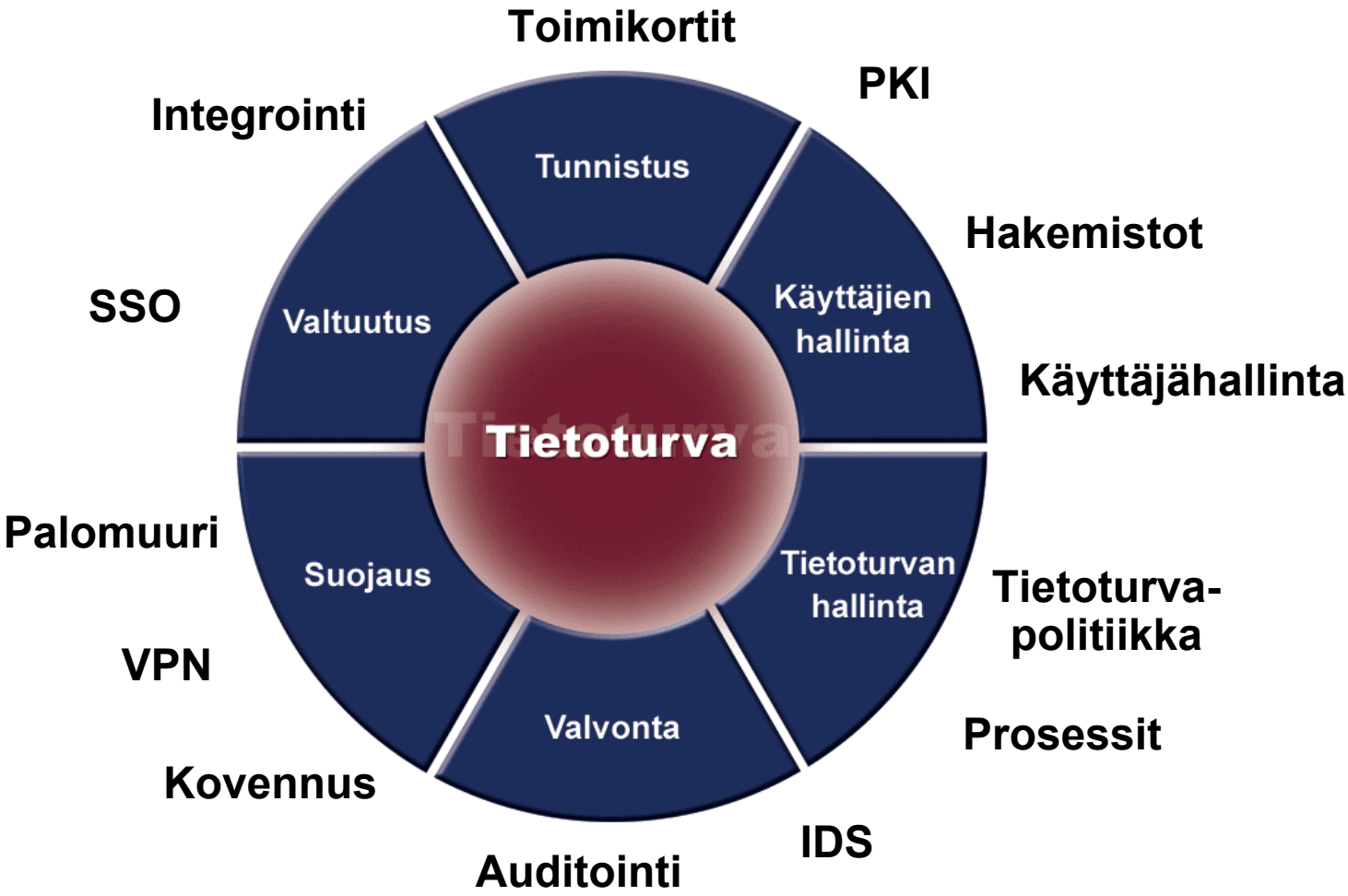
Miten PKI-projekti onnistuu?

AtBusiness Tietoturvatorstai
6.3.2003

Jari.Pirhonen@atbusiness.com
Senior Consultant, CISSP, CISA
AtBusiness Communications Oyj
www.atbusiness.com

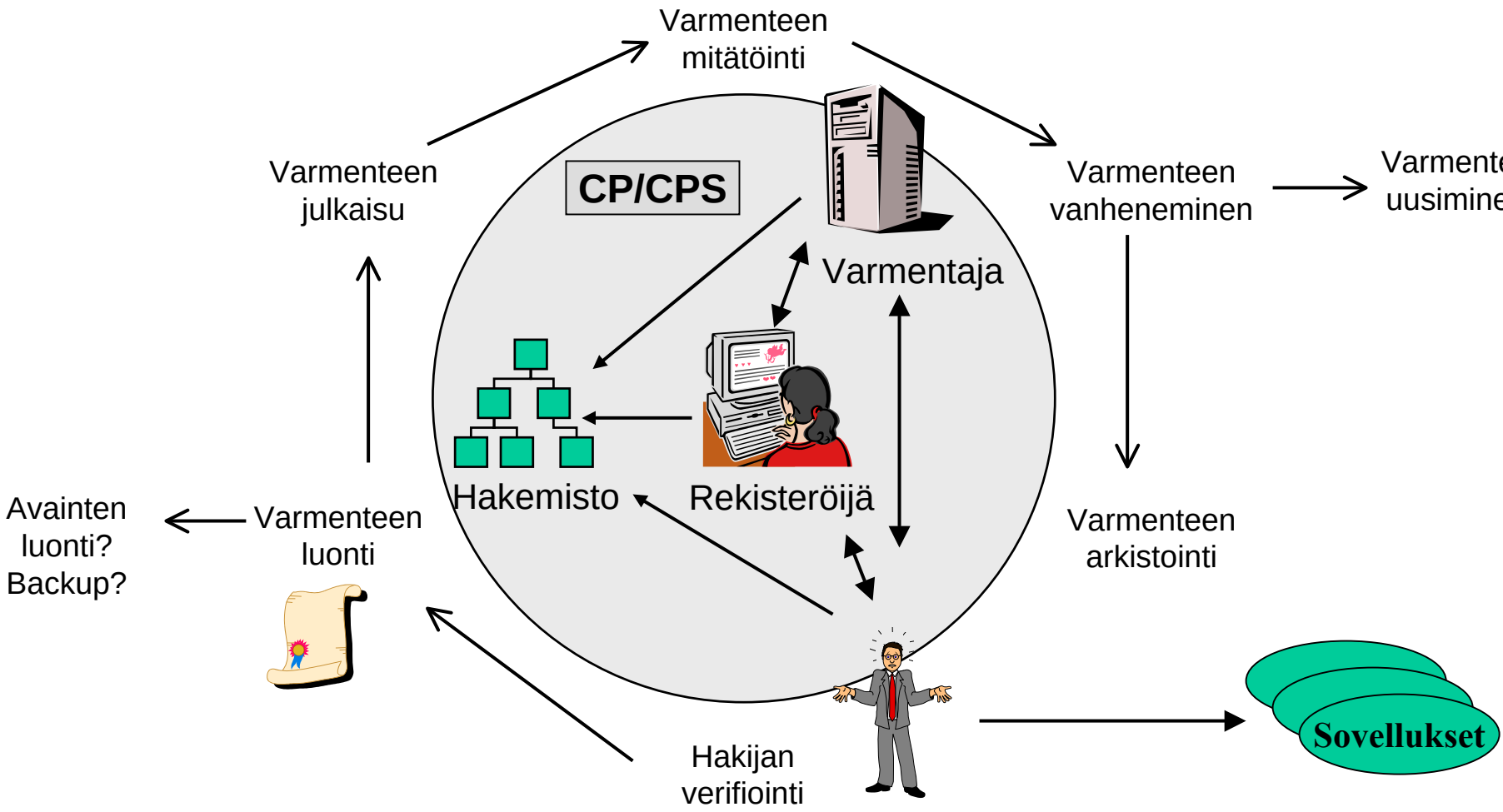
AtBusiness ja tietoturva



AtBusiness ja PKI

- Ensimmäinen PKI-projekti 1997
- Referenssejä: *Certall, TIEKE, Radiolinja*
- Lisäksi isojen yritysten sisäisiä PKI-järjestelmiä mm. finanssi- ja tele-alalta
  - Kokonaisprojektit
  - Konsultointi
    - Toimintaprosessit: varmenteen haku, myöntö, mitätöinti,…
    - CP/CPS, varmenneprofiilit, CA luontiseremonia,…
    - PKI-sovellukset: sähköposti, VPN, Web, tunnistus,…
    - Toimikortit
  - Sovelluskehitys
    - Räätälöidyt RA-sovellukset
    - PKI:n hyödyntäminen sovelluksissa
  - Hakemistot
  - Wireless/Mobile PKI
- Projekteissa käytetty kaikkia tärkeimpiä PKI- ja hakemistotuotteita
- Yli 1500 htp:n kokemus PKI-projekteista

PKI – julkisen avaimen järjestelmä

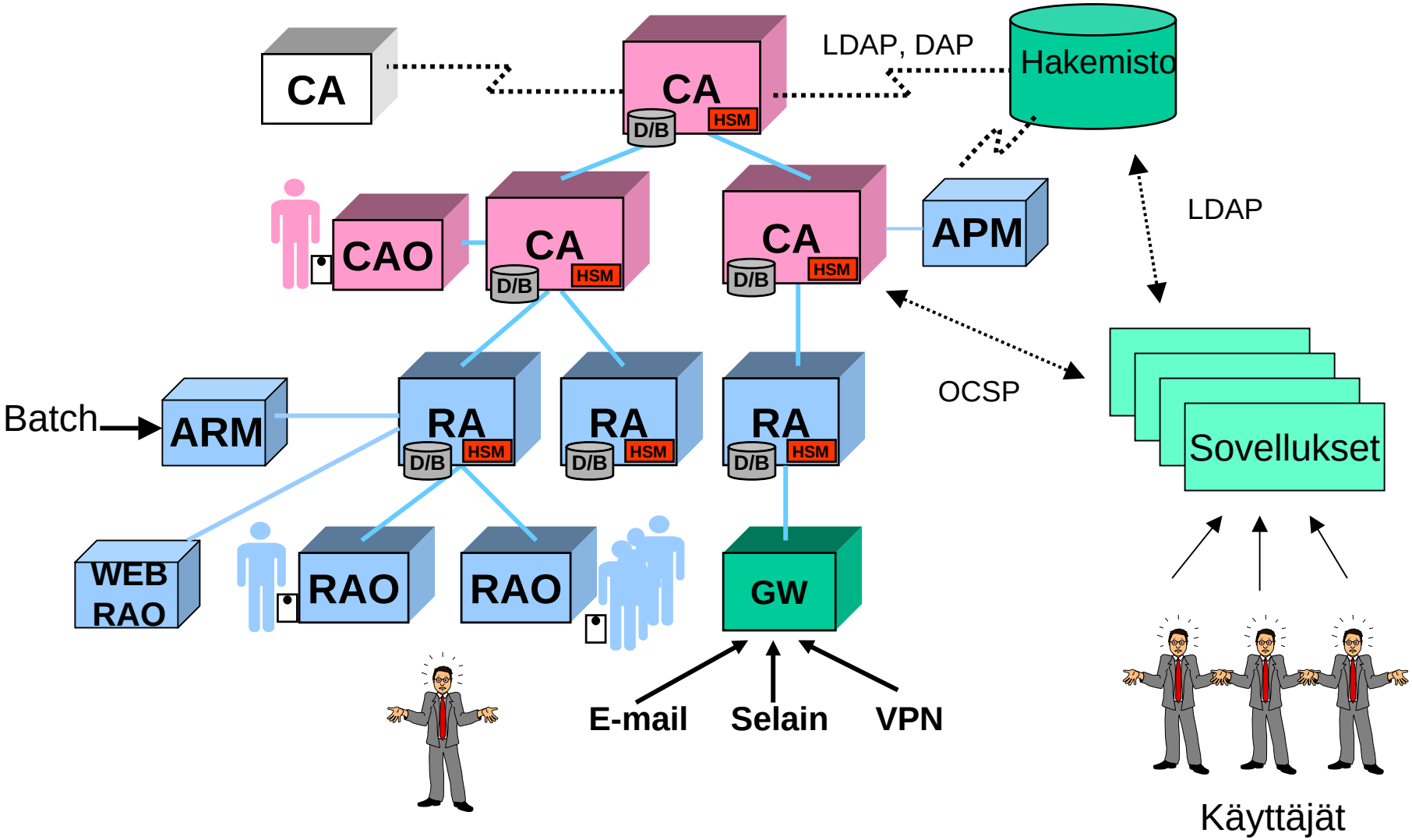


Mihin PKI tarvitaan?

- SSL
- VPN
- Sähköposti
- Vahva käyttäjätunnistus
- Sähköinen allekirjoitus
- Dokumenttien ja tapahtumien luotetut aikaleimat
- Windows
- XML
- Web Services

Turvallisuutta ja luotettavuutta vaaditaan - mikä on vaihtoehto PKI:lle?

Ympäristö voi olla monimutkainen

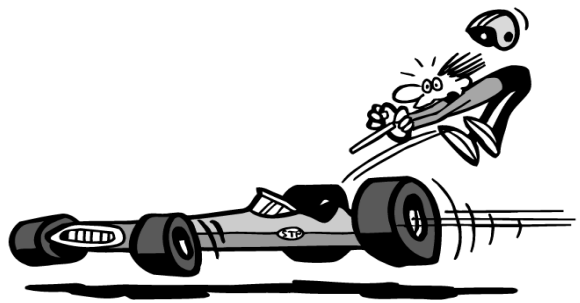


Huomioita

- Varmenteiden luominen on helppoa
- Varmenteiden luotettava myöntäminen on vaikeampaa
- Todistettavasti luotettavan ympäristön rakentaminen on työlästä
- Aiemmat käytännöt ja turvajärjestelyt eivät todennäköisesti riitä PKI:n tarpeisiin
- Hakemisto on PKI:n kriittisin käytönaikainen komponentti ja sen rakentaminen on oma haasteensa
- Varmenteiden jakelun taustalla olevien käytäntöjen ja turvajärjestelyiden tärkeyttä ei huomata ajoissa
- Tuotetoimittajan käsitys PKI-käytöstä voi erota sinun käsityksestäsi
- Sovelluksilla voi olla ”erikoinen” näkemys PKI ja hakemistokäytöstä
- Normaali projektikesto ½ - 2 vuotta

PKI-projektin erityishaasteita

- Toimintamallit
- Asenteet (suunnittelu, asennukset, ylläpito,…)
- PKI:n integrointi nykyisiin prosesseihin ja sovelluksiin
- PKI-sovelluskehitys
- Yleinen turvatason nosto
- Dokumentaatio
- Laatuvarmenteet, lainsäädäntö
- Yleiskäyttöinen vai sovelluskohtainen ratkaisu!
- Standardi-clientit vai erityinen PKI-client?
- Yksi vai useampia varmenteita?
- Windows-integrointi
- Asiakas- ja kumppani-integraatio



Oma vai ulkoistettu PKI?

	Oma varmentaja	Palvelu, oma varmentaja	Palvelu, omat varmenteet	Palvelu, yleiset varmenteet
Luottamus	Omassa hallinnassa	Mahdollisesti siirrettävissä	Palveluntarjoajaan	Palveluntarjoajaan
Käyttöönotto	Työläs	Vähemmän työläs	Helpompi	Helpoin
Toimintatavat	Omassa kontrollissa	Kohtuullinen kontrolli	Toimintamalli annettuna	Toimintamalli annettuna
Tietoturvallisuus	Omalla vastuulla	Palveluna, räätälöitävissä	Palveluna	Palveluna
Omat resurssit	Paljon	Melko paljon	Vähän	Vähiten
Ylläpito	Työläs	Palveluna, myös omia rutiineja	Palveluna	Palveluna
Varmennesisältö	Omassa kontrollissa	Voi vaikuttaa	Voi mahdollisesti vaikuttaa	Annettuna
Käyttötavat	Omassa kontrollissa	Voi vaikuttaa	Rajoitettu	Rajoitettu
Oma brändi	OK	OK	Ei	Ei
Joustavuus	Paras	Kohtalainen	Huono	Ei

Vinkkejä

- Etene askel kerrallaan, kerää tietämystä ja kokemuksia
- Aloita helpoista PKI-sovelluksista: email, VPN, SSL,…
- Varmista palvelutoimittajien osaamistaso ja resurssit
- Huomioi sopimuksissa PKI:n erityistarpeet
- Projektit ovat haasteellisia, halvalla ja hätäilemällä ei saa aikaan hyvää ratkaisua
- Muista, että PKI-projekti on infrastruktuuri- ja turvaprojekti
- Selvitä, miten tuote- tai palvelutoimittaja olettaa varmenteen elinkaareen liittyvien käytäntöjen toimivan

PKI projekti onnistuu, kun…

- Ymmärrät PKI:n mahdollisuudet ja rajoitukset
- Tiedät varmasti, miksi PKI:a tarvitset
- Projektihenkilöillä on PKI-taustaa tai heille varataan 3-6 kk aikaa PKI:n opiskeluun
- Tiedossa on *realistiset* työmääräarviot ja kustannukset
- Projektin takana on yritysjohdon tuki ja tarvittavat resurssit
- Projektipäällikkö on kokenut
- Tehdään hyvä tarvemäärittely ennen tuotteen valintaa
- Tiedostetaan, että PKI-käyttöönotto vaatii todennäköisesti muutoksia toimintatapoihin eri puolilla organisaatiota
- Tärkeimmät toimintaprosessit on ainakin alustavasti mietitty ennen tuotevalintaa
- PKI:n sisäiseen ”myyntityöhön” ja koulutukseen panostetaan