Aalto-yliopisto
Teknillinen korkeakoulu

Salaustekniikat

Tuomas Aura

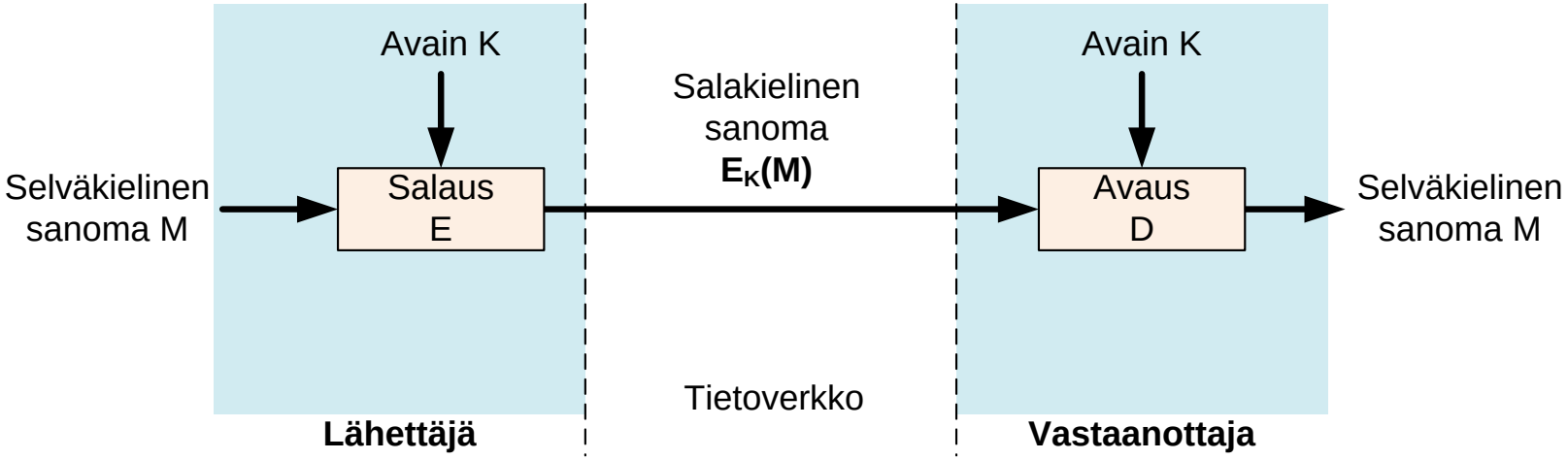
T-110.2100 Johdatus tietoliikenteeseen
kevät 2010

Luennon sisältö

1. Kryptografia
2. Salattu webbiyhteys

KRYPTOGRAFIA

Symmetrinen salakirjoitus



- Salauksen ja avaukseen tarvitaan avainta
  - Avain yleensä noin 128-bittinen satunnaisluku
- Salaus ja purku on nopeaa nykyaikaisilla prosessoreilla

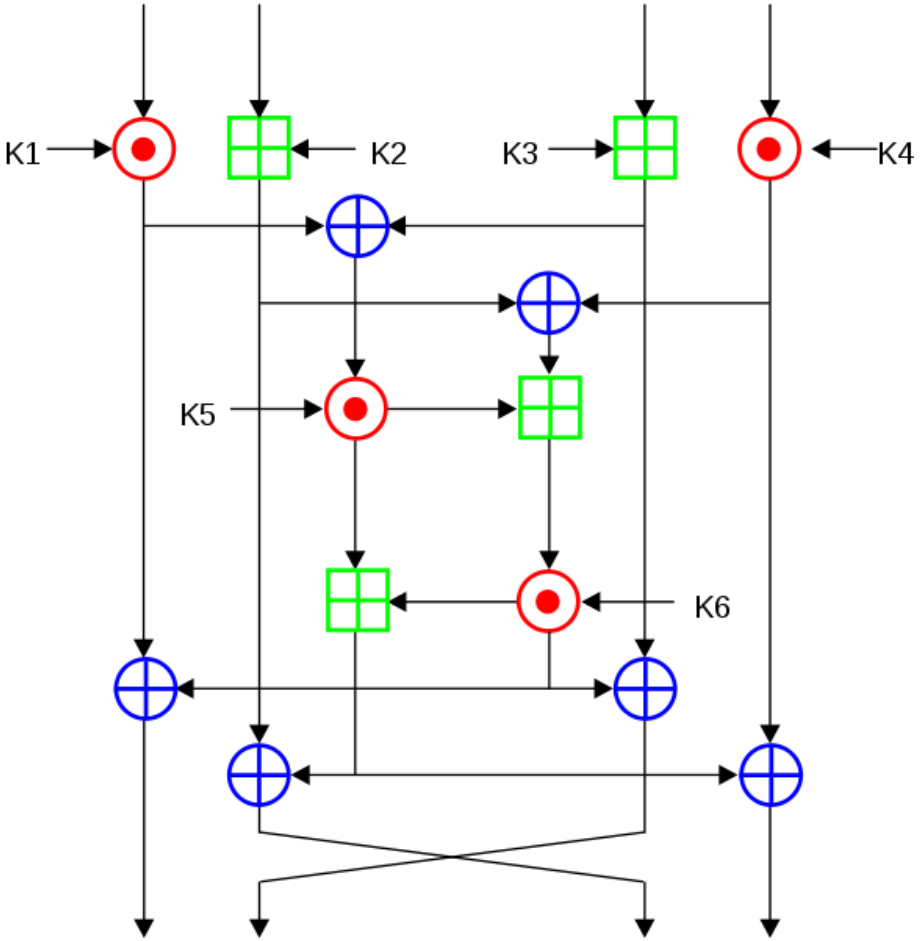
Esim. AES, 3DES, IDEA

Salauksesta

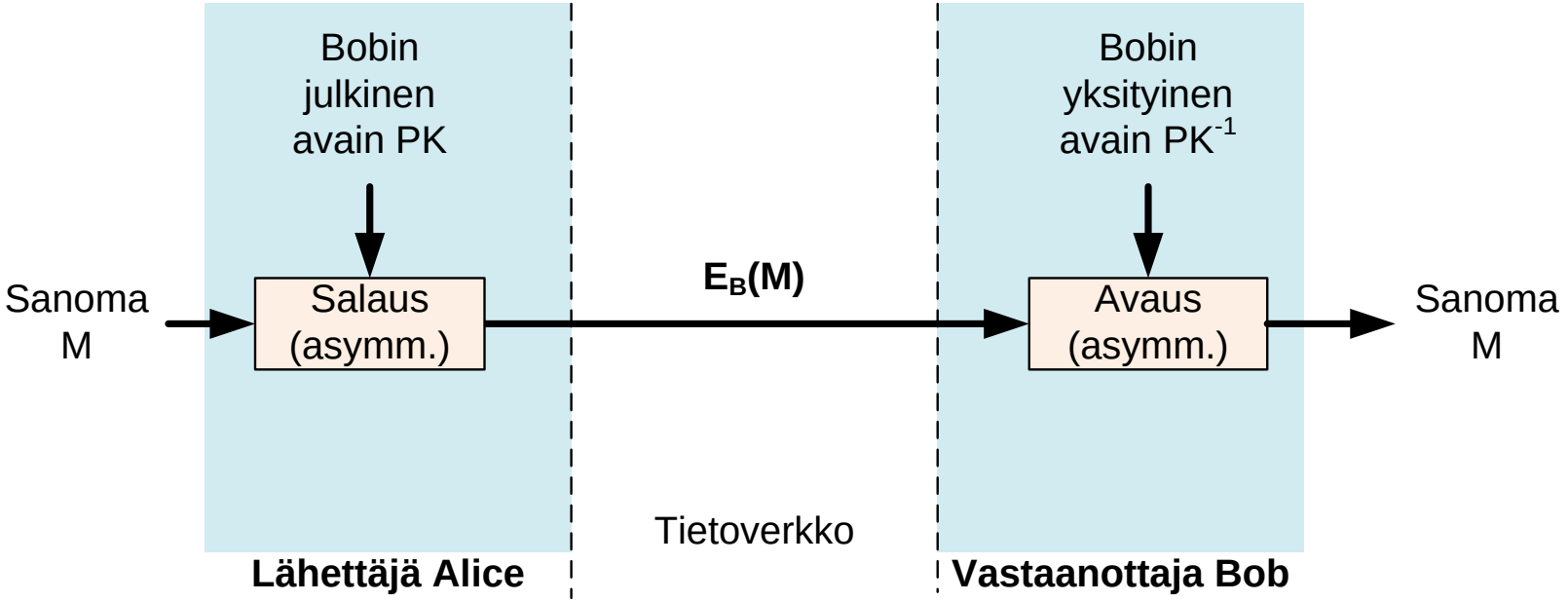
- Salaus suojaa sanoman luottamuksellisuutta, ei eheyttä
- Avain salainen, algoritmi julkinen
- Salattu data näyttää täysin satunnaiselta, jollei avain tiedossa (vain viestin pituus paljastaa jotain)
- Toteutus perustuu bittioperaatioihin
- 128-bittinen tai pitempi avain mahdoton arvata tai löytää kokeilemalla
- Nykyaikainen vahva salakirjoitus (AES, 3DES) on käytännössä murtamaton
- Ei ole mitään syytä käyttää heikkoja algoritmeja (esim. vanha DES tai oma epästandardi algoritmi)

Esimerkki

- IDEA-salausalgoritmi
- Koostuu 16-bittisten lukujen modulo-yhteenlaskusta, kertolaskusta ja xor-operaatioista
- 8 kierrosta (ks. oikealla), jotka vähitellen sotkevat selväkielen ja avaimen osat toisiinsa
- Julkaistu 1991, hitaampi kuin AES ja muut uudemmat algoritmit



Epäsymmetrinen salaus



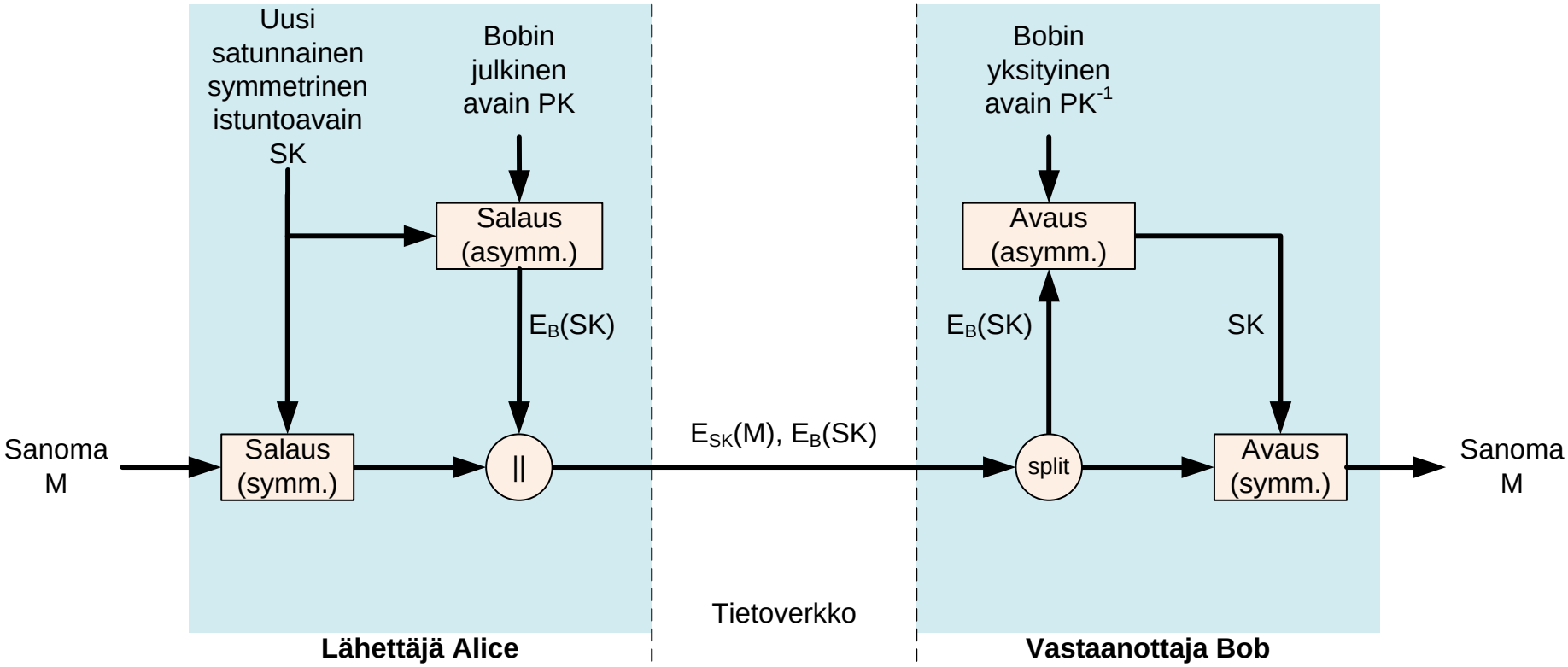
- Avainpari:
  - Salaus julkisella avaimella, avaus yksityisellä avaimella
  - Julkisen avaimen voi kertoa kaikille, yksityisen avain pidettävä salassa
- Avaimet pitkiä, salaus ja avaus melko hidasta
  - Perustuu suurten kokonaislukujen aritmetiikkaan

Esim. RSA, ElGamal

Esimerkki

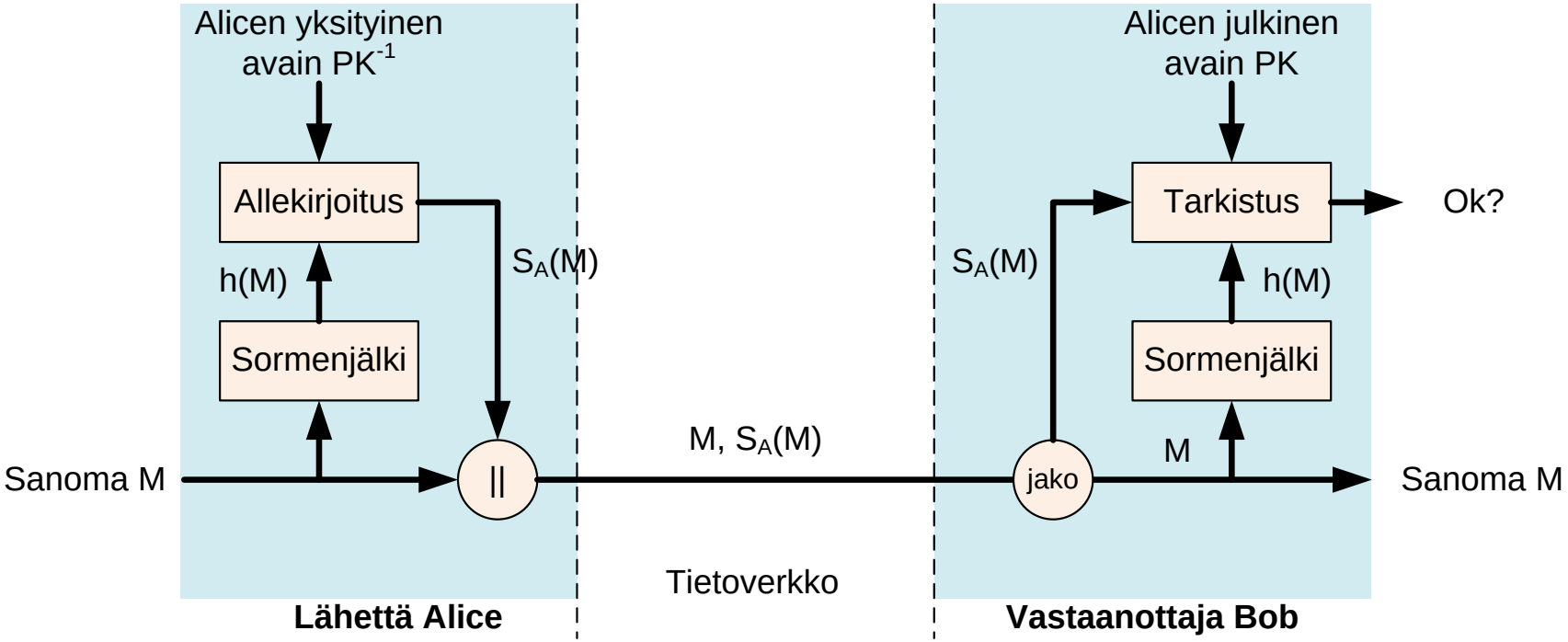
- RSA-salaus, julkaistu 1978
- p,q = suuria salaisia alkulukuja (512…1024 bittiä)
- Julkinen moduuli n = pq
- Eulerin totienttifunktio $\phi(n) = (p-1)(q-1)$
- Julkinen eksponentti e, esim. 2^16+1
- $de \equiv 1 \pmod{\phi(n)}$,
  ratkaistaan salainen eksponentti d
- Salaus $C = M^e \bmod n$
- Avaus $M = C^d \bmod n$
- Turvalliseen toteutukseen vaaditaan muita yksityiskohtia, katso esim. PKCS#1

Hybridisalaus



- Julkisen avaimen salausta käytetään yleensä vain symmetrisen avaimen siirtoon

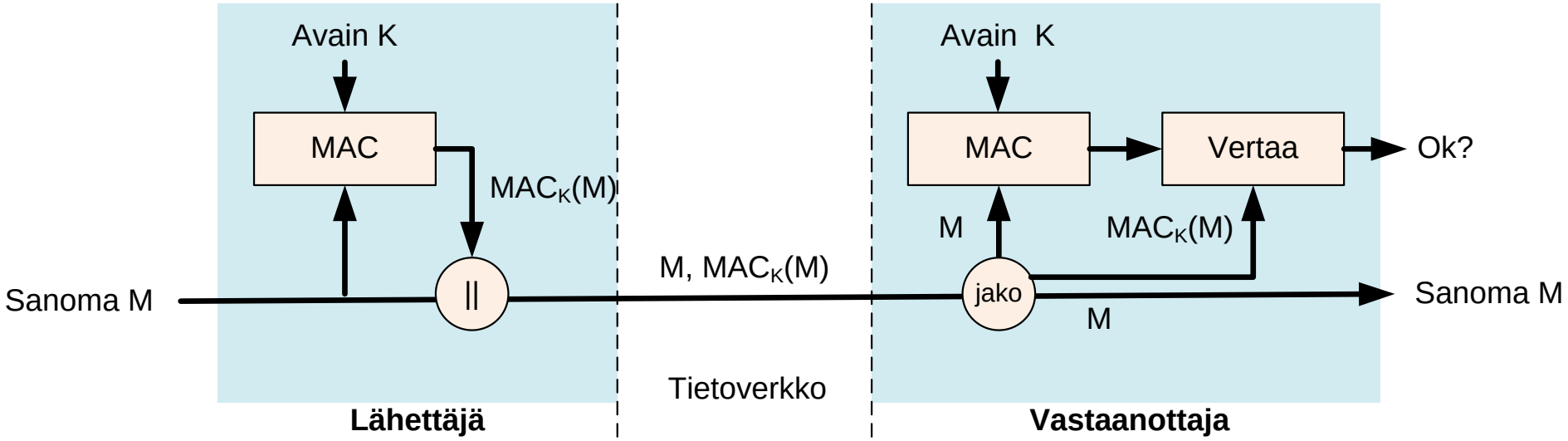
Allekirjoitus



- Allekirjoitus yksityisellä avaimella, allekirjoituksen tarkistus julkisella avaimella
- Allekirjoitus suojaa viestin eheyttä, ei luottamuksellisuutta
- Lasketaan viestistä sormenjälki (*hash*) tiivistefunktiolla ja allekirjoitetaan vain sormenjälki

Esim. RSA, DSA

Todennuskoodi



- ”Symmetrinen allekirjoitus”, MAC
- Perustuu tiivistefunktioihin tai symmetriseen salausalgoritmiin
- Nopea laskea suurelle määrälle dataa

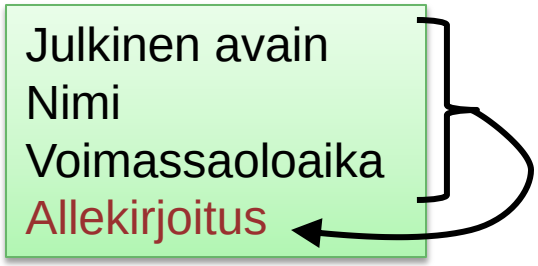
Esim. HMAC-SHA1, CBC-MAC-AES

Julkisen avaimen algoritmeista

- Julkisia avaimia on yksi per osapuoli, symmetrisiä tarvitaan yksi per yhteys
- Julkisen avaimen voi kertoa kaikille, symmetrinen täytyy pitää salassa
- Julkisen avaimen algoritmit ovat satoja kertoja hitaampia kuin symmetriset
- Yleensä epäsymmetrisiä algoritmeja käytetään alussa symmetrisen avaimen luomiseen
- Pitää tietää, kenen julkista avainta käyttää!

Varmenne

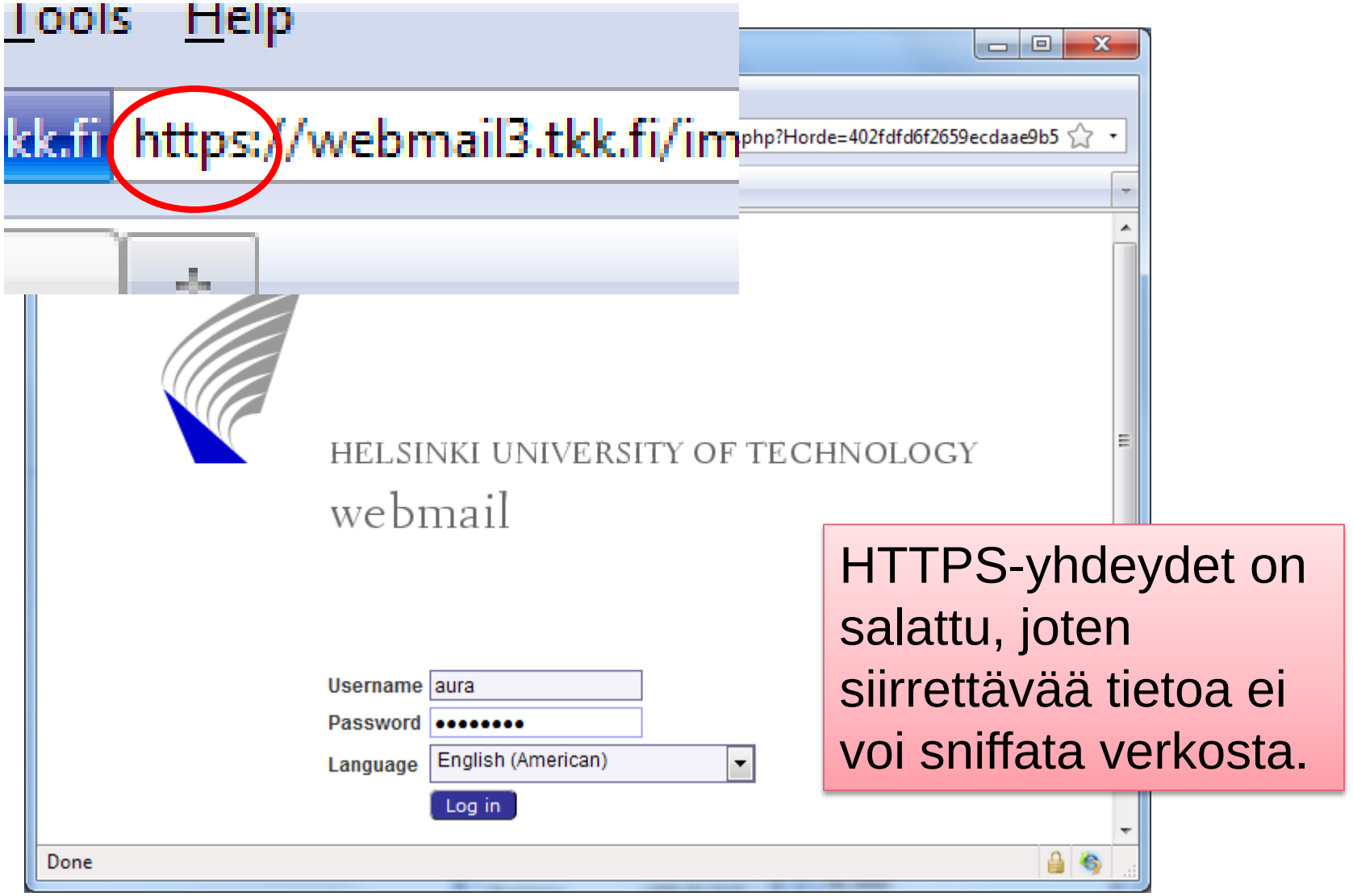
- Varmenne eli sertifikaatti
  - Varmentajan eli sertifiointiauktoriteetin (CA) allekirjoittama viesti, joka sitoo julkisen avaimen nimeen
  - Voi kertoa muutakin tietoa



- Yleensä X.509-standardin mukainen
- Varmenteita käytetään webbisivuilla, langattomissa lähiverkoissa, sähköisessä henkilökortissa ja muissa kansalaisvarmenteissa
- Kaupallisia varmentajia esim. Verisign ja TeliaSonera
- Varmentajat voivat muodostaa hierarkian, jossa ylempi varmentaja valtuuttaa alemman
- Varmentajia ja varmenteita kutsutaan julkisen avaimen infrastruktuuriksi (PKI)

SALATTU WEBBIYHTEYS

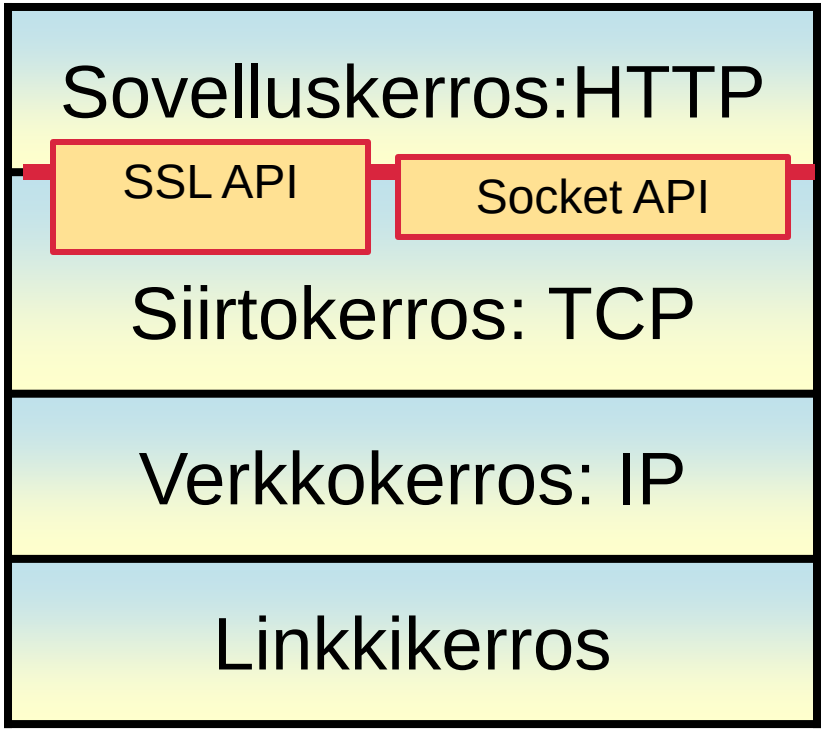
Turvallinen webbisivu (https)



HTTPS-yhdeydet on salattu, joten siirrettävää tietoa ei voi sniffata verkosta.

SSL-kerros

- SSL toteuttaa salauksen ja todennuksen TCP-yhteyksille
- SSL tarjoaa sovelluksille socket-rajapinnan tapaisen palvelun tavuvirran siirtoon, mutta suojattuna
- TLS on uudempi standardoitu version SSL:stä



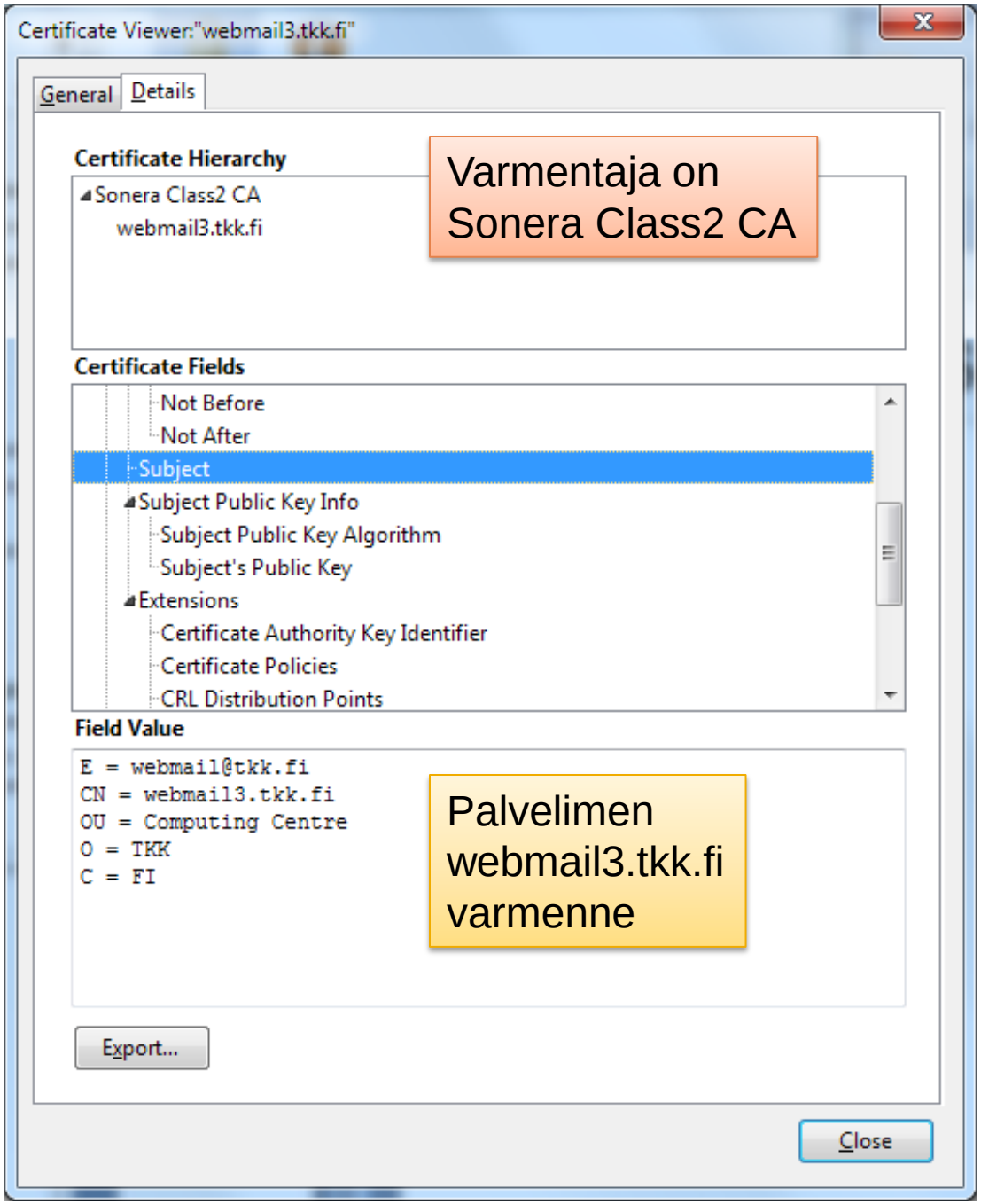
SSL-protokolla

- Kaksi osaa:
  - Kättely eli todennettu avaintenvaihto luo selaimelle ja palvelimelle symmetrisen istuntoavaimen
  - Istuntoprotokolla suojaa istunnon käyttäen symmetristä salausta, todennuskoodeja ja kättelyssä luotua istuntoavainta
- Kättely perustuu varmenteeseen ja asymmetriseen salaukseen
  - Palvelin lähettää selaimelle varmenteen, josta selviää sen julkinen RSA avain
  - Selain generoi satunnaisen istuntoavaimen ja lähettää sen palvelimelle salattuna palvelimen julkisella avaimella

Luottamusketju

1. Selaimessa on lista luotettujen kaupallisten varmentajien julkisista avaimista (”juurivarmenteet”); selain hyväksyy vain listalla olevan varmentajan allekirjoittamat varmenteet
2. Selain saa kättelyssä palvelimelta varmenteen, joka sitoo palvelimen DNS-nimen ja julkisen avaimen
3. Selain tarkistaa, että palvelimen osoitepalkissa näkyvä DNS-nimi on sama kuin varmenteessa
4. Palvelimen julkista avainta käytetään palvelimen todentamiseen avaintenvaihdossa (selain lähettää istuntoavaimen sillä salattuna)
5. Avaintenvaihdossa luotua symmetristä avainta käytetään yhteyden salaamiseen ja todentamiseen

- Myös asiakkaalla voi olla varmenne; yleensä ei ole, vaan käyttäjä todennetaan tarvittaessa salasanalla

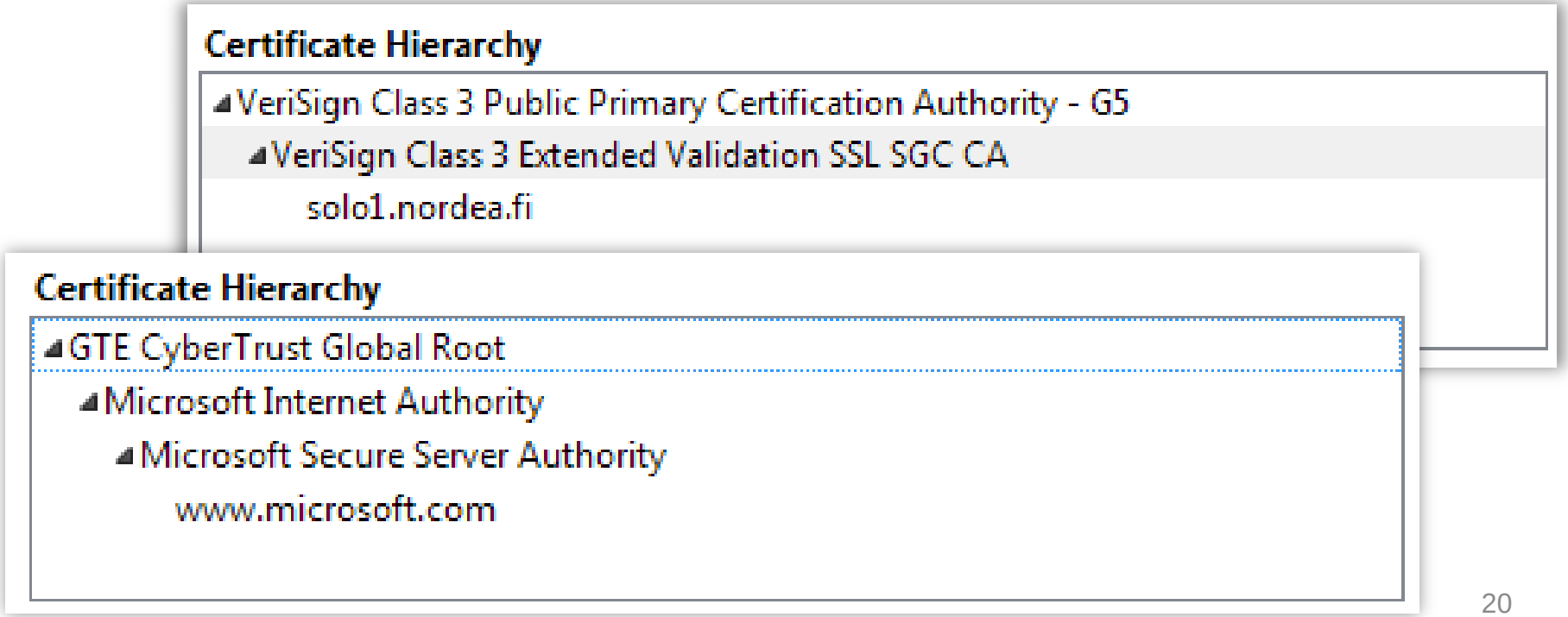


Luottamusketjun ansiosta selain voi tarkistaa, että tämä palvelin todella on webmail3.tkk.fi

Mistä käyttäjä tietää, että webmail-palvelimen nimi onkin webmail**3**?

Varmenneketju

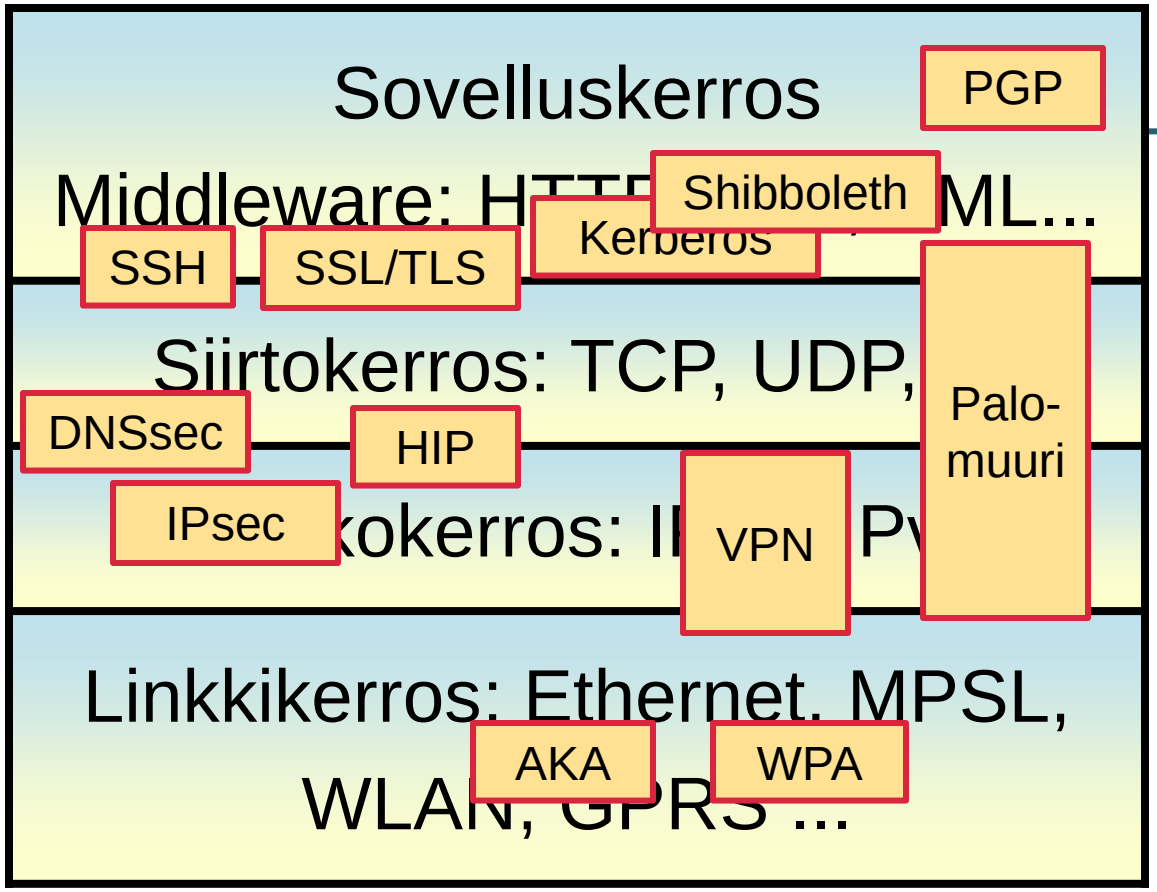
- Webbipalvelimella on yleensä varmenneketju
  - Ylin CA varmentaa itsensä (juurivarmenne, joka ei oikeastaan merkitse mitään)
  - Ylempi CA varmentaa alemman
  - Alin CA varmentaa palvelimen



Varmenneketju ja luottamus

- Selain saa kättelyssä palvelimelta varmenneketjun
- Selain tarkistaa, että ketju alkaa juurivarmenteella, joka on sen luotetussa listassa
- Selain käy varmenneketjun läpi:
  - Tarkistaa kunkin varmenteen allekirjoituksen edellisestä varmenteesta saadulla julkisella avaimella
  - Tarkistaa, että kaikki paitsi viimeinen varmenne valtuuttavat alivarmentajan
  - Tarkistaa muita yksityiskohtia
- Jos ketjun tarkistus onnistuu, alin varmenne sitoo palvelimen DNS-nimen ja julkisen avaimen toisiinsa

Tietoturvaprotokollat



Sovellusten turvallisuus, esim. sähköinen kaupankäynti

Tiedonsiirron luottamuksellisuus ja ja eheys

Verkko-infrastrustuurin luotettavuus

Lisää tietoturvasta

- T-110.4200 Tietoturvallisuustekniikka
- T-110. 5240 Network Security
- T-110.5211 Cryptosystems,
  T-79.4501 Cryptography and Data Security
- T-110.6220 Special Course in Information Security (malware)
- T-110.5200 Laboratory Works on Information Security
- T-110.5620 Tietoturvallisuuden kehittämisprosessit
- T-110. 5290 Seminar on Network Security
- T-79.5501 Cryptology