FUJITSU

PKI-arkkitehtuurin kansallinen selvitys

Terveydenhuollon atk-päivät 27.-28.5.2002

Björn-Eric Svensson
osastopäällikkö
Fujitsu Invia Oyj
email : bjorneric.svensson@invia.fujitsu.com

Fujitsu Invia Oyj

Fujitsu Invian lyhyesti

- **Pohjoismainen konserni**
  - **Suomi, Ruotsi, Tanska, Norja**
  - **liikevaihto 332 m €, henkilöstö 2400**
- **Kaksi divisioona**
  - **eServices**
  - **eSolutions**

- **Toimitamme ratkaisuja ja palveluja muun muassa PKI-ja MiddleWare alueilla**

FUJITSU

PKI = Public Key Infrastructure

- Tarjoaa infrastruktuurin luotettavien ja tehokkaiden turvapalveluiden toteuttamiseksi:
  - todennus — Osoita kuka olet !
  - eheys — Älä muuta tietojani !
  - luottamuksellisuus — Älä urki tietojani !
  - kiistämättömyys — Pidä lupauksesi
  - käyttöoikeudet — Mitä sinulla on lupa tehdä ?

- Siis PKI ***EI OLE*** sovellus, ***VAAN*** perustekniikka, jonka varaan sovelluksia voidaan toteuttaa

FUJITSU

PKI ratkaisua tarvitaan kun

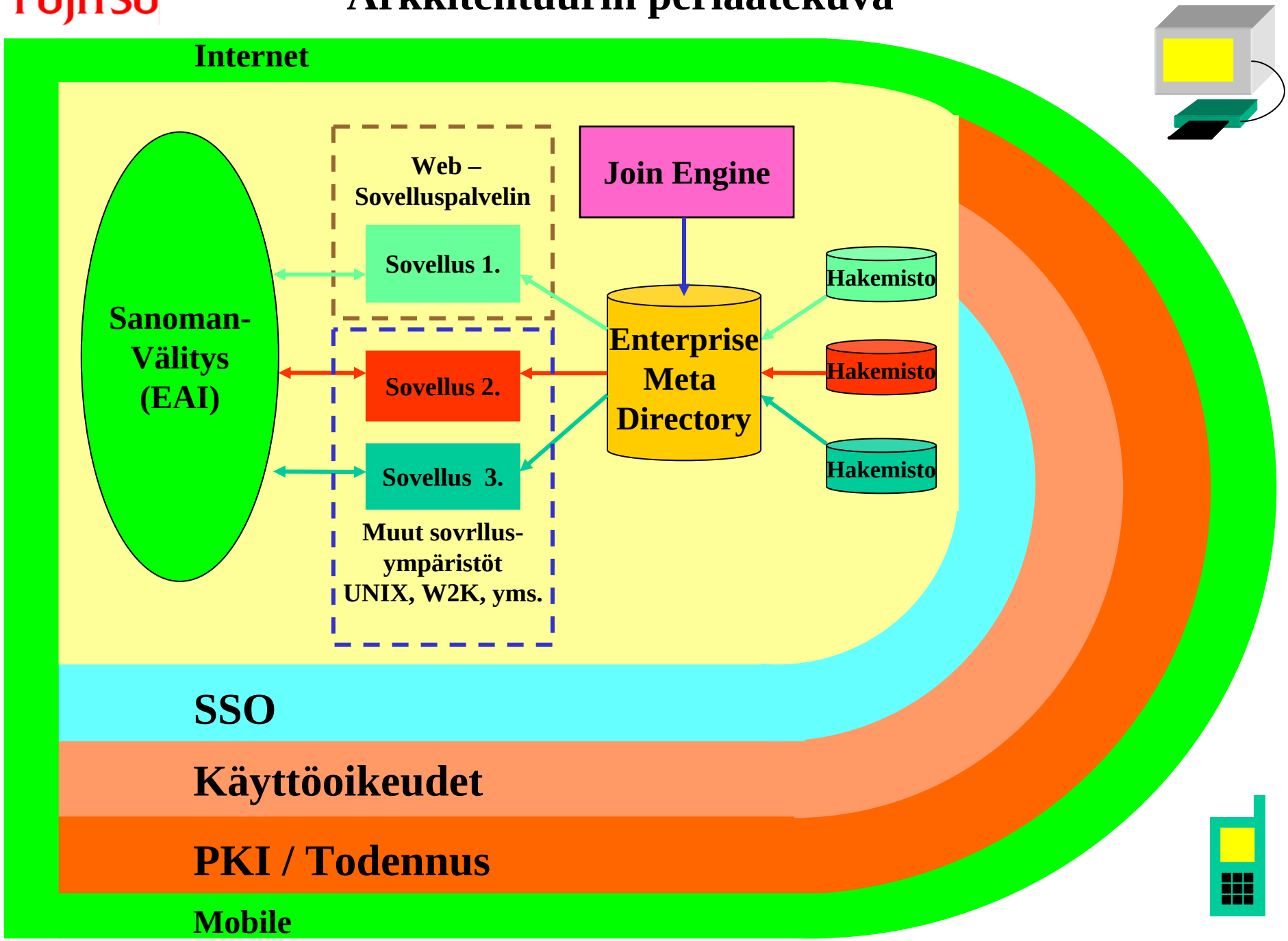
- sidosryhmille annetaan pääsy organisaation tietojärjestelmiin
- liiketoiminta edellyttää nykyistä varmempaa sisäisten käyttäjien tunnistamista ja todentamista
- tarvitaan sähköistä allekirjoitusta

FUJITSU

PKI ja yleinen arkkitehtuuri

- PKI ja hakemistosuunnitelman teko johtaa yleensä it-arkkitehtuurin analyysiin
- Sovellusten PKI-kelpoisuus
- hakemistoratkaisu ja SSO kannattaa huomioida suunnitelmassa

Arkkitehtuurin periaatekuva



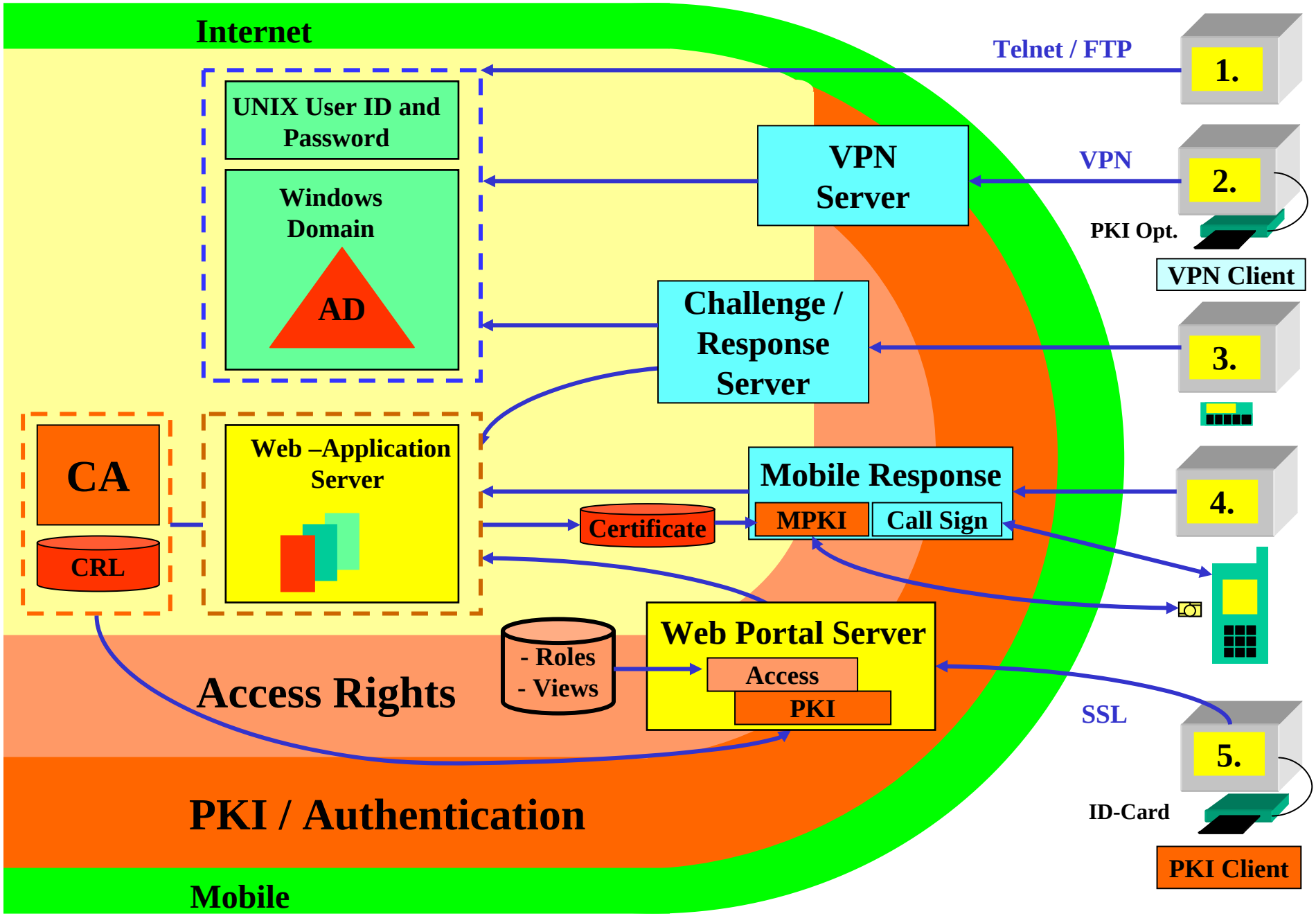
FUJITSU

Arkkitehtuurin hyödyt

- Sovellukset käyttävät yhteisiä palveluja
  - sisäänkirjaantuminen, todentaminen, kanavat
  - yhteinen hakemistoratkaisu, hakemistojen integrointi
  - sovellusten välinen integraatio (EAI)
  - sovelluskeskeisyys => kokonaisuuskeskeisyys
- Sama asia tehdään vain kertaalleen
  - pyörää ei keksitä jokaiselle sovellukselle uudestaan
  - sovellustoimittajalle voidaan esittää selkeät vaatimukset
- Sovellukset ripustetaan uuteen arkkitehtuuriin
  - käyttöönotto tehostuu ja nopeutuu

FUJITSU

PKI Architecture

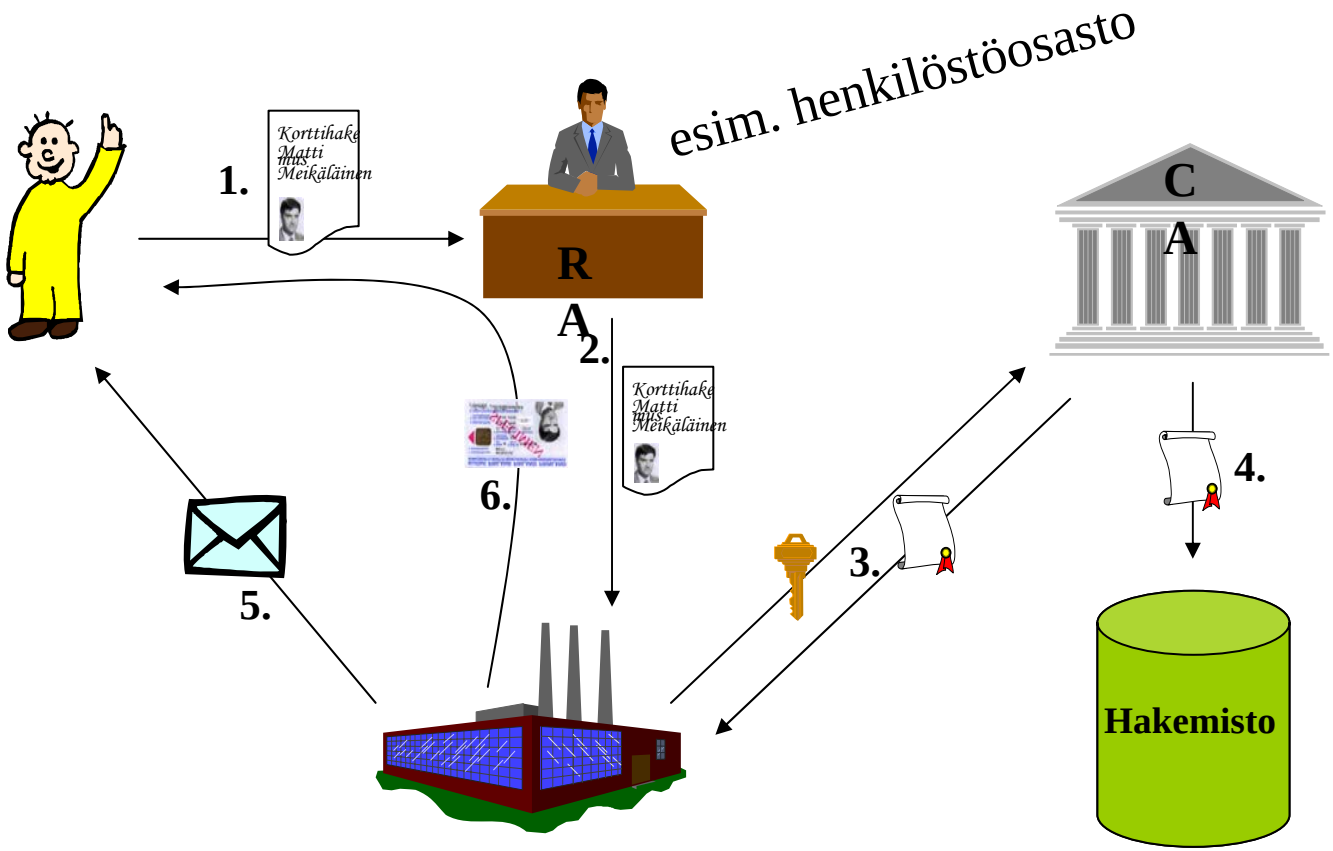


FUJITSU

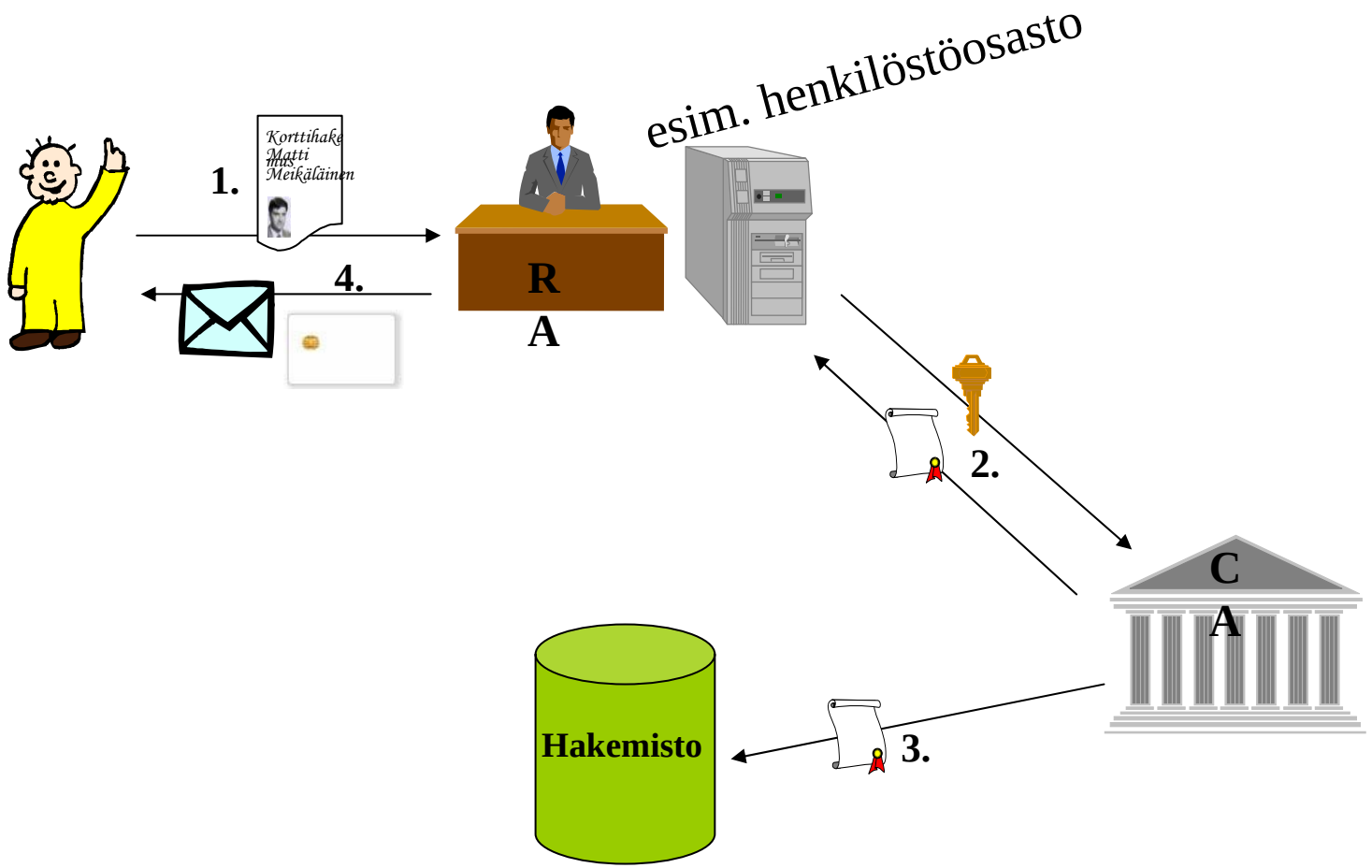
PKI tarvitsee toimivan hakemiston

- Varmenteiden julkaisu
- Sulkulistojen julkaisu
- Hakemisto on kriittinen komponentti
  - varmenteella ilman sulkulistapalvelua on hyvin vähäinen arvo

Esimerkki: Kortin hankinta vakinaiselle henkilöstölle



Esimerkki : Tilapäiskortin hankintaprosessi



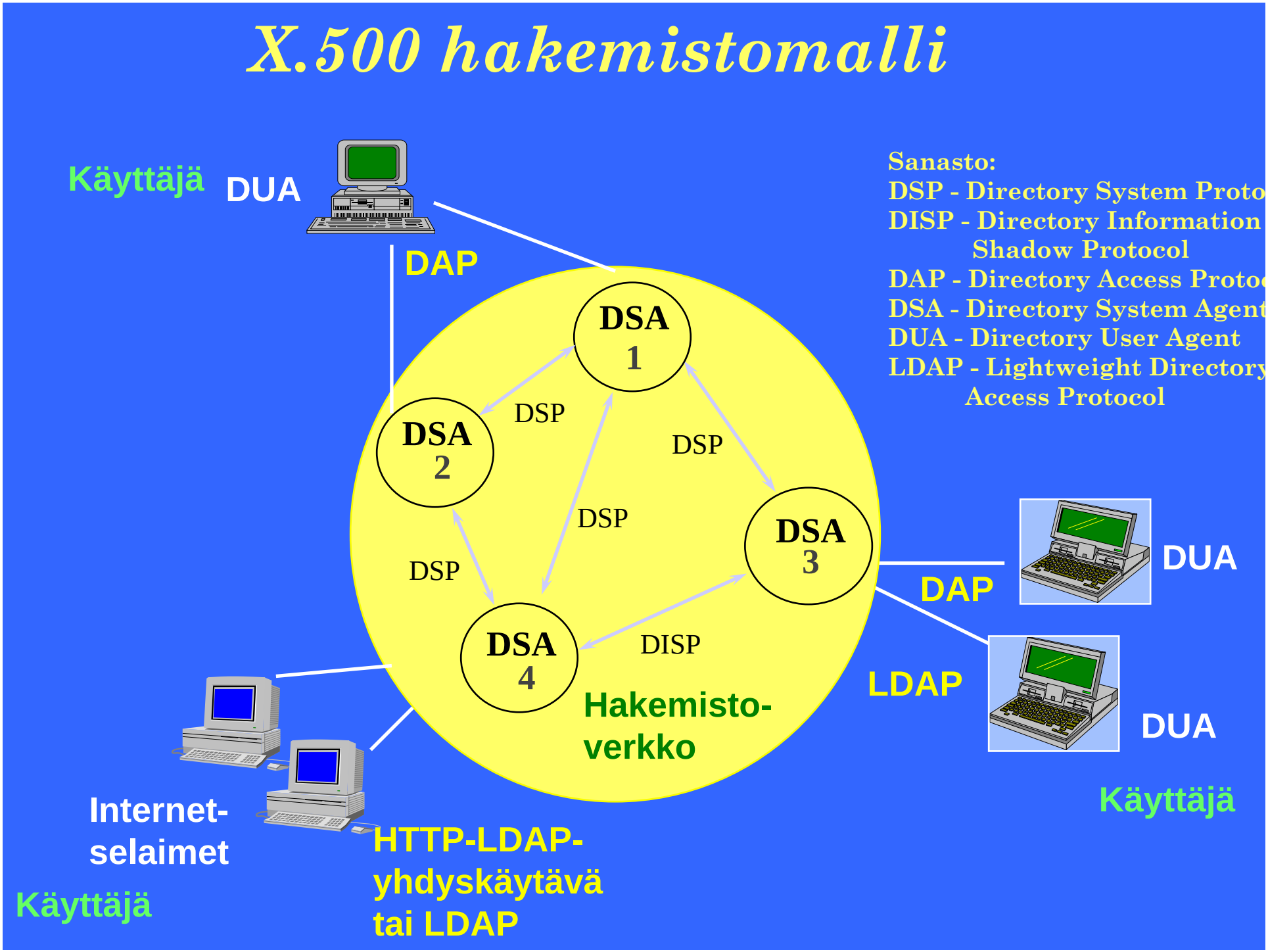
FUJITSU

Varmenteiden sijainti

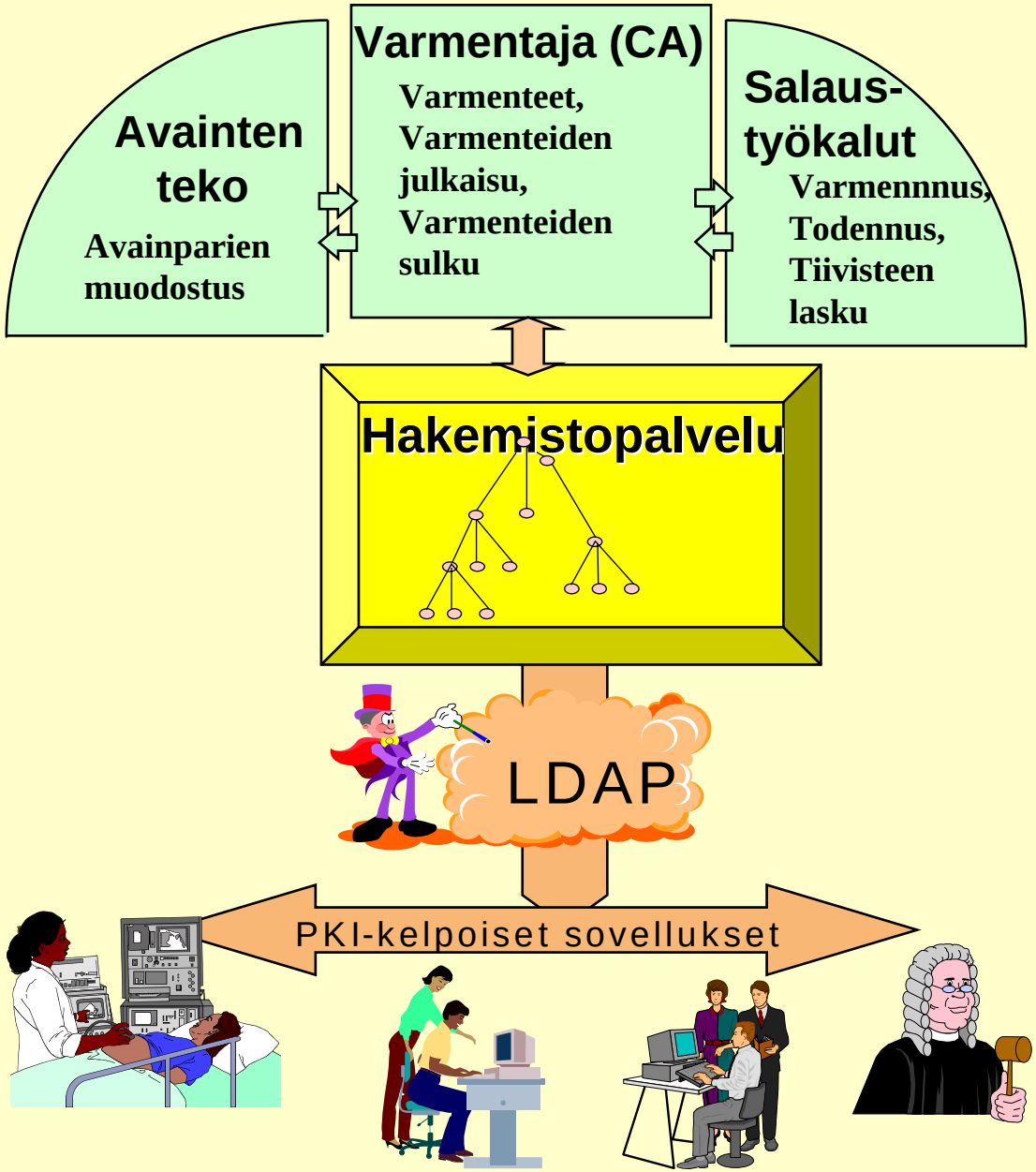
- **CA:t toimittavat varmenteet varmennehakemistoon**
  - rajoitettu schematuki CA-tuotteissa
- **Varmenteet replikoidaan enterprise-hakemiston henkilötietoihin**
  - esimerkiksi sähköpostia varten
- **Varmenteita saatetaan tarvita myös sovellushakemistoissa**
  - AD, VPN, legacy-sovellukset
- **Sulkulistojen kopiointi ei suotavaa**
  - varmenteessa viite alkuperäiseen varmennehakemistoon
  - edellyttää (lähes) on-line toimintoa

  => varmennestatuspalvelu tai validointipalvelu

X.500 hakemistomalli



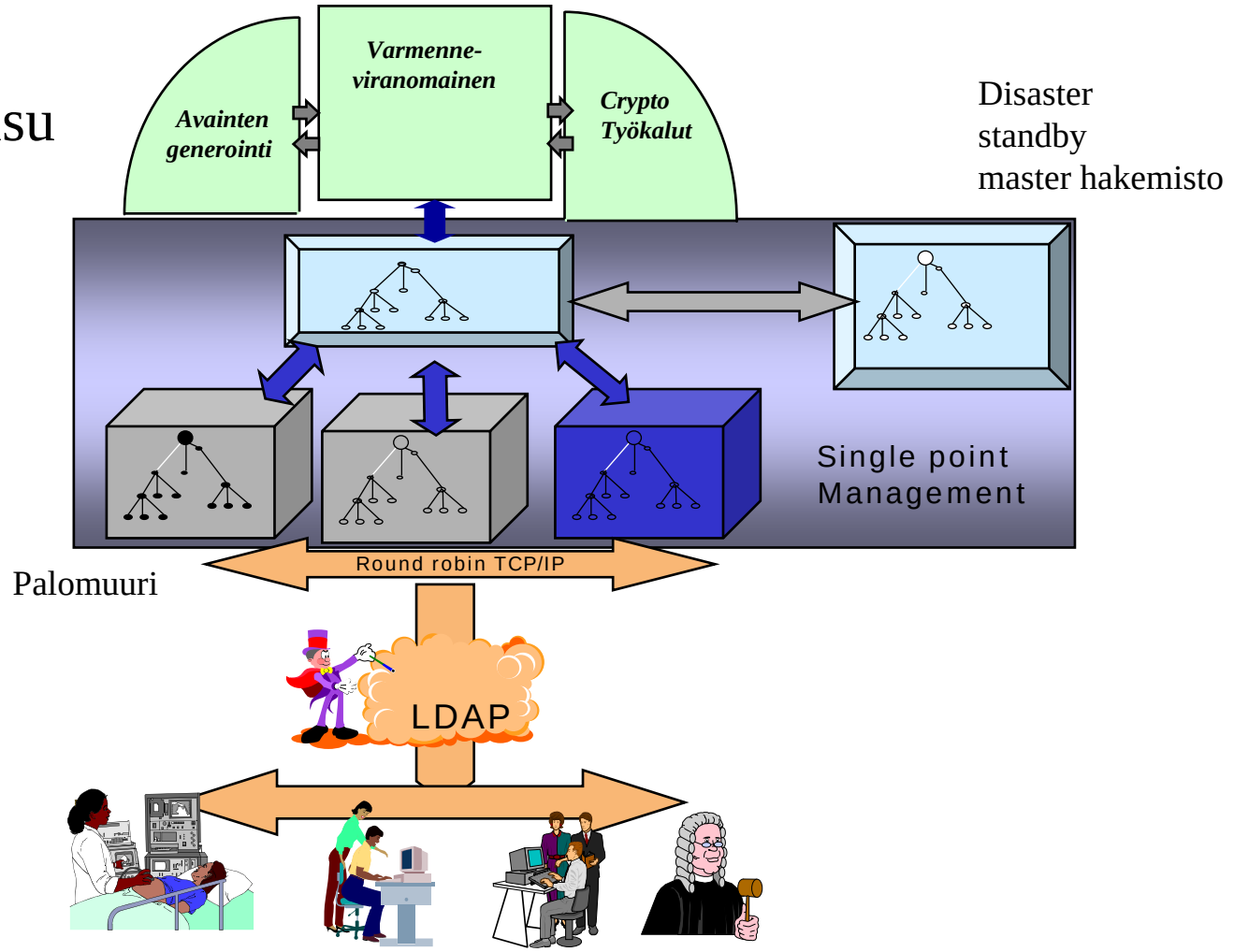
PKI-hakemisto



Korkean käytettävyyden periaate PKI/hakemistoratkaisu

Master hakemisto

Replikoidut hakemistot
hakemistojen hajautus

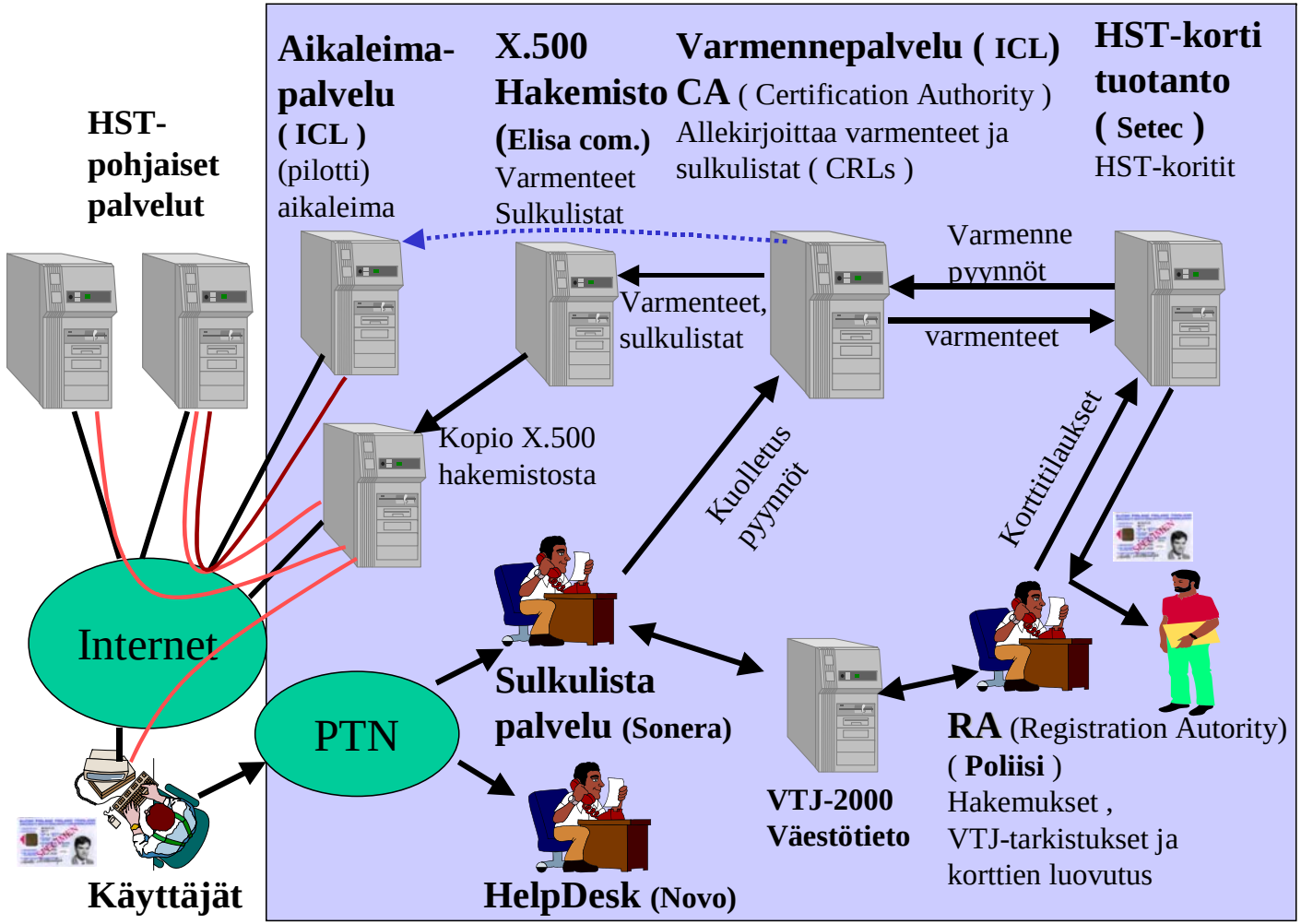


FUJITSU

Case : VRK

Suomen kansallinen HST-palvelu

Suomi : HST-PKI



Samanlainen arkkitehtuuri toimii myös teollisuusyrityksessä

FUJITSU

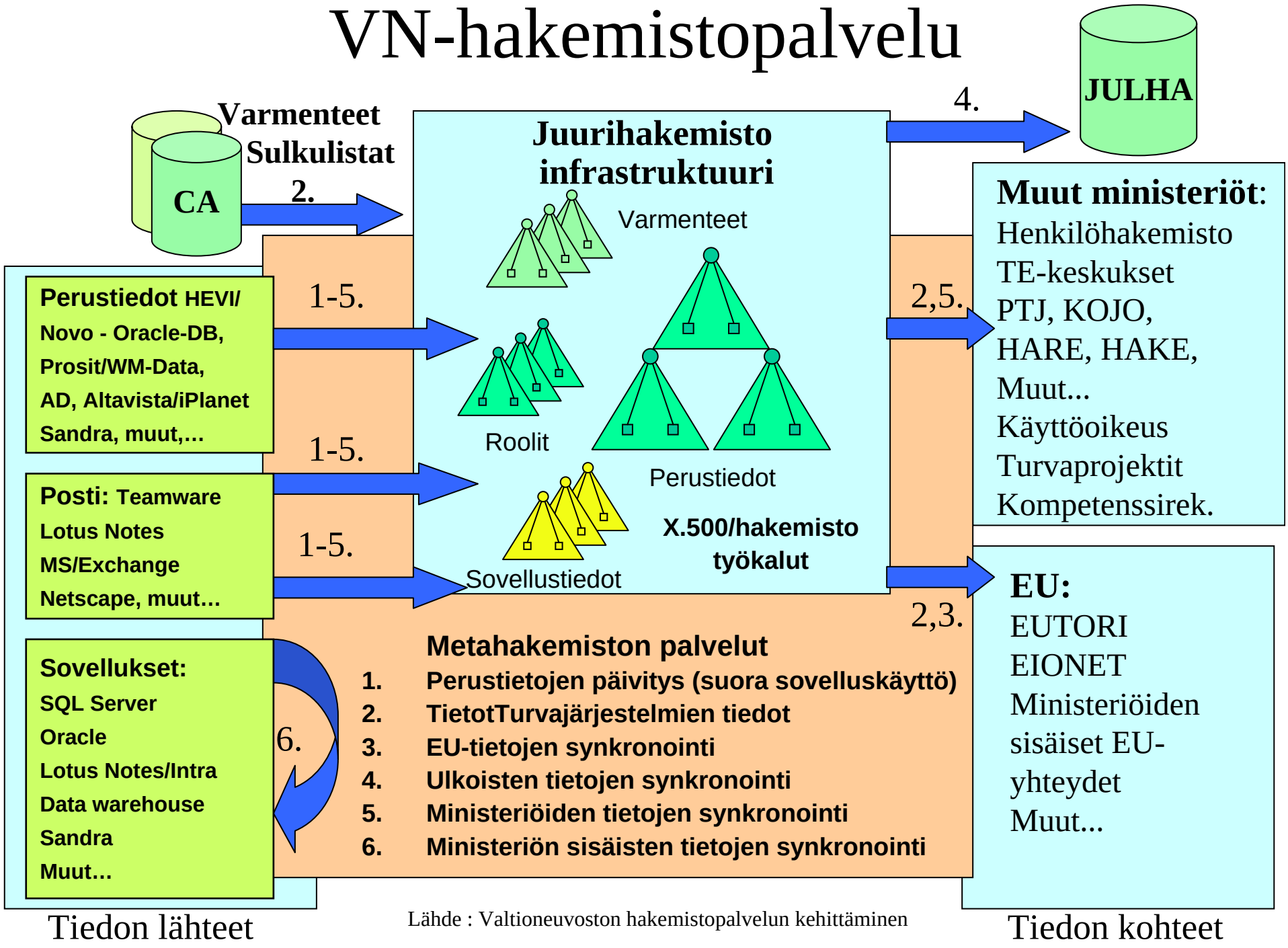
Case : Valtioneuvosto
Juurihakemiston määrittely

FUJITSU

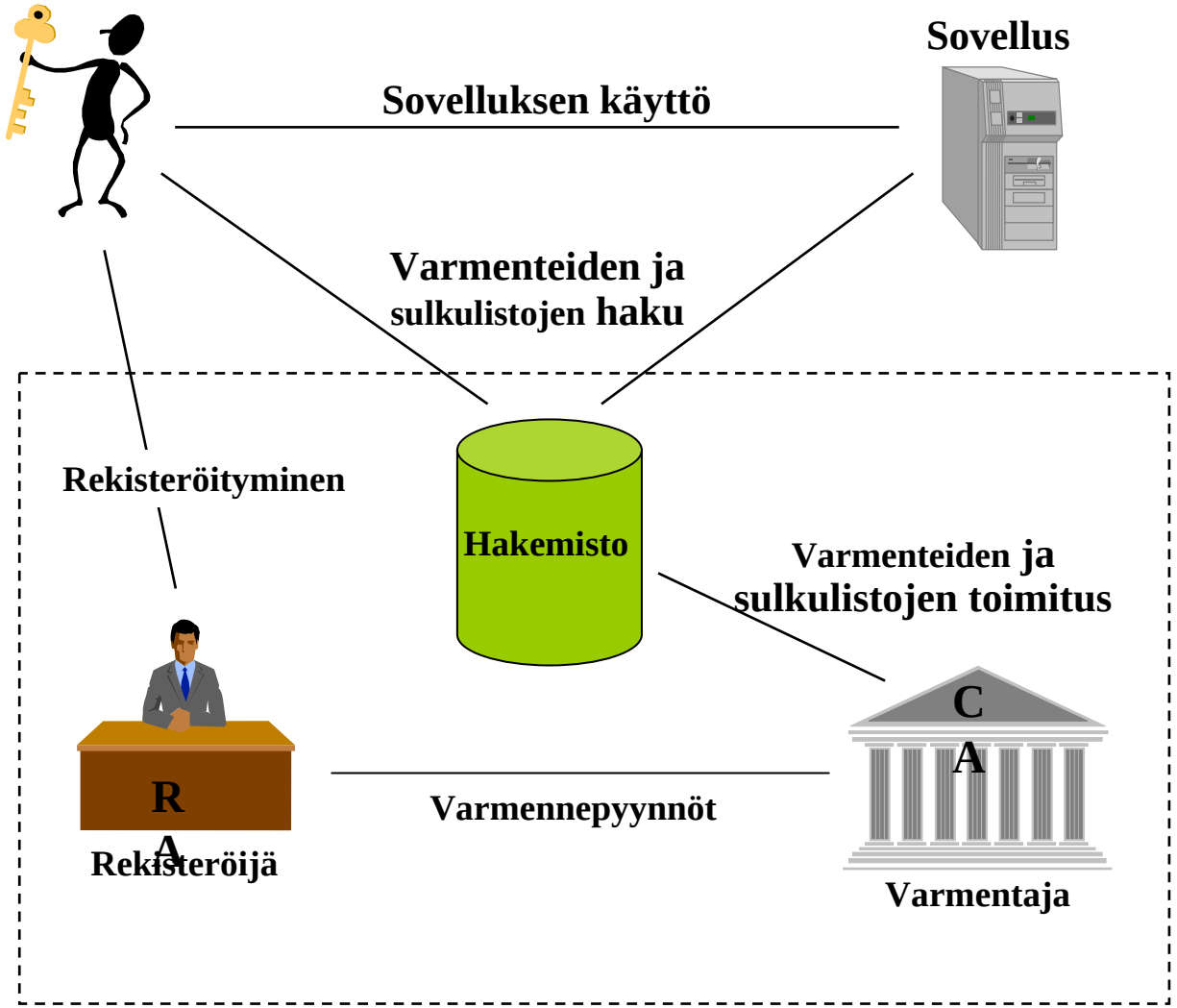
Valtioneuvoston tarve

- Valtioneuvoston yhteiset sovellukset ja palvelut tarvitsevat yhtenäisen hakemiston
- hakemistorakenteen ja ratkaisuja yhtenäistäminen
- PKI liittymä

VN-hakemistopalvelu

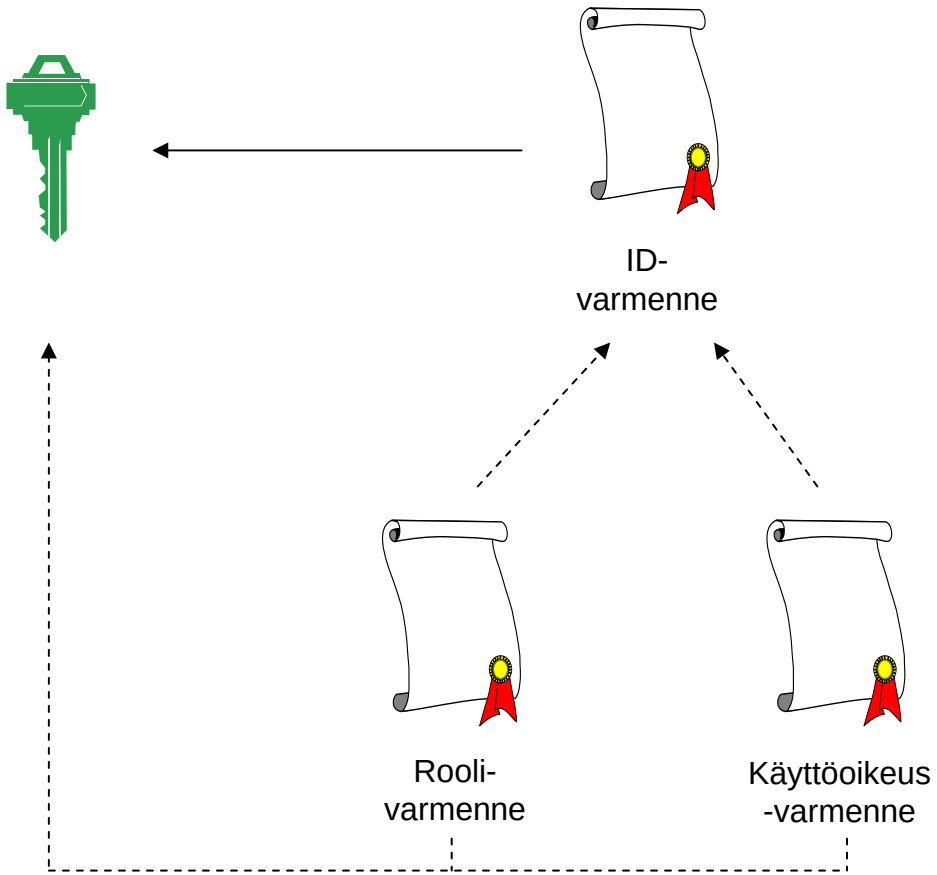


Lähde : Valtioneuvoston hakemistopalvelun kehittäminen

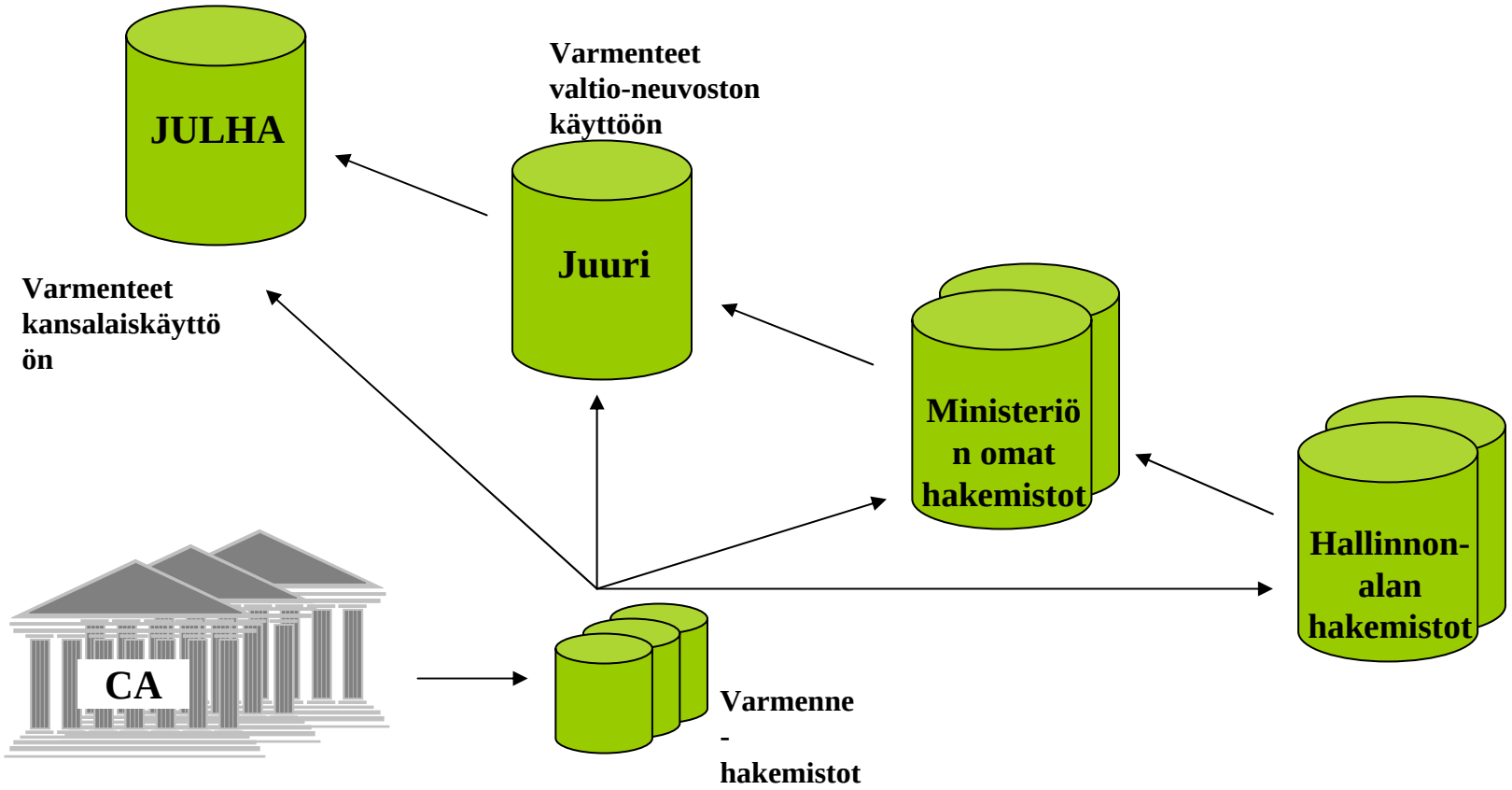

Sovellus
Sovelluksen käyttö
Varmenteiden ja
sulkulistojen haku
Rekisteröityminen
Hakemisto
Varmenteiden ja
sulkulistojen toimitus
R
A
Rekisteröijä
Varmennepyynnöt
C
A
Varmentaja

FUJITSU

Varmennehierarkia



Hakemistohierarkia



Lähde : Valtioneuvoston hakemistopalvelun kehittäminen

FUJITSU

Case : HUS

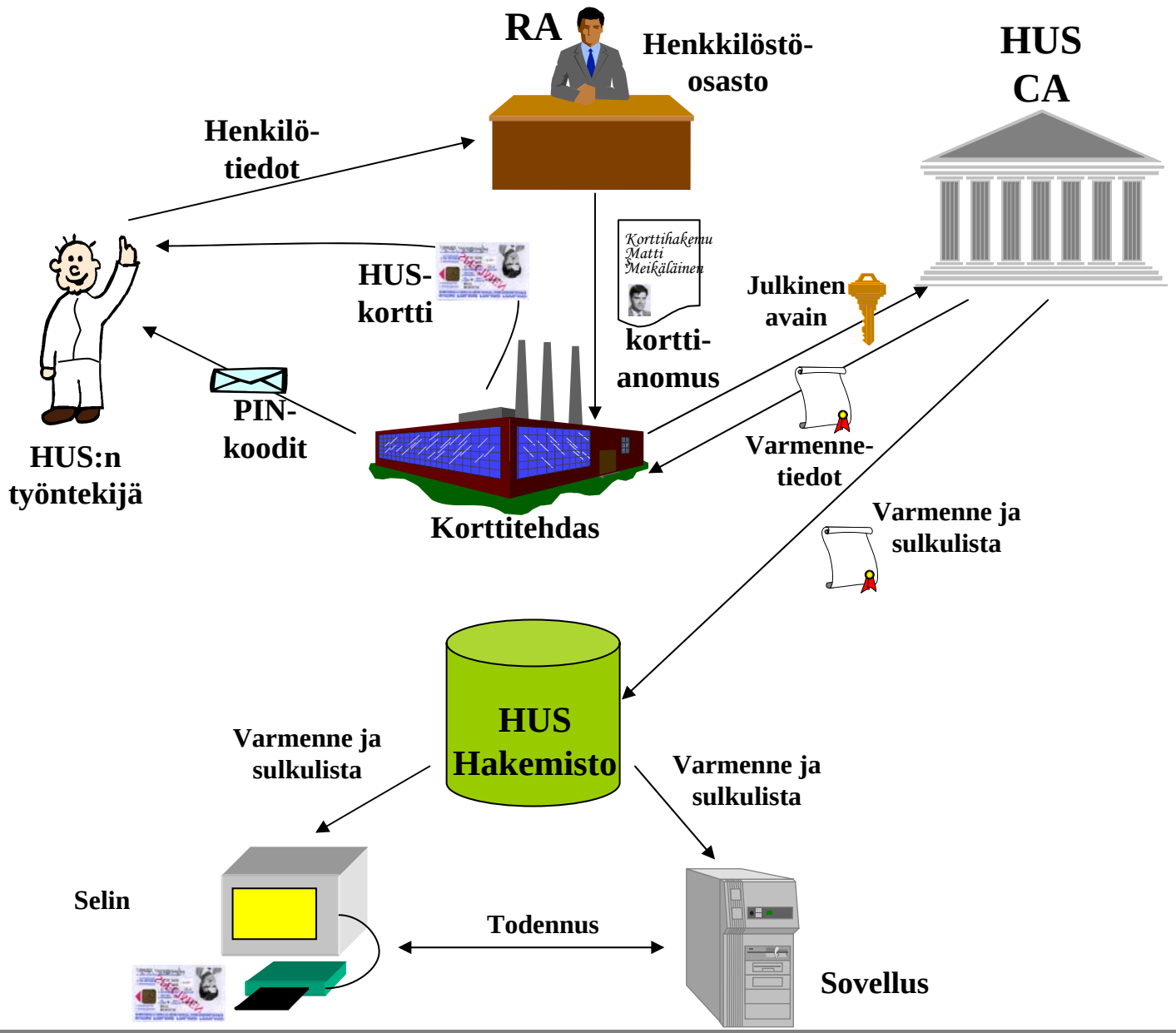
PKI- ja hakemistoarkkitehtuurin määrittely

FUJITSU

HUSin tarve

- HUS = Helsingin ja Uudenmaan sairaanhoitopiiri
- Muodostettu 1.1.2000

- Tarve :
  - yhtenäinen PKI-arkkitehtuuri, johon uudet sovellukset voi istuttaa
  - tuottaa valmiuksia sähköiseen asiointiin ja vahvaan todentamiseen
  - hankkia HUSille tietämystä PKI- ja hakemistoteknologioista



FUJITSU

Case : STAKES

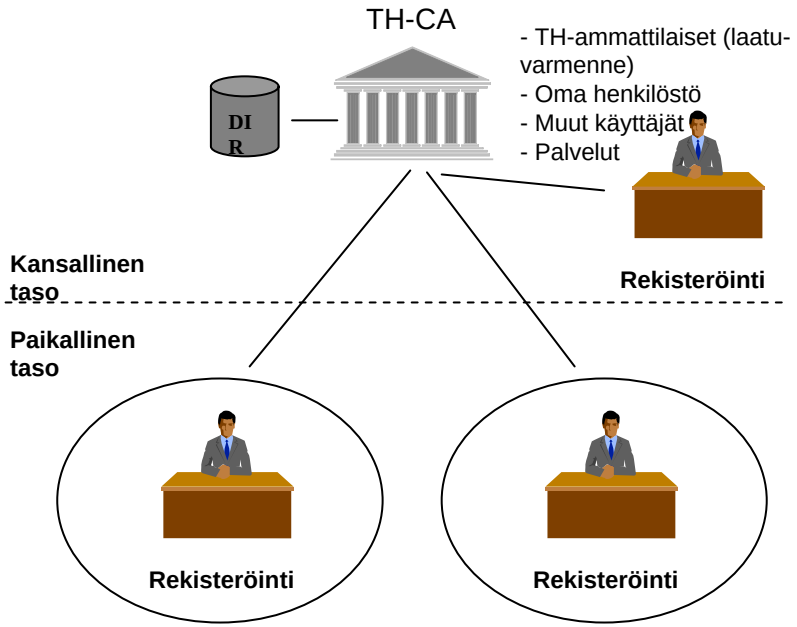
Terveydenhuollon PKI-arkkitehtuuri

FUJITSU

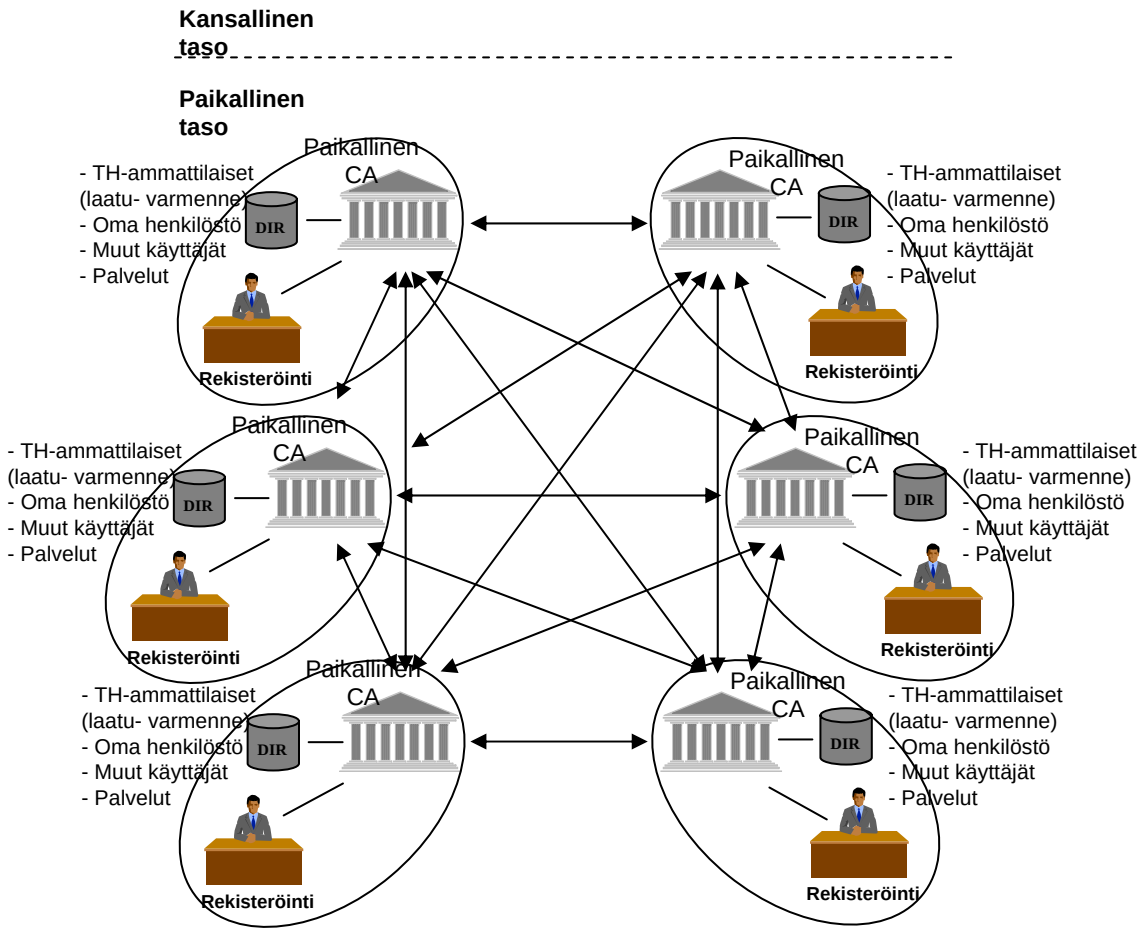
STAKESin tarve

- Tarve :
  - luoda malleja terveydenhuollon PKI-arkkítehtuureille
  - varmennepolitiikan perusvaatimusten kuvaaminen

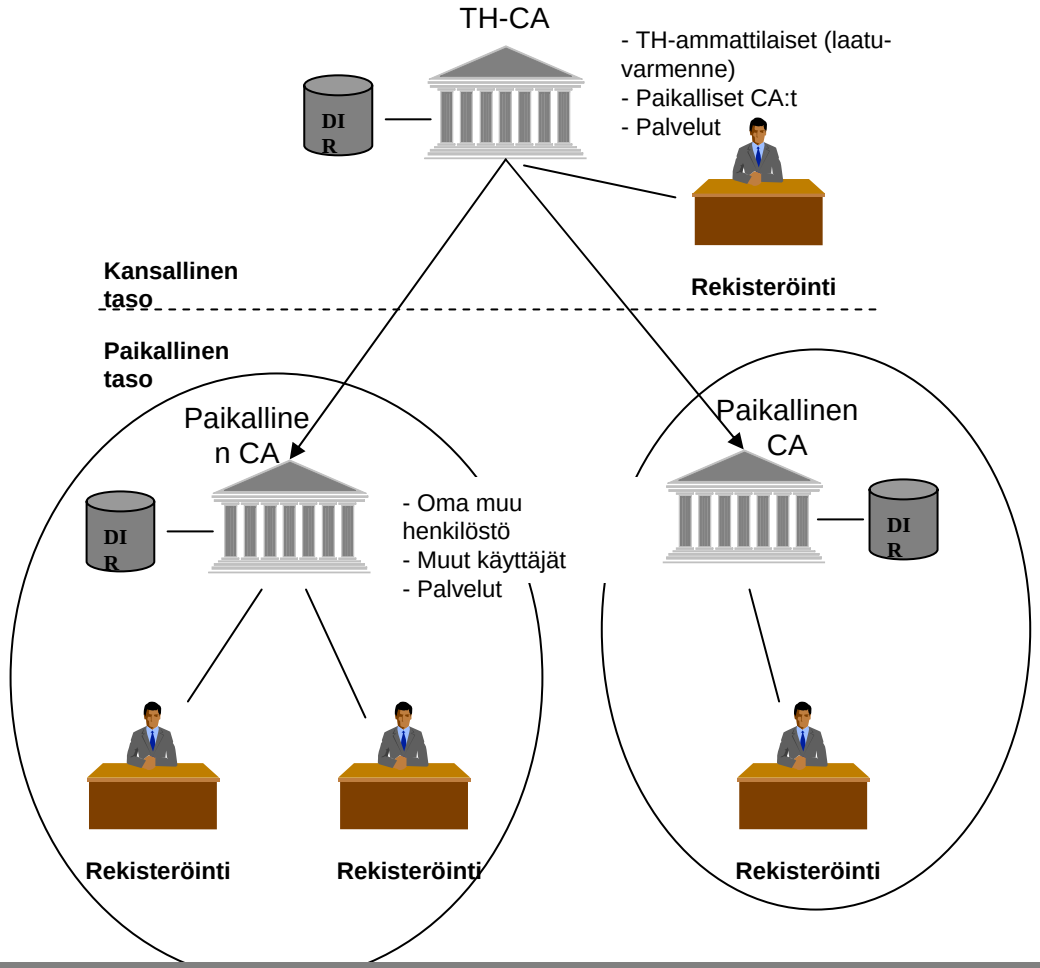
TH:n PKI - keskitetty



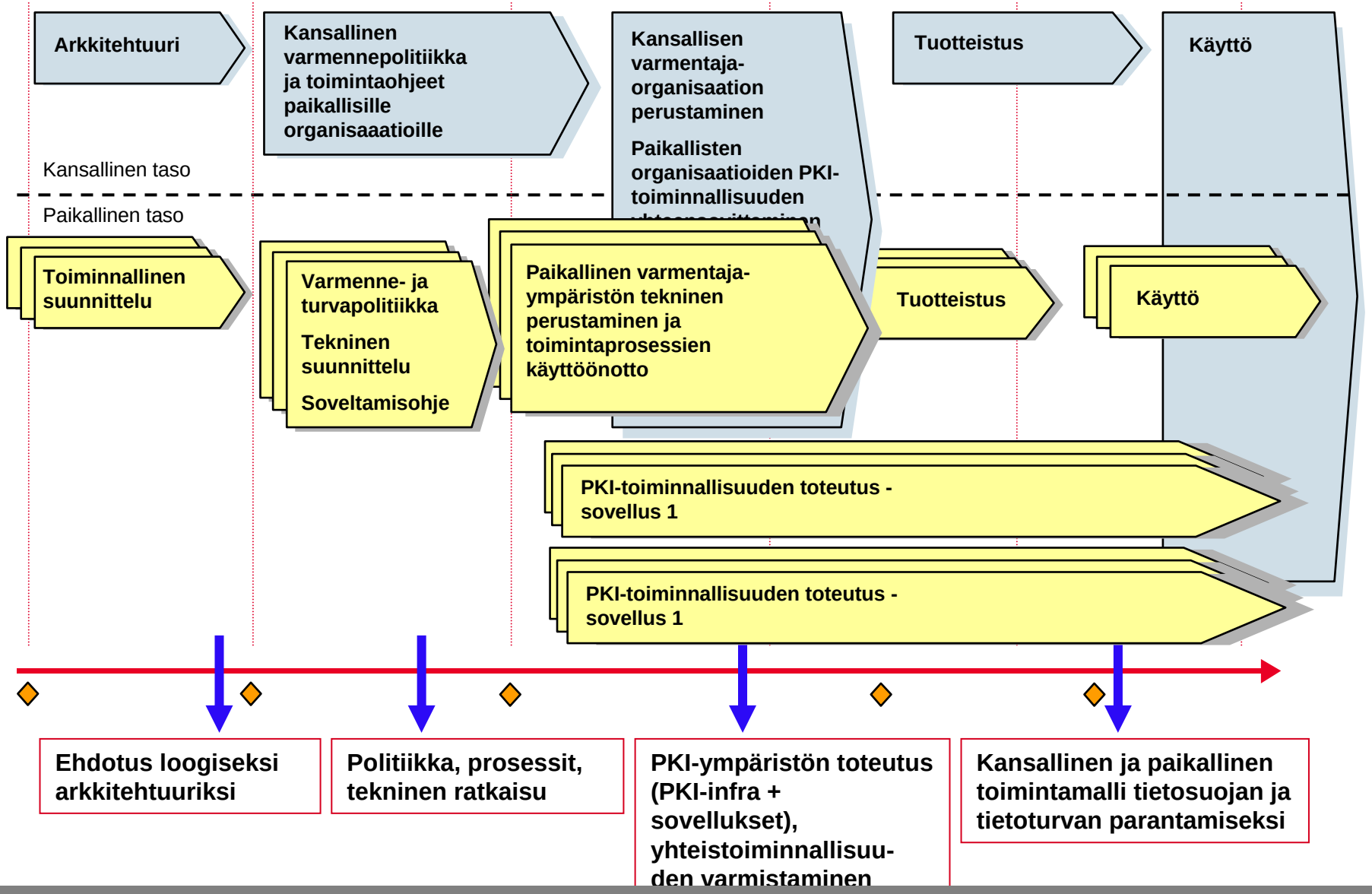
TH:n PKI - hajautus



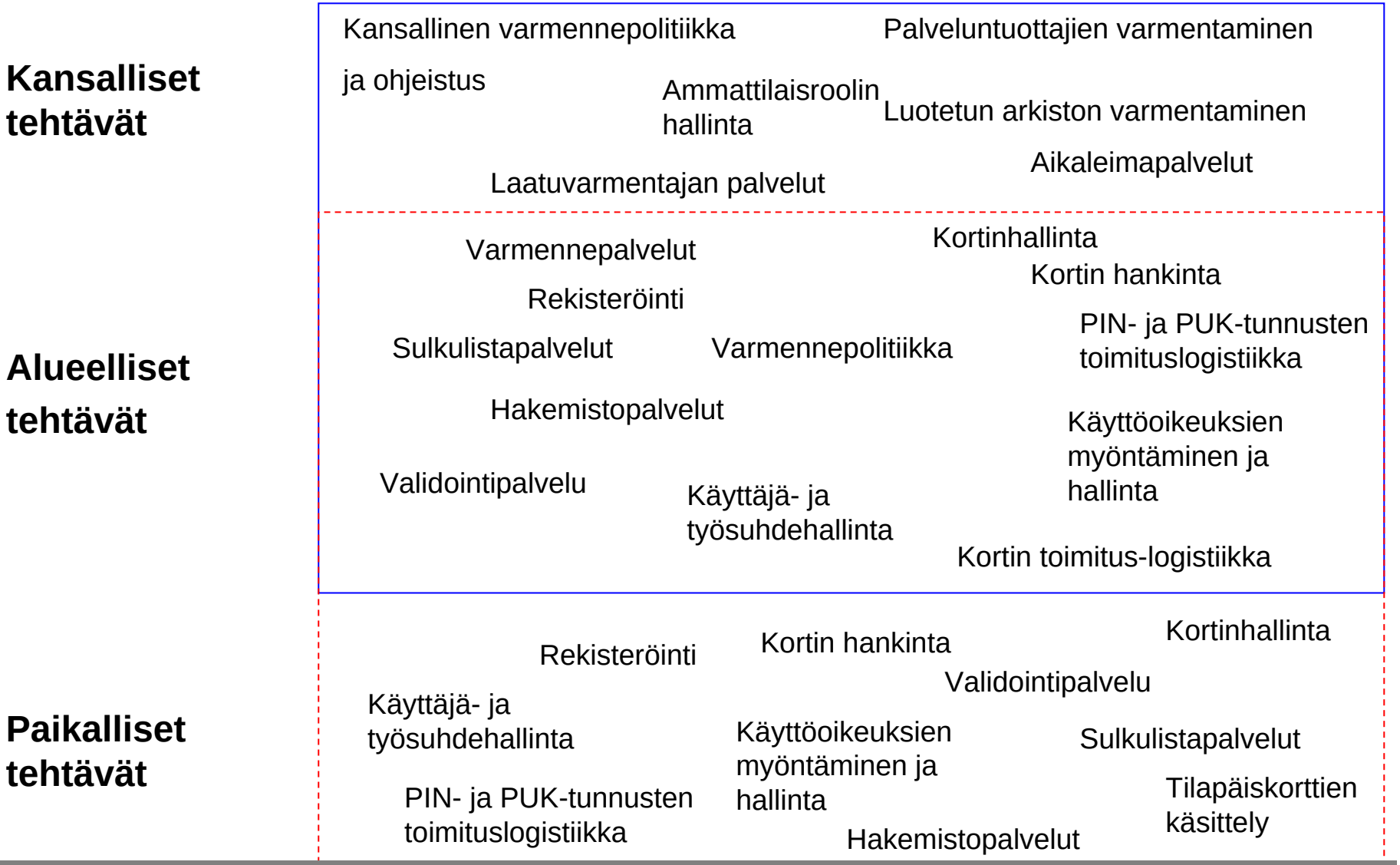
TH:n PKI – osin keskitetty



Terveydenhuollon valtakunnallisen PKI-arkkitehtuurin kehittäminen



Paikalliset, alueelliset ja valta-kunnalliset tehtävät, suositus:



FUJITSU

PKI:n käyttöönotossa muistettavaa

- **Vain riittävä PKI-kelpoinen sovellusmassa takaa onnistumisen**
- **Etene portaittain (sovellukset ja infra käsikädessä)**
  - Määritä toimiva kokonaisuus
  - Toteuta osittain ja testaa
  - Tarkista määritykset
  - Toteuta kokonaisuus
- **Muuta organisaation toimintaprosesseja tarvittaessa yhtä aikaa PKI-projektin kanssa**
  - Vireillepano/käsittely/päätös sähköisesti
- **Yhteistyö sidosryhmien kanssa**
  - Varmennepolitiikka, allekirjoitusten validointipolitiikka, …
  - Pyrittävä välttämään PKI-saarekkeita