

**Suojatut yhteydet ja varmenteet**Tatu Erkinjuntti, Jussi Isosomppi, Eino Kupias, Saku Kähäri

Raportti

Tietojenkäsittelyn koulutusohjelma

2018

Sisällys

[1 Esipuhe 1](#_Toc532399792)

[2 Sanastoa 2](#_Toc532399793)

[3. Julkisen avaimen kryptografia 3](#_Toc532399794)

[3.1 Enkryptaaminen 3](#_Toc532399795)

[3.2 Allekirjoitus 3](#_Toc532399796)

[4. Mikä on PKI? 4](#_Toc532399797)

[4.1 Yksittäisen CA:n malli 6](#_Toc532399798)

[4.2 Yksittäinen CA + monta RA:ta (registeration Authority) 7](#_Toc532399799)

[4.3 Nykyinen malli 7](#_Toc532399800)

[5. PGP ja Wot 8](#_Toc532399801)

[5.1 GPG-avaimien luonti ja julkisen avaimen allekirjoitus 9](#_Toc532399802)

[5.2 WoT 12](#_Toc532399803)

[5.3 Viestien enkryptaaminen ja dekryptaaminen 14](#_Toc532399804)

[5.4 Viestien allekirjoitus 14](#_Toc532399805)

[6 Mitä ongelmia niissä on? 15](#_Toc532399806)

[6.1 PKI:n ongelmakohdat 15](#_Toc532399807)

[6.1.1 Keneen luotamme ja miksi? 15](#_Toc532399808)

[6.1.2 Kuka käyttää avaintani? 15](#_Toc532399809)

[6.1.3 Kuinka turvallinen varmentajan järjestelmä on? 16](#_Toc532399810)

[6.1.4 Kuka ”Timo Virtanen” hän on? 16](#_Toc532399811)

[6.1.5 Onko CA:lla valtuuksia? 17](#_Toc532399812)

[6.1.6 Onko käyttäjä osa turvallisuussuunnittelua? 17](#_Toc532399813)

[6.1.7 Kuinka turvallisia sertifikaatteihin liittyvät käytännöt ovat? 18](#_Toc532399814)

[WoT ongelmat 19](#_Toc532399815)

[6.1.8 Avainten hallinta 19](#_Toc532399816)

[6.1.9 Skaalautuvuus 19](#_Toc532399817)

[6.1.10 Luottamus 19](#_Toc532399818)

[Lähteet 20](#_Toc532399819)

# Esipuhe

Ohjeistuksemme käsittelee asiaa, joka esiintyy lähes jokaisen ihmisen arjessa, tiesivät he sitä tai eivät. Nämä käsitteet ovat monille tuttuja, mutta monet eivät oikeasti tiedä mitä niillä tarkoitetaan. Siksi tärkeä osa projektiamme on avata nämä käsitteet ja selittää mitä ne käytännössä ovat.

Miksi sertifikaatteja käytetään? Digitaaliset sertifikaatit ovat laajimmin hyväksytty ratkaisu tiedon suojaamiseksi kahden tahon välillä. Niihin sisältyy omat haasteensa ja puutteensa, mutta ne ovat tällä hetkellä ainoa helposti skaalautuva ratkaisu. Lisäksi voidaan sanoa, ettei ole realistista odottaa täydellistä ratkaisua, vaan on kannattavampaa ottaa käyttöön uusia teknologioita, jotka vastaavat tietoturvan tarpeisiin riittävällä tasolla. Näistä ratkaisuista voidaan kuitenkin aina luopua, kun parempia menetelmiä innovoidaan.

Sertifikaattien käyttö ei välttämättä ilmene tavalliselle ihmiselle muuten kuin s-kirjaimena osoiterivillä (http:// vs. https://). Moni ei välttämättä myöskään edes tarkista, onko yhteys sivuun turvallinen. Tähän on kuitenkin tulossa muutos, kun selaimet alkavat varoittamaan käyttäjiä suojaamattomista verkkosivuista. Tämä kiinnittää käyttäjän huomion puutteisiin ja vaikuttaa tätä kautta suoraan esimerkiksi verkkokauppojen menekkiin, mikäli palvelu ei ole sertifikaatin puutteellisuuden vuoksi käytettävissä.

# Sanastoa

Projektin työsuunnitelmassa ei huomioida mahdollisia töitä tai esitutkimuksia, joita suoritettiin ennen projektin virallista aloitusta.

Projektin työsuunnitelma muodostui alun suunnittelun perusteella kaksivaiheiseksi:

Ensin projektiryhmä tutki varmenteita teoriatasolla ja pyrki löytämään niistä mahdollisia heikkouksia. Koska varmenteiden käsite on laaja, varatiin tähän tutkimusvaiheeseen lähes puolet projektin työaikabudjetista. Tutkimusvaiheessa pyrittiin myös hahmottamaan kahden eri avainhallintajärjestelmän (Chain of trust ja Web of trust) eroja sekä kummankin tavan hyötyjä käyttäjän kannalta.

Projektin toisessa vaiheessa projektiryhmä jakautui kahteen eri työryhmään. Toisen ryhmän tehtävä oli valmistella peruskäyttäjille suunnattu ohjeistus verkkovarmenteiden käytöstä, toisen ryhmän taas pyrkiä testaamaan varmenteista löytyviä heikkouksia sekä käyttää niitä vihamielisessä tarkoituksessa.

Suunnitelmassa huomioitiin se, että toisessa vaiheessa suoritettavat testit sekä ohjeistuksen rakenne hahmottuisivat vasta ensimmäisen vaiheen tutkimuksen myötä.

Projektityö oli tarkoitus suorittaa pääsääntöisesti Haaga-Helian Pasilan kampuksen tiloissa, mutta projektiryhmän jäsenet luonnollisesti varautuivat myös mahdollisiin etänä suoritettaviin tutkimus- ja työtehtäviin.

## Aikataulu sekä suunnitellut tehtävät

Työn aikataulu pyrittiin pitämään realistisena, huomioiden kuitenkin mahdollisuus sen joustamiseen. Alkuperäiseen aikatauluun päädytiin sillä oletuksella, että projektin aikana esiin tulleisiin havaintoihin tai ongelmiin pystyttäisiin reagoimaan ilman merkittävää vaikutusta projektin kokonaisaikatauluun. Tarkoitusena oli, että projektin toisessa vaiheessa ryhmät voisivat tukea toistensa työn etenemistä oman työryhmänsä tuloksilla.

### Projektin yleinen aikataulu

| **Viikko** | **Työtehtävät** |
| --- | --- |
| vko 43 | Teorian tutkiminen |
| vko 44 | Teorian tutkiminen |
| vko 45 | Teorian tutkiminen |
| vko 46 | Testaus |
| vko 47 | Testaus |
| vko 48 | Testaus |
| vko 49 | Ohjeistuksen sekä projektin   loppuraportin valmistelua. |
| vko 50 | Projektin loppuraportin   esitteleminen. |

### Projektin suunnitellut työvaiheet

| **Tehtävät, vaihe 1** | **Työmäärät** | | **Lopputulokset** | |
| --- | --- | --- | --- | --- |
| Public key infrastructuren tutkiminen | 10 tuntia | | Parempi tietämys PKI:staa | |
| Yleisimpien salakirjoitusmenetelmien tutkiminen (PGP, X.509) | 10 tuntia | | Parempi ymmärrys käytettävistä salakirjoitusmenetelmistä | |
| Web of Trustin tutkiminen | 10 tuntia | | Parempi tietämys WoT:sta | |
| Certificate Authorityn tutkiminen | 10 tuntia | | Parempi tietämys CA:sta | |
| Kahden varmennemenetelmän vertailu, haitat sekä hyödyt | 15 tuntia | | Varmennemenetelmien eroavaisuudet ja mahdolliset erikoisuudet | |
| Ongelmakohtien tunnistaminen varmennemenetelmistä | 20 tuntia | | Varmenteiden ongelmakohdat tunnistettu | |
| **Tehtävät, vaihe 2** | | **Työmäärät** | | **Lopputulokset** |
| Suoritettavien testien suunittelu | | 25 tuntia | | Valmis testisuunnitelma |
| Testien toteutus | | 50 tuntia | | Valitut testit suoritettu |
| Ohjeistuksen laatiminen | | 12.5 tuntia | | Valmis ohjeistus |
| Loppuraportin laatiminen | | 12.5 tuntia | | Valmis loppuraportti |
|  | |  | |  |

## Dokumentointi ja versionhallinta

Projektiryhmän jäsenille Git:n käyttäminen oli entuudestaan jo hyvin tuttua. Tämä nähtiin luontevana sekä versionhallinnan kannalta parhaimpana ratkaisuna projektidokumentoinnin yhteiseen työstämiseen. Projektia varten luotiin yksityinen Git-varasto, joihin kaikilla projektiryhmän jäsenillä oli käyttöoikeudet.

# Varmenteiden tutkimus

Koska varmenteiden teoriasta sekä niiden käytöstä on runsaasti tietoa, koettiin tutkimuksen alkuvaiheessa parhaimmaksi lähestymistavaksi projektiryhmän jäsenten itsenäinen lähdemateriaalin etsiminen. Perusajatuksena oli, että projektiryhmän jäsen arvioi lähteen sekä sen sisältämän tiedon hyödyllisyyden projektin kannalta, ja tämän jälkeen esitteli hyödylliseksi kokemansa sisällöt muille projektiryhmän jäsenille. Projektiryhmä päätti yhdessä kunkin lähteen käytöstä, ja hyväksyttyjen lähteiden työstämistä jatkettiin koko ryhmän kesken. Tällä hieman luovalla lähestymistavalla pyrittiin tehostamaan tutkimustyötä sekä käytettävien lähteiden määrää.

## PKI ja julkisen avaimen salausmenetelmä

Vaikka projektiryhmällä oli jo entuudestaan jonkin verran tietämystä varmenteista, aloitettiin tutkimus PKI:n (Public key infrastructure, julkisten avainten hallintajärjestelmä) sekä julkisen avaimen salauksen peruskäsitteistä. Nämä koettiin johdonmukaisiksi aloitusaiheiksi, joiden kautta projektiryhmä pystyi etenemään tutkimuksissaan projektin varsinaiseen aiheeseen, verkkovarmenteisiin. Tärkeäksi koettiin myös lisätiedon hankkiminen X.509 -sertifikaattien salauksista, muista PGP-salatuista avaimista sekä missä osassa ne ovat liittyen CA:n (Certificate Authority) tai WoT:n (Web of Trust) käyttöön.

## Julisten avainten hallintajärjestelmä

Johdonmukainen lähestymistapa verkkovarmenteiden tutkimuksessa oli siirtyä kahden yleisimmin käytössä olevan julkisten avainten hallintajärjestelmän (CA, WoT) tutkimukseen. Koska verkkovarmenteiden julkinen käyttö (verkkosivut) perustuu lähes yksinomaan CA:n käyttöön, keskittyi projektiryhmä ensin tähän menetelmään. WoT:n käytön tutkiminen verkkovarmenteissa muodostui haastavaksi pääasiassa siksi, että WoT:n julkinen käyttö on hyvin rajallista.

## Hyödyt ja heikkoudet

Koska tutkittujen hallintajärjestelmien käyttö poikkeaa merkittävästi toisistaan, tulee näiden osalta käsitellä niiden hyötyjä sekä haittoja erillään toisistaan, sillä ne eivät tässä yhteydessä ole suoraan vertailukelpoisia keskenään.

## CA

CA-varmenteiden käytön hyötyjä verkkopohjaisissa ratkaisuissa ei voi kiistää, vaan vakiintuneen hierarkiansa ja laajan suosionsa vuoksi niitä voidaan pitää turvallisen internet-käytön kulmakivinä. CA-varmenteet vahvistavat yksityisyyden suojaa sekä luottamusta alati vaarallisemmaksi muuttuvassa internetissä. Ne ovat olleet suuressa osassa mm. verkkokauppa- ja verkkopankkitoiminnan laajentumista. Nykyään peruskäyttäjä usein ymmärtää verkko-osoitteessa olevan pienen s-kirjaimen tai osoitepalkin ohessa olevan lukkoikonin merkityksen, ja ideaalitapauksisa osaa olla luottamasta sivustoihin, joiden varmenne on viallinen tai puuttuu kokonaan. Näin ollen voidaan sanoa, että X.509-varmenteen käyttö on tuonut internetin tietoturvallisen käytön entistä lähemmäksi peruskäyttäjän taitotasoa.

X.509-varmenteiden yleinen käyttö SSL/TLS yhteyksissä kohdistaa niihin omalta osaltaan myös uhkia. Koska digitaalinen kaupankäynti on hyvin riippuvainen varmenteiden käytöstä, ovat varmenteet luonnollisesti houkutteleva kohde häirinnälle, haavoittuvuuksien etsimiselle ja hyväksikäytölle, varsinkin rikollisuuden näkökannasta.

Tutkimuksemme aikana löysimme X.509-varmenteiden ja CA:n rakenteesta joitain ongelmakohtia, jotka tulisi niitä käyttäessä ottaa huomioon.

# Ohjeistus

Projektin toinen osatuote oli luoda ohjeistus sertifikaateista peruskäyttäjälle. Peruskäyttäjällä tarkoitetaan henkilöä, joka saattaa tiedostaa sertifikaattien olemassaolon esimerkiksi s-kirjaimesta selaimen osoiterivillä (http:// vs. https://) tai selaimen varoitusviestistä verkkosivusta. Kohde henkilöllä ei kuitenkaan välttämättä ole sen syvällisempää tietoa mitä sertifikaatit ovat, tai miten ne toimivat.

## Työn toteutus

Ohjeistus aloitettiin luomalla raaka kehikko ohjeistukselle. Tämä sisälsi intro kappaleen julkisen avaimen järjestelmään, PKI, WoT sekä näiden kahden järjestelmän vertailu keskenään. Loppuun sunnittelimme koottavaksi tarkastuslistaa sertifikaattien käyttössä mahdillisesti ilmenevistä ongelmista arkikäytössä. Tästä esimerkkinä, käyttäjä ei työympäristössä päässyt kirjautumaan työnantajan verkkoon. Tämä johtui siitä, että BIOS:sin kello oli väärässä ajassa, minkä johdosta myöskin sertifikaatin tarkistus epäonnistui. Lopullisesta tuotteesta päätimme kuitenkin tiputtaa tämän tarkistuslistan pois kokonaan. Syynä oli, että emme löytäneet juurikaan muita ilmeisiä ja ”arkipäiväisiä” ongelmia sertifikaattien käyttöön liittyen, emmekä kokeneet että on järkevää luoda listausta vain muutamaa ongelmaa varten.

Sovimme että jaamme vielä ohjeistuksesta vastuun PKI:n ja WoT:in kappaleista kirjoittajien kesken. Sovimme myös, että jokainen suorittaa itsenäisesti tutkimukset omista vastuualueistaan sekä kirjoittaa näitä koskevat kappaleet, ja että muihin kappaleisiin palataan yhdessä. Tarkoituksena oli väitellä PKI:n ja WoT:in ominaisuuksista ja paremmuudesta ja tämän pohjalta luoda vertailu.

Saatuamme vastuu alueemme valmiiksi totesimme, että PKI:n ja WoT:in vertailu keskenään toisiaan ei ole tarkoituksenmukaista. Järjestelmät eroavat käyttökohteiltaan huomattavasti toisistaan, joten muutimme viimeisen kappaleen käsittelemään järjestelmien heikkouksia omissa ympäristöissään. Tämän ohessa loimme dokumentille myös esipuheen sekä lyhyen selityksen julkisen avaimen kryptografiasta, johon kumpiki PKI ja WoT -järjestelmät perustuvat.

Koska ohjeistus on tarkoitettu peruskäyttäjälle, ja kuitenkin aiheen luenteen takia sisältää pakostikin paljon teknistä kieltä, lisäsimme ohjeistukseen vielä sanaston siinä käytetyistä termeistä.

## Tulokset

Tuloksena tästä osaprojektista syntyi ohjeistus dokumentti, Sertifikaattien Salattu maailma.

Ohjeistus koostuu seruvaavista kappaleista:

* Esipuhe
* Sanatoa
* Julkisen avaimen kryptografia
* Mikä on PKI?
* PGP ja WoT
* Mitä ongelmia niissä on?

Mielestämme ohjeistuksesta tuli tarkoituksenmukainen, eli se avaa sertifikaatien maailmaa peruskäyttäjälle.

Olemme koe luetuttaneet ohjeistuksen yhdellä henkilöllä, joka tunsi sertifikaattien käsitteen ennalta töiden puolesta, kun yrityksen sertifikaatti oli vanhentunut. Kuitenkaan syvällistä tietoa henkilöllä ei näiden toiminnasta ennalta ollut.

Tämän koehenkilön mukaan ohjeistus avasi aihetta hyvin ja oli selkeä ja helppolukuinen.

## 3.1 Enkryptaaminen

Avainparin kummatkin avaimet ovat linkitetty toisiinsa, kuitenkin siten, että julkisen avaimen avulla ei ole mahdollista saada selville käyttäjän yksityistä avainta.

## 3.2 Allekirjoitus

Avainparin yksityisellä avaimella on mahdollista digitaalisesti allekirjoittaa viestejä. Tällöin viestin vastaanottaja voi yksityistä avainta vastaavalla julkisella avaimella varmistua, että viestin lähettäjä on tosiaan, kuka tämä väittää olevansa, sekä että viestin sisältöä ei ole muokattu välillä. Toimii siis samalla tavalla, kuin käsin tehty allekirjoitus, paitsi että tämä on huomattavasti varmempi. Yksityisellä avaimella tehtyä digitaalista allekirjoitusta ei ole mahdollista jäljitellä.

Esimerkki hyvästä allekirjoituksen käyttökohteesta olisi käyttäjän palveluntarjoajien sähköpostit. Lukuisat kalasteluviestit yrittävät jäljitellä oikean palveluntarjoajan sähköposteja, ja näin saada käyttäjää syöttämään kirjautumistunnuksensa rikollisten palveluihin. Jos palveluntarjoajat käyttäisivät digitaallista allekirjoitusta viesteissään, voisi käyttäjä varmistua, että viestin lähettäjä on se, kuka tämä väittää olevansa.

# 4. Mikä on PKI?

Jos kaksi tahoa (Alice & Bob) tuntevat omat yksityiset avaimensa ja toistensa julkiset avaimet, he voivat kommunikoida turvallisesti lukuisien julkiseen avaimeen pohjautuvien protokollien avulla. Näihin protokolliin lukeutuvat mm. IPSec, PGP ja SSL. Kysymys kuuluukin, että miten he tuntevat toisensa?

PKI:n (Public Key Infrastructure) tarkoitus onkin luoda turvallinen, tehokas ja käytännöllinen tapa löytää julkisia avaimia. Nimensä mukaan kyseessä on infrastruktuuri, joka voi rakentua monilla eri tavoilla. Käytössä on lukuisia erilaisia malleja, jotka eroavat toisistaan turvallisuuden, skaalautuvuuden ja rakenteen mukaan. Tutustumme näihin erilaisiin malleihin hieman myöhemmin.

Julkisen avaimen sertifikaateissa on olemassa standardeja, jotka pystyvät tukemaan erilaisten PKI-mallien vaatimuksia. Laajimmin käytetty näistä standardeista on X.509. Tässä kappaleessa käymme läpi joitakin PKI -malleja, puhuen niiden vahvuuksista ja heikkouksista.

Palataan aiemmin heränneeseen kysymykseen. Kuinka Alice ja Bob saavat toistensa julkiset avaimet selville? Toiset toimintatavat ovat epäkäytännöllisiä ja/tai epäluotettavia. Esimerkkinä näistä:

- Konfiguroidaan jokaiselle käyttäjälle muiden käyttäjien julkiset avaimet siltä varalta, että he haluavat kommunikoida. Tämä on varmastikin turvallista, mutta ei ole mitenkään järkevästi toteutettavissa suuremmissa verkoissa.

- Levitetään julkisia avaimia laajasti esimerkiksi siihen tarkoitetulla verkkosivulla. Tämä ei ole turvallista, vaikka julkisten avaimien ei kuulukaan pitää salassa. Tässä kuitenkin herää epävarmuus siitä, onko Bobin avain oikeasti hänen, vai onko joku muu tekeytynyt häneksi.

Tämänhetkinen yleisesti hyväksytty ratkaisu on se, että on olemassa luotettuja tahoja, CA (Cerfificate Authorities), joiden tehtävä on digitaalisesti allekirjoittaa sertifikaatteja, joiden avulla varmistetaan, kenelle julkinen avain kuuluu. Arkisessa tilanteessa on liikaa olettaa, että Bobilla olisi tiedossa Alicen avaimen allekirjoittanut CA. Tämän takia tarvitaan eräänlainen sertifikaattien ketju, jota seuraamalla Bob vastaanottaa Alicen avaimen.

 Tämä saattaa kuulostaa ja näyttää yksinkertaiselta, mutta se herättää myös kysymyksiä. Mistä Bob tietää CA1:n julkisen avaimen? Voiko kaikkiin ketjun osiin luottaa? Miten hän saa juuri oikeat sertifikaatit, jotka muodostavat ketjun Alicen luo?

Tästä aiheesta puhuessa on hyvä pitää mielessä seuraavat seikat:

- Tietoturvallisuudesta puhuessa ei ole olemassa yhtä ratkaisua, joka sopii kaikille. Salassa pidettäviä asioita käsittelevien yrityksien tietoturvakäytännöt voisivat tuntua pienessä yrityksessä tukahduttavilta. Vastaavasti pienellä yritykselle riittävät tietoturvakäytännöt ovat usein lähes varmasti täysin riittämättömät toisen yrityksen silmissä.

- Olemassa ei ole täydellistä ratkaisua. On parempi käyttää nykyistä puutteita sisältävää ratkaisua sen sijaan, että ei käytetä mitään, kunnes täydellinen ratkaisu syntyy ja tulee kaikkien saataville.

- Jos turvallisuus on liian epäkäytännöllistä tai häiritsee toimintaa riittävästi, käyttäjät alkavat kiertämään sitä.

Käydään seuraavaksi läpi joitakin PKI malleja.

## 4.1 Yksittäisen CA:n malli

Tämä malli koostuu yhdestä ainoasta CA:sta koko maailmassa. Jokainen laite konfiguroitaisiin etukäteen tuntemaan tämän CA:n julkinen avain. Kaikki sertifikaatit tulisi hankkia tätä CA:ta hallinnoivalta organisaatiolta. Tämä olisikin varmasti yksinkertaisin ratkaisu.

Mutta mikä siinä on vialla?

- Maailmassa ei ole sellaista järjestöä, johon kaikki maat, yritykset, laitokset yms. luottavat.

- On epäkäytännöllistä hankkia sertifikaatti etäiseltä ja vieraalta organisaatiolta. Sertifikaatin jakamisen tapahtuisi luultavimmin sähköpostilla, eikä se ole turvallista ennen kuin sertifikaatti on käytössä turvaamassa liikennettä. Myös CA:n osalta on vaikeaa todentaa, että sertifikaatin on pyytänyt juuri se henkilö kenelle se on osoitettu.

- Tietoturvan kannalta on hyvä vaihdella avaimia tietyin väliajoin. Mitä siis tapahtuu, jos CA haluaa vaihtaa avaimensa vahvempaan tai minimoida jo sattuneita vahinkoja? Kaikki laitteet maailmassa tulisi konfiguroida uudelleen sisältämään tämä uusi avain.

- Jos jokin organisaatio saa yksinvallan markkinoilla ja maailma on riippuvainen sen hallinnoimasta teknologiasta, on mahdollista, että se hyväksikäyttää asemaansa esimerkiksi korkeiden maksujen muodossa.

Puutteista ja ongelmistaan huolimatta tällä mallilla on omat puolestapuhujansa ja sitä on myöskin implementoitu käyttöön.

## 4.2 Yksittäinen CA + monta RA:ta (registeration Authority)

Samoin tavoin kuin edellinen malli, tämäkin perustuu siihen, että on olemassa yksi CA ja kaikille laitteille on konfiguroitu tämän julkinen avain. Kaikki sertifikaatit siis allekirjoittaa tämä yksittäinen CA. Lisäksi tähän malliin kuuluu, että olemassa on useita RA:ita, joihin CA luottaa. RA:n tehtävä on autentikoida käyttäjä ja käyttäjän avain, sekä lähettää allekirjoitettu pyyntö CA:lle. Kun CA vastaanottaa allekirjoitetun pyynnön, se luovuttaa sertifikaatin. Käyttäjien näkökulmasta tämä toimintatapa muistuttaa yksittäisen CA:n mallia.

Mitä edellisen mallin ongelmia tämä rakenne ratkaisee? Kun olemassa on monta RA:ta, on hyvin todennäköistä, että ainakin yksi niistä on paremmin saatavilla kuin yksittäinen CA. Vaikka CA:n alaisuudessa on monta RA:ta, tarvitsee asiakas edelleen vain CA:n julkisen avaimen. Pelkästään CA on tietoinen RA avaimista.

RA:n kumoaminen (jos RA menettää luotettavuutensa) toimii tässä mallissa yksinkertaisesti. CA voi yksinkertaisesti vastata kyseisen RA:n pyyntöihin, jolloin se ei kykene enää suorittamaan tehtäviään.

Tämä malli kuitenkin sisältää muilta osin samat heikkoudet kuin yksittäisen CA:n infrastruktuuri.

## 4.3 Nykyinen malli

Käytössä ei ole vain yhtä ainoaa mallia. Erilaiset mallit toimivat erilaisissa ympäristöissä ja niin kauan kuin nykyiset teknologiat ovat relevantteja, tämä tuskin tulee muuttumaan. Normaalin käyttäjän on kuitenkin hyvä tietää mistä hänen avaimensa tulevat. Vastaus on melko yksinkertainen: selaimet joita käytämme, luottavat eri CA:ihin. Nämä ennalta määritellyt luottamussuhteet mahdollistavat turvalliset yhteydet verkkosivuille, ilman että käyttäjän tarvitsee tehdä mitään.

[[1](<https://pdfs.semanticscholar.org/0fc4/0e88e1aec293ddfbbc5b82c3e294e8c0ed14.pdf>)

# 5. PGP ja Wot

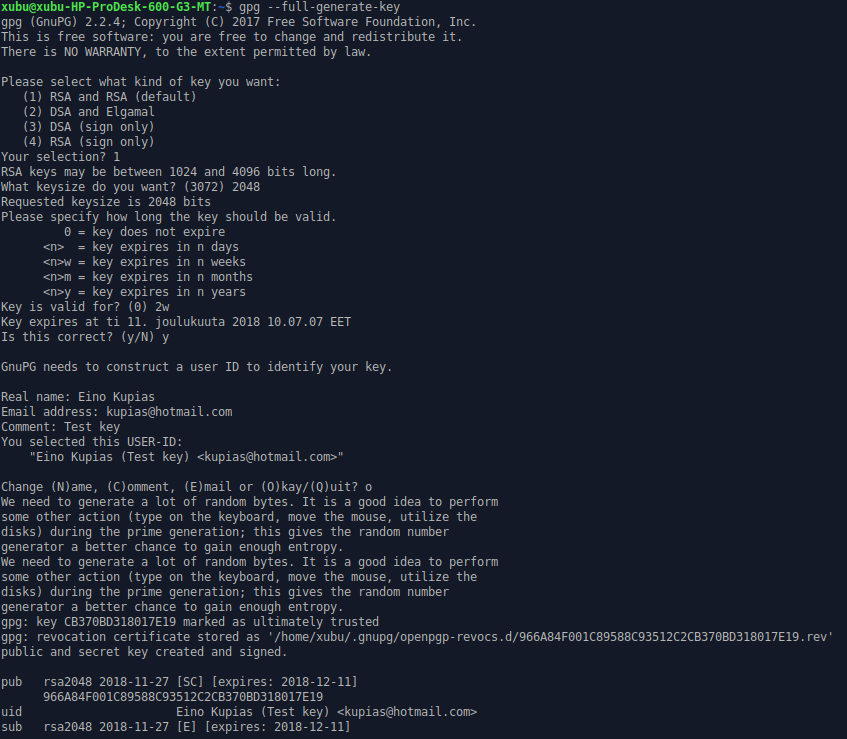
Central Authority -mallin sijaan, jossa luottamus ostetaan CA-sertifikaattien muodossa tällä voittoa tekevältä yritykseltä, PrettyGoodPrivacy (PGP)-mallissa käyttäjät luovat ja määrittelevät luottosuhteensa itse. Käsitteiden vertaaminen keskenään on kuitenkin ongelmallista, CA ei ole korvattavissa WoT -mallilla. CA on välttämätön yrityksen toimintaan verkossa, PGP soveltuu lähinnä yksityishenkilöiden väliseen, yrityksen sisäiseen viestintään tai tiedoston/viestin sisällön eheyden varmistamiseen.

PGP-avaimia käytetään sähköpostien, levyjen ja tiedostojen enkryptaamiseen tai allekirjoitukseen. Kuka tahansa voi käyttäjän julkisella avaimella encryptata tiedoston, jonka pystyy avaamaan vain yksityisellä avaimella.

Käyttäjä voi myös allekirjoittaa tiedoston/sähköpostin yksityisellä avaimellaan, ja vastaanottaja voi käyttäjän julkisella avaimella varmistaa, että tiedosto/sähköposti on tosiaan tullut oikealta henkilöltä.

Linuksin paketinhallinta käyttää tätä allekirjoitus systeemiä, jotta voidaan varmistua, että ladattu ohjelma tosiaan on peräisin kehittäjältä.

## 5.1 GPG-avaimien luonti ja julkisen avaimen allekirjoitus

Avainpari voidaan luoda mm. gpg ohjelmalla.

1. Valitaan salaus algoritmi

2. Salauksen pituus, lyhempi on turvattomampi, pidemmässä kestää pidempään luoda ja se vie enemmän tilaa

3. Avaimen voimassaoloaika. Mitä pidempään käytetään samaa avainta, sitä todennäköisemmäksi tulee, että se varastetaan/kopioidaan ja ennen pitkään saadaan murrettua. Näin ollen avaimella tulisi olla vanhentumispäivä.

4. Syötetään avaimen käyttäjän nimi, sähköpostiosoite ja valinnainen kommentti, mihin avainta käytetään.

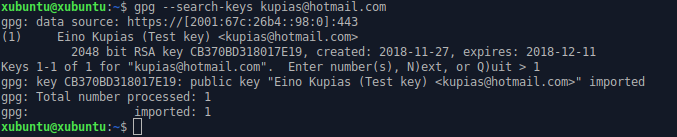
5. Seuraavaksi prosessi luo ja tulostaa avaimet näytölle.

pub on julkinen avain, joka lähetetään avainpalvelimelle. Näitä on useita (mm. MIT (Massachusetts Institute of Technology) ylläpitää), ja ne jakavat tietoa keskenään. Täten ennen pitkää julkinen avain leviää kaikille avainpalvelimille.

pub on julkinen avain, joka lähetetään avainserverille.

https://raw.githubusercontent.com/TatuE/tietoturvanHallinta/master/documents/kuvat/key-send.png?token=AdzIIZYlt2DPRX9LOftaFMHrm6L7c0U9ks5cE4JgwA%3D%3D

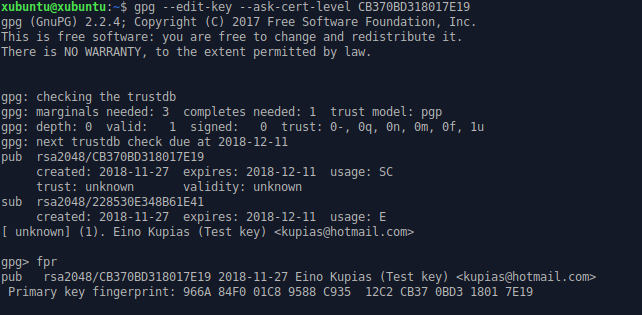
Tähän on tallennettu avaimen käyttäjän tiedot. Julkista avainta voidaan etsiä nimellä, sähköpostilla tai suoraan julkisella avaimella.



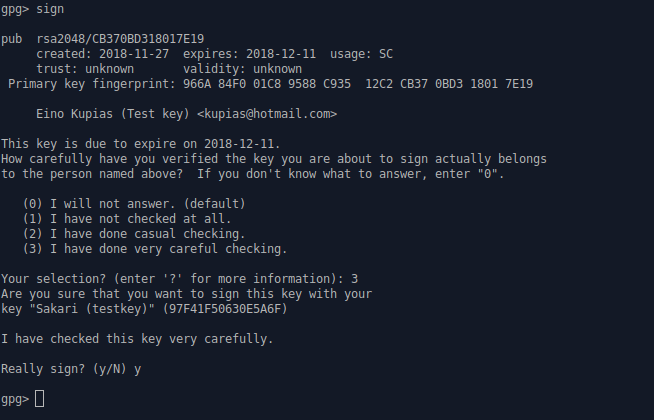
PGPn suurin ongelma on avainten käyttäjien henkilöllisyyden varmistaminen. Kuka tahansa voi luoda avainparin mille tahansa nimelle, ja täten väittää olevansa jotain muuta kuin oikeasti on. Tällöin on jokaisen käyttäjän itsensä vastuulla, luodessa luottosuhteita muiden avaimiin, varmistaa avaimen haltijan henkilöllisyys.

Toinen käyttäjä voi näin allekirjoittaa julkisen avaimen ja luoda luottosuhteen tähän. Ennen allekirjoitusta tulee kuitenkin varmistaa avaimen käyttäjän henkilöllisyys.

Käytännössä tämä tarkoittaa että, avainten allekirjoitus tulisi suorittaa kasvotusten ja vertaimella vielä allekirjoitettavan avaimen sormenjälkeä.



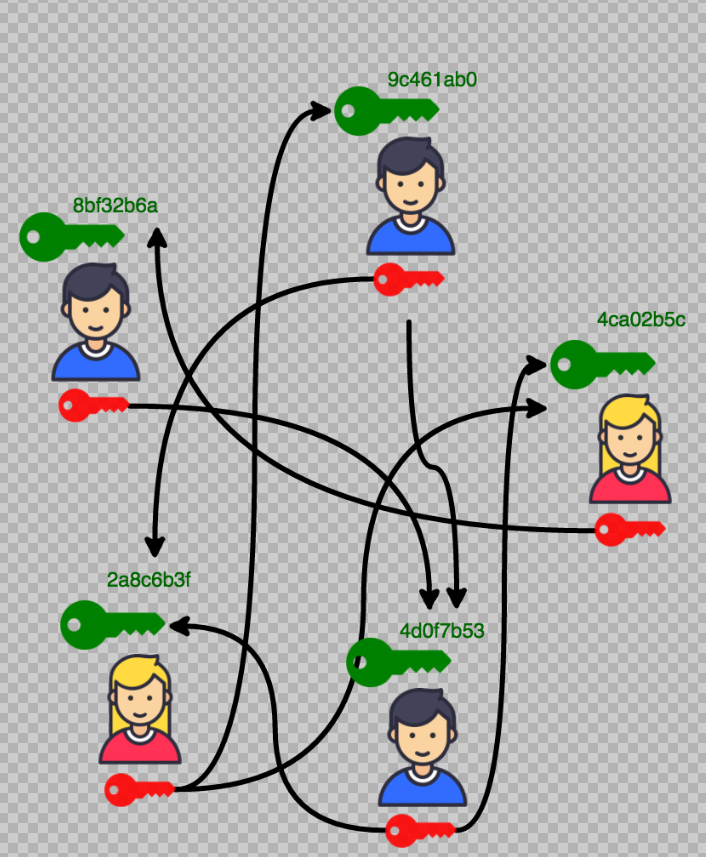
Nyt voidaan aloittaa allekirjoitusprosessi. Tämä avaa gpg-konsolin. fpr-komento vielä tulostaa julkisen avaimen sormenjäljen, josta tulisi vielä vertailla avaimen haltijan kanssa esim. kolme ensimmäistä numerojonoa.



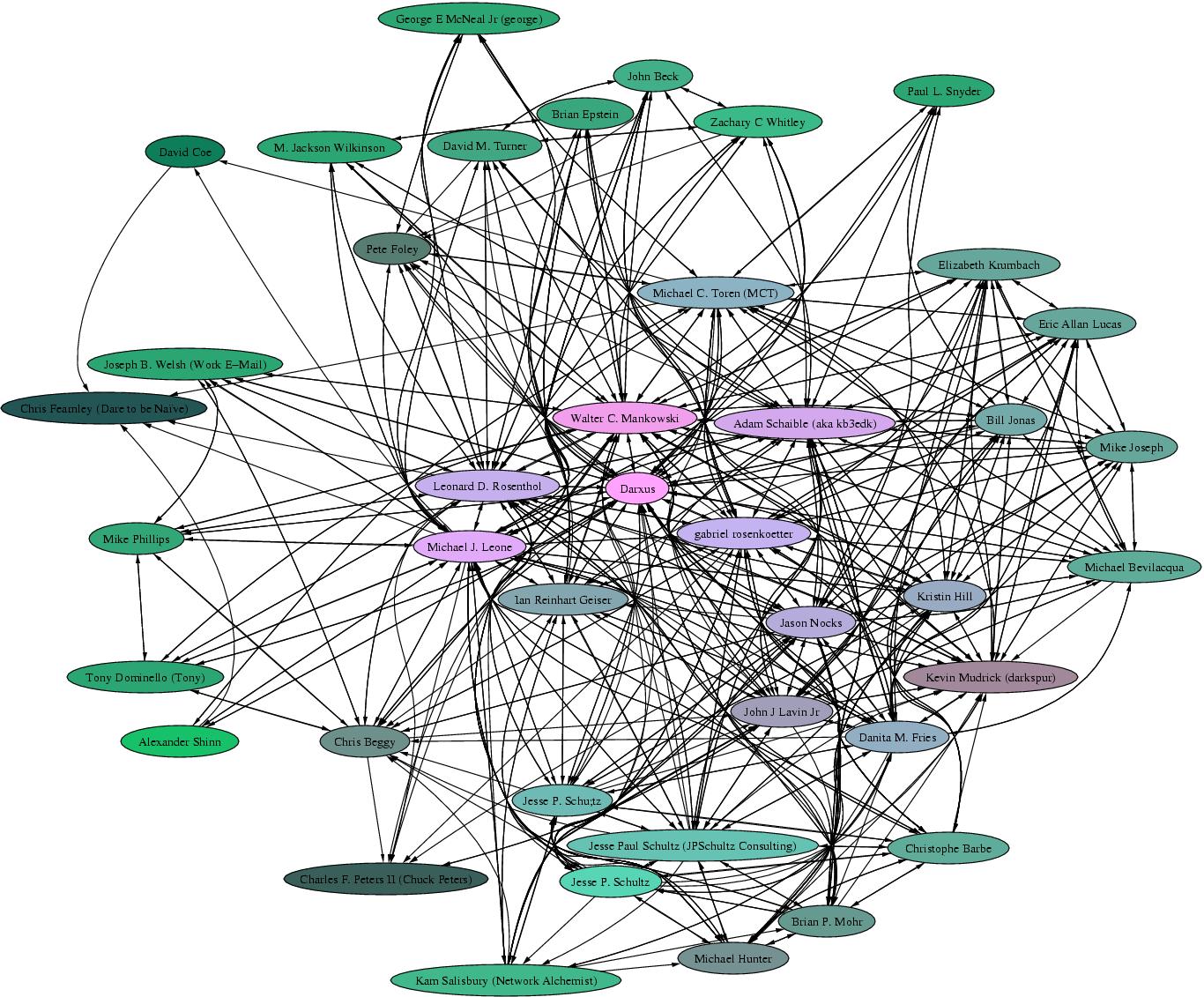
Tässä prosessissa valitaan vielä luottamuksen taso. (1) vihteehdon kohdalla voisi nostaa esille kysymyksen, onko edes järkeä hyväksyä avainta, jota ei ole tarkistanut millään lailla. (3) vaihtoehto tarkoittaa käytännössä henkilöllisyyden varmistamista virallisesta valtion takaamasta henkilöllisyystodsituksesta (passi, henkilökortti, ajokortti), sekä myös mahdollisesti henkilön tuntemista aikaisemmista yhteyksistä.

## 5.2 WoT

Koska WoT-mallissa henkilöllisyyden tarkastimen on tärkeää, järjestetään erityisiä key-signing-juhlia. Näissä käyttäjät vahvistavat toistensa henkilöllisyydet sekä allekirjoittavat toistensa avaimia. Näin muodostuu allekirjoitusten verkostoja. (Ikävä kyllä en löytänyt viitteitä suomessa järjestettävistä tapahtumista).

 [https://cran.r-project.org/web/packages/gpg/vignettes/intro.html]

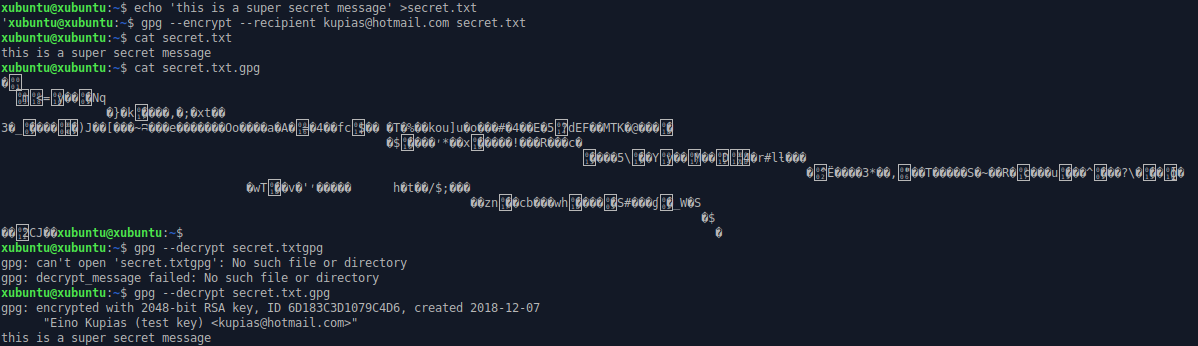
"Valmis" WoT voisi näyttää seuraavalta

 [http://www.phillylinux.org/keys/historical.html]

WoT sisältää useita linkkejä eri henkilöiden välillä. Tällöin vaikka yksi linkki tippuisikin pois, voidaan käyttää jotain toista reittiä. Tämä on WoTin suurin vahvuus CA-malliin verrattuna, jossa yhden linkin viottuminen vaikuttaa kaikkiin sen alapuolella toimiviin.

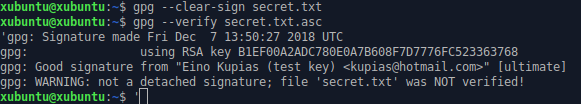
Suurin heikkous taas, että henkilöiden varmentaminen vaatii aikaa ja mahd. myös matkustelua. Verkoston luominen ja ylläpito vaatii paljon työtä.

## 5.3 Viestien enkryptaaminen ja dekryptaaminen



Komennolla `gpg --encrypt --recipient kupias@hotmail.com secret.txt` tiedosto salataan käyttäjän kupias@hotmail.com julkisella avaimella luoden salatun kopion tiedostosta .gpg tiedostopäätteellä, jolloin ainoastaan tätä vastaavalla yksityisellä avaimella tiedosto voidaan avata. Kuvassa ei kohtaa näy, mutta decryptatessa viestiä, avautui popup-ikkuna jonne yksityisen avaimen salasana tuli syöttää.

## 5.4 Viestien allekirjoitus



Komento `gpg --clear-sign secret.txt` luo tiedostosta allekirjoitetun kopion .asc päätteellä.

Komento `gpg --verify secret.txt.asc` tulostaa tiedot allekirjoituksessa käytetystä avaimesta.

Alla viellä kuva, miltä allekirjoitettu viesti näyttää.

![gpgsignemessage](<https://raw.githubusercontent.com/TatuE/tietoturvanHallinta/master/documents/kuvat/gpgsigned%20message.png?token=AdzIIQnnnq4kLIPgCuxr2EQRqRufC-M_ks5cE7bVwA%3D%3D>)

# Mitä ongelmia niissä on?

## PKI:n ongelmakohdat

Sertifikaatit ovat houkutteleva liiketoimintamalli. Niiden kirjoittaminen on lähes maksutonta, ja jos ihmiset tilaavat niitä vuosittain tietystä maksusta, syntyy huomattava liikevoitto. Vaihtoehtoisesti voit saada jonkun ylläpitämään omaa CA palvelua ja maksamaan sinulle rahaa jokaisesta sertifikaatista jonka tämä myöntää. Ala on tuottoisa, eikä parempaa yleisesti hyväksyttyä tietoturvaratkaisua ole käytössä, joten PKI:ta lobbataan paljon ja suuri osa sitä koskevasta kirjallisuudesta on PKI -kauppiaiden tuottamaa. Tämä kirjallisuus saattaa jättää puutteellisen kuvan PKI:n ongelmakohdista ja herättää myöskin kysymyksiä. Käydään niitä läpi seuraavaksi.

Turvallisuutta voidaan ajatella ketjuna; se on yhtä vahva kuin sen heikoin lenkki. CA:han pohjautuva infrastruktuuri on moniosainen, eikä sen kaikki osat ole salattuja. Ihmiset osallistuvat siihen ja tekevät virheitä. Työskentelevätkö nämä ihmiset perusteellisesti ja rehellisesti? Entä laitteet joilla he työskentelevät? Näiden laitteiden ja käytettyjen järjestelmien tulee olla turvattuja ja käytössä olevia tietoturvan työkaluja tulee hyödyntää. Nämä seikat muodostavat yhdessä kokonaisuuden PKI:n turvallisuudesta ja viittaavat mahdollisiin riskeihin.

### Keneen luotamme ja miksi?

Keneen luotamme ja miksi? Kryptografian näkökulmasta luotettavuus tarkoittaa sitä, että CA hallitsee avaimiaan turvallisesti. Onko tämä kuitenkaan riittävä perustelu sille, että sertifikaatteja jakava taho on luottamuksen arvoinen esimerkiksi arvokasta tietoa käsiteltäessä? Lisäksi voidaan kysyä, että kuka on valtuuttanut CA:n jakamaan valtuutuksia? Entä kuka on päättänyt, että tietty CA on luotettava?

### Kuka käyttää avaintani?

Yksi suurimmista riskeistä PKI:ssa liittyy omaan yksityiseen avaimeesi. Tavallinen käyttäjä säilyttää avaintaan lähes varmasti riittämättömän suojauksen takana. Emme voi tietenkään odottaa, että tavallinen käyttäjä suojaisi avaimensa samalla tasolla kuin esimerkiksi CA. Mutta miksi oman avaimen turvauksella on väliä käyttäjän kannalta? Jos yksityinen avaimesi on CA:n varmentama, voidaan se liittää suoraan sinuun, ja olet vastuussa kaikesta siitä mitä tällä avaimella allekirjoitetaan. Joidenkin lainsäädäntöjen alaisuudessa et voi edes kiistää avaimellasi allekirjoitettuja tapahtumia verkossa vaan olet juridisesti vastuussa. Vertauskohdaksi voidaan mainita esimerkiksi tietyt tilaukset puhelinlaskussasi. Voit kiistää tilanneesi matkalipun bussiin ja kauppiaalla on velvollisuus todistaa, että olet todella tehnyt kyseisen tilauksen. Näin et kuitenkaan voi toimia yksityiseen avaimeen liittyvien väärinkäyttöjen tapauksessa.

### Kuinka turvallinen varmentajan järjestelmä on?

Yksi suurimmista riskeistä PKI:ssa liittyy omaan yksityiseen avaimeesi. Tavallinen käyttäjä säilyttää avaintaan lähes varmasti riittämättömän suojauksen takana. Emme voi tietenkään odottaa, että tavallinen käyttäjä suojaisi avaimensa samalla tasolla kuin esimerkiksi CA. Mutta miksi oman avaimen turvauksella on väliä käyttäjän kannalta? Jos yksityinen avaimesi on CA:n varmentama, voidaan se liittää suoraan sinuun, ja olet vastuussa kaikesta siitä mitä tällä avaimella allekirjoitetaan. Joidenkin lainsäädäntöjen alaisuudessa et voi edes kiistää avaimellasi allekirjoitettuja tapahtumia verkossa vaan olet juridisesti vastuussa. Vertauskohdaksi voidaan mainita esimerkiksi tietyt tilaukset puhelinlaskussasi. Voit kiistää tilanneesi matkalipun bussiin ja kauppiaalla on velvollisuus todistaa, että olet todella tehnyt kyseisen tilauksen. Näin et kuitenkaan voi toimia yksityiseen avaimeen liittyvien väärinkäyttöjen tapauksessa.

### Kuka ”Timo Virtanen” hän on?

Sertifikaatit assosioivat julkiset avaimet yleensä nimien kanssa, mutta kuinka hyödyllistä tämä oikeasti on?

Kuvitellaan tilanne, jossa saat ystäväsi, Timon, sertifikaatin sähköpostilla. Saatat henkilökohtaisesti tuntea yhden Timo Virtasen, mutta kuinka monta tämännimistä henkilöä CA tuntee? Sertifikaatissa esiintyvä nimi on sinulle varmasti tuttu, mutta voitko olla täysin varma, että se on juuri oikea henkilö? Sertifikaattin nimeen lisätään yleensä muutakin tietoa, jotta nimestä saadaan tämän CA:n kannalta uniikki. Tiedätkö kuitenkaan näitä tietoja ystävästäsi? Entä sitä, että miltä CA:lta hänen sertifikaatin pitäisi tulla?

Nimien merkitys pienenee kun sertifikaattien määrät kasvavat. Nimet saattavat toimia perheen tai luokan mittakaavassa, mutta koko maailmaa ajetellen niillä ei juurikaan ole merkitystä sertifikaattien osalta.

### Onko CA:lla valtuuksia?

CA:lla on valtuuksia tehdä sertifikaatteja, mutta onko tällä arvovaltaa koskien sertifikaattien sisältöä? Esimerkiksi SSL Serverin sertifikaatissa mainitaan kaksi meitä kiinnostavaa asiaa. Avaimen haltijan nimi, sekä serverin DNS-nimi. DNS-nimien antamisesta vastaavat eri viranomaiset, eikä yksikään yleisimpien selaimien listaamista CA:sta ei kuulu siihen joukkoon. Tämä tarkoittaa, että sertifikaatissa mainittu DNS -nimi ei ole valtuutettu lause.

Mainitsimme myös avaimen haltijan nimen. SSL Serverin tapauksessa tämä nimi kuuluu mitä luultavimmin jollekin yritykselle. Niin kuin DNS-nimen kohdalla, yritysnimikkeistäkin vastaa jonkinlainen viranomainen, eivätkä selaimien sisältävät CA:t eivät kuulu myöskään tähän joukkoon.

### Onko käyttäjä osa turvallisuussuunnittelua?

Oletetaanko turvallisuuden suunnittelussa, että käyttäjä toimii parhaiden käytäntöjen mukaan? Oletetaanko, että käyttäjä tarkastaa käyttämänsä sivun sertifikaatit ja toimii saamansa tiedon perusteella. Sivun sertifikaatti voi olla täysin liittymätön siihen sivuun, jolla käyttäjä vierailee, eikä tämä tiedo ole itsestään näkyvillä. Entä osaako käyttäjä hyödyntää saamaansa tietoa?

Jos käyttäjä on osa turvallisuussuunnittelua, voi hänen huolimattomuutensa rikkoa muuten toimivan turvallisuuden asetelman.

### Kuinka turvallisia sertifikaatteihin liittyvät käytännöt ovat?

Sertifikaatit eivät itsestään luo turvallisuutta, vaan niistä saatavan hyödyn eteen täytyy nähdä vaivaa. Hyviin käytäntöihin liittyy monia seikkoja:

- Onko avaimen käyttöikä laskettu, vai onko se valittu sattumalta tai yleisen käytännön mukaan? Avaimilla on kryptograafinen käyttöikä, joka elää uusien teknologioiden mukaan. Voidaan siis laskea aika, joka salauksen murtamiseen kuluu. Lisäksi voidaan laskea aika, jonka sisällä on todennäköistä, että avain menetetään esimerkiksi varkauden vuoksi.

- Tukeeko sertifikaatin myyjä sulkulistojen käyttöjä? Sulkulistat (Certification Revocation List, CRL) on sisäänrakennettu joihinkin sertifikaattistandardeihin, mutta monet välttelevät niiden käyttöä, koska ne ovat vanhanaikaisia ja kankeasti käytettäviä. Mutta jos niitä ei käytetä, niin miten sertifikaattin sulkeminen / peruminen suoritetaan?

- Jos sulkulistoja sovelletaan, niin miten avaimien vaarantuminen tai väärinkäyttö havaitaan, jotta lisäys sulkulistalle laukeaa? Voidaanko sulkeminen tehdä jälkikäteen, jos sertifikaatin haltija kieltää käyttäneensä avainta aikaisemmin johonkin kyseenalaiseen?

- Kuinka pitkä julkisesta avaimesta luodaan ja miksi kyseinen pituus on valittu? Käyttääkö "kauppias" 512-bittistä RSA avainta, koska se on nopeampi, vai 2048-bittistä avainta, koska joku sanoi, että se on turvallisempi?

- Vaatiiko näiden sertifikaattien oikeanlainen käyttö toimintaa käyttäjän taholta?

SSL yhteyden muodostuminen on helppo todeta selainta käytettäessä (vihreä lukko), mutta oletetaanko, että käyttäjä tarkistaa kenen kanssa hän on oikeasti salatussa yhteydessä? Jos et lue vastaanottamaasi sertifikaattia, et saa tätä selville.

- Vaikka lukisitkin sertifikaatin, et välttämättä tunnista toista osapuolta, mutta voit ainakin arvioida paremmin, että

haluatko jakaa salaista tietoa.

- Käytetäänkö sertifikaatteja vain koska ne ovat tällä hetkellä muodissa ja niistä puhutaan? Käytetäänkö niitä, vaikka ei tiedetä mitenne toimivat ja miten niitä kuuluisi käsitellä? On realistista epäillä, että suuri osa sertifikaateista on asennettu väärin, eikä niiden käytöstä todellisuudessa ole kaikille asiakkaille juuri minkäänlaista hyötyä.

[3]

## WoT ongelmat

### Avainten hallinta

Matka PGP-avainparin luomisesta käyttökelpoiseen WoT:iin on suuri. Lähtökohtaisesti jokainen uusi kontakti tulisi varmentaa kasvokkain henkilöllisyystodistusta vastaan. Yksi hyvä paikka oman WoT:in rakentamiseen on avaintenjako-bileet, mutta näitä ei välttämättä pienemmissä maissa juuri järjestetä, saati sitten pienemmillä paikkakunnilla. Nopealla google haulla ei esimerkiksi Suomesta löytynyt tällaisia tapahtumia.

Mikäli avaimia ei varmenneta henkilökohtaisesti avaimen sormenjälkeä vertailemalla, altistaa julkisen avaimen lataaja itsensä potentiaalisesti MITM-hyökkäykselle.

### Skaalautuvuus

WoT-mallissa jokaisen käyttäjän julkinen avain ladataan avain serverille. Toimiakseen suuressa mittakaavassa maailmanlaajuisesti WoT-servereiden tulisi olla valtavia, mikä ei tällä hetkellä ole kovinkaan realistinen ajatus. Systeemi toimii tällä hetkellä suhteellisen hyvin ”pienen porukan” kesken.

### Luottamus

Kaikki WoT:issa perustuu luottamukseen. Käyttäjä voi itse hallita omia luottamussuhteitaan. Ei ole kuitenkaan realistista, että yhdellä käyttäjällä olisi kovin suuri luottamuksen verkko. Tämän takia käyttäjä voi myös periä omien luottamiensa hekilöiden luottamussuhteet, vertaa facebookissa henkilöllä x on 3 yhteistä sinun kanssasi. Mutta kysymys herää, kuinka pitkälle ketjua pitkin olet valmis kulkemaan oman piirisi ulkopuolisilla luottosuhteilla?

# Lähteet

1. https://pdfs.semanticscholar.org/0fc4/0e88e1aec293ddfbbc5b82c3e294e8c0ed14.pdf

2. https://en.wikipedia.org/wiki/Root\_certificate

3. https://www.schneier.com/academic/paperfiles/paper-pki-ft.txt

4. https://www.gnupg.org/

5. https://www.youtube.com/watch?v=Lq-yKJFHJpk

6. https://cran.r-project.org/web/packages/gpg/vignettes/intro.html