisäksi toteutetaan seuraavat toimenpiteet:
9. Edellytetään vahvaa, vähintään kahteen tekijään perustuvaa käyttäjätunnistusta. [1].

3 YubiKey

3.1 Yubico ja Yubikey

Yubico on vuonna 2007 Ruotsissa perustettu tietoturva-alan yritys, joka erikoistuu kaksivaiheisen todennuksen ratkaisuihin. Yubico on palkittu maailmanlaajuisesti yrityksen kaksivaiheisen todennuksensa ratkaisuista sekä innovatiivisuuksista tietoturva-alalla. [4]. Yubico on erityisesti tunnettu YubiKey -turva-avaimista, joita voidaan käyttää kaksivaiheisessa tunnistautumisessa.

YubiKey on Yubico-yrityksen luoma fyysinen avain, jota voidaan käyttää niin fyysisellä, kuin myös ohjelmistotasolla kaksivaiheisena tunnistautumisena. Ensimmäinen YubiKey-avain (YubiKey 1.0) julkaistiin vuonna 2008 Security Now-nimisessä podcastissa.

> YubiKey 1.0 lanseerataan Security Now -podcastissa kaksi viikkoa sen jälkeen, kun Stina tapaa podcastin isännän Steve Gibsonin liukuportaiden yläpäässä RSA-konferenssissa San Franciscossa.(suomennettu.) [5].

Siitä eteenpäin Yubico on kehitellyt uusia versioita avaimista, joihin on tuotu uusia ominaisuuksia ja paranneltu tietoturva-salauksia. YubiKey-avaimiin on myös tuotu ominaisuuksia, joiden ansiosta niitä pystytään käyttämään eri yrityksien verkkopalveluissa, esimerkiksi U2F kaksivaiheista standardia käyttää mm. Google, Facebook, Dropbox sekä GitHub.

> 2014 - Google ottaa käyttöön tuen U2F-turva-avaimille Gmailissa ja Chromessa.(suomennettu.)
>
> 2015 - Dropbox ja GitHub ottavat käyttöön tuen FIDO U2F -turva-avaimille, ja GitHubin käyttäjäyhteisö äänestää FIDO U2F -tuen Firefoxin halutuimmaksi ominaisuudeksi.(suomennettu.)
>
> 2017 - Facebook ottaa käyttöön U2F-tuen.(suomennettu.) [5].

3.2 YubiKey 5 NFC

Yubicolla on useampia erilaisia YubiKey-malleja, joita he valmistavat ja niistä työasemassa käytettäväksi valikoitui YubiKey 5 NFC-malli. YubiKey toimii kirjautumisessa lisävarmenteena käyttäjätunnuksen ja salasanan lisäksi. YubiKey 5 NFC valikoitui sen hyvien ominaisuuksien sekä sopivan hinnan mukaan käytettäväksi työasemissa.

YubiKey 5 NFC tukee FIDO2-applikaatiota, jota pystytään käyttämään Windows 10:en kirjautumisessa 2FA-ratkaisuna. Se tukee useampaa kryptograafista spesifikaatiota: RSA 2048, RSA 4096 (PGP), ECC p256, ECC p384. [6]. Avaimessa on IP68-luokitus eikä se tarvitse pattereita toimiakseen. YubiKey 5 NFC -avaimen hinta kuluttajille on noin 60 euroa kirjoittamishetkellä ja sen ominaisuuksista on kerrottu tarkemmin alla olevassa kuvassa 2.

Specifications

USB Type	USB-A
NFC-enabled	Yes
Authentication Methods	Passwordless, Strong Two Factor, Strong Multi-Factor
Identity & Access Management	AWS Identity and Access Management (IAM), Centrify, Duo Security, Google Cloud Identity, Idaptive, Microsoft Active Directory, Microsoft Azure AD, Okta, Ping Identity
Productivity & Communication	Google Account, Microsoft account, Salesforce.com
Password Managers	1Password, Keeper®, LastPass Premium, Bitwarden Premium
Function	WebAuthn, FIDO2 CTAP1, FIDO2 CTAP2, Universal 2nd Factor (U2F), Smart card (PIV-compatible), Yubico OTP, OATH – HOTP (Event), OATH – TOTP (Time), Open PGP, Secure Static Password
Certifications	FIDO 2 Certified, FIDO Universal 2nd Factor (U2F) Certified
Cryptographic Specifications	RSA 2048, RSA 4096 (PGP), ECC p256, ECC p384
Design & Durability	IP68 rated, Crush Resistant, No Batteries Required, No Moving Parts
Device Type	FIDO HID Device, CCID Smart Card, HID Keyboard
Manufacturing	Made in USA and Sweden

Kuva 2. YubiKey 5 NFC-avaimen tekniset tiedot [6].

3.3 YubiKey työasemassa

YubiKey-avain toimii työasemassa Windows-kirjautumisen kaksivaiheisena todennuksena. Jokaiselle käyttäjälle asetetaan tilin kirjautumiseen henkilökohtainen YubiKey-avain, joka täytyy liittää tietokoneen USB-porttiin kirjautumisen yhteydessä.

YubiKey-avaimia hallinnoi työaseman järjestelmänvalvoja, joka ainoastaan pystyy muuttamaan tilien asetuksia ja näin ollen hallinnoimaan avaimia. Tällä estetään tilanteet, jossa muut kuin järjestelmänvalvojat pystyisivät ohittamaan kaksivaiheisen todennuksen.

Avaimista otetaan liitoksen yhteydessä tiedot ylös, ja ne säilötään TL-III hyväksyttyyn paikkaan, jolloin pystytään seuraamaan avaimien kulkua ja tiedetään avainten sen hetkiset omistajat.

YubiKey-avaimia voi uusiokäyttää. Kun käyttäjä ei enää tarvitse YubiKey-avainta, se luovutetaan takaisin. Avamet resetoidaan YubiKey manager-ohjelmaa käyttäen.

4 VeraCrypt

4.1 VeraCrypt lyhyesti

VeraCrypt on ilmainen avoimen lähdekoodin tiedostosalainohjelma, jolla pystytään joko luomaan salattuja kontteja tai salaamaan kokonaisia tallennuslevyjä. VeraCrypt-ohjelmisto on forkkaus, eli kopio itsenäisenä projektina TrueCrypt-ohjelmasta, jonka kehittäminen lopetettiin vuonna 2014. [7].

Työaseman asennusvaiheessa versiot 1.22 & 1.23 olivat ainoita Traficomin auditoimia ja hyväksymiä versioita. Näistä versioista päädyttiin käyttämään uudempaa versiota, joka oli 1.23.

VeraCrypt-ohjelmistosta on kirjoittamisen aikana auditoitu kaksi uudempaa versioita, joten tällä hetkellä siitä on neljä eri versiota, jotka ovat hyväksytty käyttöön Traficomin laatiman käyttöpolitiikan mukaisesti. Hyväksytyt versiot ovat 1.22, 1.23, 1.24 & 1.25. [8].

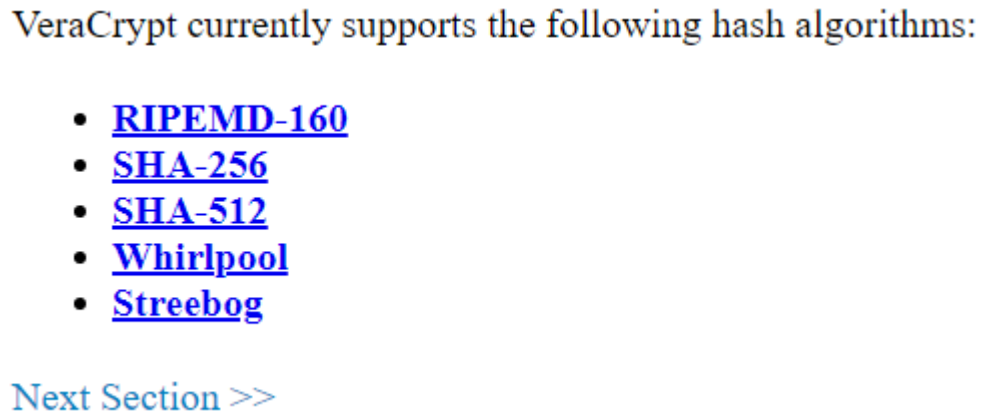
4.2 VeraCryptin tekniset tiedot

VeraCrypt tukee useita eri salausalgoritmejä joilla tallennuslaitteita pystytään salaamaan. Alla olevassa taulukossa on listattu kaikki käytettävissä olevista salausalgoritmeistä.

Taulukko 2. Salausalgoritmit [9].

Algorithm	Designer(s)	Key Size (Bits)	Block Size (Bits)	Mode of Operation
AES	J. Daemen, V. Rijmen	256	128	XTS
Camellia	Mitsubishi Electric and NTT of Japan	256	128	XTS
Kuznyechik	National Standard of the Russian Federation GOST R 34.12-2015	256	128	XTS
Serpent	R. Anderson, E. Biham, L. Knudsen	256	128	XTS
Twofish	B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, N. Ferguson	256	128	XTS
AES-Twofish		256; 256	128	XTS
AES-Twofish-Serpent		256; 256; 256	128	XTS
Camellia-Kuznyechik		256; 256	128	XTS
Camellia-Serpent		256; 256	128	XTS
Kuznyechik-AES		256; 256	128	XTS
Kuznyechik-Serpent-Camellia		256; 256; 256	128	XTS
Kuznyechik-Twofish		256; 256	128	XTS
Serpent-AES		256; 256	128	XTS
Serpent-Twofish-AES		256; 256; 256	128	XTS
Twofish-Serpent		256; 256	128	XTS

VeraCrypt tukee seuraavia Hash-algoritmejä: RIPEMID-160, SHA-256, SHA-512, Whirlpool & Streebog. [10].


VeraCrypt currently supports the following hash algorithms:

- RIPEMD-160
- SHA-256
- SHA-512
- Whirlpool
- Streebog

Next Section >>

Kuva 3. Hash-algoritmit [10].

4.3 VeraCrypt työasemassa

Opinnäytetyön käytännön toteuttamisvaiheessa uusin Traficomin auditoima ja hyväksymä versio oli 1.23., joten sitä päädyttiin käyttämään työasemassa. [8].

Työaseman koko kiintolevy salattiin ohjelmaa käyttäen. Salaukseen käytettiin ohjeistusta ja vaatimuksia niin yrityksen tietoturvapolitiikkaa seuraten, kuin myös Traficomin virallisien ohjeistuksien mukaan, jotka Traficom oli yritykselle antanut vaatimusmäärittelyä tehtäessä. Näin ollen työasema oli salattu hyväksytysti TL-III materiaalia varten. Yritys on tehnyt yhteistyötä Traficomin kanssa salausratkaisua hankkiessaan, ja yritykselle on tehty vaatimusmäärittely työasemien salauksissa.

> Salausratkaisua hankittaessa vaatimusmäärittelyssä tulee huomioida erityisesti
>
> 1. toiminnallisten vaatimusten (käytettävyys) tarpeiden täyttyminen,
>
> 2. tiedon suojaustaso,
>
> 3. edellisestä johdetut mahdollisen tuotejoukon rajoitukset sekä
>
> 4. tiedon omistajan (kansallinen, EU, NATO, jne.) erityisvaatimukset [11].

5 Yhteenveto

Lopputuloksena valmistui TL-III turvallisuusluokan mukaisesti kovennettu työasema, jota yrityksessä pystytään tulevaisuudessa käyttämään TL-III ja TL-IV materiaalin käsittelyyn hyväksytysti. Työasemasta kirjoitettiin täysvaltaiset käyttöönotto- sekä käyttöohjeet, jotta sen käyttäminen olisi mahdollisimman selkeää sekä turvaluokitusten mukaista.

Kun kaikki asetukset ja kovennukset olivat valmiit, yrityksen tietoturvatiimi auditoi ja totesi sen TL-III vaatimuksien mukaiseksi. Työaseman käyttö turvaluokitellun tiedon käsittelyyn vaatii vielä joko Traficomin tai tiedon omistajan päätöksen.

Työaseman valmistuttua se esiteltiin yrityksessä, jolloin se todettiin täyttävän asetetut vaatimukset ja olevan tarpeiden mukainen. Työasema oli siis valmis hyväksytettäväksi korkeintaan TL-III tiedon käsittelyyn yrityksessä.

6 Pohdinta

Opinnäytetyön aihe oli itselleni varsin kiinnostava ja opin paljon uutta sekä hyödyllistä prosessin edetessä. Suurimpina mielenkiinnonkohteina ja myös yllätyksinä olivat Traficomin tiukat vaatimukset, joita projektissa joutui paljon pohtimaan. Projektia tehdessä opin hyvin paljon eri turvaluokitusten vaatimustasoista ja syistä niiden olemassaololle, sillä tietoturva nykypäivänä on kriittisen tärkeää työelämässä monella eri tasolla.

Projekti oli osaltani puoliohjattua, joten pääsin itse myös suunnittelemaan ja pohtimaan vaatimuksia työasemalle ja kehittelemään tarvittavia ratkaisuja, jotta työasema saatiin vaatimusten tasolle. Ohjeistusta ja apua projektiin sain esimieheltäni sekä kollegoilta niin ICT- kuin myös tietoturvatiimistä, mutta pääasiallisesti suurimman osan selvitystyöstä tein itse.

Tulevaisuudessa samankaltaiset projektit olisivat kiinnostavia ja mielekkäitä, sillä tämän kaltaisissa projekteissa joutuu hyvin paljon tekemään selvitystyötä ja pohtimaan, miten toteutukset pystytään hoitamaan. Tässä projektissa myös sai ja joutui välillä käyttämään omaa harkintaa, jotta toteutukset saatiin hoidettua asianmukaisella tavalla.

Lopuksi voin sanoa, että nautin projektin käytännönosuudesta, sillä siinä pääsi tekemään tutkimustyötä sekä myös tekemään asioita fyysisesti työasemalle.

Lähteet

[1] **Kansallinen turvallisuusviranomainen. 2020.** Katakri 2020 - Tietoturvallisuuden auditointityökalu viranomaisille. [Online] 2020. [Viitattu: 21.8.2022.] https://um.fi/documents/35732/0/Katakri+-+2020_1218.pdf/ab9c2d4a-5031-3670-6743-3f8921dce8c9?t=1608302599246.

[2] **Fisher, Tim. 2022.** How to Use the Netstat Command. *Lifewire.* [Online] 14.9.2022. [Viitattu: 14.9.2022.] https://www.lifewire.com/netstat-command-2618098.

[3] **Margosis, Aaron. 2019.** LGPO.exe - Local Group Policy Object Utility, v1.0. *Microsoft Techcommunity.* [Online] 6.10.2019. [Viitattu: 21.8.2022.] https://techcommunity.microsoft.com/t5/microsoft-security-baselines/lgpo-exe-local-group-policy-object-utility-v1-0/ba-p/701045.

[4] **Yubico.** Awards. *Yubico.* [Online] [Viitattu: 13.9.2022.] https://www.yubico.com/about/awards/.

[5] **Yubico.** Yubico innovation history. *Yubico.* [Online] [Viitattu: 21.8.2022.] https://www.yubico.com/about/yubico-innovation-history/.

[6] **Yubico.** YubiKey 5 NFC. *Yubico.* [Online] [Viitattu: 21.8.2022.] https://www.yubico.com/fi/product/yubikey-5-nfc/.

[7] **Rubens, Paul. 2014.** VeraCrypt a Worthy TrueCrypt Alternative. *eSecurity Planet.* [Online] 13.10.2014. [Viitattu: 21.11.2022.] https://www.esecurityplanet.com/applications/veracrypt-a-worthy-truecrypt-alternative/.

[8] **Traficom. 2022.** Liikenne- ja viestintävirasto Traficomin NCSA-toiminnon hyväksymät salausratkaisut. *Traficom.* [Online] 19.9.2022. [Viitattu: 21.11.2022.]

https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/ncsa/liikenne-ja-viestintavirasto-traficomin-ncsa-toiminnon-hyvaksymat-salausratkaisut.

[9] **VeraCrypt.** Encryption Algorithms. [Online] [Viitattu: 13.9.2022.] https://www.veracrypt.fr/en/Encryption%20Algorithms.html

[10] **VeraCrypt.** Hash Algorithms. [Online] [Viitattu: 13.9.2022.] https://www.veracrypt.fr/en/Hash%20Algorithms.html.

[11] **Valtiovarainministeriö. 2016.** Vahti 2015 - Ohje salauskäytännöistä. *Suomidigi.fi.* [Online] 4.11.2015. [Viitattu: 10.2.2022.] https://www.suomidigi.fi/sites/default/files/2020-06/Vahti_2_2015_pdf.pdf.

Liitteet

Liite 1. Yritykselle luodut ohjeet fyysisten porttien kovennukseen.

Uusien USB-massamuisti laitteiden estäminen

1. Avaa Local Group Policy Editor
2. Computer Configurator -> Administrative Templates -> System -> Device Installation -> Device Installation Restrictions
3. ”Prevent installation of devices not described by other policy settings” -> ENABLE
    a. Tämä estä kaikkien UUSIEN laitteiden tunnistamisen koneeseen, jos koneessa on valmiiksi ollut jo joku USB laite, sen laitteen asennus täytyy poistaa Device Managerista.

Paina OK ja sen jälkeen OK

Uusien USB-massamuisti laitteiden hyväksyminen

1. Avaa Local Group Policy Editor
2. Computer Configurator -> Administrative Templates -> System -> Device Installation -> Device Installation Restrictions
3. “Allow installation of devices that match any of these device instance IDs” -> ENABLE
    a. Paina “Show…” ja lisää listaan valtuutettavan laitteen ID
        i. Massamuisti USB laitteen ID saa haettua komentoriviltä komennolla *wmic diskdrive get PNPDeviceID*

Paina OK ja sen jälkeen OK

YubiKey avaimien hyväksyminen

1. Avaa Local Group Policy Editor
2. Computer Configurator -> Administrative Templates -> System -> Device Installation -> Device Installation Restrictions
3. “Allow installation of devices that match any of these device IDs” -> ENABLE
    a. Paina “Show…” ja lisää listaan valtuutettavan laitteen ID
        i. YubiKey laitteen ID saa haettua Device Managerista ”Smart cards” kohdan alta.
        ii. Valitse laite -> Properties -> Ylhäältä Details -> Property kohdasta valitaan Hardware IDs

Paina OK ja sen jälkeen OK

Liite 2. Yritykselle luodut ohjeet yhteyksien koventamiseen palomuurilta.

Verkkoliikenteen estäminen palomuurilta

1. Avataan Control Panel -> System and Security -> Windows Defender Firewall
2. Vasemmalta valitaan “Advanced settings”, tietokone pyytää admin tunnuksia jotta palomuurin asetuksia voi muokata.
3. Overview kohdassa alhaalla painetaan ”Windows Defender Firewall Properties”
4. Muokataan kaikista kolmesta välilehdestä (Domain-, Private- ja Public Profile) kohdista:
    a. Inbound connections: ”Block all connections”.
    b. Outbound connections: “Block”.
5. Luodaan uudet säännöt sekä Inbound Rules, että myös Outbound Rules kohtiin jossa estetään kaikkien ohjelmien yhteydet.
    a. Avataan jompikumpi sääntökohta ja valitaan oikealta ”Actions” välilehden alta ”New Rule…”.
    b. Valitaan ”Custom” ja Next >.
    c. Valitaan ”All programs” ja Next >.
    d. “Protocol and Ports” kohdassa painetaan suoraan Next >.
    e. ”Scope” kohdassa painetaan suoraan Next >.
    f. ”Action” kohdassa valitaan ”Block the connection” ja painetaan Next >.
    g. ”Profile” kohdassa tarkistetaan että täpät ovat jokaisessa kohdassa (Domain, Private ja Public) ja painetaan Next >.
    h. Nimeksi annetaan ”Block ALL Programs” ja painetaan Finish.
6. **Sama toistetaan myös toiseen rules sääntökohtaan.**

Liite 3. Yritykselle luodut ohjeet YubiKeyn asennukseen ja käyttöönottoon.

YubiKeyn asennus

1. Lataa sivulta: Computer Login Security Tools | YubiKeys | Yubico YubiKey 64 bit asennusohjelma “Download Yubico Login for Windows (64 bit)”.
2. Asenna asennusohjelma ja aja se tietokoneella, jolloin ohjelma asentaa ”Login Configurator” ohjelman, millä otetaan YubiKey käyttöön.
    a. Asennuksen jälkeen tietokone vaatii uudelleenkäynnistystä.
3. Käynnistä Login Configuration ohjelma -> ohjelma vaatii adm tunnuksia käynnistyessä.
    a. Paina Next > Welcome kohdassa.
4. Seuraavassa kohdassa valitaan seuraavat täpät:
    a. Slots: Slot 2 (Tämä on automaattisesti valittu uusilla avaimilla)
    b. Challenge: Use existing secret if configured – generate if not configured.
    c. Valitaan Generate recovery code (Automaattisesti valittu)
    d. Otetaan täppä pois “Create backup device for each user”
5. Seuraavassa kohdassa valitaan käyttäjä jolle YubiKey asennetaan -> valitse se käyttäjä jollekka luodaan avain.
6. Ohjelma pyytää, että laitetaan YubiKey tietokoneen USB porttiin.
    a. Ohjelma tunnistaa avaimen heti kun se laitetaan USB porttiin ja kertoo avaimen serial numberin ja Slottien configuroinnit. Paina Next >
7. Ohjelma ohjelmoi avaimen ja sen jälkeen pyytää poistamaan avaimen koneesta. -> Irroita avain.
8. Ohjelma luo recovery avaimen -> se otetaan talteen.
9. YubiKey asennus on valmis! Tietokone pyytää tästä lähtien käyttäjän syöttämään YubiKey avaimen tietokoneeseen kirjautumisen yhteydessä.
    a. Kirjautuminen tapahtuu normaalisti käyttäjänimellä ja salasanalla sekä tästä eteenpäin lisäksi yubikey avaimella.

Liite 4. Yritykselle luodut ohjeet VeraCrypt-salauksen asetukseen.

VeraCrypt konfigurointi

1. Asennuksen jälkeen avataan VeraCrypt ohjelma jolla salataan tietokoneen levy.
2. Paina ”Create Volume” ja valitse kolmas vaihtoehto ”Encrypt the system partition or entire system drive” ja paina Next >.
3. Type of System Encryptioniksi valitaan “Normal” ja painetaan Next >.
4. Area of Encryptiksi valitaan ”Encrypt the Windows system partition” ja painetaan Next >.
5. Number of Operating Systems valitaan “Single-boot” ja painetaan Next >.
6. Encryption Algorithm valitaan algoritmi (tämä on automaattisesti AES-256 salaus) ja Hash Algorithm valitaan ja painetaan Next >.
7. Asetetaan salasana. Valitaan myös **”Use PIM”**
8. PIM kohtaan asetetaan korkeampi kuin default arvo.
9. Collecting Random Data kohdassa täytyy liikutella hiirtä, jolloin VeraCrypt kerää satunnaista dataa jota käyttää salausavaimien luomisessa.
    a. Seuraavassa kohdassa VeraCrypt kertoo luoneensa salausavaimen, tässä kohdassa painetaan Next >
10. Rescue Disk kohdassa VeraCrypt luo ZIP kuvan tietokoneelle,
    a. Tämän jälkeen mennään tiedoston sijaintiin ja ZIP tiedosto täytyy purkaa USB tikulle sen ROOT folderiin.
    b. Avaa ZIP tiedosto ja pura sen sisältö USB tikulle.
11. Rescue Disk kohdan jälkeen VeraCrypt vielä varmistaa, että palautustikku on luotu joko onnistuneesti tai epäonnistuneesti. Paina Next >.
12. System Encryption Pretest vaiheessa painetaan ”Test” ja VeraCrypt testaa että salaus asentuu oikein. Tietokone käynnistyy uudelleen tässä vaiheessa. Valitaan Yes.
    a. Tietokoneen käynnistyessä tietokone pyytää VeraCrypt salaukseen asetettua salasanaa ja tämän jälkeen myös PIM arvoa. Syötä ensin salasana, paina Enter ja syötä PIM arvo.
13. Kirjaudu tunnuksilla takaisin koneelle ja VeraCrypt käynnistyy ilmoittaen ”Pretest Completed”.
14. Paina ”Encrypt” ja tämän jälkeen ”OK”, tietokone pyytää vielä admin tunnuksia ennen salauksen aloittamista.
15. VeraCrypt aloittaa salauksen ja ilmoittaa kun salaus on valmis.

Kun salaus on valmis, ohjelma ilmoittaa siitä ponnahdusikkunalla josta valitaan OK ja painetaan lopuksi Finish.