Varmennejärjestelmä ja kertakirjautuminen – miksi ja miten?

Varsinais-Suomen sairaanhoitopiirin ratkaisu

Yrjö Koivusalo
tietohallintapäällikkö
VSSHP

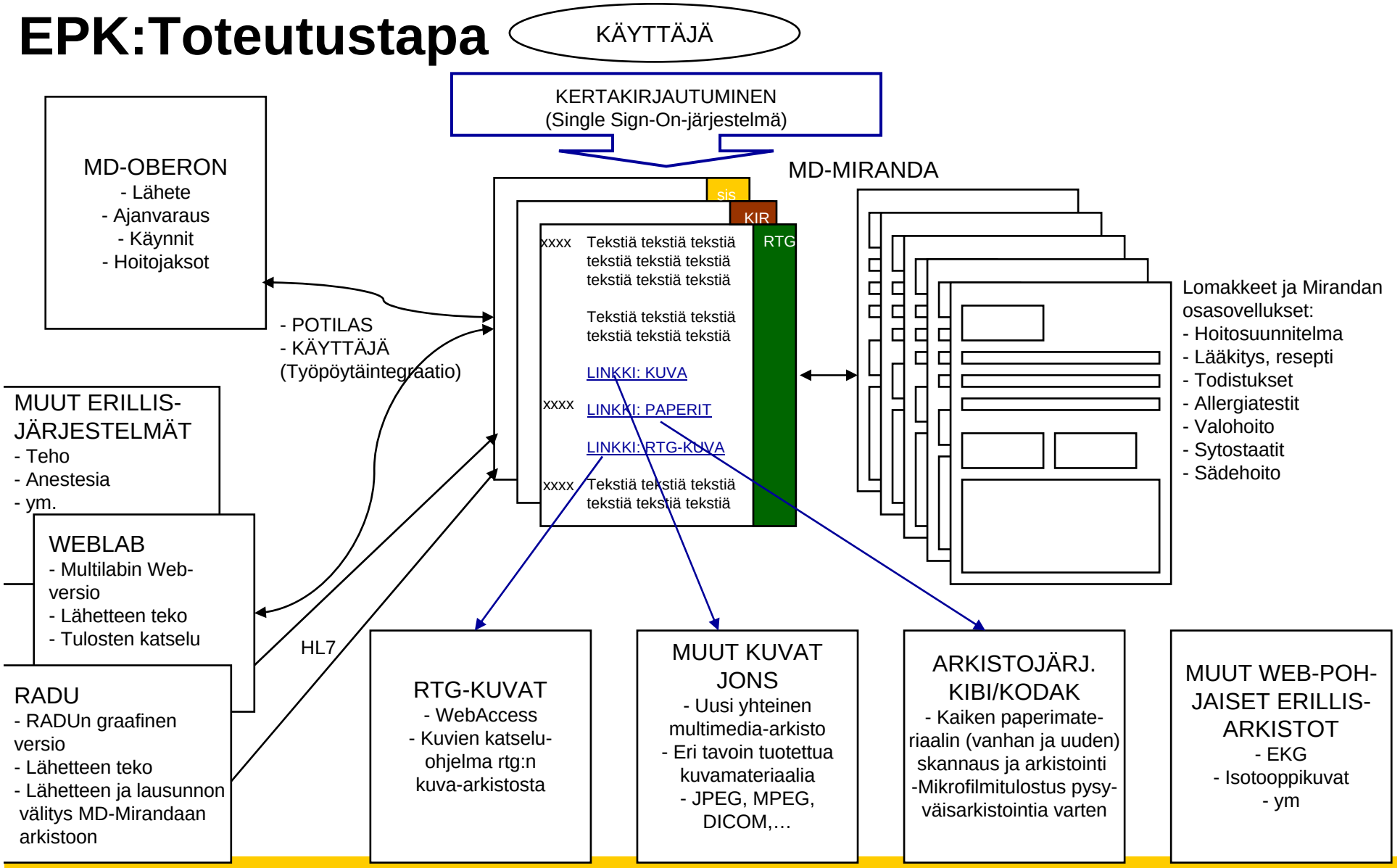
Esityksen sisältö

- Miksi PKI Varsinais-Suomen sairaanhoitopiiriin?
- Varmennejärjestelmä – miten ratkaistiin?
- Kertakirjautuminen – miten ratkaistiin?

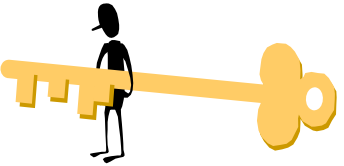
EPK-projekti = Elektroninen PotilasKertomus

- Tavoitteena kokonaisvaltainen sähköinen potilaskertomus V-SSHP:ssa – ’Paperiton ja filmitön sairaala’
- Aikataulu 2002-2005
- Pilottiyksikkö marraskuussa 2003 käyttöön otettu uusi T-sairaala

EPK:Toteutustapa



PKI = Public Key Infrastructure



- Tarjoaa infrastruktuurin luotettavien ja tehokkaiden turvapalveluiden toteuttamiseksi:
  - Todennus — Osoita kuka olet !
  - Tiedon eheys — Älä muuta tietojani !
  - Luottamuksellisuus — Älä urki tietojani !
  - Kiistämättömyys — Pidä lupauksesi !

- Terveydenhuollossa nämä vaatimukset ovat aivan keskeisiä
- PKI ei ole kuitenkaan sovellus, VAAN perustekniikka, jonka varaan sovelluksia voidaan toteuttaa

PKI:n hyödyntäminen

- Käyttäjän todentaminen (1. tavoite VSSHP:ssa)
  - Sisäänkirjautuminen => salasanojen vähentäminen/poistaminen
  - Käyttäjä- ja käyttöoikeuksien hallinta => sama identiteetti eri järjestelmissä
  - Järjestelmien etäkäyttö
- Sähköinen allekirjoitus (2. tavoite VSSHP:ssa)
  - Virallisten dokumenttien e-käsittely ja allekirjoitus (esim. sairaskertomukset, reseptit, lausunnot)
- Tiedonsiirron salaus
  - Järjestelmien etäkäyttö
  - Sähköposti

Varmennepalvelut – miten ja miksi?

Varmennepalvelut

- Varmentaja tuottaa luotettavaa sähköistä identiteettiä (henkilöille ja laitteille)
- Varmentaja liittää kohteeseen sähköisen identiteetin, jonka kelpoisuutta/luotettavuutta ylläpidetään sulkulistan avulla.
- Varmennepalveluja tuottavat:
  - Organisaatiot itselleen (kuten nyt VSSHP)
  - VRK tuottaa kansalaisvarmenteita, virkavarmenteita ja organisaatiovarmenteita
  - Varmennepalveluja tuottavat muiden toimintojensa ohessa myös esim. teleoperaattorit

Alueellisen toimijan rooli kansallisessa PKI-arkkitehtuurissa

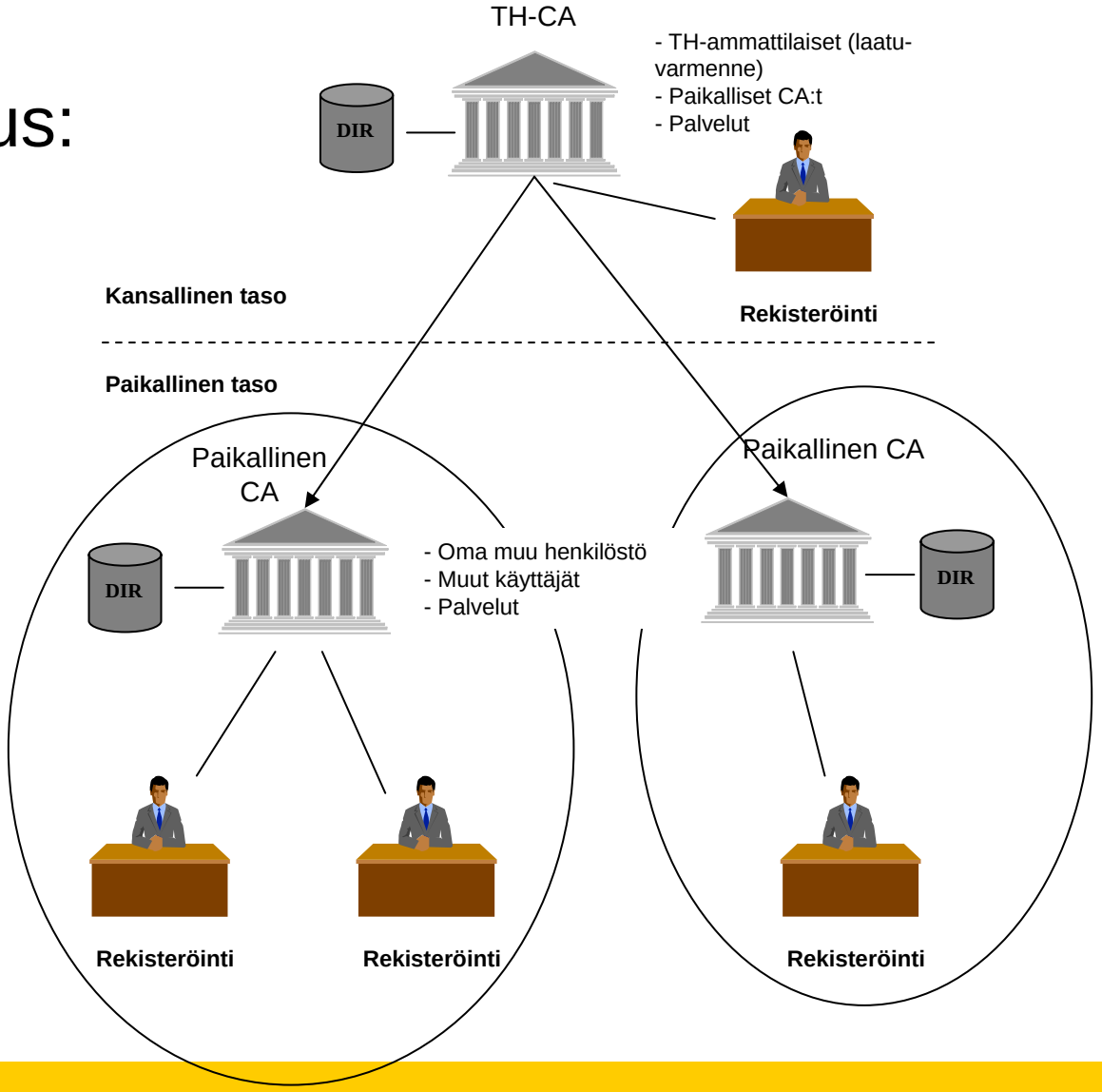
Paikallis- tai alueorganisaatioiden vastuulla on

- Vastata siitä, että alueellinen varmennepolitiikka vastaa kansallisia määrityksiä
- Hallita käyttöoikeuksia ja työsuhteita ja tuottaa niiden tarvitsemat tunnistamis- ja varmennepalvelut
- Tuottaa paikalliset (ei laatusertifiointia edellyttävät) allekirjoitus- ja varmennepalvelut henkilöille, järjestelmille ja ohjelmistoille
- Hallita dynaamisia rooleja ja tuottaa asiakirjoihin tieto kulloisestakin roolista tarvittaessa
- Ylläpitää alueellisia varmenne- ja hakemistopalveluja

(Ehdotus Sosiaali- ja terveydenhuollon sähköisen asioinnin arkkitehtuuriksi - terveydenhuollon PKI-arkkitehtuuri / OSKE 4/02)

TH:n PKI – osin keskitetty

Suositus:



Varmennepalvelujen luonne

Ostajan kannalta kyseessä lähes aina pitkäjännitteinen sitoutuminen, varmentajan vaihtaminen on kallis operaatio. Esim. kaikki kortit uusittava

Varmentajan olisi siis syytä jatkaa toimintaa niin kauan kuin asiakas sitä tarvitsee.

Kaupallinen varmentaminen ei ollut osoittautunut kannattavaksi

Luonteeltaan mitä suurimmassa määrin 24/7 toimintaa

Toimiminen itse varmentajana

Riskitön vaihtoehto, toiminnan riittävä jatkuvuus varmaa

Hallitut kustannukset

Isompi alkuinvestointi, mutta jakamalla kustannuksia saa alaspäin

Varmennepolitiikka ja toimintaperiaatteet omassa kontrollisssa, esim. siirtyminen ”Laatuvarmentajaksi”

Vaatii ammattitaitoista henkilöstöä, mutta toiminnan voi ulkoistaa (esim. VRK)

Ulkoistuksen voi kilpailuttaa halutuin välein

Esiintulleita erityisvaatimuksia varmennepalvelulle ja ratkaisumalli

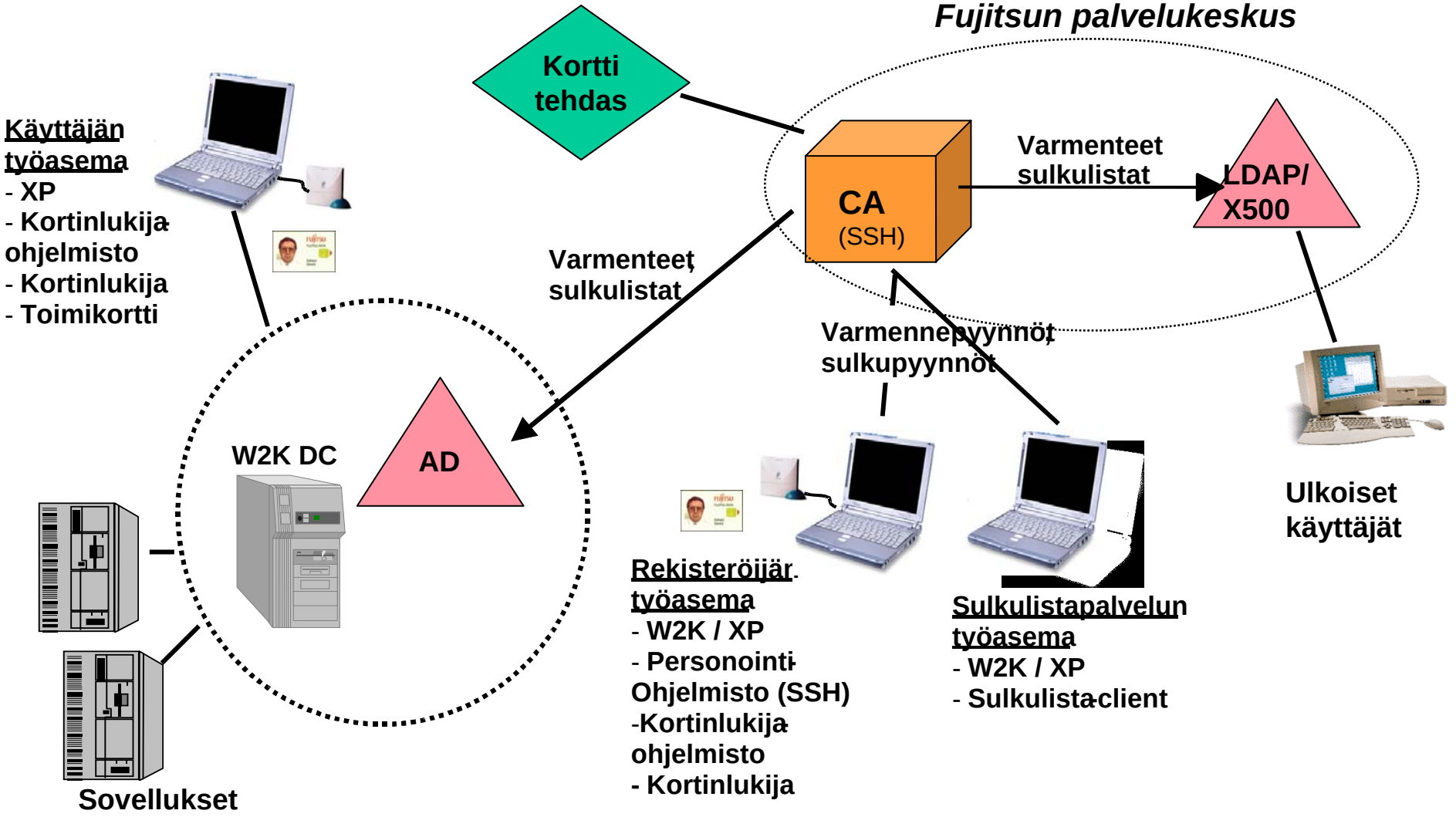
- Key recovery
- Hajautettu rekisteröinti
- Hajautettu korttituotanto
- Keskitetty korttituotanto
- AD-hakemistojen tuki
- Smartcard logon
- Tilapäiskortit

Nämä vaatimukset katsottiin voitavan ratkaista parhaiten omalla varmennejärjestelmällä.

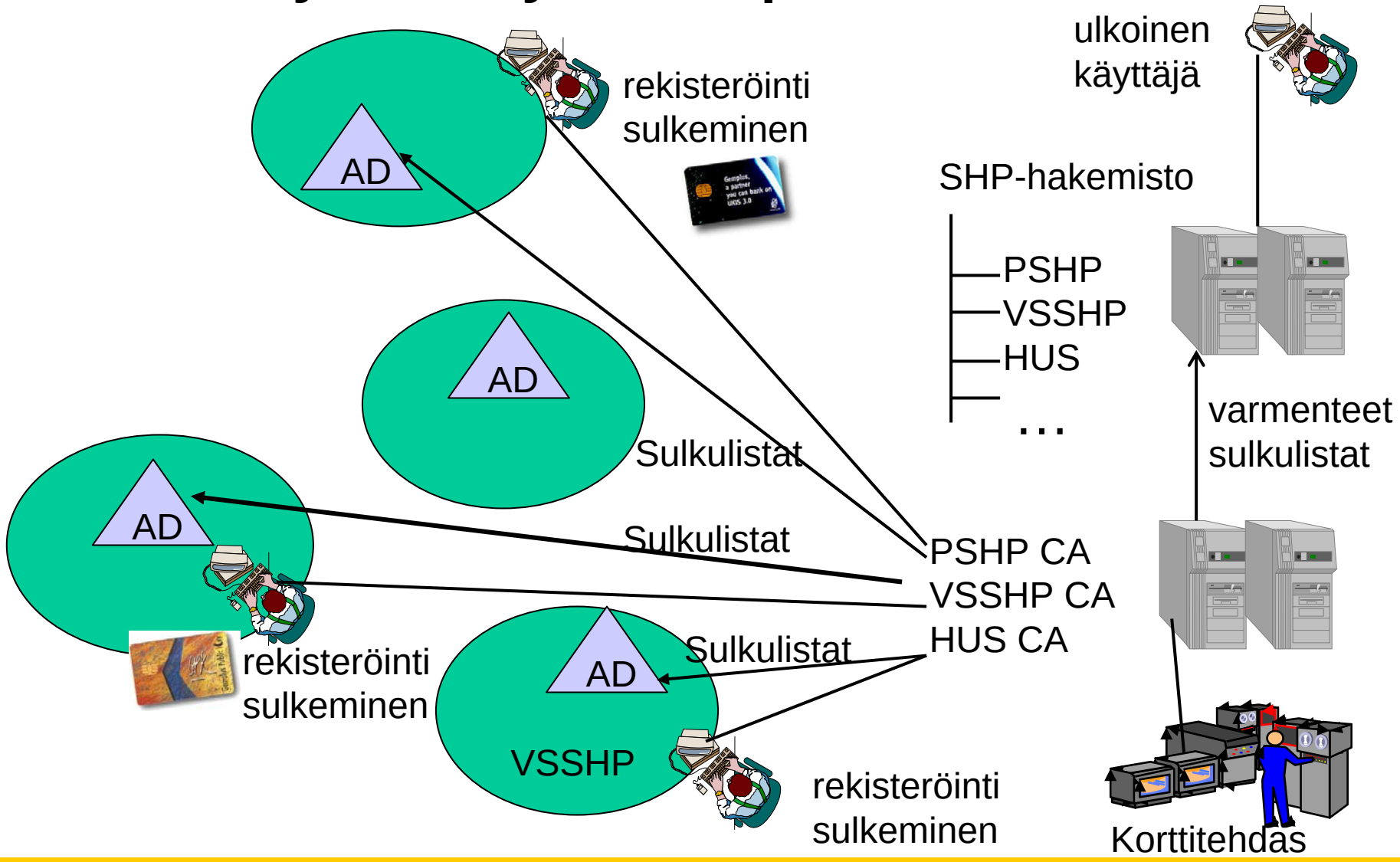
Kokonaistoimittajaksi valittiin Fujitsu kesäkuussa 2003.

Rakennettiin yhteiskäyttöiseksi – nyt mukana Pirkanmaan shp, HUS ja Satakunnan shp.

VSSHP PKI-ympäristö



SHP CA – yhteiskäyttöinen palvelu



Kertakirjautumisratkaisu

Kertakirjautuminen = SSO

2 näkökulmaa:

- Käyttäjä: yhdellä tunnuksella joka paikkaan
- Ylläpitäjä: tietoturva ja käyttäjien keskitetty ylläpito

- Perinteisesti jokaiseen sovellukseen eri käyttäjätunnus ja salasana
- Samalla käyttäjätunnuksella ja salasanalla päästään eri sovelluksiin (salasanasynkronointi)
- Yhdellä kirjautumisella päästään useaan sovellukseen
- Kirjautuminen toimikortilla (PIN-koodi)

Kertakirjautumisen vaatimukset sairaalassa

- Tarve kirjautua useasti työpäivän kuluessa samalle tai eri työasemalla / sovelluksiin
  - Jaetut työasemat (monta käyttäjää yhdellä työasemalla)
  - Liikkuva työ (yhdellä käyttäjällä monta työasemaa)
- Tarve mahdollistaa allekirjoituksen teko toisen käyttäjän ollessa sisäänkirjautuneena
  - Usean lukijan tuki (kiinteä lukija, mobiili lukija)
- Nopeus, nopeus, nopeus
- Usein ei riitä pelkän sisäänkirjautumisen kontrollointi – pitää kontrolloida käyttäjän oikeuksia sovelluksen sisälläkin: kenen potilaan tietoihin tässä yhteydessä saa mennä

Toiminnalliset vaihtoehdot

- Skenaario 1: ”nopeasti yleistunnuksella työasemaan ja sen jälkeen vahvasti kortilla sovelluksiin ja domain-palveluihin”
  - – Windows ei toimi näin
- Skenaatio 2: ”nopeasti yleistunnuksella työasemaan ja sen jälkeen vahvasti kortilla sovelluksiin. Henkilökohtaisiin domain-palveluihin haluttaessa kirjaudutaan työasemalle uudelleen omalla kortilla”
  - – Ei tue sovellusten integrointia domain-logoniin
- Skenaario 3: “kirjaudutaan työasemaan kortilla, jolloin kaikki AD-perustaiset sovellukset ovat käytössä. Muihin sovelluksiin erillinen (kerta)kirjautuminen.”
  - – Edestakainen sisäänkirjautuminen hitaampaa kuin edellä (1&2)

Vaatimukset

- Sisäänkirjauksen oltava nopea => Skenaario 2
- Tuettava toimikorttia
- Ratkaisun oltava kattava (keskeiset sovellukset mukaan)
  1) MD -sovellukset : Miranda, Oberon, Titania (Umbriel, Ariel)
  2) Musti -sovellukset : WinRadu
  3) Web-sovellukset: WebAccess, WebLab
- Medici Datan tuotteet ovat keskeisessä asemassa kliinisessä työssä
- Jatkossa integroitavia tuotteita on lisää

Tavoitetilan toiminnallisuus (1)

- Käyttäjän näkökulma / yleiskäytössä oleva työasema
  - Työasema on valmiina käynnissä yleistunnuksella
  - Käyttäjä syöttää toimikortin ja antaa PIN-tunnuksen, jonka jälkeen SSO:n piirissä olevat sovellukset voidaan käynnistää ilman tunnuskyselyjä
  - Kortin poistaminen lukitsee kaikki SSO:n piirissä olevat istunnot
  - Muut käyttäjät eivät pääse työasemalta SSO-sovelluksiin ilman edellisen käyttäjän uloskirjausta

Tavoitetilan toiminnallisuus (2)

- Käyttäjän näkökulma / henkilökohtainen työasema
  - Käyttäjä kirjautuu työasemaan toimikortilla antaen PIN-tunnuksen
  - Henkilökohtaiset palvelut ja SSO-sovellukset ovat automaattisesti käytössä vahvalla todentautumisella

Tavoitetilan toiminnallisuus (3)

- Ylläpitäjän näkökulma
  - Käyttäjät luodaan kertaalleen yleiseen hakemistoon yleisillä käyttäjä-, rooli-, ryhmä- ja organisaatiotiedoilla
  - Sovellukset on integroitu SSO-palveluun eivätkä ne edellytä erillistä sisäänkirjausta
  - Sovellukset osaavat hyödyntää yleisen käyttäjähakemiston tietoja ja tarvittaessa liittää ne osaksi omaa rooli-/käyttöoikeustietoa

Tekninen ratkaisu

- Ei käytetä valmiita SSO-tuotteita, vaan sovellusmuutoksiin perustuvia ratkaisuja
- Medici Datan MD-Ariel ytimenä
  - MD-sovellusdomain (käyttäjähallinta Umbrielissa)
  - Muut sovellukset (henkilötunnisteen välitys Umbrielista sovellukselle)
- Muiden sovellusten integrointi käyttämään Umbrielia myös käyttöoikeuksien osalta on suuri työ
- Aikataulu edellytti todentamisinfraa taustalle
  - mPollux Security Server

Tilanne huhtikuussa 2004

- Varmennepalvelu ja hakemisto toiminnassa, n. 500 korttia tehty ja jaettu
- SSO-järjestelmän ydin valmiina ja keskeiset tuotteet käytössä tai ainakin testipenkissä
- Ensimmäiset sähköisesti allekirjoitettavat lomakkeet toteutettu
- Sairauskertomuksen allekirjoitusratkaisun 1. vaihe työn alla