- ✓Julkisen avaimen infrastruktuuri
- ✓Varmenteet
- ✓Autentikointi

JULKISEN AVAIMEN INFRASTRUKTUURI

Public Key Infrastructure (PKI)

* TLS palvelinsertifikaatit
* julkiset varmentajat eli CA:ta
* TLS –istunnon vaiheet
* S/MIME sähköpostin salausprotokolla

- Varmennuksen käsitteistöä

TLS – protokolla

Entinen SSL, versiosta 3.0 alkaen nimeltään TLS
= ohjelmisto, jota käyttää yli 90% Internetin suojatuista yhteyksistä

Tukee mm. seuraavia palveluja:
sähköposti , verkkopankit , verkkokauppa , tiedostonsiirto

TLS - sertifikaatit

TLS on tyypillinen **hybridisalausohjelmisto**, joka sisältää seuraavat toiminnot:

1. Osapuolten autentikointi
2. Symmetrisestä avaimesta sopiminen
3. Tiedonsiirron salaus symmetrisellä salauksella
4. Digitaaliset allekirjoitukset (tiedonsiirron eheyden tarkistus)

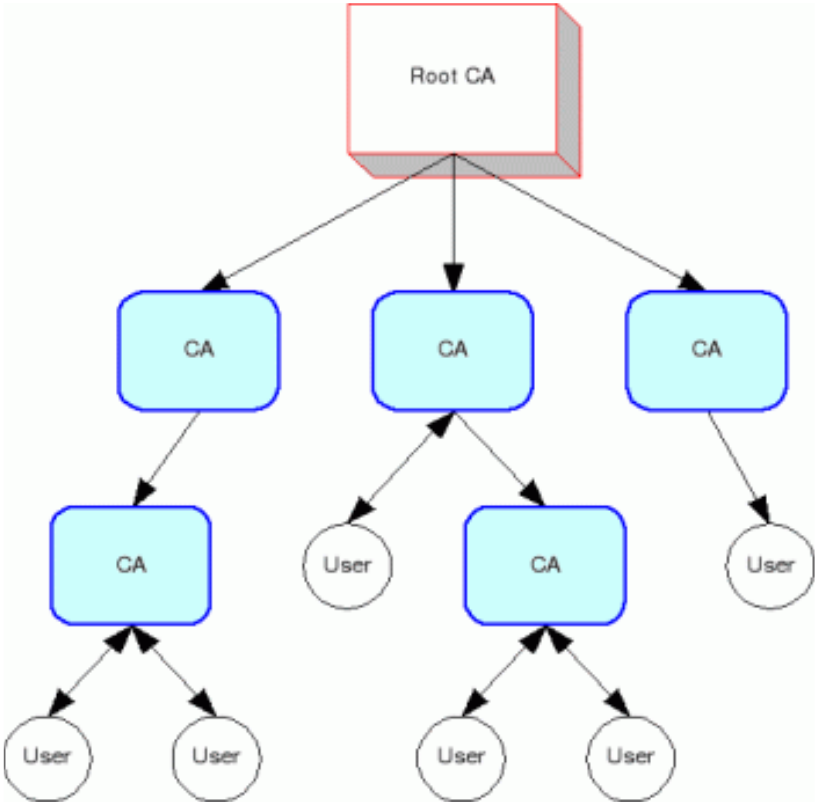
TLS hyödyntää julkisen avaimen infrastruktuuria, jonka keskeinen osa on julkisten varmentajien (CA = Certification Authority) verkko.

TLS - palvelimet hankkivat joltain CA:lta varmenteen eli sertifikaatin, joka sisältää palvelimen julkisen avaimen vahvalla salauksella digitaalisesti allekirjoitettuna. Palvelimen aitouden todennus tapahtuu sertifikaatin avulla.

https://www.symantec.com/ssl-certificates/

PKI = Julkisen Avaimen Infrastruktuuri

Julkisten varmentajien verkko



Julkisen avaimen salaus vaatii luotettavan julkisten avainten myöntäjän ja rekisterin ylläpitäjän

TLS – palvelimet hankkivat CA:lta digitaalisesti allekirjoitetun sertifikaatin, joka sisältää palvelimen julkisen avaimen.

Päämääränä on se, että verkossa ei voi toimia tahoja, jotka antaisivat vääriä julkisia avaimia ja näin voisivat napata käyttäjien salaisiksi tarkoitettuja viestejä

TLS -sertifikaatin muotomääritys = X.509

Sertifikaatti on määrämuotoinen tiedosto, jonka **tärkein sisältö on palvelimen julkinen avain.** Muita tietoja ovat mm. sertifikaatin voimassaoloaika ja sertifikaatin aitouden varmistavan digitaalinen allekirjoitus ja siinä käytetty algoritmi.

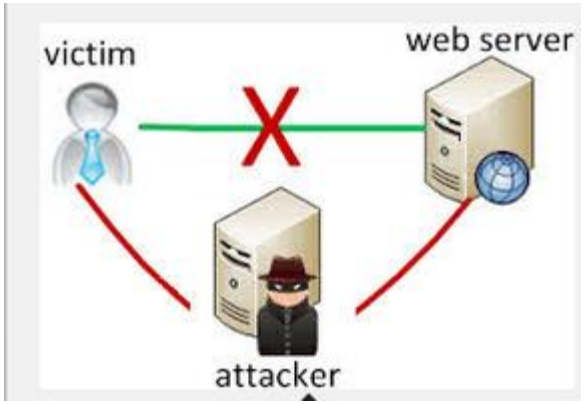
X.509 Certificate
Version : 1
Serial Number : 7983
Algorithm: SHA256WithRSAEncryption
Issuer: VeriSign Ltd
Validity :
Not Before July 12 2008 13:00 GMT
Not After July 12 2009 13:00 GMT
Subject:
Subject Public Key Info Matti Matikainen, Rovaniemi
Public Key Algorithm RSAencryption
Subject Public Key: RSA (1024 bit)
Modulus: 33 35 19 d5 0c… …..f3 31 e1
Exponent: 65537
Certificate Signature Algorithm SHA256WithRSA Encryption
Certificate Signature a5 55 7c d3 … .. 76 90 a0 c4 (2048 bits)

Palvelimen julkinen avain n

Miksi sertifikaatteja tarvitaan?

Man in the Middle hyökkäys

Sertifikaattien ja koko julkisten varmentajien käytön tarkoituksena on estää Man in the Middle hyökkäyksiä, jossa kolmas osapuoli E tulee käyttäjien A ja B väliin esiintyen yhteyden toisena osapuolena molempiin suuntiin. E voi lukea dataa, sekä muuttaa sitä. CA -järjestelmän tarkoitus on estää väärien julkisten avainten levittäminen ja näiden avulla tapahtuvat hyökkäykset. Palvelimen sertifikaatti sisältää palvelimen julkisen avaimen digitaalisesti allekirjoitettuna tiedostona, jota on teoriassa mahdoton väärentää.



Salatun yhteyden vaiheet

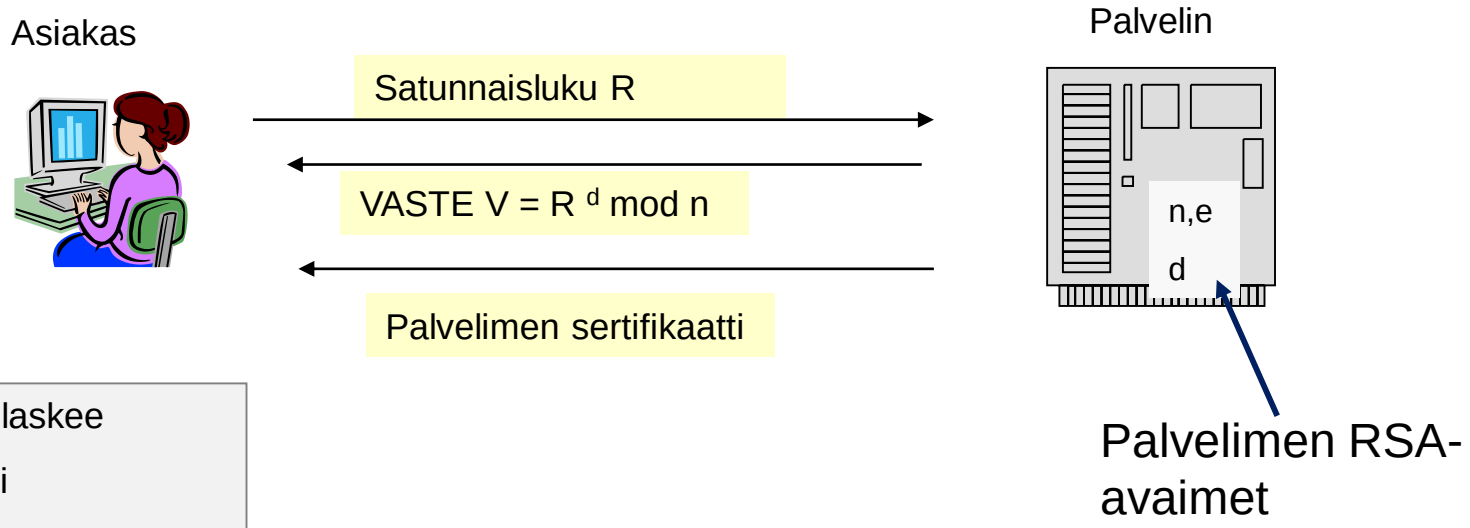
Kurssin aiemmissa luvuissa on jo esitetty TLS:n eri vaiheiden käyttämät algoritmit (RSA –autentikointi, ECDHE key exchange ja digitaalinen allekirjoitus). Alla kaavio TLS istunnon kulusta

	Tyypillinen algoritmi
“Kättely” (handshake)	
Autentikointi	**RSA**
Symmetrisestä avaimesta sopiminen	**ECDHE**
Tiedon siirto salattuna	**AES**

1. Handshake

- Kun asiakas (selain) ottaa yhteyden palvelimeen, tämä kysyy, mikä on asiakaskoneen tukema korkein TLS – versio ja mitä salausalgortmeja selain tukee.
- Asiakas vastaa esimerkiksi: ”Käytössä on enintään TLS 1.1, ja salausalgoritmit (AES, RSA, sha1RSA)
- Yhteys muodostetaan käyttäen tätä konfiguraatiota

2. Haaste-vaste autentikointi



Jos täsmää, palvelimen aitous on tarkistettu

Huom! Asiakkaan todentamisessa Suomessa useimmiten tarvitaan käyttäjätunnus- salasanayhdistelmä, joiden lisänä käytetään salausavaimiin perustuvaa mobiilivarmennusta tai perinteisiä kertakäyttösalasanalistoja (poistuvat s. 2019)

3. Symmetrisestä avaimesta sopiminen

Tavallisimmat menetelmät ovat nykyään:

1. RSA key exchange (käyttö vähenemässä)
2. ECDHE key exchange (mm. verkkopankit)

4. Tiedonsiirron salaus

Siirrettävä tieto salataan TLS:ssä useimmiten AES256 –salauksella

Sähköpostin salaus S/MIME

Sähköpostin salaamisessa käytetään protokollaa nimeltä S/MIME

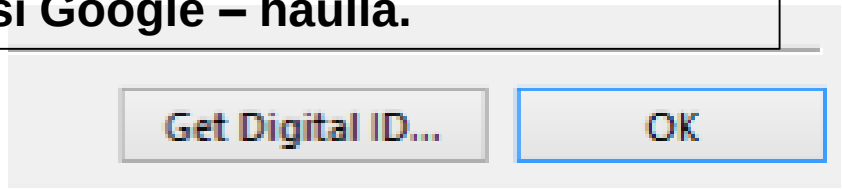
Sähköposti on kuin postikortti. Usein unohdetaan kuinka turvaton sähköposti on. Suojaamaton sähköpostiviesti on kuin postikortti: kun viesti liikkuu verkossa, se on luettavissa.

Tietosuojavaltuutetun kannanoton (Dnro 1431/41/2007) mukaan suomalainen yritys ei saa lähettää asiakkaidensa tai työntekijöidensä henkilötietoja suojaamattomalla sähköpostilla. Myös rekisterien ylläpitäjien tulee suojata henkilötiedot ja käsitellä niitä huolellisesti. Henkilötiedoksi katsotaan esimerkiksi henkilötunnuksen ja nimen yhdistelmä.

Myös Suoman valtion **VAHTI –ohjeiden** mukaan ”muita kuin julkisia henkilötietoja ei saa lähettää suojaamattomalla sähköpostilla” (koskee erityisesti henkilötunnuksen ja nimen yhdistelmää)

Mm. Outlook– ja Outlook365 -ohjelmissa sähköpostiohjelmissa on mahdollista lähettää kryptattuja viestejä käyttämällä **S/MIME- protokollaa**.

Lähettääksesi ja vastaanottaaksesi salattuja viestejä, sinun tulee hankkia CA:lta (Microsoft) tarvittavat avaimet ”Get Digital ID” -toiminnolla. Ohjeet löytyvät suomeksi Google – haulla.



S/MIME toimii samalla periaatteella kuin TLS Internet palveluissa

- Viesti salataan lohkosalaimella, esim. AES:llä.
- Viestin mukana vastaanottajalle lähetetään istuntoavain salattuna vastaanottajan julkisella avaimella.
- Koko ”paketti” salataan vielä lähettäjän yksityisellä avaimella

- Vastaanottaja purkaa ensin ”paketin” lähettäjän julkisella avaimella, sitten hän purkaa salausavaimen kryptauksen ja lopuksi purkaa salatun viestin.

Toimenpiteet takaavat viesti muuttumattomuuden ja lähettäjän autenttisuuden.

Lisää autentikointiin eli todennukseen liittyviä käsitteitä

Autentikointi
suom. varmennus/todennus

”**Varmennus** on prosessi, jossa yksi osapuoli vakuuttuu jonkin kiistattoman todisteen kautta toisen osapuolen identiteetistä”

Varmennus voidaan määritellä myös **online -palvelun alussa suoritettavana protokollana**, jossa asiakkaan identiteetti varmistetaan. Protokollan tuloksena joko hyväksyminen tai hylkäys.

Mihin varmentaminen perustuu?

Yleiseti varmennus voi perustua kolmeen tekijään:

1. Johonkin ominaisuuteesi (sormenjälki)
2. Johonkin, jonka tiedät (pin koodi)
3. Johonkin, jonka omistat (ID kortti, SIM)

”TWO FACTOR AUTHENTICATION”

Tarkoittaa yleisesti hyväksyttyä periaatetta, jonka mukaan yksi yo. listan tekijöistä ei yksin ole riittävä, vaan varmentamisessa vaaditaan vähintään kaksi tekijää: esim. sähköinen henkilökortti ja PIN koodi.

”HEIKKO” JA ”VAHVA” AUTENTIKOINTI

Engl. Weak authentication, Strong authentication
Termeihin ei sisälly arviota tai vertailua menetelmien turvallisuudesta.

”Heikko autentikointi” tarkoittaa sitä, että käyttäjä tunnistautuu käyttäjätunnuksella tai kiinteällä salasanalla, johon voi liittyä kertakäyttösalanalistan käyttö. Salausalgoritmeja ei käytetä.

”Vahva autentikointi” tarkoittaa, että varmennuksessa käytetään jotain salausprotokollaa, esim. RSA:ta. Tavallisin muoto on haaste – vaste autentikointi satunnaisluvulla.

Yksi- ja kaksisuuntainen autentikointi

Yksisuuntaisessa autentikoinnissa vain toinen osapuoli varmennetaan.

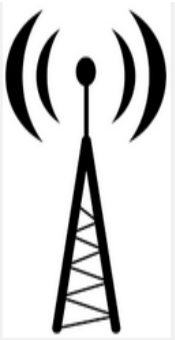
Kaksisuuntaisessa autentikoinnissa molemmat osapuolet todistavat identiteettinsä-

Yksisuuntainen satunnaislukuautentikointi

gsm

Operaattori lähettää satunnaisen haasteluvun **R** kännykälle

Kännykkä lähettää vasteluvun RES (K,R) operaattorille, joka tarkistaa vasteen oikeellisuuden vastaavalla laskulla



2G – verkossa mobiilipuhelin varmennetaan, mutta tukiaseman ei tarvitse varmentaa itseään puhelimelle. Autentikointi on siten yksisuuntainen.

3G-ja 4G – verkoissa myös tukiasema varmennetaan

Kaksisuuntainen satunnaislukuautentikointi (esim. RSA:lla)

A

A lähettää satunnaisluvun Ra

B lähettää (RSA(Ra,d_B), Rb)

A lähettää vasteena RSA(Rb, d_A)

B

Selitys; B:n vastaus sisältää vasteen haastelukuun R_a, vaste on R_a salattuna B:n yksityisellä avaimella d_B. Lisäksi B lähettää oman haasteluvun R_b A:lle. A lähettää lopuksi vasteen, joka on R_b salattuna A:n yksityisellä avaimella.

Molemmat verifioivat vasteluvut purkamalla ne vastapuolen julkisella avaimella. Viestit lisäksi yleensä salataan vastaanottajien julkisilla avaimilla.

Mobiilivarmenne

Online- palvelujen käyttäjät ovat Suomessa todentaneet itsensä pitkään pankkivarmenteilla, joissa käytetään kertakäyttösalasanalistoja.

Mobiilioperaattorit Sonera, Elisa ja DNA ovat tuoneet markkinoille **mobiilivarmenteet**, jotka ovat syrjäyttämässä pankkien kertakäyttösalasanalistat.

MOBIILIVARMENNE KÄYTTÄÄ RSA – AVAIMIA

Älypuhelimen SIM- kortissa on mobiilivamennetta varten RSA -avainpari.

TOIMINTA: Kun käyttäjä kirjautuu tietokoneellaan esim. KELA:n sivuille, sivu pyytää asiakasta varmentamaan identiteettinsä. Käyttäjä valitsee mobiilivarmenteen, jolloin sivusto pyytää avaamaan kännykän, käynnistämään mobiilivarmennesovelluksen ja syöttämään siihen nelinumeroisen PIN – koodin. Koodin syötettyään asiakas pääsee palveluun.

(Verkkopankkien tunnuslukusovellukset vastaavat mobiilivarmennetta.)

Mobiilivarmenne kaaviona