Käyttäjätietojen ja käyttöoikeuksien hallinta

Tieturi
Data Security
14.10.2004

Jari Pirhonen – www.iki.fi/japi
Turvallisuuspäällikkö, CISSP, CISA
Samlink – www.samlink.fi

Samlink

Samlink

- Suunnittelemme ja tuotamme suomalaista pankkitekniikkaa
  - otto- ja antolainausjärjestelmät, korttijärjestelmät, itsepalvelujärjestelmät, tuotantopalvelut
- Asiakkaina säästöpankit, paikallisosuuspankit sekä luottolaitoksia ja pankkiiriliikkeitä
  - 40 säästöpankkia, 262 konttoria
  - 42 itsenäistä osuuspankkia, 142 konttoria
- Omistajina säästöpankit
  - Aktia isoin omistaja
- 2003: liikevaihto 58 M€, henkilöstö 266

Samlink

Esityksen sisältö

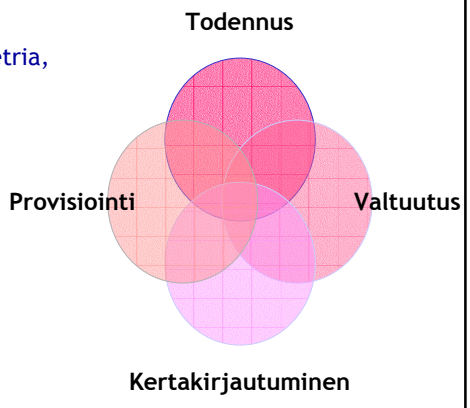
- Haaveet ja todellisuus
- Tunnistus, todennus, valtuutus, istunnonhallinta
- Käyttäjätietojenhallinta remonttiin - ratkaisuvaihtoehtoja
- Hakemistojen ja PKI:n rooli
- Tuote- ja palvelutarjontaa

Huom. Esitys ei perustu Samlinkin ratkaisuihin, vaan luennoijan kokemuksiin useista hakemisto-, PKI-, käyttäjähallinta- ja sovellusprojekteista.

Samlink

Komponentit

- Todennus
  - Salasanat, token, älykortti, biometria, pankkitunnukset, SMS
- Valtuutus
  - Sovellukset, tiedot, tapahtumat
  - Roolit, ryhmät, profiilit
- Kertakirjautuminen
  - Istunnonhallinta



- Provisiointi eli käyttäjätietojen hallinta
  - Resurssit, ohjelmat, oikeudet
  - Käyntikortit, nimikyltit, kulkukortit

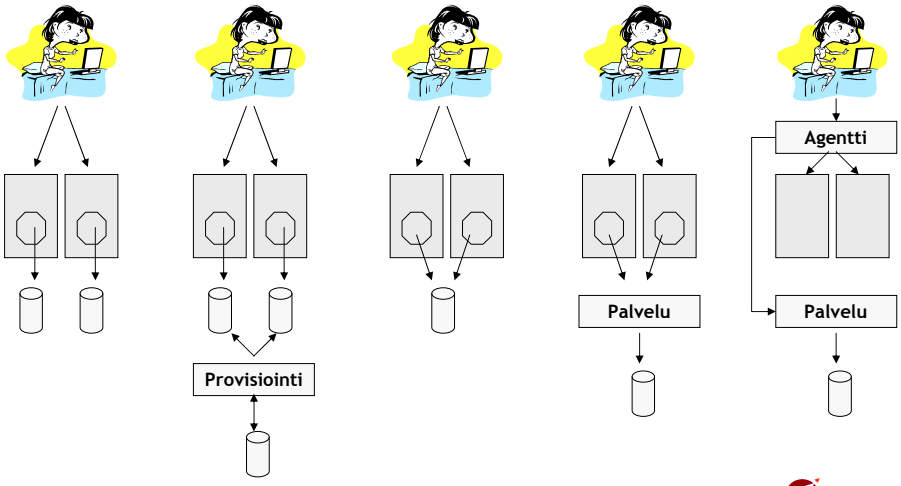
Samlink

Haaveita

- Yhtenäinen tietoturvapolitiikka
- Parempi käyttäjäkokemus
- Käyttäjätietojen hallinta erillään sovelluksista
- Käyttäjätietojen ajantasaisuus
- Käyttäjätietojen hallinta hajautettavissa
- Todennustapa valittavissa
- Sovelluksille yhtenäinen ratkaisu ”annettuna”
- Kertakirjautuminen
- Roolipohjainen valtuutus
- Helppo auditointi ja kattava raportointi
- Kustannustehokkuus
- Työmäärän pienentäminen

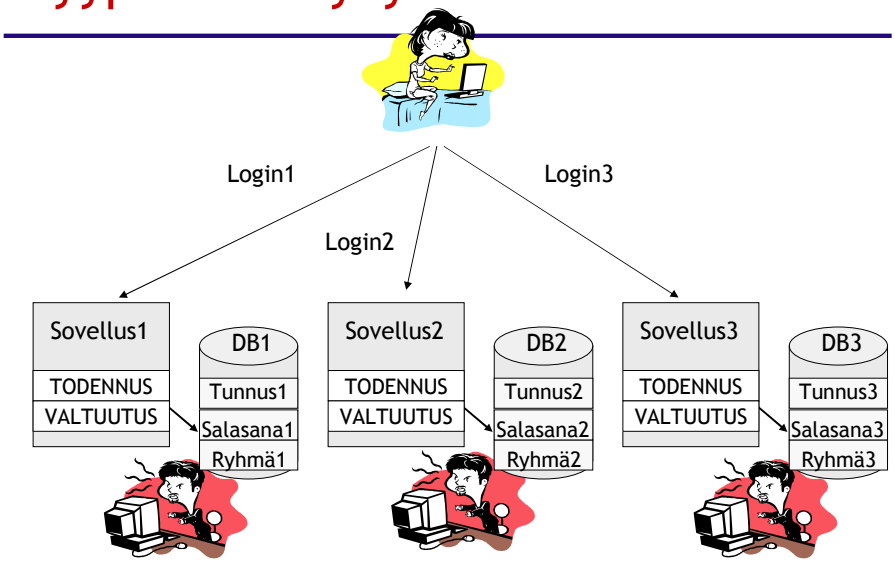
Samlink

Toteutustapoja



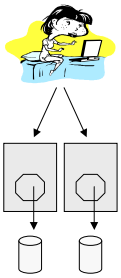
Samlink

Tyypillinen nykytilanne



Samlink

Tyypillinen nykytilanne

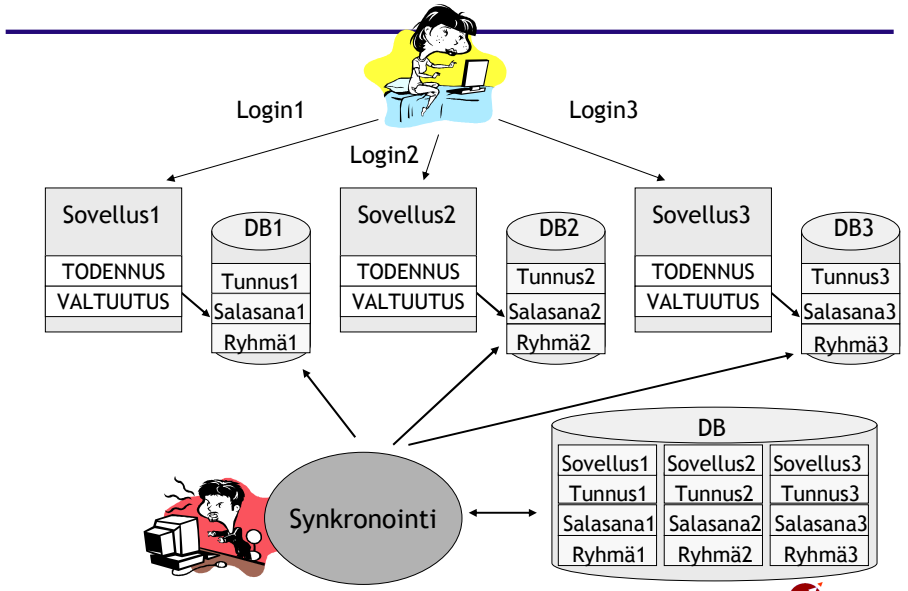


+ Ei sovellusmuutoksia
+ Sovelluksella vapausasteita

- Sovelluskohtaiset ratkaisut
- Käyttäjätiedot hajautettu
- Hallinta ei ole ajantasaista
- Hallintatyökalut erilaisia
- Tietoturvapolitiikat sovelluskohtaisia
- Auditointi ja raportointi hankalaa
- Tilanteen korjaaminen kallista ja työlästä

Samlink

Provisiointi – vaihtoehto 1

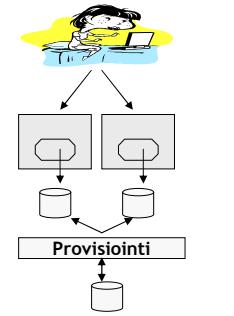


Samlink

Provisiointi – vaihtoehto 1

+ Ei sovellusmuutoksia
+ Käyttäjätiedot keskitetty
+ Hallinta helpottuu

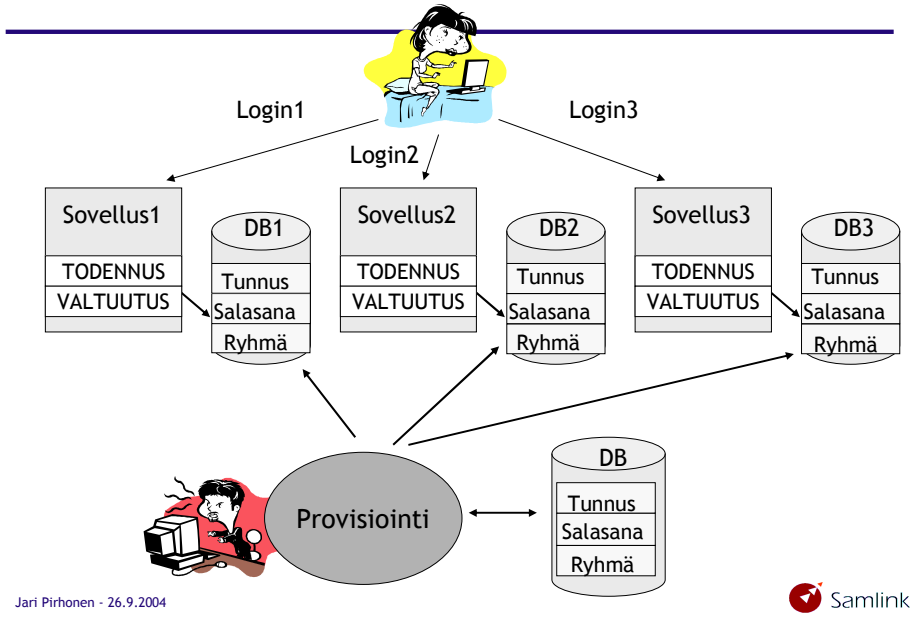
- Käyttäjäkokemus ei parane
- Ei kertakirjautumista
- Salasanat
- Ylläpitokonfliktit
  - keskitetty vs. sovelluskanta



Tuotteita:
- BMC
- Netegrity
- IBM
- CA
- Sun

Samlink

Provisiointi – vaihtoehto 2

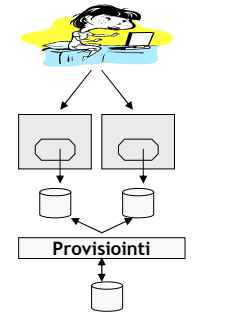


Samlink

Provisiointi – vaihtoehto 2

+ Käyttäjäkokemus paranee
+ Käyttäjätiedot keskitetty
+ Hallinta helpottuu
+ Workflow

- Ei kertakirjautumista
- Sovellusmuutokset
  - tunnusten ja salasanojen formaatti
  - salasanojen vanheneminen
  - ryhmien ja profiilien käyttö
- Ylläpitokonfliktit
  - keskitetty vs. sovelluskanta



Tuotteita:
- Netegrity
- IBM
- CA
- Sun

Samlink

Käyttäjähakemisto

Login1

Login2

Login3

Sovellus1	DB1	Sovellus2	DB2	Sovellus3	DB3
TODENNUS		TODENNUS		TODENNUS	
VALTUUTUS		VALTUUTUS		VALTUUTUS	

KÄYTTÄJÄT | RYHMÄT

tunnus salasana rooli	tunnus salasana rooli	dn1 dn2 dn3	dn4 dn5 dn6

Samlink

Käyttäjähakemisto

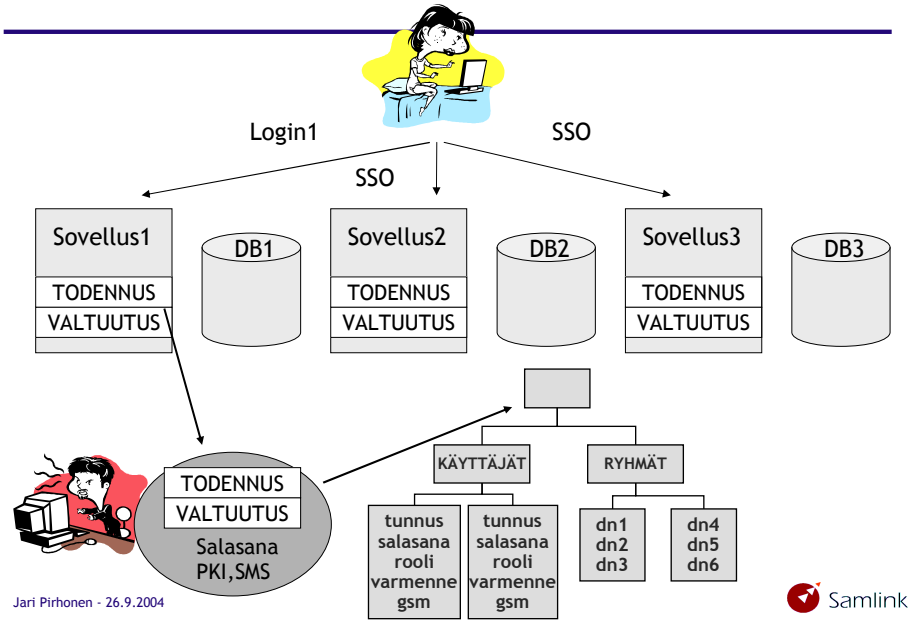
+ Käyttäjäkokemus paranee
+ Käyttäjätiedot keskitetty
+ Hallinta helpottuu
+ Sovellusten LDAP-tuki
+ Auditointi

- Ei kertakirjautumista
- Sovellusmuutokset
  - uusi todennus ja valtuutustapa
- Valmissovellusten tuki organisaation hakemistorakenteelle

Tuotteita:
- Sun
- IBM
- Novell
- CA
- Siemens

Samlink

Palvelu + API

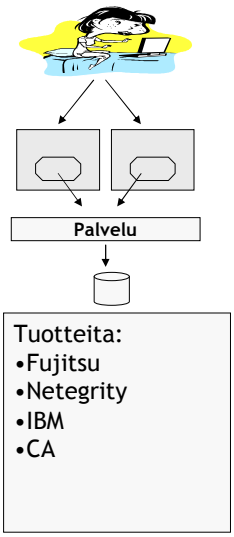


Samlink

Palvelu + API

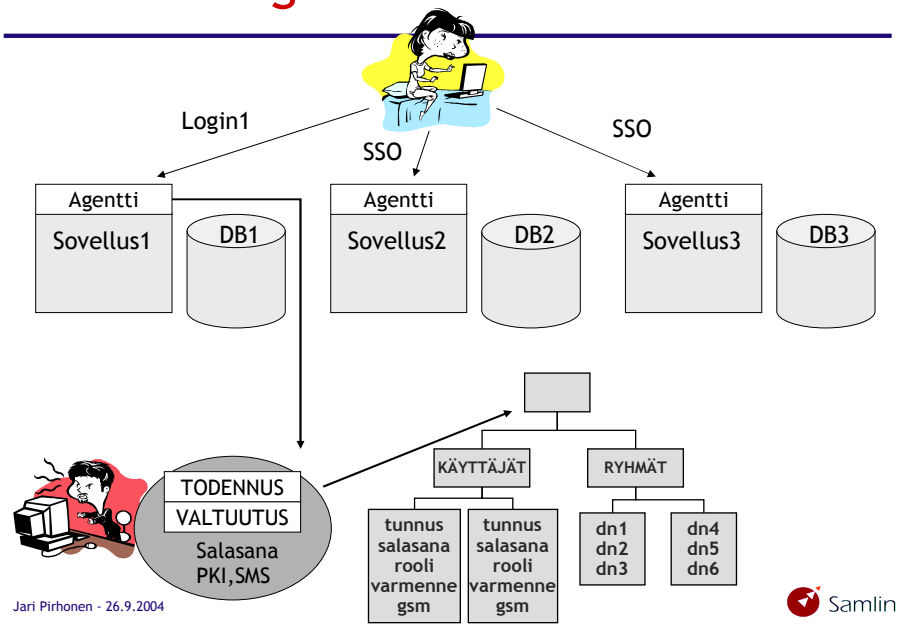
+ Käyttäjäkokemus paranee
+ Kertakirjautuminen
+ Hallinta helpottuu
+ Useita todennusvaihtoehtoja
+ Auditointi ja raportointi

- Sovellusmuutokset
  - palvelu API
- Valmissovellusten tuki
- Sitoutuminen toimittajaan



Samlink

Palvelu + agentti

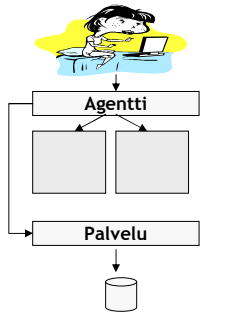


Samlink

Palvelu + agentti

+ Käyttäjäkokemus paranee
+ Kertakirjautuminen
+ Hallinta helpottuu
+ Useita todennusvaihtoehtoja
+ Auditointi ja raportointi
+ Ei sovellusmuutoksia

- Muut kuin web-sovellukset



Tuotteita:
- Netegrity
- IBM
- HP
- Sun
- Novell
- UbiSecure

Samlink

PKI

+ Vahva todennusmekanismi
+ Käyttäjäkokemus paranee
+ Hallinta helpottuu
+ Osittainen kertakirjautuminen
+ Todennus- ja valtuutuspalvelut tukevat

- Sovellustuki
- Valmissovellusten tuki organisaation PKI:lle
- Varmenteen linkittäminen käyttäjätietoihin
- Toimikortin hallinta

Samlink

Muita vaihtoehtoja

- Windows-työasematunnistuksen hyödyntäminen
  - Käyttäjätiedot välitetään työasemasta sovellukselle
- Työaseman SSO-sovellus
  - Sovellusten sisäänkirjautuminen automatisoidaan ja piilotetaan käyttäjältä
  - Vaatii työasemasovelluksen ja integrointityötä
  - Novell, Passlogix
- Erilaiset variaatiot ja kombinaatiot

Samlink

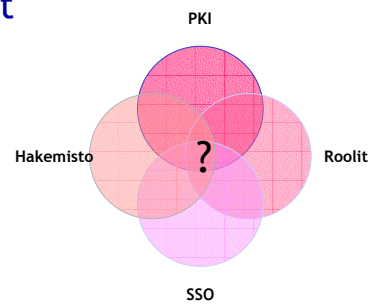
Haasteita

- Tuotteiden tuki eri alustoille vaihtelee: web-palvelin, sovelluspalvelin, tietokanta, käyttöjärjestelmä, web-selain, hakemisto,…
- Käyttäjähallintaominaisuudet vaihtelevat
- Organisaatiolaajuisten hallintaprosessien, ryhmien, roolien, yms. muodostaminen
- Sovellusintegrointi
- Kustannukset
- Organisaatioiden välinen luottamus

Samlink

Toteutuksessa huomioitava

- Nykyiset arkkitehtuurivalinnat
- Nykyiset prosessit
- Sovellukset
  - Toteutustapa (web vs. client/server)
  - Elinikä
  - Muutosmahdollisuus
- Tavoite
  - Käyttäjäkokemus vs. käyttäjähallinta vs. kustannustehokkuus vs. tietoturva
  - Kattavuus
  - Nykytilan viilaus vs. täydellinen remontti
- Budjetti



Samlink