PKI – vaikeuksien kautta voittoon?

Data Security 2001, Tieturi
9.10.2001
Jari.Pirhonen@atbusiness.com
Senior Security Consultant, CISSP
AtBusiness Communications Oyj
www.atbusiness.com

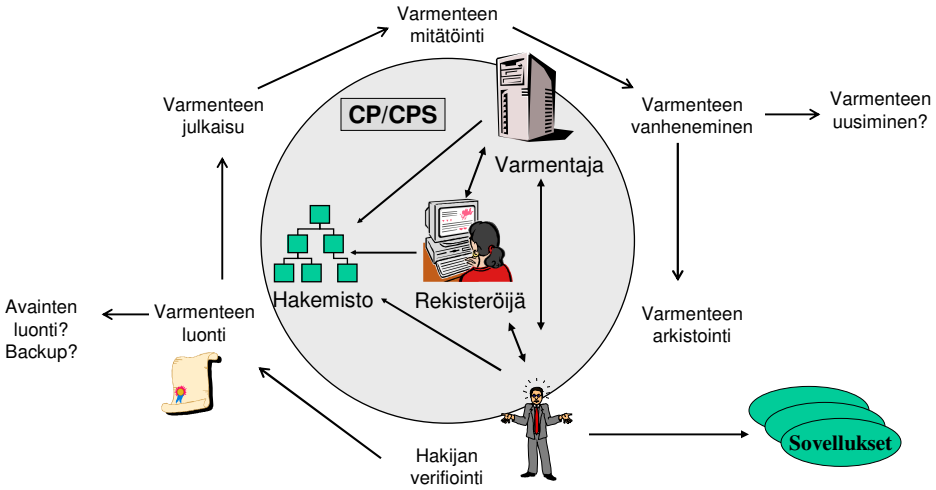
PKI AtBusiness

- Ensimmäinen PKI-projekti 1997
- PKI-asiakkaita: isot yritykset, pankit, teleoperaattorit, varmennepalvelun tarjoajat
- Certall, TIEKE
- Osaaminen
  - Kokonaisprojektit
  - Konsultointi
  - CP/CPS
  - Sovelluskehitys
  - Mobile PKI
  - RSA, Baltimore, iPlanet, W2K
  - Hakemistot

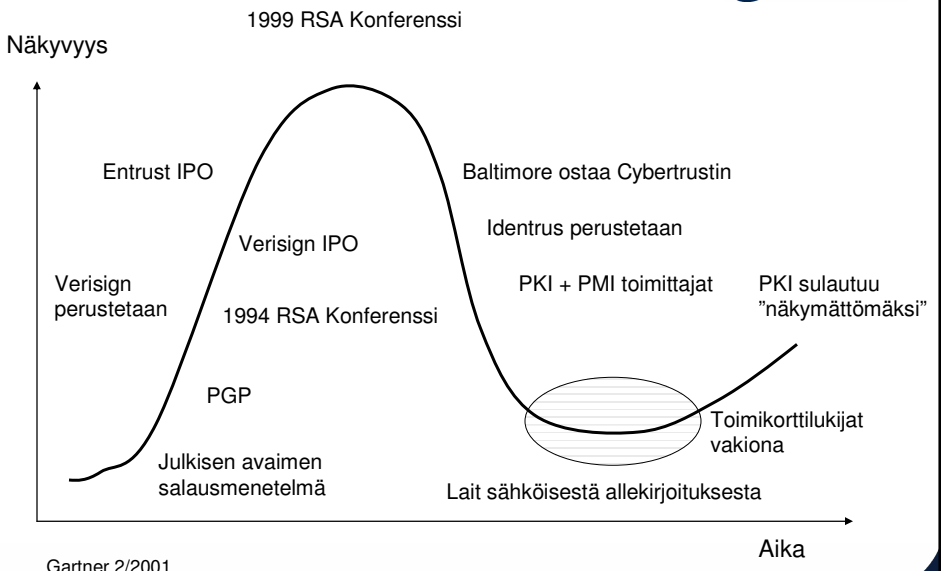
Termit hallussa?

- Varmentaja (CA)
  - (1) ohjelmisto
  - (2) ohjelmisto, laitteet, tilat, henkilöresurssit, toimintatavat,…
- Luotettu kolmas osapuoli (TTP)
  - varmennepalvelu, joka toimii laadukkaasti ja luotettavasti
- Varmenneviranomainen
  - varmentaja viranomaisstatuksella
- Rekisteröijä (RA)
  - (1) ohjelmisto
  - (2) taho, joka todentaa hakijan ja hakemuksen oikeellisuuden
- Varmennepolitiikka (CP)
  - dokumentti, joka kuvaa varmenteet ja sallitut käyttötavat
- Varmennekäytäntölausuma (CPS)
  - dokumentti, joka kuvaa varmentajan toimintaa, luotettavuutta ja vastuita

PKI – julkisen avaimen järjestelmä

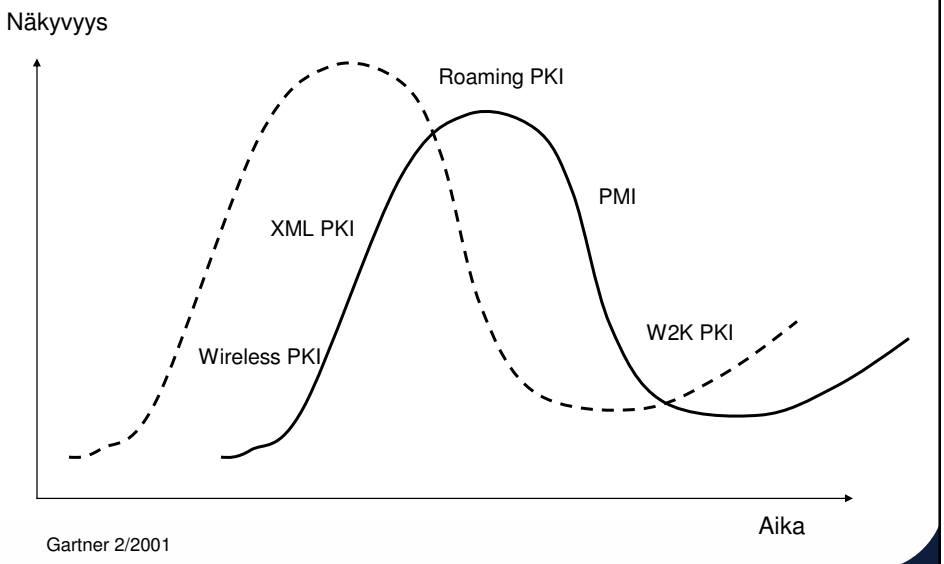


Hype?



Gartner 2/2001

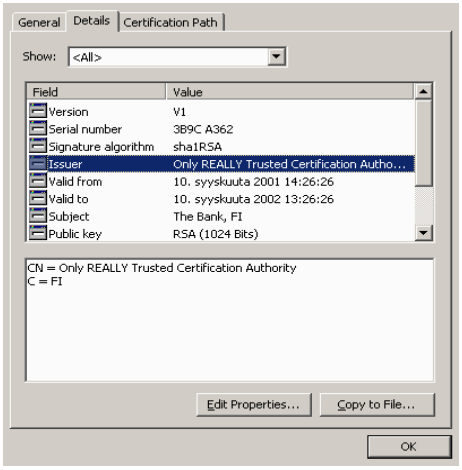
Seuraava hype-aalto?

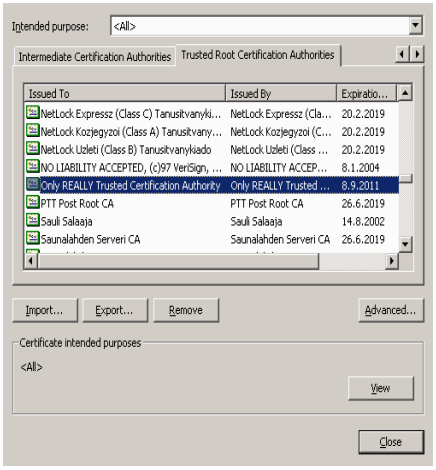


Gartner 2/2001

Halvalla ja nopeasti?

atbusiness



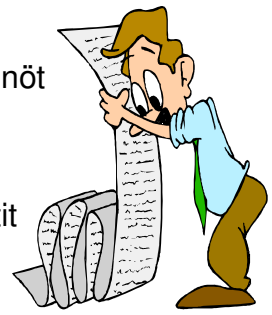


Järkevästi ja turvallisesti?

atbusiness

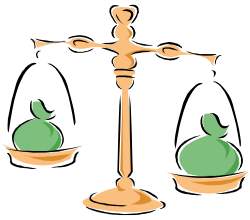
DOKUMENTOINTI

- Vaatimukset: sovellukset, käyttäjät, tietoturva, lait, toipuminen, vastuuhenkilöt, varmenteiden elinkaari,…
- Laitetilat, kassakaapit, turvamoduulit, palomuurit, IDS,…
- Käyttöpolitiikat ja toimintatavat
- Varmenneprofiilit
- Varmennepolitiikat ja varmennuskäytännöt
- Tietoturvapolitiikat ja toimintatavat
- Vastuiden eriyttäminen
- Asennussuunnittelu, asennusdokumentit
- Ylläpito, valvonta, arkistointi
- Muutosten hallinta ja valvonta
- Auditointi



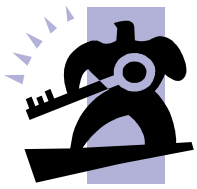
Varmenteet yritykselle

1. Oma varmentaja
2. Oma varmentaja palveluna
3. Kaupallinen varmentaja, omat varmenteet
4. Luotetaan yleisesti käytössä oleviin varmenteisiin



Oma varmentaja

- Työläin
- Toimintatavat suunniteltavissa vapaasti, mahdollisuus integroida olemassa oleviin prosesseihin
- Tietoturvallisuus omassa kontrollissa
- Vaatii omia henkilöresursseja
- Laitetilojen erikoisjärjestelyt
- Ylläpidon erikoisjärjestelyt
- Koulutus
- Oma brändi
- Laajentaminen helppoa

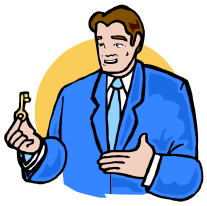


Oma varmentaja palveluna

- Vähemmän työläs
- Nopeampi käyttöönotto
- Kohtuullinen kontrolli toimintatapoihin
- Oma brändi
- Vähemmän omia henkilöresursseja
- Luottosuhde palveluntarjoajaan
- Tilat ja ylläpito palveluna
- Sopimukset monimutkaisia
- Palvelujen laajentaminen työläämpää
- Varmentajan siirtäminen omaan hallintaan myöhemmin voi olla mahdotonta

Kaupallinen varmentaja

- Helppo
- Melko nopea käyttöönotto
- Toimintamalli annettuna
- Ei omaa brändiä
- Ei omia tiloja, resursseja
- Mahdollisuus vaikuttaa varmenteen sisältöön?
- Sopimukset yksinkertaisempia
- Luottosuhde palvelutarjoajaan
- Palvelujen laajentaminen hankalaa
- Varmentajan siirtäminen omaan hallintaan myöhemmin mahdotonta



Luotetaan “yleisiin” varmenteisiin

- Nopea käyttöönotto
- Toimintamalli annettuna
- Ei omaa brändiä
- Yleinen varmenne => luottosuhde määriteltävä muualla
- Ei omia resursseja
- Ei sopimuksia
- Ei kontrollia varmennettaviin
- Luottosuhde palvelutarjoajaan
- Integrointivaikeudet?
- Joustamaton

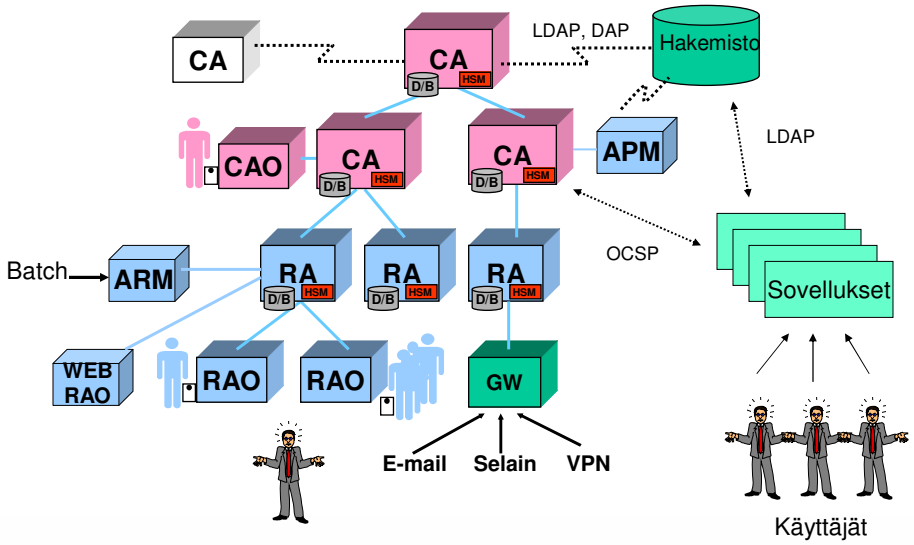
Toimikortti?

- Hyvä väline, mutta ei välttämätön PKI:lle
- Vaihtoehtoina muut tokenit, levy, kännykkä
- PKI-sääntö numero 1: suojaa salaiset avaimet!

Projektin haasteita

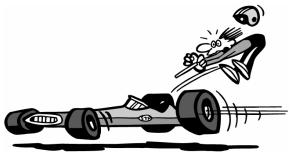
- Projektointi (20/80)
- Yhteensopivuusongelmat
- Sovellusten PKI-ominaisuudet
- Luottamussuhteet ja vastuut
- Kustannukset
- Asenteet (suunnittelu, asennukset, ylläpito,…)
- PKI:n integrointi nykyisiin prosesseihin
- PKI sovelluskehitys
- Yleinen turvatason nosto
- Laatuvarmenteet
- Yleiskäyttöinen vai sovelluskohtainen ratkaisu!
- Standardi-clientit vai erityinen PKI-client?
- W2K

Ympäristö



Yleisiä kompastuskiviä

- Varmenneprofiilit
- Skandimerkit
- Turvamoduulit
- Hakemisto
- Asennukset
- Toimikortit ja lukijat
- Operointi, ylläpito, valvonta, varmistukset
- Yhteensopivuusongelmat
- Valmissovellusten PKI-tuki
- Kustannukset
- Sopimukset



Yllättäviä kustannuksia?

- Palomuurit, IDS
- Turvamoduulit
- Turvaräkit, kassakaapit
- Toimikorttien hallinta
- Asennustyöt
- Integrointityöt
- Rekisteröintipisteet
- Lisähenkilökunta: ylläpito, rekisteröinti, tuki,…

Vinkkejä

- Hyvin määritelty on puoliksi tehty
- Älä haukkaa kaikkea kerralla - pilotoi!
- Varmista palvelutoimittajien osaamistaso
- Huomioi sopimuksissa PKI:n erityistarpeet
- Muista, että PKI-projekti on infrastruktuuriprojekti

PKI:n hyödyntäminen

- VPN-yhteydet
- Käyttäjätunnistus
- Sähköpostin salaus ja allekirjoitus
- Web-formien allekirjoitus
- Tiedostosalaus
- Tietoliikenneverkon komponenttien varmentaminen
- Omat sovellukset

- Web-selaimet ja –palvelimet, VPN-tuotteet ja eräät sähköpostiohjelmat ensimmäisiä kunnolla PKI:tä tukevia sovelluksia

PKI:n lupauksia

- Yhtenäinen, luotettava tunnistus kaikille käyttäjille, palveluille ja verkkokomponenteille
- Ennalta tuntemattoman käyttäjän ”hyväksyminen”
- Mobiili identiteetti
- Useita palveluja yhdellä tunnisteella
- Helppokäyttöisyys
- Kaiken verkkoliikenteen salaus
- Luotettava sähköposti
- Laillisesti pätevät digitaaliset allekirjoitukset
- Verkossa solmittujen sopimusten kiistämättömyys
- Skaalautuvuus

PKI kannattaa, jos…

- Ymmärrät PKI:n mahdollisuudet ja rajoitukset
- Tiedät varmasti, miksi PKI:ta tarvitset ja mitä sillä saavutat
- Projektin takana on yritysjohdon tuki ja tarvittavat resurssit
- Käyttötarpeet oikeuttavat tarvittaviin panostuksiin
- Ei ole kiire ☺

PKI SWOT

Vahvuudet	Heikkoudet
• Perusta sähköisille palveluille • Tunnustettu tekniikka • Helppokäyttöisyys (kuluttajalle) • Monikäyttöisyys • Sähköinen allekirjoitus • Riittävä turvataso	• Tuotteiden yhteensopimattomuus • Standardien keskeneräisyys • Monimutkaisuus (kehittäjälle) • Teknologiakeskeisyys • Laiteriippuvuus • Kuluttajat eivät tarvitse PKI:tä • Kuluttajapaketin puuttuminen
Mahdollisuudet	**Uhat**
• Sähköiset palvelut • Verkkopalvelut • Yhteistyö, innostus • Rooli/attribuuttivarmenteet • Globaali yhteistyö	• Paikalliset ratkaisut • Algoritmeista löydetään heikkouksia • Lisääntyneet turvallisuusvaatimukset • Kriittistä käyttäjämassaa ei saavuteta • PKI:lle löytyy vaihtoehto • Loppukäyttäjän ympäristö liian vaikea • Päätelaitteiden runsaus • Business-vaatimukset unohdetaan

TIEKE 3/2001

PKI toimittajat

Haastajat	Johtajat
•IBM/Tivoli •Microsoft •Equifax •iPlanet	•Verisign •Entrust •Baltimore •RSA
•DST •CertCo •eScotia •UniSecurity	•Certicom •Cylink •Arcanus
Niche	Visionäärit

Gartner 5/2001

PKI + PMI + XML

atbusiness

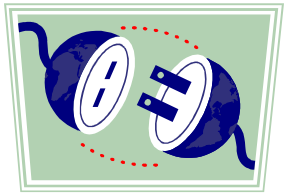
Tunnistus, valtuutus (PMI)
SAML, XACML

Hallinta (PKI)
XKMS

Allekirjoitus
XML-DSig

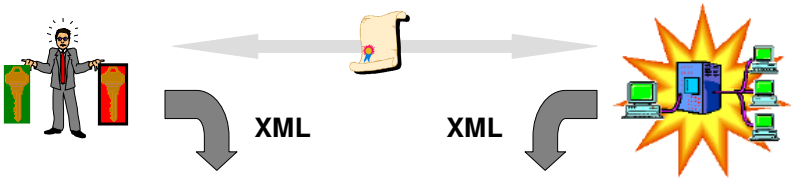
Viestinvälitys
SOAP

- Entrust + enCommerce
- Baltimore + SelectAccess
- RSA + Securant



PKI + XKMS

atbusiness



XKMS Palvelut

Avainten generointi
Salaus
Tulkkaus
Allekirjoitukset
Allekirjoituksen tark.

PKIX
SPKI
PGP

Varmenteen haku
Varmenteen käsittely
Varmenteen voimassaolo
Luottamusketjun käsittely
Mitätöinnin tarkistus

X-KRSS, X-KISS

Mobile PKI

- Avaimet SWIM-kortilla (WIM+SIM)
- Kortilla viittaukset varmenteeseen (LDAP URL)
- Saman PINin takana mahdollisesti useita varmenteita
- WTLS 3, signText, PKI Portaali
- Vaatii uudet puhelimet, SWIM-kortit, palvelut,…
- Toimiva, yhteensopiva kortinlukija ☺
- WAP-autentikointi?
  - web-palvelut
  - Digi-TV
  - työasema

Summa summarum

- Projektit ovat haasteellisia, halvalla ja hätäilemällä ei saa aikaan hyvää ratkaisua
- PKI:lle ei ole todellisia vaihtoehtoja näköpiirissä
- Etene askel kerrallaan, kerää tietämystä ja kokemuksia
- Kehitys kehittyy (XML, WAP), täydellistä ratkaisua voi odottaa voi ikuisesti…