BCP eduroam ja varmennekäytännöt

Tunniste	FN4.1 Funetin Parhaat käytännöt -dokumentti
Päiväys	20.3.2015
Otsikko	eduroam ja varmennekäytännöt
Työryhmä	MobileFunet
Laatijat	Tomi Salmi/CSC, Tuukka Vainio/Turun yliopisto
Vastuutaho	Tomi Salmi/CSC
Tyyppi	Suositus

1. Johdanto

Varmenteita eli sertifikaatteja käytetään tietotekniikassa laajasti varmentamaan viestinnän osapuolet toisilleen. Esimerkiksi verkkopalvelun käyttäjä voi varmenteen avulla varmistua, että hän on asioimassa oikean palvelimen ja toimijan kanssa. Pelkkä varmenne ei kuitenkaan vielä lisää tai toteuta tietoturvaa, vaan varmenne on pelkästään tapa tallentaa tietoa yhteisesti sovitulla tavalla. Kuka tahansa voi luoda rajattomasti varmenteita, mutta vasta varmenteeseen tallennetut tiedot ja niiden varmistamisen mahdollisuus kokonaisuutena lisäävät tietoturvaa.

Kansainvälisessä verkkovierailujärjestelmässä eduroamissa varmennetarkistus on osa autentikointia. Tähän dokumenttiin on koottu eduroamissa hyväksi todettuja EAP-varmennekäytäntöjä, jotta saavutettaisiin mahdollisimman hyvä yhteensopivuus erilaisten päätelaitteiden kanssa tietoturvaa ja käytettävyyttä unohtamatta. Dokumentti on suunnattu erityisesti eduroamin käyttöönottovaiheessa oleville verkkoylläpitäjille.

2. Varmenteet eduroamissa

Liityttäessä eduroam-verkkoon varmennetta käytetään lähes kaikilla mahdollisilla EAP-autentikointityypeillä (Extensible Authentication Protocol) varmentam aan käyttäjälle, että tämä on tekemisissä oikean RADIUS-palvelimen (Remote Authentication Dial-In User Service) kanssa ennen käyttäjätunnuksen ja salasanan luovuttamista. Tätä varten autentikoivalle IdP-palvelimelle on hankittava X.509-palvelinvarmenne, joka voi olla joko itseallekirjoitettu (oma CA, Certification Authority) tai hankittu tunnetulta luotetulta CA:lta. Näiden eroja on käsitelty luvussa 2.1. Jos RADIUS-palvelin toimii vain proxyna ilman käyttäjäautentikointia, palvelinvarmennetta ei tarvita. Käyttäjien päätelaitteisiin täytyy jaella ja ottaa käyttöön juurivarmenteen julkinen osa. Varmenneketjun hallintaa ja jakelua on käsitelty luvussa 2.2. Kolmas luku käsittelee varmenteen uusimista, ja neljäs luku varmenteen teknisiä ominaisuuksia mahdollisimman hyvän päätelaiteyhteensopivuuden takaamiseksi.

2.1 Oma vai julkinen CA?

Varmenteella on aina joku myöntäjä, eli varmentaja (CA, Certification Authority). Varmenteen voi hankkia luotetulta julkiselta CA:lta, tai ylläpitäjä voi pystyttää ylläpidettäväkseen oman CA:n. Omalla CA:lla varmenteita voi luoda maksutta rajattomasti, mutta CA:n ylläpito edellyttää julkisten avainten hallintajärjestelmän (PKI, Public Key Infrastructure) tuntemusta. CA:n ylläpidosta koituu kustannuksia ainakin tehdyn työn kautta. EAP-TLS:ää käytettäessä autentikoidaan palvelimen lisäksi myös päätelaite kukin omalla varmenteellaan, jolloin varmennemäärän kasvaessa omasta CA:sta on saatavissa eniten hyötyjä.

Oman CA:n käytössä haittapuolena eduroamissa on se, ettei mikään päätelaite lähtökohtaisesti tunne tällaista CA:ta, joten varmenteen julkinen osa on asennettava jokaiseen päätelaitteeseen erikseen. Varmenne voidaan jaella esimerkiksi sähköpostitse tai intranetin kautta, mutta jakelumalli sekä käyttäjäohjeistus on suunniteltava hyvin. Erillisten provisiointisovellusten käyttäminen on suositeltavaa. Juurivarmenteen vaihtuminen aiheuttaa sen, että kaikkien sen varaan konfiguroitujen päätelaitteiden varmenne on uusittava. Oman CA:n varmenteelle kannattaa tämän vuoksi asettaa pitkä voimassaoloaika. Omia varmenteita tehtäessä tulee kiinnittää huomiota myös varmennetiedostojen kokoon. Omalla CA:lla voi helposti tulla luoneeksi tarpeettoman isoja varmenteita, mikä hidastaa EAP-kättelyä. Monien RADIUS-palvelinten mukana toimitetaan testikäyttöön tarkoitettu testivarmenne. Tällaista testivarmennetta ei luonnollisestikaan pidä käyttää tuotantoympäristössä.

Käytettäessä tunnettua CA:ta varmenteen julkinen osa voi löytyä valmiina ainakin osasta päätelaitteita. Vaikka varmenne löytyisi päätelaitteesta valmiina, se pitää osata valita verkon asetuksia määritettäessä, mikä edellyttää jälleen käyttöjärjestelmäkohtaista ohjeistusta. Valittiinpa joko julkinen tai oma CA, käyttäjiä on joka tapauksessa ohjeistettava noutamaan ja asentamaan tai vähintäänkin valitsemaan päätelaitteesta oikea varmenne verkkoasetuksia määriteltäessä.

Tunnetun CA:n käyttämisessä on olemassa yksityistä CA:ta suurempi riski väliintulohyökkäyksille (MitM, Man in the Middle). Riski seuraa siitä, että kaikki päätelaitteet eivät tee varmennetarkistusta riittävän kattavasti. Jotkut päätelaitteet esimerkiksi tarkistavat vain, että palvelinvarmenteen myöntäjä on sama kuin juurivarmenteella, mutta eivät tarkasta palvelimen nimeä. Vihamielinen käyttäjä voi näin ollen pystyttää RADIUS-palvelimen ja hankkia sinne saman tunnetun CA:n allekirjoittaman aidon varmenteen kerätäkseen käyttäjien tunnuksia ja salasanoja. [1] IT-tuen tulisi mahdollisuuksien mukaan ohjeistaa ja varmistaa, että käytetty varmenne ja palvelimen nimi on määritetty käyttäjien konfiguraatioissa.

Varmenteen puutteellinen tarkistus koskee erityisesti Android- ja Windows Phone -käyttöjärjestelmiä. Molemmissa on mahdollista määritellä juurivarmentaja, mutta tarkistuksen voi myös ohittaa helposti. Kummallekaan käyttöjärjestelmälle ei myöskään pysty määrittelemään autentikointipalvelimen nimeä. Androidin tuli version 4.3 (Jelly Bean) mukana mahdollisuus määrittää EAP-asetukset automaattityökalujen avulla, kun aiemmin kaikki EAP-asetukset piti tehdä manuaalisesti käyttöjärjestelmän valikoiden kautta [2] .

Automaattiprovisointityökaluja, kuten eduroam CAT:ia (eduroam Configuration Assistant Tool) tai MDM-järjestelmiä (Mobile Device Management) käytettäessä varmenteen asentaminen päätelaitteeseen ei enää muodostu kynnyskysymykseksi pohdittaessa valintaa tunnetun CA:n tai itseallekirjoitetun varmenteen välillä. Itseallekirjoitetulla varmenteella on saavutettavissa mainittuja tietoturvahyötyjä, minkä vuoksi sitä voi pitää kahdesta vaihtoehdosta suositeltavampana jos tarvittava CA-osaaminen löytyy. Oman yksityisen CA:n ja julkisen CA:n kautta hankitun varmenteen edut ja haitat on koottu alla olevaan taulukkoon.

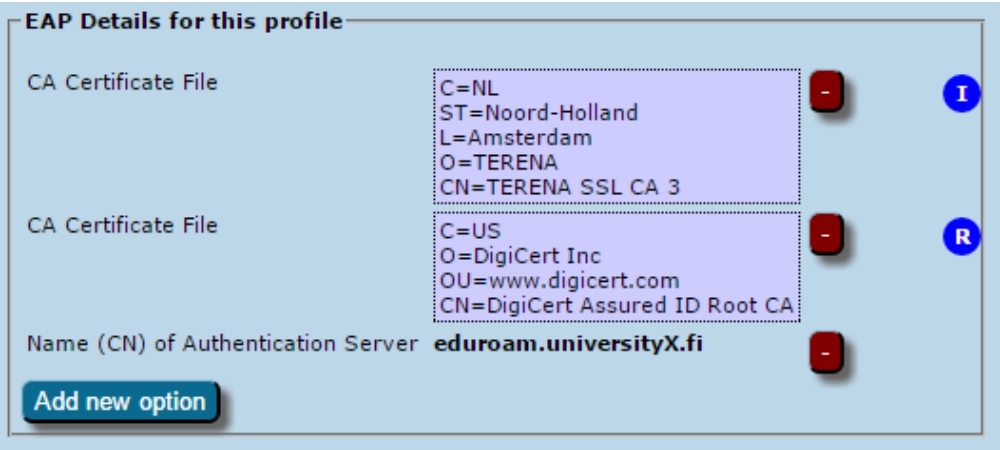
Oma yksityinen CA	**Julkinen CA**
Edut	
• Varmenteet maksuttomia • Tietoturvahyödyt	• Varmenne mahdollisesti valmiina päätelaitteissa
Haitat	
• Edellyttää PKI-osaamista • Varmenteen jakelu päätelaitteisiin järjestettävä	• Yleensä maksullinen • Suurempi riski väliintulohyökkäyksille

Itseallekirjoitetun ja julkisen CA:n allekirjoittaman varmenteen käytön edut ja haitat.

Eurooppalaisilla kansallisiin tutkimusverkkoihin (NREN, National Research and Education Network) kuuluvilla organisaatioilla on mahdollisuus liittyä oman paikallisen NREN:n kautta yhteiseurooppalaisesti kilpailutettuun GÉANT Associationin tarjoamaan varmennepalveluun (TCS, Trusted Certificate Service). Palvelun kautta organisaatiot voivat hankkia omaan käyttöönsä TERENA:n allekirjoittamia palvelinvarmenteita. Suomessa Funet (Finnish University and Research Network) tarjoaa palvelua Suomen korkeakouluille ja muille jäsenilleen. [3]

2.2 Varmenneketjun hallinta ja jakelu

Autentikointipalvelimen ja päätelaitteen autentikoinnin yhteydessä käytettävä varmenneketju koostuu juurivarmenteesta, mahdollisista välivarmenteista sekä palvelinvarmenteesta. Päätelaitteessa tulee olla vähintään luotettu juurivarmenne ennen eduroam-autentikoinnin aloittamista. Päätelaitteissa on vaihtelevasti tunnettujen CA:iden varmenteita, ja itseallekirjoitetut niistä luonnollisesti puuttuvat kokonaan. Ylläpitäjien tulee toteuttaa juurivarmenteen jakelu tai tuottaa käyttöjärjestelmäkohtainen loppukäyttäjäohjeistus siitä miten ja mistä varmenteen voi noutaa ja asentaa. Loppukäyttäjien avuksi suunnattuja helppokäyttöisiä provisiointisovelluksia, kuten eduroam CAT:ia kannattaa hyödyntää mahdollisuuksien mukaan.



Koko varmenneketjun määritteleminen eduroam CAT -profiiliin.
RADIUS-tunnistautumispalvelin lähettää autentikointivaiheessa vähintään palvelinvarmenteen. Varmenneketjun välivarmenteet voidaan siirtää EAP-autentikoinnin yhteydessä tai ne voidaan tallentaa päätelaitteeseen juurivarmenteen tavoin etukäteen. Jos välivarmenteet ovat valmiina päätelaitteessa, vähenee EAP-kättelyn tiedonsiirron tarve, mikä nopeuttaa autentikointia. Varmenneketjussa voi olla useita välivarmenteita, ja määrän lisääntyessä myös autentikoinnin ajallinen kesto pitenee.

Erityisesti omalla CA:lla tehtynä varmenteiden kokoon tulee kiinnittää huomiota. Kasvava koko paitsi pidentää kättelyä, saattaa myös keskeyttää sen kokonaan. Päätelaitteiden yleinen maksimikoko varmenneketjulle on 64 kilotavua, mikä saavutetaan noin 60 edestakaisella EAP-lähetyksellä. Monet tukiasemat katkaisevat EAP-kättelyn jo 50 lähetyksen kohdalla. [4]

Toimivuuden kannalta koko varmenneketjun tallentaminen päätelaitteeseen provisiointityökalulla on varmin ratkaisu. Tästä esimerkkinä Applen käyttöjärjestelmillä (ainakin iOS 7 ja 8) on ollut ongelmia TCS:n varmenneketjun kanssa, koska ketjun nykyinen välivarmenne on aiemmin ollut itseallekirjoitettu juurivarmenne. Käyttöjärjestelmässä esiasennettuna ja luotettuna on varmenteen itseallekirjoitettu versio, eikä iOS siksi kaikissa tilanteissa hyväksy saman varmenteen uutta versiota EAP-kättelyn yhteydessä palvelimen lähettämänä. Provisiointisovelluksella asennettaessa tätä ongelmaa ei ole. Oheisessa eduroam CAT -kuvakaappauksessa palveluun on oikeaoppisesti liitetty juurivarmenteen (R = Root) lisäksi myös varmenneketjun välivarmenteet (I = Intermediate), jolloin ne asentuvat loppukäyttäjän päätelaitteeseen CAT-asennuspaketin suorittamisen yhteydessä.

2.3 Varmenteen vaihtaminen

Palvelinvarmenteen vaihto tulee ajankohtaiseksi viimeistään kun sen voimassaolo on päättymässä. Julkisen CA:n allekirjoittamat varmenteet ovat tyypillisesti voimassa 1-3 vuotta. Niin kauan kuin CA pysyy samana, varmenteen vaihto on suoraviivainen toimenpide, koska päätelaitteisiin määriteltyä juurivarmennetta ei tarvitse vaihtaa ja muutoksia tarvitaan vain autentikointipalvelimen päässä. Uuden palvelinvarmenteen käyttöönoton yhteydessä varmenne kannattaa laittaa automaattiseen valvontaan, joka seuraa sen voimassaoloaikaa. Myös varmennetoimittajat tyypillisesti muistuttavat etukäteen toimittamansa palvelinvarmenteen voimassaoloajan päättymisestä.

Juurivarmenteiden voimassaoloajat ovat yleensä huomattavasti pidemmät. Julkisen CA:n varmennetta hankittaessa on silti hyvä varmistaa, että kyseisellä juurivarmenteella on jäljellä runsaasti voimassaoloaikaa. Vastaavasti omaa CA:ta käytettäessä juurivarmenteen voimassaoloaika tulee asettaa pitkälle tulevaisuuteen. Jos käytetty juurivarmenne vaihtuu, täytyy myös päätelaitteiden konfiguraatiota muuttaa. Tämä on sitä raskaampi ja hitaampi toimenpide mitä enemmän päätelaitteita on konfiguroitu tämän IdP:n käyttäjäksi. CA:n valinta on siis mietittävä huolella heti eduroamin käyttöönoton yhteydessä.

Varmenteen mitätöinnissä on hyvä huomioida, että eduroamissa autentikointi ja varmennetarkistus suoritetaan jo ennen varsinaisen verkkoyhteyden muodostumista. Tästä seuraa se, että mitätöityäkin varmennetta vasten pystytään autentikoitumaan. Vaikka supplikantti autentikoinnin jälkeen suorittaisikin sulkulistan tarkistamisen, käyttäjätunnus ja salasana on jo tässä vaiheessa ehditty luovuttaa, mahdollisesti vihamieliselle, autentikointipalvelimelle.

2.4 Varmenteen ominaisuudet

Seuraavassa on listattu muutamia varmenteiden ominaisuuksia sekä niihin liittyviä suosituksia. Ohjeilla pyritään mahdollisimman hyvään yhteensopivuuteen erilaisten päätelaitteiden ja käyttöjärjestelmien kanssa.

Palvelimen nimi

Palvelimen nimi tulee syöttää varmenteen Subject-kenttään nimitiedoksi (CN, Common Name) täydellisenä toimialuenimenä (FQDN, Fully Qualified Domain Name). Suositeltavaa on asettaa sama nimi myös subjectAltName-tietoihin. Niin sanottuja wildcard-nimiä ei pidä käyttää.

Allekirjoitusalgoritmi

Suositeltavin on SHA-2 (esim. SHA-256). SHA-1-algoritmin tuki on hiljalleen päättymässä, ja MD5-algoritmia ei pitäisi käyttää enää missään.

Avaimen pituus

Jotkut käyttöjärjestelmät eivät hyväksy alle 1024-bittisiä avaimia. Uusiin ympäristöihin kannattaa ottaa käyttöön 2048-bittiset avaimet.

CRL Extension

Windows 8 ja Windows Phone 8 vaativat tai ne on mahdollista konfiguroida vaatimaan varmennesulkulistan URL (CRL, Certificate Revocation List), jolloin URL on oltava syntaksiltaan oikeanmuotoinen. Kumpikaan käyttöjärjestelmä ei kuitenkaan lataa varsinaista CRL-tiedostoa, vaikka URL olisi määritelty.

BasicConstraint Extension

Asetuksen on oltava “CA:FALSE (critical)”, eli palvelinvarmenne ei ole CA-varmenne. Ainakin OS X Mountain Lionin kanssa on todettu ongelmia jos BasicC onstraint-määritys puuttuu.

X509v3 Extended Key Usage (EKU)

Windowsit edellyttävät, että määriteltynä on vähintään yksi ominaisuus. EAP-käytössä eduroamissa ominaisuutena on "Server authentication".

Lähteet: [4] [5] [6]

3. Käyttäjätuki

Kun eduroam on otettu kampuksella käyttöön, sen olemassaolosta tulee viestiä kattavasti. Lisäksi tarvitaan käyttöjärjestelmäkohtainen selkeä ohjeistus eduroamin tietoturvallisesta konfiguroinnista eri päätelaitteisiin. Omien laitteiden käytön tukemiseksi on suositeltavaa tuottaa loppukäyttäjäohjeistukset, koska eduroamissa tyypillisesti käytetään enemmän omia laitteita kuin organisaation omassa keskitetyssä ylläpidossa olevia. Korkeakouluissa eduroamin tietoturvallisesta käyttöönotosta kannattaa kertoa uusien opiskelijoiden ja henkilökunnan perehdytystilaisuuksissa.

Konfigurointiohjeistuksissa täytyy kiinnittää huomiota tapaan, jolla tietoturvatarkistukset konfiguroidaan. Ohjeissa on vaarallisen helppoa yksinkertaistaa ja neuvoa ohittamaan varmennetarkistukset, mutta tämä heikentää tietoturvaa ja ohjaa käyttäjiä vääränlaiseen toimintatapaan. Tietyt käyttöjärjestelmät on helppo konfiguroida väärin ja vieläpä niin, että liittyminen verkkoon toimii kotiverkossa, mutta ei vierailtaessa jonkun muun organisaation ylläpitämässä eduroamissa. Selkeyden vuoksi kirjautuminen ilman realmia kotiverkossa tulisi estää. Ilman realmia tehty konfiguraatio saa muuten aikaan sen, että konfiguraatio on näennäisesti oikea kotiverkkoon, mutta roamauskelvoton vierailtaessa muualla.

Ohjeita ja suosituksia eduroam-tuen toteuttamiseen löytyy muun muassa sivustoilta eduroam.org [7] ja terena.org [8].

Erinomainen työkalu loppukäyttäjien eduroam-käyttöönoton helpottamiseen on jo edellä mainittu eduroam CAT [9]. Työkalulla verkkoylläpitäjät voivat luoda omille käyttäjilleen helppokäyttöiset organisaatiokohtaiset eduroam-asennuspaketit. Oman eduroam-verkon tiedot kuten RADIUS-palvelimen nimi, tuetut EAP-tyypit sekä varmenneketju syötetään CAT-palveluun, joka generoi valmiit asennuspaketit. Kun määritykset ovat valmiit, käyttäjät voivat noutaa asennuspaketit CAT-sivustolta. Omaan intranetiin CAT-linkin voi luoda niin, että käyttäjä päätyy suoraan oman organisaation asennuspakettien lataussivulle. Asennusohjelmien käyttö ei edellytä käyttäjältä verkko-osaamista. CAT:n on todettu vähentävän IT-tuen tehtäviä eduroam-asioissa kun virheellisten konfigurointien määrä on vähentynyt. Palvelun käyttö on maksutonta, ja käyttöönotto aloitetaan ottamalla yhteyttä omaan paikalliseen NRENiin, Suomessa Funetiin.

4. Lähteet

[1] The eduroam architecture for network roaming, [https://tools.ietf.org/html/draft-wierenga-ietf-eduroam-05]

[2] Elenkov, Nikolay: Android Security Internals: An In-Depth Guide to Android's Security Architecture, 2015, s. 248-249

[3] Csc.fi: Funetin palvelut, Varmennepalvelu [https://www.csc.fi/fi/funet-varmennepalvelu]

[4] Freeradius.org: Certificate Compatibility [http://wiki.freeradius.org/guide/Certificate-Compatibility]

[5] Terena.org: EAP Server Certificate considerations [https://wiki.geant.org/display/H2eduroam/EAP+Server+Certificate+considerations]

[6] Microsoft.com: Certificate requirements when you use EAP-TLS or PEAP with EAP-TLS [https://support.microsoft.com/en-us/kb/814394]

[7] eduroam.org: eduroam Service Definition [https://www.eduroam.org/index.php?p=docs]

[8] Terena.org: How to offer helpdesk support to end users [https://wiki.geant.org/display/H2eduroam/How+to+offer+helpdesk+support+to+end+users]

[9] eduroam CAT [https://cat.eduroam.org/]