PKI
Käytännön kokemukset ja SWOT-analyysi

TIEKE
Toimivan Sähköisen Asioinnin Edellytykset

6.3.2001
Jari.Pirhonen@atbusiness.com

Projektin tavoitteet ja toteutus

Tavoite
- Kerätä ja dokumentoida kokemuksia PKI-projekteista ja –käytöstä
- Tehdä PKI SWOT-analyysi
- Pohja TSAE-ryhmän omalle työlle
- Työraportti julkiseksi, http://www.tieke.fi/ => e-edellytykset

Rajaukset
- Keskittyminen PC-maailmaan
- Näkökulmana erityisesti käyttäjien/asiakkaiden/kuluttajien PKI-käyttö

Toteutus
- Toteutustavaksi sovittiin 10 TSA-ydinryhmän jäsenorganisaation haastattelu
- Haastateltavat valittiin ilmoittautumisjärjestyksessä

Haastatellut yritykset

- Certall (2)
- Done Information (2)
- Elisa Communications (1)
- VRK (3)
- ICL Invia (2)
- Nordea (2)
- Osuuspankki (4)
- Sonera SmartTrust (1)
- KELA (1)
- TietoEnator (5)

yhteensä 23 henkilöä

Tulokset

- Yleissävy negatiivinen, koska haettiin kokemuksia muiden opiksi
- Ongelmien ratkaisu suoraviivaista – tyydyttiin heikompaan lopputulokseen, ongelma kierrettiin tai tehtiin ylimääräistä työtä
- Hyvää tietoa mahdollisista sudenkuopista PKI:ta suunnitteleville
- Paljon ideoita TSAE-ryhmän jatkotoimenpiteiksi
- Laaja, useasta näkökulmasta mietitty SWOT-analyysi

Kokemukset & kommentit

- Toimikorttilukijat
- ID2 Personal
- VRK:n sähköinen henkilökortti
- Varmenteet
- Sovellukset
- Sovelluskehitys
- Yhteensopivuus

Toimikorttilukijat

- Paljon asennusongelmia, yhteensopivuusongelmia, toimivuusongelmia
- Saatavuus huono kuluttajille
- Windows 95/98/NT/2000 + sarjaportti, PCMCIA, USB
- Yleensä asennus vaatii ylläpitotaitoja
- Käyttöjärjestelmät ja sovellukset eivät tue toimikortteja
- Eri toimittajien ajurit epäyhteensopivia
- Windows 2000 + USB on helppo asennus
- Uusimmat ajurit alkavat olla toimivia

Toimikorttilukijoiden tulisi olla integroituja laitteeseen tai valmiiksi asennettuja. Minimivaatimuksena hyvät yhteensopivuustaulukot ja ohjeistukset.

ID2 Personal

- Ainoa vaihtoehto toistaiseksi
- Vaatii ATR-tietojen lisäämistä INI-tiedostoon, jos ID2 ei tunnista korttia oletusarvoisesti
- Ei ole lokalisoitu
- Yhteensopivuusongelmia muiden sovellusten kanssa, ID2 tehnyt muutoksia omaan tuotteeseensa
- Elisan kuluttajapaketissa vanha versio

Tarvitaan ilmainen, lokalisoitu, todellinen plug-n-play sovellus. Tarvitaan vaihtoehtoja ID2:lle.

VRK:n sähköinen henkilökortti

- VRK:n työ edistänyt PKI:n leviämistä
- Vieläkin vahvempaa panosta haluttiin: markkinointi, kuluttajapaketti, sovellukset
- Teknologiapainotteisuus
- ”Oikea” SATU-numero (FINUID) VRK:n takana
- Yritykset huolissaan globaalista toimivuudesta

Tarvitaan lisää sähköistä henkilökorttia hyödyntäviä sovelluksia. FINUID-tunnuksesta todellinen verkkoidentiteetti sallimalla yritysten myöntää oikea, VTJ-yhteensopiva SATU-tunnus helpommin.

Varmenteet

- Hankalaa ellei jopa mahdotonta suunnitella varmenne- ja tuoteriippumattomia sovelluksia
- Skandiongelmat
- Varmenteet tuoteriippuvaisia
- Sovellukset varmenneriippuvaisia
- Esim. W2K SC-logon vaatii, että varmenne tehty W2K CA:lla, varmenteen oltava kortilla ensimmäinen ja varmenteessa oltava sähköpostiosoite
- Yrityskohtaiset varmenneprofiilit

Sovellukset tehtävä joustaviksi.

Sovellukset

- Käyttö: etäkäyttö, email, työasemaan kirjautuminen
- Ei ole todellista ”tappajasovellusta”
- Liian vähän VRK:n korttia hyödyntäviä sovelluksia
- Sovellukset tuotesidonnaisia
- Valmissovellukset eivät yleensä tue toimikortteja
- Vain kotimaiset sovellukset tukevat VRK:n korttia
- Palvelinsovellus ei tunnista toimikortin vaihtoa
- SSL-yhteys jää päälle vaikka toimikortti poistetaan lukijasta
- Useita varmenteita per käyttäjä

Selainten ja sovellusten tulisi tukea toimikortteja ilman apusovelluksia. Löydettävä keino, jolla palvelinsovellus saa tietoa lukijan tilasta. Kuluttajatason PKI-tietämystä lisättävä.

Sovelluskehitys

- Pula PKI-osaajista
- Sovelluksiin ”PKI-kuorrutus”, ei todellista PKI:n hyödyntämistä
- Sovellukset vaativat muutoksia, koska clientin tilasta ei saada tietoa
- Yrityskohtaiset ”SATU-numerot”, joita joudutaan ristiintaulukoimaan B2B-sovelluksissa
- Yhteensopivuusongelmat yllätyksinä

Sovellusten tuettava useita varmentajia, hakemistoja ja varmenteita. Kansallinen sähköinen identiteetti helpottaisi sovellustyötä. Osaajia tarvitaan lisää

Yhteensopivuus

- Varmenneprofiilit
- Tuotekohtaiset ratkaisut
- Standardien tulkinta

PKI-tuotteet saatava monipuolisimmaksi ja yhteensopiviksi. Uusimmat selaimet ja sähköpostiohjelmat käyttöön.

Yleisiä PKI-ongelmia

- Osaajien puute
- Tuotteiden kypsymättömyys
- Yhteensopivuusongelmat
- PKI:n ymmärtäminen
- Business-tarpeiden ymmärtäminen
- Toimittajien intressit
- Liikkuvan käyttäjän tarpeet
- Erilaiset päätelaitteet
- Identiteettien, korttien ja PIN-koodien runsaus
- Luottamuksen evaluointi
- Monimutkaisuus
- Kalleus

SWOT / PKI vahvuudet

- Perusta sähköiseen asiointiin (3)
- Tunnustettu tekniikka (2)
- Käyttömukavuus (2)
- Monikäyttöisyys (1)
- Digitaalinen allekirjoitus (1)
- Riittävä turvataso (1)

- Standardit
- Päätelaiteriippumattomuus
- Ennalta tuntemattoman käyttäjän tunnistaminen
- Valtiovallan panostus
- Sovellustyön helppous

SWOT / PKI heikkoudet

- Tuotteiden yhteen-sopimattomuus (4)
- Ongelmat standardeissa (1)
- Monimutkaisuus (1)
- Teknologialähtöisyys (1)
- Varmenne sidottu laitteeseen (1)
- Kuluttaja ei tarvitse PKI:tä (1)
- Loppukäyttäjän paketti (1)

- Tunnistaminen ja maksaminen eri PKI-kehityspoluilla
- X.509 keskittyy tunnistamiseen
- CPS
- Laatuvarmenteet
- Kustannukset
- Teknologian uutuus
- vaadittavat lisälaitteet ja –ohjelmistot
- Vähäinen PKI-tietous
- PIN
- Erilaiset PKI:t
- Toimittajien erilaiset intressit

SWOT / PKI mahdollisuudet

- Sähköisen kaupankäynnin ja asioinnin mahdollistaja (5)
- Verkkopalvelujen edut (2)
- Yhteistyö, innostus (1)
- Rooli-/attribuuttivarmenteet (1)
- Globaali yhteistoiminta (1)

- Yksi väline – kaikki palvelut
- Laatuvarmenteet
- Uusi tapa kommunikoida
- Toimikorttien, varmenteiden ja palveluiden yhteensopivuus
- Biometriikka
- Asiakassuhteen aloittaminen verkossa
- Oppiminen kokemusten kautta
- Digitaalinen allekirjoitus
- Sirukorttien yleistyminen
- Bluetooth
- Kännykkä + varmenteet
- Henkilön yksilöivä avain
- PKI:n markkinointi
- Sähköinen asiointi
- Windows 2000

SWOT / PKI uhat

- Ratkaisut eivät toimi globaalisti (2)
- Löydetään heikkouksia algoritmeissa (2)
- Lisääntyvät tietoturva-vaatimukset (1)
- Kriittinen massa ei synny (1)
- Korvaava tekniikka (1)
- Loppukäyttäjän ympäristö (1)
- Päätelaitteiden kirjo (1)
- Businesstarpeet unohdetaan (1)

- Erilaiset varmennesisällöt
- Laatuvarmenteet
- PKI:n kyseenalaistaminen
- Satsaus mobiilipuolelle
- Resurssivaatimukset
- Kahdensuuntainen varmennus
- Tekniikan vaikeus palveluntarjoajille
- Riittävää kilpailua ei synny
- Syntyvien rekistereiden väärinkäyttö
- Markkinointi ei onnistu
- Luotettavien tahojen eriytyneisyys