

EndCryptor

Versio 2.5.5 www.endcryptor.com. Valmistaja Enternet Oy.

Contents

Yleiskuvaus	2
Ominaisuudet	3
Pikaohje	4
Lähetys ja vastaanotto	6
Optiot	8
Työkalut	10
Varmistus ja palautus	13
Vie (export) selväkieliseen muotoon	15
Siirrä tietokanta	16
Unohdettu salasana	18
Kovalevyn hajoaminen	19
Lisensointi	20
Kontaktin lisätiedot	22
Julkisten avainten perustiedot	24
SSL:n ja selainpohjaisen salauksen riskit	27
Tekniset tiedot	33

Tämän documentin päiväys: Maaliskuu 26, 2025

Yleiskuvaus

Erinomainen suoja nykyajan hyökkäyksiä vastaan

EndCryptor suojaa vanhat salatut viestit vaikka hakkeri saisi haltuunsa nykyiset salausavaimet. EndCryptor on suunniteltu suojaamaan ennen hakkerointia muodostettu salattu liikenne ja myös toipumaan hyökkäyksestä.

Helppokäyttöinen

Käyttäjän ei tarvitse olla salaustekniikan ammattilainen. Ohjelman käyttöliittymä on samanlainen kuin tavanomaisessa sähköpostiohjelmassa.

Päästä päähän salattu

Viesti salataan lähettäjän koneella ja salaus avataan vastaanottajan koneella. Vain oikea vastaanottaja voi avata viestin.

Kvanttivyökkäyksen kestävä

Saattaa olla mahdollista, että ennen vuotta 2030 on kvanttietokoneita, jotka voivat avata klassiset julkiset avaimet. EndCryptor käyttää klassisten julkisten avainten lisäksi uusia kvanttivyökkäyksen kestäviä avaimia. *On otettava huomioon, että nykyinen salattu liikenne on helppo kopioida ja tallettaa odottamaan kvanttikoneiden valmistumista ja niiden avulla tapahtuvaa salauksen avausta.* USA'n standardointiorganisaation raportissa 'NIST Internal Report NIST IR 8547 ipd' todetaan: 'even if quantum computers are a decade away, organizations must begin the migration to post quantum cryptography today to avoid having their encrypted data exposed once quantum computers become operational in the future. This threat, often referred to as "harvest now, decrypt later," underscores the necessity of acting immediately...'

Nykyaikainen salausmenetelmä ja nykyaikaiset julkiset avaimet

Symmetrisen salausmenetelmän ja julkisten avainten toteutus perustuu julkisesti nähtävillä ja saatavilla olevaan koodiin. Klassinen avain on Curve25519, kvanttivyökkäyksen kestävä avaimet ovat Kyber-1024, Frodokem-1344 ja mceliece6688128f (round 4). Kyber on USAn standardi, Saksan valtion 'Federal Office for Information Security' suosittelee Frodokem ja mceliece avainten käyttämistä, katso BSI TR-02102-1. Klassisia ja kvanttivyökkäyksen kestäviä avaimia käytetään hybrid asetelmassa, jolloin hyökkääjän on kyettävä murtamaan kaikki asetelmassa olevat avaimet. Tämä hybridi avainten laskenta tehdään tavalla 'Concatenate hybrid key agreement scheme', raportissa ETSI TS 103 744 V1.1.1 ('ETSI is a European Standards Organization (ESO). .. the recognized regional standards body dealing with telecommunications, broadcasting and other electronic communications networks and services.'

Ominaisuudet

- Sekä lähettäjällä että vastaanottajalla tulee olla EndCryptor asennettuna. Käyttäjä tarvitsee toimivan sähköpostiosoitteen - samaa osoitetta voidaan käyttää tavallisiin ja salattuihin sähköposteihin. Viestit kirjoitetaan EndCryptorilla ja ne vastaanotetaan sillä. Salattu viesti on tiedosto, joka on tavallisen sähköpostin liitteenä.
- Lähetetyt ja vastaanotetut viestit ovat talletettuina salattuina käyttäjän tietokoneella - ne voidaan lukea, kun oikea sisäänpääsyn salasana on annettu EndCryptoriin. Viesteihin voidaan tehdä etsintöjä ja niitä voidaan siirrellä eri käyttäjän luomien kansioiden välillä.
- Viestit voidaan viedä (exportata) selväkielisinä eml formaattisina levyille. Näin ne voidaan tuoda (importata) sähköpostin arkistointisovelluksiin. Niitä voidaan katsella eri sähköpostisovelluksilla ja ne voidaan raahata ja tiputtaa niissä oleviin sähköpostikansioihin. Tämä export -ominaisuus mahdollistaa viestien selväkielisen arkistoinnin.
- Talletetut salatut viestit voidaan kopioida varmistuksiin ja ne voidaan avata varmistuksista joko henkilökohtaisella tai yrityskohtaisella export-avaimella. EndCryptor voi ottaa varmistuksen omasta tietokannastaan ja sitten palauttaa sen käyttöön. Tuo varmistus voidaan salata. Vaihdeettavat viestit voidaan kirjoittaa varmistusmielessä myös varmistus-sijaintiin heti kun ne kirjoitetaan levyille.
- Viestien tiivistys. Haluttu määrä satunnaisia tavuja lisätään viestiin (esim. 0 - 5000), jotta alkuperäisen viestin pituus häivyttettäisiin - salatut viestit ovat eri pituisia, vaikka niiden sisältö on sama.
- Viestillä voi olla useampi vastaanottaja. Kontakteja voi ryhmitellä.
- Jos internet -yhteyttä pidetään liian suurena riskinä, voidaan EndCryptoria käyttää kokonaan irti verkosta. Kun tällöin viesti talletetaan levyille, voidaan sen vastaanottajat tallettaa tekstimuodossa. Viesti ja lista sen vastaanottajista voidaan tallettaa käyttäjän määrittelemään kansioon levyllä. Nämä siirretään käyttäjän toimesta varsinaiselle internet-yhteyden omaavalle koneelle esim. muistitikulla. Samoin avattavat saapuvat viestit siirretään EndCryptor-koneelle käyttäjän toimesta.
- EndCryptor voidaan asettaa tarkkailemaan haluttua kansiota levyllä ja ilmoittamaan, kun sinne tulee salattuja viestejä.
- EndCryptorin tietokanta ja viestit voidaan sijoittaa siirrettävälle medialle (esim. USB tikulle) ja käyttää sieltä. Näin on mahdollista käyttää EndCryptoria esim. toimiston ja kodin tietokoneelta (kun tietokannan ja viestit sisältävä USB tikku on silloin koneessa kiinni). Tyhjän kannan koko on noin 1MB.

Pikaohje

Jos haluat aloittaa suojatun sähköpostiviestinnän, tulee sinulla ensin olla vastaanottajan julkinen avainpaketti. Kun se on saatavilla, raahaa ja tiputa se EndCryptoriin. Voit myös klikata Uusi kontakti nappulaa vastaanottaaksesi paketin. Viestisi vastaanottajalla tulee myös olla sinun julkinen avainpakettisi.

Voit tallettaa oman julkisen avainpakettisi levyille Menun kohdasta Työkalut→Oma julkinen avainpaketti.

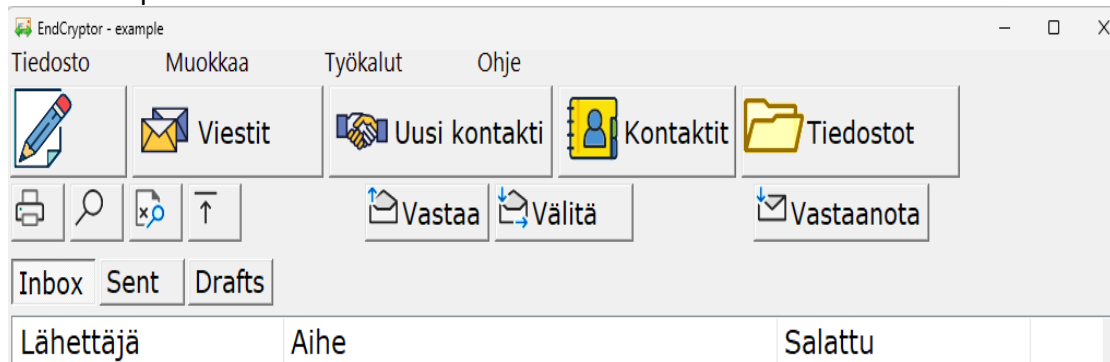
Jos jokin ryhmä haluaa kommunikoida jäsenten välisesti, on kätevintä koota heidän avainpakettinsa yhteen zip -tiedostoon ja sitten jakaa se jäsenille turvallisesti suojatun web sivuston tai suojatun tiedostonsiirron avulla. Kun saatu avainpaketti tiputetaan EndCryptoriin, otetaan automaattisesti siitä uudet kontaktit käytettäviksi.

Kun EndCryptorissa kaksi henkilöä alkavat kommunikoida, he sopivat asiasta ja lähettävät jollakin tavoin esim. normaalin sähköpostin liitteenä toisilleen omat julkiset avainpakettinsa. Tämän jälkeen he voivat vaihtaa viestejä. On siis huomattava, että viestin lähettäjällä tulee olla vastaanottajan avainpaketti ja viestin saajalla tulee olla lähettäjän avainpaketti. Avainpaketti sisältää mm. lähettäjän julkiset allekirjoitusavaimet (Edwards ja Dilithium avaimet), joilla vastaanottaja tarkastaa, että viesti tulee avainpaketin luojalta.

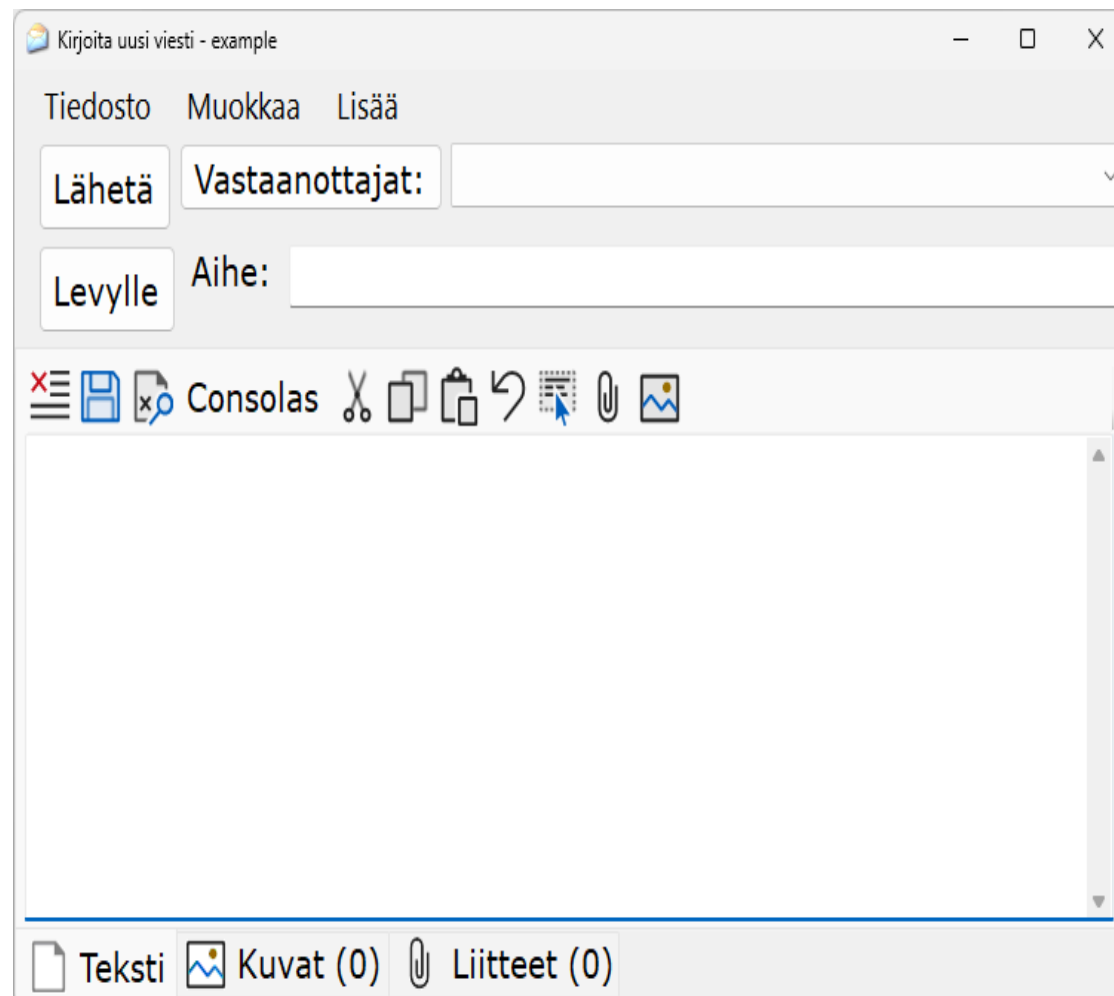
Kun alussa siis vaihdetaan avainpaketteja tulee niin tehdä vain luotettavan tahon kanssa, aiotaanhan jakaa salatuissa viesteissä luottamuksellista tietoa. On oltava tarkkana, että toinen osapuoli on se, joka hän väittää olevansa ja esim. sähköpostiosoitteen tulee olla sama kuin aikaisemmin tai selvästi henkilölle ja tämän organisaatiolle kuuluva. Kun avainpaketti on EndCryptorissa ja kontakti on luotu, ei sen sähköpostiosoitetta voi muuttaa ennenkuin viestejä on vaihdettu.

Jos pidetään mahdollisena, että avainpaketteja on muutettu niiden ollessa lähetyksessä, voidaan se havaita menemällä Kontaktit->Lisätiedot->MITM hyökkäystä dialogiin.

Esimerkki pääikkunasta:



Esimerkki uuden viestin kirjoittamisesta:



Lähetys ja vastaanotto

Alla esimerkki sähköpostitilin asetuksista. Käyä menun Työkalut→Sähköpostitilit valintaa.

Muokkaa sähköpostitilin asetuksia ✕

Sähköposti

Lähetysasetukset

Käyttäjä

Piilota merkkien arvot +

Salasana

SMTP palvelin

Vastaanottoasetukset

Sama käyttäjä ja salasana kuin lähetyksessä

Käyttäjä

Piilota merkkien arvot +

Salasana

IMAP palvelin

Hae uudet viestit automaattisesti

Vastaanota käyttäen omaa sähköpostiohjelmaa:

EndCryptor viestin (.nnd päätteisen tiedoston) voit avata sen ollessa sähköpostin liitteenä jollain seuraavalla tavalla:

- Tallenna liite ja raahaa ja pudota se Resurssienhallinasta EndCryptoriin.
- Tallenna liite ja valitse liite EndCryptorin Tiedostot nappulan kautta.

Lähetä itse käyttäen Levylle nappulaa

Rastita Työkalut→Optioista joko 'Lähetä itse levyltä' tai 'Valitse lähetysaikana'. Tällöin uudessa viestissä on esillä 'Levyllä' nappula, mikä tallettaa lähetettävän viestin levyllä. Viesti on .nnd loppuinen tiedosto, jonka voit toimittaa vastaanottajalle haluamallasi tavalla. Tuo .nnd tiedosto voidaan myös raahata ja pudottaa 'Lähetetyt' kansioista tartumalla siihen sen nimestä otsikon oikeassa kulmassa.

Optiot

Viestin allekirjoitus

Teksti, joka tulee viestin loppuun – tyyppillisesti lähettäjän nimi ja yritys.

Käytä piilokopio kenttää piilottamaan vastaanottajia

Uuden viestin vastaanottajien ensimmäinen henkilö tulee lähtevän sähköpostin 'Vastaanottajat' kenttään. Jos vastaanottajina on vain ryhmiä tulee joku vastaanottajista tuohon kenttään.

Salattuun viestiin lisättävien satunnaisten tavujen määrä

Tavuja lisäämällä voidaan piilottaa viestin todellinen pituus – salatut viestit ovat eri pituisia vaikka niiden sisältö on sama.

Pakkauksen lisäasetuksia

Pakkauksella tarkoitetaan tiedon tiivistämistä. Pakkauksen purku palauttaa tiedon alkuperäiseen tilaan.

Asetus 'Huomaa pakkautumattomuus automaattisesti' merkitsee, että isohkot liitetiedostot, jotka eivät pienene niitä tiivistettäessä, jätetään pakkaamatta. Voit myös antaa lisää tiedostotyyppisiä, joita ei pakata.

Kopioi viesti pilvipalveluun, jos sen koko ylittää:

Tämä optio näyttää ikkunan, josta iso salattu viesti voidaan raahata tai kopioida pilvipalveluun. Näytetyt koot: oikea koko/koko verkossa. Tuo koko verkossa vastaa sähköpostin palveluntarjoajan asettamaa suurinta sallittua liitteiden tai itse sähköpostin kokoa.

1. Kopioi salattu viesti (.nnd loppuinen tiedosto) pilvipalveluun.
2. Lähetä saatu linkki EndCryptorilla vastaanottajille.

Viestin liitteiden suurin yhteenlaskettu koko voi olla 2 teratavua (TB).

HUOM: Salatun sähköpostin sisältävä tiedosto voidaan kopioida myös Lähetetyt -kansion tiedostonimestä.

Ylikirjoitus

Kun tiedosto poistetaan levyltä käyttöjärjestelmä vain merkitsee sen poistetuksi. Varsinainen sisältö jää levyille. EndCryptor tavallisesti ylikirjoittaa tiedoston nolilla ennen kuin poistaa sen. Tilanne on ongelmallinen, jos levy on SSD (Solid State Drive) levy. SSD levy ei sijoita uutta sisältöä entisen päälle – näin ylikirjoittamisesta ei ole hyötyä. Tässä voi määritellä toimintaa levykohtaisesti.

Tarkkaile tähän kansioon tulevia .ndd tiedostoja

EndCryptor käynnistää ohjelman 'efw.exe' - EndCryptor File Watcher - joka pyytää käyttöjärjestelmää kertomaan aina kun uusi .ndd loppuinen tiedosto tulee tähän kansioon. Ohjelma myös itse tarkastaa kansion 5 minuutin välein. Uusi tiedosto siirretään oletus sisääntulokansioon ja käyttäjää informoidaan. Huomaa, että jos kansio on pilvessä, ei pilven ohjelmisto ehkä informoi käyttöjärjestelmää eikä EndCryptor tällöin saa tätä tietoa. Myös pilvi voi näyttää tiedoston olevan kansiossa ennenkuin se on kokonaan saatavilla - tästä voi koitua ongelmia kun 'efw.exe' yrittää siirtää tiedoston sisääntulokansioon. Kun 'efw.exe' on käytössä, on tehtäväpalkin ilmaisinalueella pieni EndCryptor File Watcher'in kuvake. Ohjelman, joka kirjoittaa tiedoston tarkkailtavaan kansioon kannattaa nimetä tiedosto niin, että sillä on aluksi .tmp tiedostopääte. Kun tiedosto on kokonaan kirjoitettu, tulee se nimetä .ndd loppuiseksi.

Työkalut

Liitteiden asetukset

Tässä Menun Työkalut osassa määritellään hyvin isojen liitteiden käsittely. Näitä liitteitä ei salata uudelleen paikallista tallennusta varten kun niitä lähetetään ja vastaanotetaan. Vastaanotettaessa iso liite talletetaan selväkielisenä tässä annettuun kansioon. Kun sähköposti viedään (exportataan .eml muotoon) näitä isoja liitteitä ei exportata, vain sähköpostin teksti exportataan. Tässä myös annetaan suurin sallittu koko liitteelle, joka voidaan exportata (tämä koskee siis niitä liitteitä, jotka lähetettäessä tai vastaanotettaessa eivät ylittäneet hyvin ison liitteen rajaa).

Viestin liitteiden suurin yhteenlaskettu koko voi olla 2 teratavua eli 2 000 000 000 000 tavua. Viestin liitteiden suurin sallitu lukumäärä on 100.

Selaa

Kansio

C:\Users\\AppData\Local\Enternet_fi\EndCryptor\Instance_1\files\
sisältää nämä kansiot:

Kansio	Käyttö
erroneous	Vastaanotetut, mutta virheellisiksi havaitut viestit
incoming	Saapuneet uudet viestit
outgoing	Ulosmenevät sekä lähetetyt
processed	Saapuneet ja onnistuneesti avatut viestit

Saatat haluta joskus poistaa tiedostoja outgoing, processed ja erroneous kansioista. Optioissa voi rastittaa valinnan, jonka mukaan juuri lähetetty tiedosto poistetaan outgoing kansioista. Älä poista tiedostoa incoming kansioista, ellei ole olemassa jotain virhetilannetta, joka vaatii sitä. Jos samassa koneessa on eri identiteettejä eli instansseja niin ne nimetään seuraavasti: Instance_1, Instance_2, ...

Vastaanotetut varmenteet

EndCryptor tallettaa sähköpostipalvelimilta saadut varmenteet ja laskee niiden käyttökerrat ja näyttää varmenteiden ominaisuuksia. On mahdollista vaatia, että varmenne sisältää Certificate Transparency SCT-luettelo osan. Tällöin esimerkiksi estetään muiden kuin julkisesti hyväksytyjen Varmentajien (Certificate Authority) myöntämien varmenteiden käyttö, joita saatetaan käyttää liikenteen avaamiseen.

Varmenteita voidaan tuoda ja viedä. On mahdollista sallia ja kieltää varmenteita. Tietyn varmenteen salliminen/kieltäminen on hyvin kehittynyt optio ja edellyttää

käyttäjältä asiaan paneutumista. Syynä varmenteen salli/kielto -option tarjoamiseen on varmenteiden eli SSL/TLS salauksen infrastruktuuriin liittyvät ongelmat – tästä kerrrotaan enemmän englanninkielisessä teknisessä dokumentaatiossa. Tässä todetaan, että mikäli hyökkäys pahantahtoisella varmenteella onnistuu, hyökkääjä ei voi avata salattua viestiä mutta saa haltuunsa sähköpostitilin tunnuksen ja salasanan.

Lukijan on hyvä tietää, että jos lukija käyttää tavanomaista sähköpostiohjelmaa – joissa ei yleensä ole suojausta pahantahtoisia varmenteita vastaan – on mahdollista, että hän joutuu alttiiksi tälle hyökkäykselle.

EndCryptor laskee varmenteiden käyttökerrat ja vaikka käyttäjä ei käyttäisikään varmenteiden salli/kielto -optiota, hän kuitenkin tunnistaa hyökkäyksessä käytetyn varmenteen sen käyttökertojen perusteella. Esimerkiksi käyttäjä matkustaa ulkomaille ja joutuu siellä hyökkäyksen kohteeksi. Myöhemmin havaitaan, että jotakin varmennetta, jota sähköpostipalvelimen hallinnoija ei tunnista, on käytetty vain kerran.

Proxy asetukset

Jos proxya käytetään EndCryptor ohjaa lähetys ja vastaanotto liikenteen proxylle.

Proxy voi olla tässä tietokoneessa (osoitteessa '127.0.0.1') tai jossain verkossa. Proxya voidaan käyttää tarkkailemaan ohjelman toimintaa tai ohjaamaan liikenne haluttua reittiä sähköpostipalvelimille. Joskus proxeja käytetään anonymisaation saavuttamiseksi: käyttäjä yrittää piilottaa kohdepalvelimen tarkkailijalta, joka on lähellä käyttäjää ja piilottaa käyttäjän IP osoitteen tarkkailijalta, joka on lähellä palvelinta. Tässä tapauksessa käytetään tyyppiä socks5 proxya, esimerkiksi voidaan käyttää Tor anonymisaatioverkkoa (asetus socks5 proxy osoitteessa 127.0.0.1, portti 9150) ja asennetaan 'Tor Browser Bundle'. EndCryptor tekee yhden perusjutun estääkseen kohdepalvelimen paljastumisen - DNS kyselyä kohdepalvelimen IP osoitteen saamiseksi ei tehdä.

Tietoturva-asiantuntijat näyttävät olevan sitä mieltä, että absoluuttista anonymisaatiota on hyvin vaikea saavuttaa vaikka käytettäisiin hyvin erikoistuneita ohjelmia. Esimerkiksi sähköpostin ollessa kyseessä niin kun se lähtee lähettäjän palvelimelta niin monessa tapauksessa käytössä ei ole edes SSL/TLS suojausta vastaanottajan palvelimeen ja lähettäjän ja vastaanottajan sähköpostiosoitteet ovat näkyvillä.

On huomioitava, että EndCryptorin palvelinvarmenteen oletus tarkastusoptio (Kumoamistarkastus verkossa) voi paljastaa kohdepalvelimen. Jos tätä valintaa käytetään, Windows voi ladata verkosta uusia juurivarmenteita ja palvelimen varmenteen sulkulistan, varmenteen tarkastus voi myös lähettää sen sarjanumeron varmenteen myöntäjälle - tämä 'Online Certificate Status Protocol' liikenne voi paljastaa käyttäjän ja kohdepalvelimen IP osoitteen osaavalle tarkkailijalle. Tämän tilanteen välttämiseksi valitse menuussa Työkalut->Vastaanotetut varmenteet ja rastita valinta 'Hyväksy jos sallittu ja voimassaoleva' (sinun tulee ehkä tuoda ko.

varmenne saataville ensin). Lukijan, joka on äärimmäiseen asti tietoturvatietoinen on hyvä tietää, että kun varmennetta katsotaan Windowsissa, se tarkastetaan ja tämä voi käynnistää paljastavan liikenteen.

Varmistus ja palautus

Varmistusten näkökulmasta EndCryptor koostuu tietokannasta ja tallennetuista viesteistä. Tietokannassa ovat mm. salausavaimet ja muu tieto, jota tarvitaan ohjelman toimintaan. Sekä tietokannan tiedot että levyllä olevat viestit on salattu. Salattuja viestejä voi lukea ohjelman kautta, kun oikea sisäänkirjautumisen salasana on annettu – tämä on normaali tapa lukea viestejä. Toinen tapa on käyttää Export avaimia ja varmistettuja salattuja viestejä ja viedä (export) viestit selväkieliseen muotoon tiedostoiksi – näin viestit voidaan aina lukea vaikka edes tietokannan varmistusta ei olisi saatavilla, on vain oltava Export avaintiedosto ja levyllä talletetut viestit (tai niiden kopiot varmistuksessa). Henkilökohtainen Export avaintiedosto talletetaan ohjelman ensimmäisessä käynnistyksessä.

EndCryptor voi ottaa varmistukset tietokannasta ja viesteistä. Toinen vaihtoehto on, että yrityksen varmistusohjelmisto tekee tämän.

Kun EndCryptor käynnistyy, eikä olemassaolevaa tietokantaa löydy, niin yhtenä vaihtoehtona annetaan mahdollisuus palauttaa tietokanta varmistuksesta. Tämä tapahtuu esimerkiksi ensimmäisessä käynnistyksessä. Jos haluat simuloida tilannetta, niin nimeä kansio, jossa tietokanta on (EndCryptor_store) uudestaan (EndCryptor_store_org) ja käynnistä EndCryptor.

Kun tietokanta varmistetaan se voidaan vielä erikseen salata henkilökohtaisella Export avaimella.

Kun tietokanta on palautettu varmistuksesta, kysytään varmistettujen viestien sijaintia – tämän jälkeen kopioidaan tietokannan indeksoimat viestit niiden oikeaan paikkaan.

Viestit voidaan varmistaa, kun EndCryptor sulkeutuu tai välittömästi silloin kun viesti kirjoitetaan levyllä. **Täten on mahdollista aina avata jokainen lähetetty ja vastaanotettu viesti, vaikka käyttäjän kovalevy hajoaisi (mikäli varmistukset ovat muualla).**

Tietyn tyyppisten yritysten tai palveluiden on lain mukaan joissakin maissa pystyttävä näyttämään jokainen käsitelty sähköposti.

Varmistukset konfiguroidaan Työkalut→Varmistuksen asetukset valinnasta.

Export avaimia on kahdenlaisia: käyttäjän henkilökohtainen ja yrityksen avain. Yrityksen avaimen käyttö edellyttää sen erillistä asentamista käyttäjän toimesta. Kun eri käyttäjät asentavat yrityksen Export avaimen, voi tuon avaimen luoja avata kaikkien näiden käyttäjien talletetut viestit.

Viestien avaus varmistetuista viesteistä tehdään menusta Tiedosto→Vie varmistuksesta.

Mikäli yrityksen oma ohjelmisto tekee varmistukset (kanta ja viestit) seuraava kansio ja sen alikansiot tulee varmistaa:

C:\Users

Jos käyttäjä on sijoittanut tietokannan muualle kuin oletuspaikkaan, on tämä huomioitava. Käytä menun 'Työkalut→Selaa→Tietokannan kansiota' nähdäksesi missä tietokanta on.

Jos EndCryptor varmistaa tietokannan, siitä tehdään yksi tiedosto ohjelman sulkeutuessa. Tämä varmistus voidaan salata henkilökohtaisella Export avaimella. Jokaista päivää kohti säilytetään 5 viimeisintä varmistusta ja korkeintaan 2 edellistä varmistuspäivää talletetaan. Jos näiden sääntöjen perusteella varmistustiedostoa ei säilytetä, se ylikirjoitetaan ja poistetaan. Varmistuksen sisältävä kansio voi olla verkkokansio.

Viestit ovat seuraavassa kansiossa:

C:\Users\EndCryptor_store\emsgs

ellei käyttäjä ole sijoittanut tietokantaa muualle kuin oletuskansioon. Ylläolevassa 'Instance_X' tarkoittaa Instance_1, Instance_2 jne. eri identiteettien lukumäärän mukaisesti.

Viestejä voi varmistaa koska tahansa, myös ohjelman ollessa käynnissä.

Vie (export) selväkieliseen muotoon

Kun viesti lähetetään tai vastaanotetaan, se salataan uudestaan levyllä talletusta varten (käyttäen eri salausavaimia kuin .nnd viestissä). Nämä paikallisesti tallennetut viestit voidaan varmistaa kopioimalla ne sopivalle medialle. Ne voidaan myöhemmin avata eli viedä (export) näistä kopioista ilman tietokantaa käyttäen henkilökohtaista tai yrityksen Export avainta.

Kun EndCryptor käynnistetään ensimmäisen kerran, se tallettaa henkilökohtaisen (salasanalla suojatun) Export avaimen. Lisäksi käyttäjä voi asentaa erillisen yrityksen Export avaimen. Yrityksen Export avaimen avulla voidaan avata usean eri käyttäjän viestejä – tämän voi tehdä tuon yrityksen avaimen luoja. Yrityksen ei tarvitse välttämättä käyttää samaa avainta kaikille käyttäjille, voidaan käyttää esimerkiksi osastokohtaisia avaimia.

Export avaimet kannattaa tallettaa siirrettävälle medialle, esimerkiksi USB muistille.

Oletusarvoisesti viestit ovat kansiossa:

```
C:\Users\\AppData\Local\Enternet_fi\EndCryptor\Instance_X\  
EndCryptor_store\emsgs
```

Yksittäiset salatut tiedostot näyttävät tältä:

```
10_1885387336_a_1663277279_789AF06969FC0275.dat on itse viesti  
10_1885387336_b_1984071552_789AF06969FC0275.dat on viestin liite
```

Viesti viedään eml formaattiin, jota esimerkiksi sähköpostin arkistointijärjestelmät ymmärtävät. Ne voidaan myös raahata ja pudottaa tavanomaisten sähköpostiohjelmien paikallisiin kansioihin. Viety selväkielinen viesti sisältää itse viestin ja sen liitteet.

EndCryptor pitää kirjaa siitä, mitkä viestit on viety.

Siirrä tietokanta

Käyttäjän tietokone voi sisältää useita eri EndCryptorin instansseja. Tyypillisesti vain yhden, mutta jos henkilöllä on erilaisia organisatoorisia rooleja voi hänellä olla eri EndCryptor tietokanta jokaiselle eri identiteetille. Voi tulla tilanne, jossa organisatoorinen rooli siirtyy toiselle henkilölle ja siihen liittyvä instanssi tietokantoinen tulee siirtää toiseen tietokoneeseen.

Siirrä tietokanta ja tallennetut viestit toiseen tietokoneeseen USB tikun avulla:

Menetelmä 1.

1. Aktivoi siirrettävä instanssi ja paikallista tietokanta menusta 'Työkalut→Selaa→Tietokannan kansiota'. Sulje tämä instanssi ja laita hiiri kansion 'EndCryptor_store' päälle ja tee oikean hiirinäppäimen klikkaus. Valitse 'Lähetä kohteeseen' ja ota kohteeksi USB tikku. Windows kopioi tietokannan ja tallennetut viestit muistitikulle.
2. Nimeä tietokoneellasi oleva kansio 'EndCryptor_store' nimellä 'EndCryptor_store_vanha'.
3. Käynnistä EndCryptor kohdetietokoneessa. Jos tämä on EndCryptorin ensimmäinen käynnistys kohdekoneessa, niin 'Määritä tietokanta' ikkuna tulee esille. Mene kohtaan 5.
4. Jos 'Määritä tietokanta' ikkuna ei tule esille, on ensimmäisessä esille tulevassa ikkunassa 'Lisää identiteetti' nappula oikeassa yläkulmassa. Paina sitä nappulaa. Anna identiteetille nimi (sen organisatoorisen roolin mukainen) ja paina 'Lisää' nappulaa. Odota kunnes ikkuna 'Määritä tietokanta' tulee esille.
5. Ikkunassa 'Määritä tietokanta' valitse '**Lisää olemassaoleva kanta**' ja paina OK. Valitse sitten USB tikulla oleva sinne kopioitu 'EndCryptor_store' kansio ja paina OK. EndCryptor kopioi nyt tietokannan ja viestit oikeaan paikkaan kohdekoneessa. Kopioinnin jälkeen EndCryptor sulkeutuu automaattisesti.
6. Käynnistä EndCryptor kohdekoneessa ja valitse juuri luotu instanssi, joka on valmis käyttöön.

Oletetaan nyt, että haluat käyttää samaa identitettiä kahdelta eri tietokoneelta – kuten esimerkiksi toimiston ja kodin tietokoneelta. Tässä tapauksessa tietokannan on oltava pysyvästi USB tikulla tai vastaavalla mediolla, joka liitetään aina kulloinkin käytettävään tietokoneeseen ennenkuin EndCryptor käynnistetään.

Siirrä tietokanta ja viestit USB tikulle, käytä sitä 2 eri koneelta A (nykyinen, kanta tässä) ja B:

Menetelmä 2.

1. Tee edellisen Menetelmä 1:n askeleet 1 ja 2. Muista nimetä A:n kovalevyllä oleva kanta nimellä 'EndCryptor_store_vanha'.
2. Käynnistä EndCryptor koneessa A. Jos ikkuna 'Määritä tietokanta' tulee esille mene kohtaan 4.
3. Jos ikkuna 'Määritä tietokanta' ei tule esille, niin ensimmäisen esille tulevan ikkunan oikeassa yläkulmassa on nappula 'Lisää identiteetti'. Paina sitä. Anna identiteetille nimi ja paina 'Lisää' nappulaa. Odota kunnes ikkuna 'Määritä tietokanta' tulee esille.
4. Ikkunassa 'Määritä tietokanta' valitse '**Paikallista olemassaoleva kanta**' ja paina OK. Valitse USB tikulla oleva sinne juuri kopioitu kansio 'EndCryptor_store' ja paina OK. Tämä EndCryptorin instanssi käyttää nyt USB tikulla olevaa kantaa. Tarkasta, että voit lukea tallennettuja viestejä.
5. Sulje EndCryptor koneessa A ja liitä USB tikku toiseen tietokoneeseen B.
6. Käynnistä EndCryptor koneessa B. Jos ikkuna 'Määritä tietokanta' tulee esille, mene kohtaan 8.
7. Jos ikkuna 'Määritä tietokanta' ei tule esille, niin ensimmäisen esille tulevan ikkunan oikeassa yläkulmassa on nappula 'Lisää identiteetti'. Paina sitä. Anna identiteetille nimi ja paina 'Lisää' nappulaa. Odota kunnes ikkuna 'Määritä tietokanta' tulee esille.
8. Ikkunassa 'Määritä tietokanta' valitse '**Paikallista olemassaoleva kanta**' ja paina OK. Valitse USB tikulla oleva sinne juuri kopioitu kansio 'EndCryptor_store' ja paina OK. Tämä EndCryptorin instanssi käyttää nyt USB tikulla olevaa kantaa. Tarkasta, että voit lukea tallennettuja viestejä.

Ota huomioon, että ei ole mahdollista käyttää USB tikulla olevaa kantaa ja sitten alkaa taas käyttämään koneessa A olevaa vanhaa kantaa. Kun viestejä vaihdetaan tietokantaa päivitetään sisältämään uusia klassisia ja kvanttihyökkäyksen kestäviä avaimia. Tämä saatu tieto menetetään, jos vanhaa versiota kannasta käytetään. Jos haluat siirtää kannan USB tikulta tietokoneeseen tee Menetelmä 1:n askeleet 3-6.

Unohdettu salasana

Vain oikea sisäänkirjautumisen salasana mahdollistaa tietokannan ja siten ohjelman käytön.

Mikäli viestien liitteitä on selväkielisenä, ovat ne kansiossa:

...EndCryptor_store\pltxt_files

Voit viedä tallennetut viestit selväkieliseen muotoon

Voit käyttää Export avaimia ja viedä viestit selväkieliseen muotoon. Tarvitset avaintiedoston ja sen salasanan. Henkilökohtainen Export avaintiedosto tallennettiin ohjelman ensimmäisen käynnistyksen yhteydessä. Sinun tulee luoda uusi identiteetti, jotta voi käyttää ohjelmaa sen kautta ja viedä sen identiteetin viestit selväkielisiksi, jonka salasana on unohtunut. Tallennetut viestit ovat levyllä, tyypillisesti kansiossa:

C:\Users\\AppData\Local\Enternet_fi\EndCryptor\Instance_X\
EndCryptor_store\emsgs

Ylläolevassa kansiopolussa identiteettien vaihtuminen muuttaa Instance_1 osaa (Instance_1, Instance_2, ...).

Toimi seuraavasti:

1. Nimeä nykyinen kansio 'EndCryptor' uudestaan nimellä 'EndCryptor_vanha' niin että polku siihen on [C:\](#)...\Enternet_fi\EndCryptor_vanha\
2. Käynnistä EndCryptor ja valitse 'Aloita 60 päivän koeaika' ja asenna uusi EndCryptor. Tarkoituksena on mahdollistaa viestien vienti tämän instanssin avulla. Voit käyttää myös jotain toimivaa instanssia, jos sellainen on olemassa, tällöin ylläolevaa askelta 1 ei tarvita.
3. Kun EndCryptor on käynnissä valitse menusta 'Tiedosto→Vie varmistuksesta'.
4. Valitse kansio: [C:\](#)...\Enternet_fi\EndCryptor_vanha\Instance_X\
EndCryptor_store\emsg, missä X on unohdetun salasanan instanssi.
5. Valitse kansio, johon viestit viedään.
6. Noudata annettuja ohjeita.

Jos käytössäsi on useita eri identiteettejä nimeä 'EndCryptor_vanha' takaisin nimellä 'EndCryptor', jotta voit taas käyttää niitä.

Lisää tietoja tämän dokumentin osiossa 'Vie (export) selväkieliseen muotoon'.

Kovalevyn hajoaminen

EndCryptor vaihtaa jatkuvasti uusia julkisia avaimia kontaktien kanssa viestejä vaihdettaessa – tämä edellyttää synkronisaatiota kontaktien välillä. Jos vanha tietokanta, jossa ei ole uusimpia muutoksia, palautetaan varmistuksesta, voi sattua, että jonkin viestin vastaanottaja ei saakaan saapunutta viestiä avattua. Tällöin on molempien osapuolten poistettava toisensa kontakteista. Kontaktin deletoiminen ei vaikuta jo avattujen viestin näkymiseen ohjelmassa. Sitten toinen osapuoli lisää toisen takaisin kontakteihin ja lähettää viestin. Sen avauduttua vastaanottajalla voidaan luottaa siihen, että kaikki viestit osapuolten välillä taas avautuvat.

Lisensointi

Ohjelma lopettaa lähetyksen ja vastaanoton kun 60 päivän koeaika on päättynyt ellei lisenssiä ole. Tämä tapahtuu myös, jos aikaperusteinen lisenssi umpeutuu. Tallennettuja viestejä voi aina katsella.

Jokainen tietokone, jossa on EndCryptorin tietokanta, tarvitsee lisenssin. Samassa tietokoneessa voi olla useita eri EndCryptor instansseja eli tietokantoja eli käyttäjän identiteettejä (käyttäjän eri rooleja varten) - vain yksi lisenssi tarvitaan yhtä tietokonetta kohti. Sama lisenssi tulee asentaa kaikkiin samassa koneessa oleviin eri instansseihin. Tietokone, jossa on vain ohjelmakoodi (ei kanta) ei tarvitse lisenssiä - tällöin siihen liitetään tarvittaessa esim. USB muistitikku, jossa kanta on.

Siirrettävä USB muistiväline, joka sisältää kannan tarvitsee lisenssin, muistiväline voi sisältää useita eri identiteettejä eli kantoja mutta vain yksi lisenssi tarvitaan.

Jos tietokone on verkon palvelin niin jokainen palvelimella oleva EndCryptor kanta tarvitsee oman lisenssin (emme suosittele kannan sijoittamista palvelimelle).

Lisenssejä voi tilata ohjelman kautta tai websivulta www.endcryptor.com. Jos tilaus tehdään ohjelman kautta, on maksutapa ennakkomaksu pankkisiirrolla. Websivulta tilatut ja samalla maksetuksi tulevat lisenssit toimitetaan tilauksen yhteydessä sähköpostilla.

Jos tilaus tehdään ohjelman kautta ennakkomaksulla voi tilauksen käsittely kestää yhden työpäivän. Yksi henkilö vastaanottaa sähköpostilla lisenssitiedoston, joka voi sisältää oikeuden useisiin lisensseihin (sisältää siis maksetun lukumäärän). Tämä tiedosto annetaan organisaatiossa niille, jotka lisenssiä tarvitsevat.

Lisenssejä on kahdenlaisia: aikaperusteisia ja versioon perustuvia.

Aikaperusteinen lisenssi antaa oikeuden käyttää uusinta versiota lisenssin loppumiseen saakka. Uudista aikaperusteinen lisenssi, kun on alle 1 kuukausi sen loppumiseen. Tällöin uuden lisenssin aikaan lisätään vanhan käyttämätön osuus. Muissa tapauksissa lisenssin alkamispäivä on sen myöntämispäivä. Versioperusteinen lisenssi antaa oikeuden käyttää tiettyä versiota ajasta riippumatta. Lisenssi esimerkiksi versiolle 2 on lisenssi kaikille ohjelman versioille 2.x, kaikilla x:n arvoilla.

Maksutiedot ennakkomaksussa:

Enternet Oy
Finland
Alv tunnus: FI 08210504

Pankki: Nordea Bank Finland Plc, Helsinki
SWIFT: NDEAFIHH
IBAN numero: FI08 1220 3000 2499 00

Tekninen huomautus:

Yksittäiset salatut viestit eivät sisällä sellaisia tietoja, joiden perusteella Enternet Oy voisi päätellä viestin olevan tietyn lisenssinhaltijan lähettämä.

Kontaktin lisätiedot

Tuhoa saapumattoman viestin salausavain

Paina 'Kontaktit' valitse kontakti ja paina 'Lisätiedot' ja valitse 'Info'. Esille tulee:

Tietoa viesteistä, jotka suojattu jatkuvasti vaihtuvilla avaimilla

Viimeisin kvanttisuoja minulle

20/04/2023

Viimeisin kvanttisuoja minulta

20/04/2023

Voit tuhota avaamattoman viestin salausavaimen.

Hakkeri voi avata viestin, joka on lähetetty mutta jota ei ole avattu, jos hänellä on tietokanta ja sisäänkäynnin salasana.

Minulle lähetetyt mutta avaamattomat viestit:

Tuhoa avain ?

Viestin numero

2

Suurin avaamani viestin numero:

3 20/04/2023 11:39:26

Suurin viestin numero, jonka olen lähettänyt:

1 20/04/2023 12:57:20

OK

Hakkeri voi kopioida viestin internetissä ja estää sinua saamasta sitä tehden viestin avaamisen mahdottomaksi. Jos sitten hakkeri onnistuu varastamaan EndCryptorin tietokannan koneeltasi ja onnistuu esim. näppäimistökaappauksen avulla saamaan salasanasi, hän voi avata aikaisemmin kopioimansa viestin. Voit estää tällaisen tilanteen tuhoamalla tällaisen avaamattoman viestin salausavaimen. Viestin avaamiseen tarvittavat tiedot poistetaan tietokannasta. Jos viestiä yritetään avata, annetaan samanlainen ilmoitus, kuin jos viesti olisi jo aikaisemmin avattu. Ota huomioon, että jos olet juuri vastaanottanut useita viestejä, jotka eivät ole

salausjärjestyksessä, ja avaat viimeiseksi salatun, niin muut näkyvät tässä listassa. Tee salausavaimen tuhoaminen vasta huolellisen harkinnan jälkeen.

Man In The Middle hyökkäyksen paljastaminen

Paina 'Kontaktit' valitse kontakti ja paina 'Lisätiedot' ja valitse 'MITM hyökkäyksestä'. Tämä testi tarkastaa, onko molemmilla osapuolilla sama sisäinen tila salausprotokollassa. Jos tilanne on se, että sisäinen tila on sama, ei käynnissä ole 'man-in-the-middle' hyökkäystä.

Man-in-the-Middle testi

Tee kohdat 1, 2 ja 3 esimerkiksi puhelinta tai chat-palvelua käyttäen.

1. Varmista, että henkilö, joka väittää olevansa:

todella on tämä henkilö.

2. Tarkastakaa, että molemmat olette avanneet viimeisimmän viestin toiselta.

Viimeisimmän lähettämäsi viestin numero:

Viimeisimmän vastaanottamasi viestin numero:

Paina Peruuta, jos jompikumpi ei ole avannut toisen viimeistä viestiä.

3. Allaolevien kahden tarkastussumman tulee olla molemmilla samat.

Molempien tulee lukea/näytää toiselle toinen allaolevista merkkijonoista

Ovatko tarkastussummat molemmilla samat?

Samat Eri

Julkisten avainten perustiedot

Julkisiin avaimiin perustuva salaustekniikka on nykyaikaisen suojatun viestinnän perusta. Tässä esitetään lyhyesti ilman teknisiä yksityiskohtia näiden avainten perustiedot. Samalla kerrotaan suojausmekanismeistamme tunnettuja hyökkäyksiä vastaan.

Käytämme julkisia avaimia seuraavista syistä:

- Muodostaaksemme jaetun salaisuuden
- Toipuaksemme hyökkäyksestä

Tärkeimmät hyökkäystavat:

- Yksityisen avaimen varkaus
- Man-in-the-middle hyökkäys ensimmäisessä avainten vaihdossa

Julkiset avaimet mahdollistavat jaetun salaisuuden muodostamisen.

Kun osapuolet vaihtavat julkisia avaimia, he voivat laskea arvon, jonka vain he voivat tietää. Kolmas henkilö, joka näkee vaihdetut julkiset avaimet ei voi laskea tätä arvoa. Tätä laskettua arvoa kutsutaan jaetuksi salaisuudeksi ja siitä voidaan muodostaa itse salausavain, jota käytetään viestin salaukseen. Tällaista menetelmää kutsutaan Diffie-Hellman avaintenvaihdoksi sen keksijöiden Whitfield Diffien ja Martin Hellmanin mukaan.

Tämä ratkaisee hyvin tärkeän ongelman: kuinka kommunikoida turvallisesti salausavain toiselle henkilölle? Lähettämällä ja vastaanottamalla julkinen avain.

Jokaisella julkisella avaimella on vastaava yksityinen avain. Julkisen avaimen luoja tietää automaattisesti sen yksityisen avaimen. Jaettu salaisuus lasketaan tämän yksityisen avaimen ja toisen osapuolen julkisen avaimen avulla.

Kvanttihyökkäyksen kestävässä avaimissa käytetään nk. Key Encapsulation Mechanism (KEM) menetelmää. Siinä henkilö A käyttää henkilö B:n julkista avainta ja encapsuloi jaetun salaisuuden salatuksi tekstiksi. Tämä lähetetään B'lle, joka decapsuloi sen omistamansa yksityisen avaimen avulla ja saa haltuunsa saman jaetun salaisuuden.

Julkiset avaimet mahdollistavat toipumisen hyökkäyksestä.

Nyt kolmas henkilö, joka tarkkailee julkisten avainten vaihtoa ei pysty laskemaan jaettua salaisuutta, koska häneltä puuttuu jommankumman julkisen avaimen yksityinen avain. Tilanne kuitenkin muuttuu, jos hän onnistuneesti lähettää vakoiluohjelman, joka varastaa yksityisen avaimen tietokoneesta. Tällöin hän voi laskea jaetun salaisuuden ja voi avata kaikki ne viestit, joissa tuota jaettua salaisuutta on käytetty.

Meillä on nyt ongelma: kuinka toipua yksityisen avaimen paljastumisesta? EndCryptor ratkaisee tämän luomalla uusia julkisia avaimia ja lähettämällä ne.

Hyökkääjän täytyy taas pystyä varastamaan yksityinen avain – jos hän ei siinä onnistu, hän ei voi enää avata uusia viestejä.

Jotkut julkisiin avaimiin perustuvat järjestelmät käyttävät samaa julkista avainta vuosia. Jos sen yksityinen avain paljastuu esimerkiksi hakkeroinnin seurauksena kaikki tämän avaimen avulla salatut viestit voidaan avata. On havaittu tietokoneviruksia, jotka pyrkivät löytämään yksityisiä avaimia.

EndCryptor muodostaa paljon julkisia avaimia. Ensimmäiset viestit käyttävät pitkän ajan julkista avainta, jonka käyttäjä on julkistanut aikaisemmin kaikille. Tämän jälkeen jokainen viesti sisältää uusia lyhytaikaisia julkisia avaimia. Ne on tarkoitettu vain tämän vastaanottajan kanssa tapahtuvan viestinnän suojaamiseen. Niitä kutsutaan lyhytaikaisiksi avaimiksi, koska niitä käytetään vain lyhyen aikaa, esimerkiksi vain yhden viestin suojaamiseen. Kun henkilö, jonka yksityinen avain on paljastunut, lähettää uuden viestin ja se on vastaanotettu, voidaan muodostaa uusi jaettu salaisuus – hyökkäjä on menettänyt mahdollisuutensa avata uhrille tulevia viestejä.

Man-in-the-middle hyökkäys

Tämä hyökkäys voidaan tehdä, kun henkilö lähettää julkisen avaimensa toiselle henkilölle viestinnän alussa. Kryptologiassa tämä hyökkäys kuvataan kolmen henkilön avulla: Alice, Bob ja Mallory. Alice ja Bob haluvat kommunikoida suojatusti ja Mallory haluaa avata heidän viestinsä.

Alice lähettää julkisen avaimensa Bobille, mutta Mallory sieppaa sen ja luo oman avaimensa ja lähettääkin sen Bobille muka Alicen avaimena. Bob luo oman vastauksensa, jossa on hänen julkinen avaimensa ja lähettää vastauksen Alicelle. Taas Mallory sieppaa viestin ja korvaa Bobin avaimen omalla avaimellaan. Nyt Mallory voi esiintyä kumpanakin henkilönä.

Man-in-the-middle hyökkäys: Alice \leftarrow \rightarrow Mallory \leftarrow \rightarrow Bob.

Alice ja Bob eivät tiedä, että on olemassa Mallory, joka vaihtoi heidän julkiset avaimensa omiinsa. Nyt Mallory avaa jokaisen Alicen ja Bobin lähettämän viestin, ja

sitten taas salaa sen uudestaan omien salausavaintensa avulla ja lähettää sen viestin vastaanottajalle.

Perinteisesti tällainen hyökkäys estetään varmenteilla tai käyttämällä jotain kommunikaatiota Alicen ja Bobin välillä, jotta voidaan verrata tarkastussummia vaihdetuista ensimmäisistä viesteistä. Varmenteisiin perustuvaa ratkaisua käytetään internet yhteyksissä suojattuihin web palvelimiin (https eli TLS/SSL) - siihen sisältyy joitain riskejä, katso 'SSL:n ja selainpohjaisen salauksen riskit' osio tässä dokumentissa. Sähköpostin salauksessa käytetään varmenteita (S/MIME tai sovelluskohtaisia ratkaisuja) tai tarkastussummien vertailua.

Tässä EndCryptorin tasossa käyttäjät voivat verrata tarkastussummia paljastaakseen hyökkäyksen.

Kun EndCryptorissa Alice ja Bob alkavat kommunikoida, he sopivat asiasta ja lähettävät jollakin tavoin esim. normaalin sähköpostin liitteenä toisilleen omat julkiset avainpaketinsä. Tämän jälkeen he voivat vaihtaa viestejä. On siis huomattava, että viestin lähettäjällä tulee olla vastaanottajan avainpaketti ja viestin saajalla tulee olla lähettäjän avainpaketti. Avainpaketti sisältää mm. lähettäjän julkiset allekirjoitusavaimet (Edwards ja Dilithium avaimet), joilla vastaanottaja tarkastaa, että viesti tulee avainpaketin luojalta.

Kun alussa siis vaihdetaan avainpaketteja tulee niin tehdä vain luotettavan tahon kanssa, aiotaanhan jakaa salatuissa viesteissä luottamuksellista tietoa. On oltava tarkkana, että toinen osapuoli on se, joka hän väittää olevansa ja esim. sähköpostiosoitteen tulee olla sama kuin aikaisemmin tai selvästi henkilölle ja tämän organisaatiolle kuuluva. Kun avainpaketti on EndCryptorissa ja kontakti on luotu, ei sen sähköpostiosoitetta voi muuttaa ennenkuin viestejä on vaihdettu.

Jos pidetään mahdollisena, että avainpaketteja on muutettu niiden ollessa lähetyksessä, voidaan se havaita menemällä Kontaktit->Lisätiedot->MITM hyökkäykestesti dialogiin.

Jos jokin ryhmä haluaa kommunikoida jäsenten välisesti, on kätevintä koota heidän avainpaketinsä yhteen zip -tiedostoon ja sitten jakaa se jäsenille turvallisesti suojatun web sivuston tai suojatun tiedostonsiirron avulla. Kun saatu avainpaketti tiputetaan EndCryptoriin, otetaan automaattisesti siitä uudet kontaktit käytettäväksi.

SSL:n ja selainpohjaisen salauksen riskit

Tämä osa käsittelee selainpohjaisen salauksen (SSL/TLS/https) riskejä - tätä tekniikkaa käytetään salattaessa yhteys web palvelimeen (tyypillisesti selain näyttää lukon osoitekentässä yrittäen näin vakuuttaa käyttäjän yhteyden turvallisuudesta). **Tämän sivun tulisi kiinnostaa tahoja, joille markkinoidaan sähköpostin salausratkaisuja, jotka perustuvat selaimiin ja jotka eivät siten tarvitse mitään ohjelmien asennusta käyttäjän koneeseen.**

Maaliskuussa 2017 Wikileaks julkaisi vuotoja koskien CIA:n hakkerointiaineistoa. Eräissä näistä dokumenteista on ohjeita CIA:n omille viruskirjoittajille: 'DO NOT solely rely on SSL/TLS to secure data in transit. Numerous man-in-middle attack vectors ... ' eli **'Älä luota yksinomaan SSL/TLS 'ään turvataksesi liikkuvaa tietoa. Lukuisia man-in-middle hyökkäystekniikoita ja julkistettuja vikoja protokollassa.'** ja **'Koska tämä uloin kerros voidaan avata hyökkääjän toimesta (esim. man-in-the-middle tekniikalla), jokainen tällainen salaus tulee tehdä vain tiedon sulauttamiseksi eikä sen turvaamiseksi' - CIA:n mukaan SSL/TLS/https kelpaa siis vain siihen, että se saa tiedon näyttämään tavanomaiselta internet liikenteeltä.**

Aikaisemmin marraskuussa 2011 Wall Street Journal julkaisi 'Surveillance Catalog' -luettelon ja Wikileaks julkaisi listan kansainvälisistä tiedustelurityksistä ja heidän laitteistaan 'WikiLeaks Spy Files' -julkaisussa. Ohessa joitakin esimerkkejä esitteistä, joissa kuvataan laitteiden ominaisuuksia: "Laitte voi myös purkaa SSL salauksen, jos se on asennettu 'man-in-the-middle' konfiguraatioon ..."; "Tarkkaile epäilyllä salattua viestintää Gmailiin, Hush mailiin jne., tarkkaile epäilyllä pankkisiirtoja jne.". **"Sieppaa mikä tahansa liikenne, joka käyttää SSL'ää tai TLS'ää. Kun asennettu, laitteet voivat mennä liikenteen väliin mihin tahansa SSL tai TLS yhteyteen ... käyttäjät ovat tuudittautuneet väärään turvallisuuden tunteeseen, jota tarjoavat selaimen. sähköpostin tai VoIP salaukset";** "Mutta 'man-in-the-middle' tekniikalla voidaan siepata liikenne ja aito varmenne ja korvata se väärällä varmenteella ja saada tietokone luulemaan, että liikenne sujuu normaalisti".

Kuinka tämä on mahdollista?

Kun selain ottaa yhteyden HTTPS - SSL tai TLS palvelimeen, lähettää palvelin selaimelle varmenteen, joka todistaa käyttäjälle, että hän todella on yhteydessä haluttuun palvelimeen. Miten varmenne voi tehdä tämän? Palvelimen omistaja on - ennenkuin on aloittanut toimintansa - ottanut yhteyttä Varmentajaan (Certificate Authority), ja todistanut tälle, että hän omistaa ja hallitsee palvelinta. Palvelimen omistaja on lähettänyt Varmentajalle palvelimen julkisen avaimen ja Varmentaja on allekirjoittanut tämän omalla avaimellaan.

Kaikissa tietokoneissa, jotka käyttävät SSL/TLS'ää, on varasto, jossa on eri julkisten Varmentajien julkiset avaimet. Nämä julkiset avaimet ovat varmenteissa, joita kutsutaan juurivarmenteiksi. Kun palvelimelta tuleva varmenne tarkastetaan, sen

aitous riippuu viime kädessä tästä juurivarmenteesta - tulee olla oikea digitaalinen allekirjoitusketju juurivarmenteesta palvelimelta tulevaan varmenteeseen.

Nyt jokainen, joka tietää juurivarmenteen julkisen avaimen yksityisen avaimen, voi esiintyä minä tahansa web palvelimena, purkaa niiden salauksen ja muuttaa liikenteen sisältöä käyttäen 'man-in-the-middle' tekniikkaa - tämä selitetään myöhemmin. Siis, varmenteiden infrastruktuurista johtuen jokainen julkisesti hyväksytty Varmentaja voi - jos se kääntyy 'ilkeäksi' - tehdä tämän jokaiselle SSL/TLS'ää käyttävälle tietokoneelle. Varmentaja yksinkertaisesti myöntää varmenteen palvelimelle ja antaa käytetyn julkisen avaimen yksityisen avaimen hyökkääjälle - joka voi nyt voi avata ja muuttaa tähän yksittäiseen palvelimeen kohdistuvan liikenteen. Ilkeäksi muuttunut Varmentaja voi myös antaa juurivarmenteen yksityisen avaimen hyökkääjälle - joka voi nyt hyökätä jokaista SSL/TLS palvelinta vastaan myöntämällä itse tarvittaessa varmenteen uhriksi valitulle palvelimelle.

Voidaan argumentoida, että jos suojattava tieto on riittävän sensitiivistä, on liian iso riski siihen, että jokin noin 600 julkisesta Varmentajasta kääntyy 'ilkeäksi' tai pakotetaan jonkin hallituksen toimesta siihen tai sillä on lahjottu työntekijä tai se joutuu hakkeroiduksi. On huomattava, että viime vuosina on kehitetty ns. 'Certificate Transparency' projekti, joka koittaa minimoida tämän kaltaisia mahdollisuuksia - tästä myöhemmin.

Varmentaja Trustwave myönsi helmikuun 4 päivä 2012, että he olivat antaneet yhdelle yksityiselle asiakkaalle juurivarmenteen yksityisine avaimineen erillisen laitteen sisällä ('man-in-the-middle' laite), joka generoi tarvittaessa varmenteen halutulle palvelimelle. Tämä tehtiin, jotta voitaisiin avata ja tarkkailla kaikkea yrityksen SSL/TLS liikennettä, katso https://www.theregister.co.uk/2012/02/14/trustwave_analysis/ .

Nyt siis jokainen tietokoneen varmennevarastossa oleva varmenne tekee tyhjäksi tälle tietokoneelle tapahtuvan SSL/TLS liikenteen, jos varmenteen yksityinen avain joutuu väriin käsiin.

Hyökkääjä voi asettaa oman varmenteensa tähän varastoon esim. pakottamalla käyttäjän asentamaan sen, tai 'ilkeä' kotiapulainen (ns. evil maid hyökkäys), ilkeä tullivirkailija tai tietokonevirus voi tehdä sen. Jotkut antivirus tai lasten tietokoneen käyttöä valvovat ohjelmat asentavat omat juurivarmenteensa tähän varastoon voidakseen avata ja tarkastaa SSL/TLS liikenteen. On ollut tilanteita, joissa tällaisen juurivarmenteen yksityinen avain on ollut kaikille ko. ohjelman käyttäjille sama - tällöin käyttäjä etsii omasta tietokoneestaan tuon yksityisen avaimen ja voi sen avulla avata kaikkien muiden ko. ohjelman käyttäjien liikenteen.

Tutkijat julkaisivat artikkelin varmennevarastoon sijoitettujen ei-julkisten Varmentajien myöntämien varmenteiden aiheuttamista ongelmista artikkelissa "Rusted Anchors: A National Client-Side View of Hidden Root CAs in the Web PKI Ecosystem. In CCS '21, November 15–19, 2021, Virtual Event, Republic of Korea". He

löysivät 5 kk aikana yli 1.7 miljoonaa tällaista varmennta ja noin 5000 organisaatiota, jotka myöntävät näitä. Joukossa on organisaatioita, jotka julkaisevat varmenteita, joilla yritetään omia tunnetutun julkisen varmentajan identiteettiä.

Tekniikka, jossa virus asentaa varmenteen varmennevarastoon mainitaan **Hacking Team** yrityksestä vuodetuissa materiaaleissa. Tuo yritys myy vakoiluohjelmia hallituksille ja lain täytäntöönpanoviranomaisille. Tällaiset tahot pystyvät helposti määräämään internet palvelujen tarjoajat asentamaan vaadittavat laitteet liikenteen avaamiseksi. On huomattava, että myös erilaiset wifi pisteet ja internet kahvilat voivat avata käyttäjän liikenteen, jos niillä on tarvittava yksityinen avain (tai niillä on laite, jossa vaadittava yksityinen avain on).

Heinäkuussa 2019 Kazakhstan alkoi toteuttaa politiikkaa, jossa osaa internetin käyttäjistä pakotettiin asentamaan hallituksen toimittama varmenne tietokoneisiinsa, kun he selaimen avulla menivät tietyille salatun yhteyden vaativille websivuille. Asiasta julkaistun raportin (<https://censoredplanet.org/kazakhstan>) mukaan salaus purettiin mm. seuraavilta kohteilta: Gmail, Google, Facebook, Messenger, mail.ru, translate.google.com, Instagram ja Youtube.

Voi olla myös hyvin vaarallista käyttää tuntemattoman tietokoneen selainta ottamaan yhteyttä web palvelimeen - tuossa koneessa voi olla hyökkääjän asentama juurivarmenne ja kone voi helposti ohjata liikenteen man-in-the-middle laitteeseen.

On olemassa hyökkäys, joka käyttää internetin DNS järjestelmää: hyökkääjä onnistuu muuttamaan joidenkin internetin DNS palvelinten tietueita. Tämän jälkeen hyökkääjä pyytää joltain Varmentajalta uusia varmenteita hyökkäyksen kohteena olevalle palvelimelle. Tämän jälkeen se voi matkia tätä palvelinta käyttäjälle. Tällainen hyökkäys paljastui marraskuussa 2018, se kohdistui 50 Lähi-idässä olevaan yritykseen ja hallitusten virastoihin. Lisätietoa saa haulla 'DNSpionage' ja Brian Krebsin selonteosta osoitteesta <https://krebsonsecurity.com/2019/02/a-deep-dive-on-the-recent-widespread-dns-hijacking-attacks/>

Mielenkiintoinen on myös tilanne, jossa palvelimen yksityinen avain on paljastunut. Yksityinen avain voidaan hakkeroida, vuotaa ilkeän työntekijän toimesta tai se voidaan vaatia luovuttamaan viranomaisille. Jos palvelimen SSL/TLS liikennettä ei ole määritelty käyttämään ns. 'Perfect Forward Secrecy (PFS)' asetuksia voidaan yksityisen avaimen avulla avata aikaisemmat nauhoitetut yhteydet. Jos PSF on määritelty, vaaditaan man-in-the-middle tekniikka yhteyden aikana, jotta salaus saadaan avattua - se onnistuu, koska palvelimen yksityinen avain on tiedossa. Tämä ei vaadi mitään ylimääräisiä varmenteita uhrin koneessa.

U.S.A 'n hallitus vaati salatun sähköpostin tarjoaja Lavabit -yritystä luovuttamaan palvelimen SSL/TLS varmenteen yksityisen avaimen todennäköisesti kerätäkseen todisteita Edward Snowdenia vastaan, katso https://www.wired.com/2013/10/lavabit_unsealed/ .

Suosituksessa OpenSSL ohjelmassa havaittiin **Heartbleed** haavoittuvuus huhtikuussa 2014, se paljasti palvelimen muistin hyökkääjälle. Virhe oli koodissa 2 vuotta, mutta myös vanhemmat nauhoitetut SSL yhteydet (ilman PSF'ää) saadaan avattua muistista haetun yksityisen avaimen avulla. "Hyökkäsimme itseämme vastaan ulkopuolelta jättämättä jälkiä. Käyttämättä mitään ylimääräisiä oikeuksia pystyimme varastamaan itsellemme salatut avaimet, joita käytettiin X.509 varmenteissamme, käyttäjien nimiä ja salasanoja, pikaviestejä, sähköposteja ja liiketoiminnalle kriittisiä dokumentteja ja viestintää."

Tammikuun 14, 2020 Microsoft ilmoitti, että kriittinen haavoittuvuus on havaittu varmenteiden tarkastusohjelmassa. Havainnosta Microsoftille ilmoitti NSA, katso <https://media.defense.gov/2020/Jan/14/2002234275/-1/-1/0/CSA-WINDOWS-10-CRYPT-LIB-20190114.PDF> . NSA:n mukaan "esimerkkejä missä vaikutukset voivat ilmetä: **HTTPS yhteydet, allekirjoitetut tiedostot ja sähköpostit** ja allekirjoitettu käyttäjän koodi. **NSA arvio haavoittuvuuden olevan vakavan ja että kehittyneet kybertoimijat ymmärtävät allaolevan vian hyvin nopeasti ja että jos haavoittuvuutta hyväksikäytetään, tulevat edellämainitut osa-alueet olemaan perustavanlaatuisesti haavoittuvia.**" Tämä tarkoittaa, että hyökkääjä, joka käyttää tätä vikaa, voi aloittaa 'man-in-the-middle' hyökkäyksen ilman tietoa yksityisistä avaimista. USA:n Cert koordinaattori (<https://kb.cert.org/vuls/id/849224/>) sanoo "Hyväksikäyttämällä tätä haavoittuvuutta hyökkääjä saattaa voida onnistua huijaamalla luomaan oikealta näyttävän allekirjoitusketjun haavoittuvassa Windows järjestelmässä. Tämä saattaa mahdollistaa erilaisia jatkotoimia sisältäen, muttei rajoittuen TLS-salatun liikenteen sieppaamiseen (avaamiseen, suom. huom.) ja muuttamiseen ja huijattujen Authenticode allekirjoitusten luomiseen.". Haavoittuvien versioiden joukossa on Windows 10, joka julkaistiin heinäkuun 29 päivä 2015.

Muistatko vielä mitä vuodetuissa CIA'n papereissa sanottiin: 'Älä luota yksinomaan SSL/TLS'ään turvataksesi liikkuvaa tietoa. Lukuisia man-in-middle hyökkäystekniikoita ja julkistettuja vikoja protokollassa.'

Kuinka 'man-in-the-middle' (MITM) tekniikka toimii? Tämä hyökkäys voidaan tehdä käyttäjän tietokoneen ja palvelimen välillä sellaisen hyökkääjän toimesta, joka tietää sopivan yksityisen avaimen (joko juurivarmenteen tai palvelimen). Kun käyttäjä aloittaa yhteyden palvelimeen hyökkääjä esiintyy palvelimena. Palvelimelle taas hyökkääjä esiintyy käyttäjänä.

MITM hyökkäys: Käyttäjä ↔ Hyökkääjä ↔ Palvelin.

Useat yritykset käyttävät erityisiä laitteita avaamaan oman SSL/TLS liikenteensä. Tämän mahdollistamiseksi yritys asentaa käyttäjien tietokoneiden varmennevarastoihin oman juurivarmenteensa. Nyt esim. tietynlaiset palomuurilaitteet voivat avata ja taas uudestaan salata käyttäjille menevän liikenteen. Tarkoituksena on esim. etsiä viruksia tietovirrasta. Citizen Lab'in raportissa "Planet Blue Coat: Mapping Global Censorship and Surveillance Tools,

January 2013" (from <https://citizenlab.ca/publications/>) kuvataan kuinka tällaisia laitteita käyttävät myös valtiot, joilla on historiaa ihmisoikeuksien loukkaamisessa.

MITM hyökkäystä voidaan käyttää SSL/TLS pohjaisiin sähköposti ja webmail -ratkaisuihin. On myös olemassa VPN ratkaisuja, jotka käyttävät selainta. Selainpohjaiset salausratkaisut yleensä käyttävät markkinointiargumentteina sitä, ettei käyttäjän tarvitse asentaa mitään muita ohjelmia tietokoneeseensa - vain selain riittää.

Joskus selainpohjaiset sähköpostin salausratkaisut tekevät selaimessa javascriptillä viestin salauksen (esim. PGP). Tämä ei tuo suojaa MITM hyökkäystä vastaan - hyökkääjä muuttaa javascript koodia ennenkuin lähettää sen uhrille esim. niin, että käytetyn salausmenetelmän salausavain välitetään hyökkääjälle (esim. PGP:n yksityinen avain).

EndCryptor käyttää TLS'ää ottaessaan yhteyttä käyttäjän sähköpostipalvelimeen, sähköpostipalvelimet edellyttävät sitä. EndCryptor salaa viestin ennenkuin palvelimeen muodostetaan yhteys - onnistunutkaan MITM hyökkäys ei voi paljastaa viestin sisältöä. EndCryptorin kyseessä ollen hyökkääjä voi saada vain sähköpostin käyttäjätunnuksen ja salasanan haltuunsa. EndCryptor myös tallettaa kaikki saamansa varmenteet, ne voidaan myöhemmin analysoida, jos epäillään hyökkäystä. EndCryptor voidaan konfiguroida niin, että se hyväksyy palvelimelta vain tietyn varmenteen, tämä estää väärin varmenteiden käytön. Tämä on tunnettu tekniikka ja siitä käytetään nimitystä 'certificate pinning'.

Googlen kehittämä Certificate Transparency project (<https://www.certificate-transparency.org/>) yrittää parantaa varmenteiden infrastruktuuria. Tässä projektissa yritetään tallettaa kaikki maailmassa julkisten Varmentajien toimesta myönnetty varmenteet, jotta havaittaisiin tietyille palvelimelle myönnetty vihamieliset varmenteet. Suurimmat julkiset Varmentajat ovat siinä mukana ja myös hakukoneet voivat lähettää havaitsemiaan varmenteita projektille. Huhtikuun 30, 2018 jälkeen myönnettyjä varmenteita ei enää hyväksytä Chrome selaimessa ellei niiden mukana ole projektin vaatimaa lisäosaa (Signed Certificate Timestamp eli SCT), joka todistaa, että varmenne on toimitettu projektille. Google: "Eryityisesti Certificate Transparency mahdollistaa sellaisten varmenteiden havaitsemisen, joita on virheellisesti myönnetty Varmentajien toimesta tai pahantahtoisesti saatu moitteettomilta Varmentajilta. Se myös mahdollistaa sellaisten Varmentajien tunnistamisen, jotka ovat alkaneet toimia vilpillisesti ja myöntävät pahantoisia varmenteita."

Jos julkisesti hyväksytty Varmentaja myöntää varmenteen palvelimelle, se tulee tallettaa läpinäkyviin logeihin. Domainin (palvelimen) omistaja voi tehdä kyselyjä logeihin ja tarkastaa, että palvelimelle on myönnetty vain hänen haluamansa varmenteet. Väärää varmennetta voidaan käyttää MITM hyökkäyksissä kunnes se havaitaan ja kumotaan ja käyttäjät saavat tiedon kumoamisesta. Tällaisesta järjestelmästä voidaan tehdä johtopäätös, että on täytynyt tapahtua vakavia väärinkäytöksiä, koska tarvitaan näin iso systeemi.

Projekti sanoo <https://www.certificate-transparency.org/benefits>: "Todella, välikohtauksia, joita aikaisemmin on peitelty ja vähätelty ja jotka itse asiassa aiheuttivat kokonaisen Varmentajan sulkemisen, voidaan paljastaa paljon aikaisemmin ja korjata yksinkertaisesti kumoamalla yksittäinen varmenne."

Certificate Transparency järjestelmään lisäämistä ei tehdä paikallisille ei-julkisen Varmentajan myöntämille varmenteille ja jotka on lisätty käyttäjän varmennevarastoon käyttäjän tai jonkin ohjelman kuten antivirus, palomuuuri, virus jne. toimesta. Selain, joka ei hyväksy julkisen Varmentajan varmennetta puuttuvan SCT osan vuoksi, hyväksyy varmenteen, jos se ei ole julkisen Varmentajan myöntämä. Selain olettaa tällöin, että varmennetta käytetään paikallisesti tai esim. SSL/TLS liikenteen avaamisen virustarkastuksen vuoksi.

Salausratkaisut, jotka käyttävät SSL/TLS'ää ilman selainta, eivät välttämättä noudata selainten käytäntöä ja vaadi CT lisäosaa.

Tekniset tiedot

Perusteellisemmat tiedot ovat englannin kielisessä documentaatiossa.

Klassiset avaimet ovat Edwards avain Ed25519 ja Curve25519, jota käytetään mm. selaimissa. Edwards avainta käytetään digitaaliseen allekirjoitukseen ja Curve25519 avainta Diffie-Hellman laskentaan.

Kvanttihyökkäyksen kestävät avaimet ovat Kyber-1024, Frodokem-1344 ja mceliece6688128f (round 4). Kyber on USAn standardi, Saksan valtion 'Federal Office for Information Security' suosittelee Frodokem ja mceliece avainten käyttämistä, katso BSI TR-02102-1. Klassisia ja kvanttihyökkäyksen kestäviä avaimia käytetään hybrid asetelmassa, jolloin hyökkääjän on kyettävä murtamaan kaikki asetelmassa olevat avaimet. Tämä hybridi avainten laskenta tehdään tavalla 'Concatenate hybrid key agreement scheme', raportissa ETSI TS 103 744 V1.1.1 ('ETSI is a European Standards Organization (ESO). .. the recognized regional standards body dealing with telecommunications, broadcasting and other electronic communications networks and services.')

Digitaalisissa allekirjoituksissa käytetään Ed25519 avainta ja CRYSTALS-Dilithium3 allekirjoitusta. On huomattava, että USAn standardointiorganisaatio NIST suosittelee CRYSTALS-Dilithium allekirjoituksia. Vain ensimmäiset viestit käyttävät allekirjoituksia, myöhemmät käyttävät Keccak mac-koodia, jossa käytetään avainta, joka on muodostettu jaetusta salaisuudesta.

Symmetrinen salaus tehdään Chacha20'llä ja 256 bittisellä avaimella.

Ed25519, Curve25519 ja Chacha20 ja toteutus käyttää SUPERCOP'in ja NaCL kirjaston (European Network of Excellence in Cryptology II projecteja, rahoittajana European Commission) referenssitoteuksia. Kyber-1024 toteutus on Githubissa: pq-crystals/kyber, FrodoKEM-1344 toteutus on myös Github'issa: PQCrypto-LWEKE. Mceliece6688128f koodi on round-4 NISTPQC 'submission package'ssa. Dilithium koodi on Github'issa: pq-crystals/dilithium