

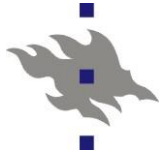


HELSINGIN YLIOPISTO
HELSINGFORS UNIVERSITET
UNIVERSITY OF HELSINKI

Mobiilivarmenteen käyttö Helsingin yliopistossa

Ville Tenhunen, Juha Ojaluoma
24.10.2008

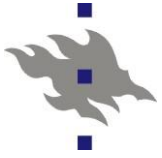




Sisältö

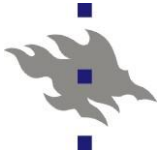
- HY:n ja Methics Oy:n projekti
- Mitä palveluita voidaan toteuttaa?
- Kansalaisvarmenne ja mobiilivarmenne
- Mobiilivarmenteen käyttö
- Autentikointi
- Digitaalinen allekirjoitus
- Käyttäjätilin aktivointipalvelu
- Standardit ja niiden uudistaminen
- Johtopäätöksiä ja kysymyksiä





HY:n ja Methics Oy:n projekti

- Tavoitteena on selvittää HY:ssä
 - HY:n oman MSSP AE –järjestelmän ylläpito- ja käyttökustannukset suhteessa VETUMA:n nykyiseen käyttöön
 - Mobiilin tunnistamisen hyödyt ja mahdollisuudet
- Pilotointi
 - Pilotoidaan kansalaisvarmenteen käyttöä HY:n infrastruktuurissa
 - Pilotoidaan lisäarvopalveluita
- Standardointi
 - Selvitetään standardoinnin tarpeet
 - Tehdään tarvittavat ehdotukset standardointiyhteisöille

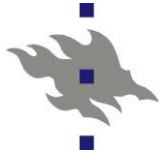


Mitä palveluita voidaan toteuttaa?



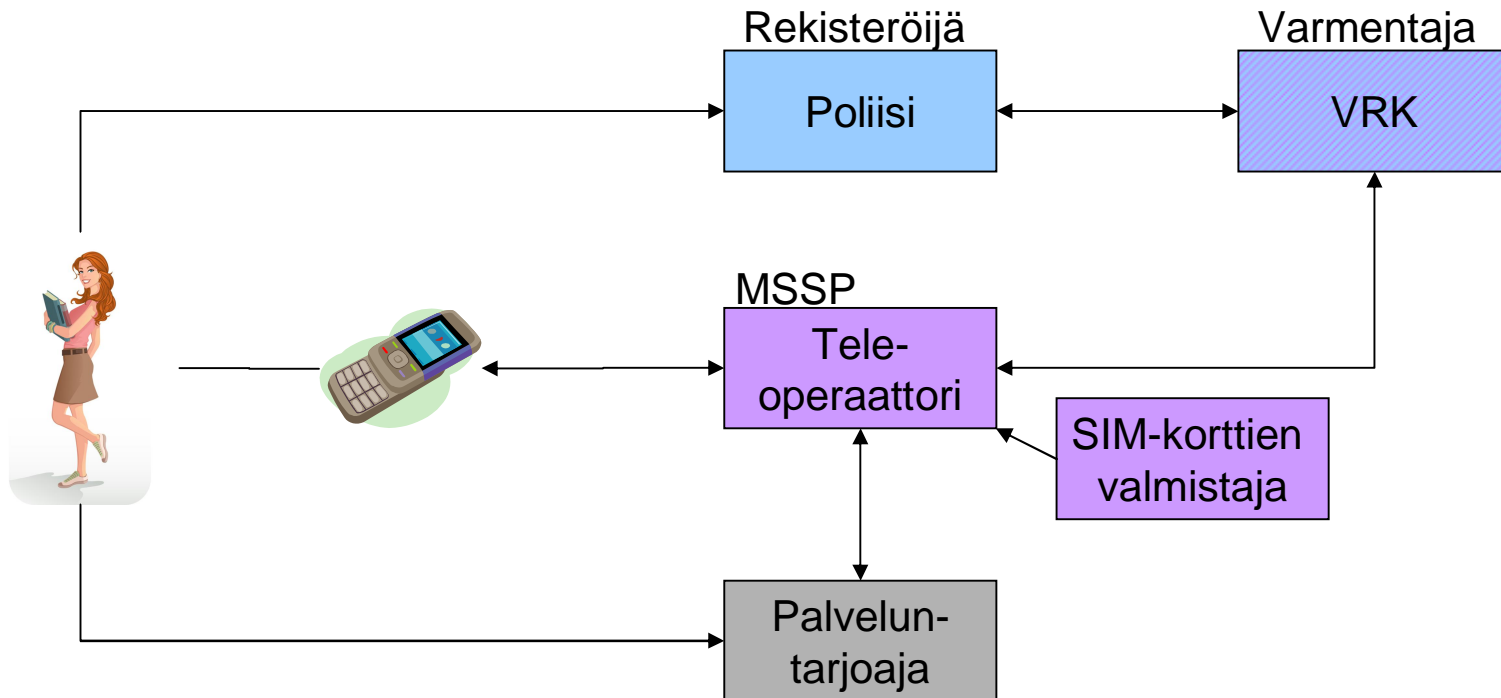
- Opiskelijan vahva tunnistaminen
 - Sisäänkirjaantuminen (Shibboleth)
 - Salasanan vaihtopalvelu
 - Käyttöluvan aktivoiminen
- Ylläpito henkilöstön vahva tunnistaminen
 - Ulkoiset VPN yhteydet
- Muut palvelut, joissa tarvitaan vahvaa tunnistamista
 - Muut julkiset palvelut joskus tulevaisuudessa
- Profiilitiedon välitys
 - Sähköisen opiskelijatodistuksen välittäminen yliopistojen välillä

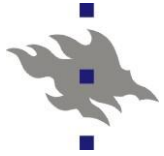
Sähköisessä tunnistamisessa erotetaan toisistaan vahva ja heikko tunnistaminen.



Kansalaisvarmenne

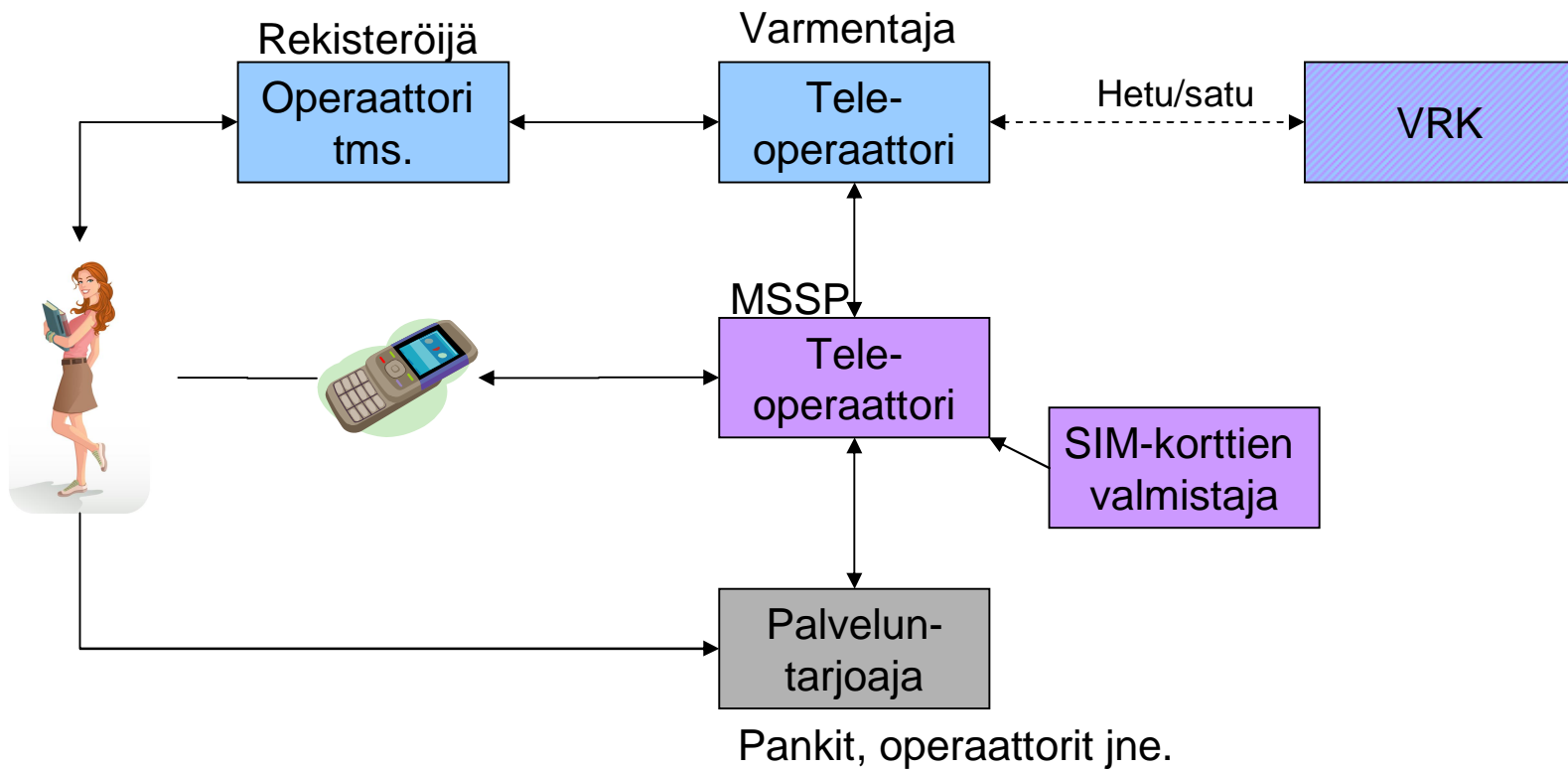
■ Kansalaisvarmenne ≠ Mobiilivarmenne





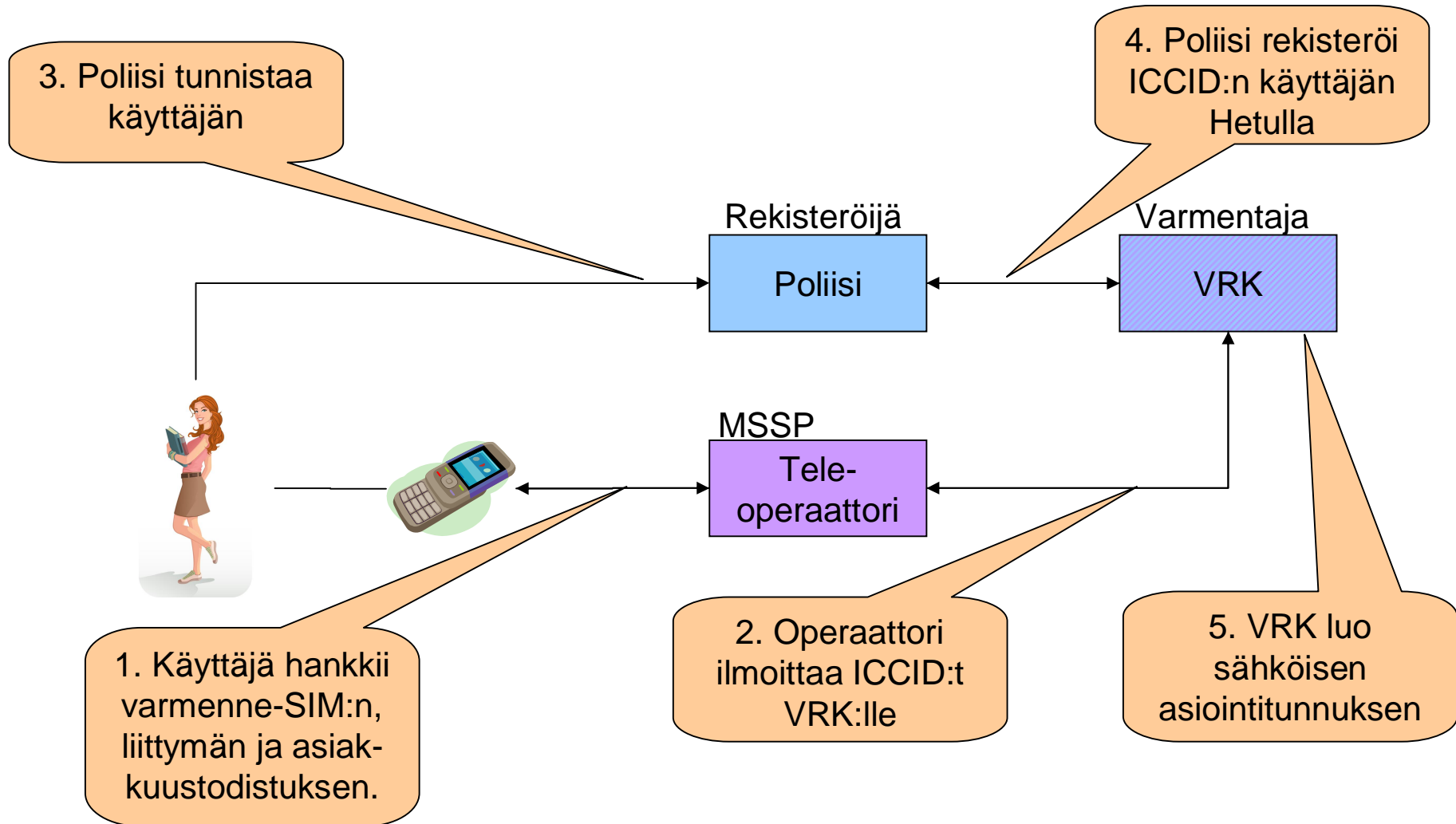
Mobiilivarmenne

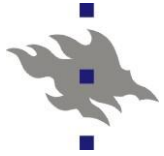
■ Kansalaisvarmenne ≠ Mobiilivarmenne



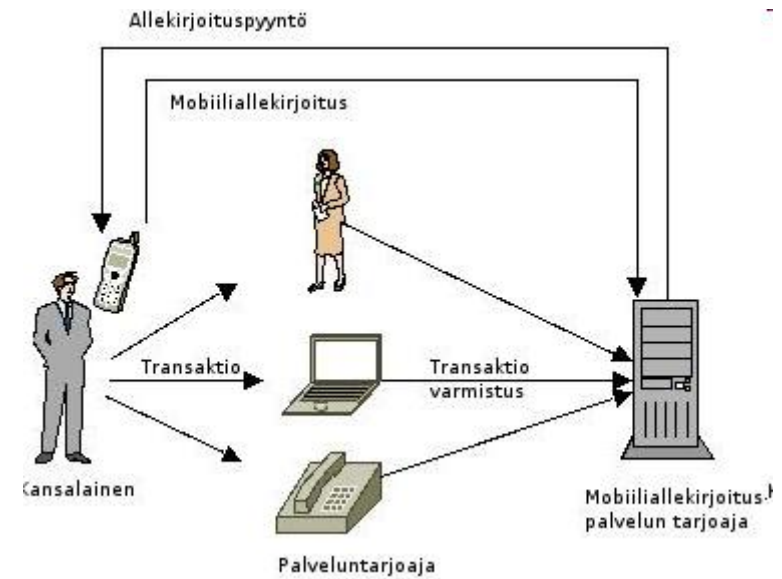
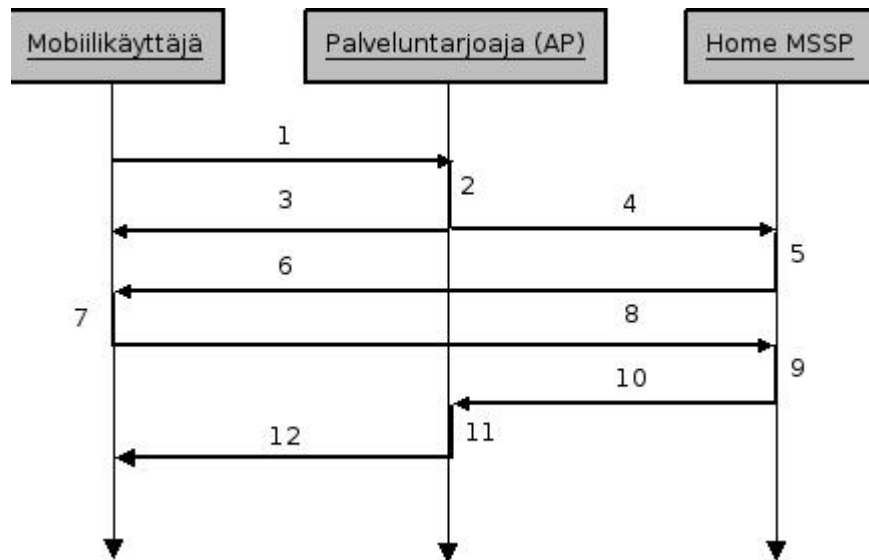


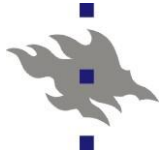
Kansalaisvarmenteen rekisteröinti





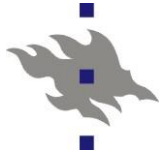
Mobiilivarmenteen käyttö





Autentikointi



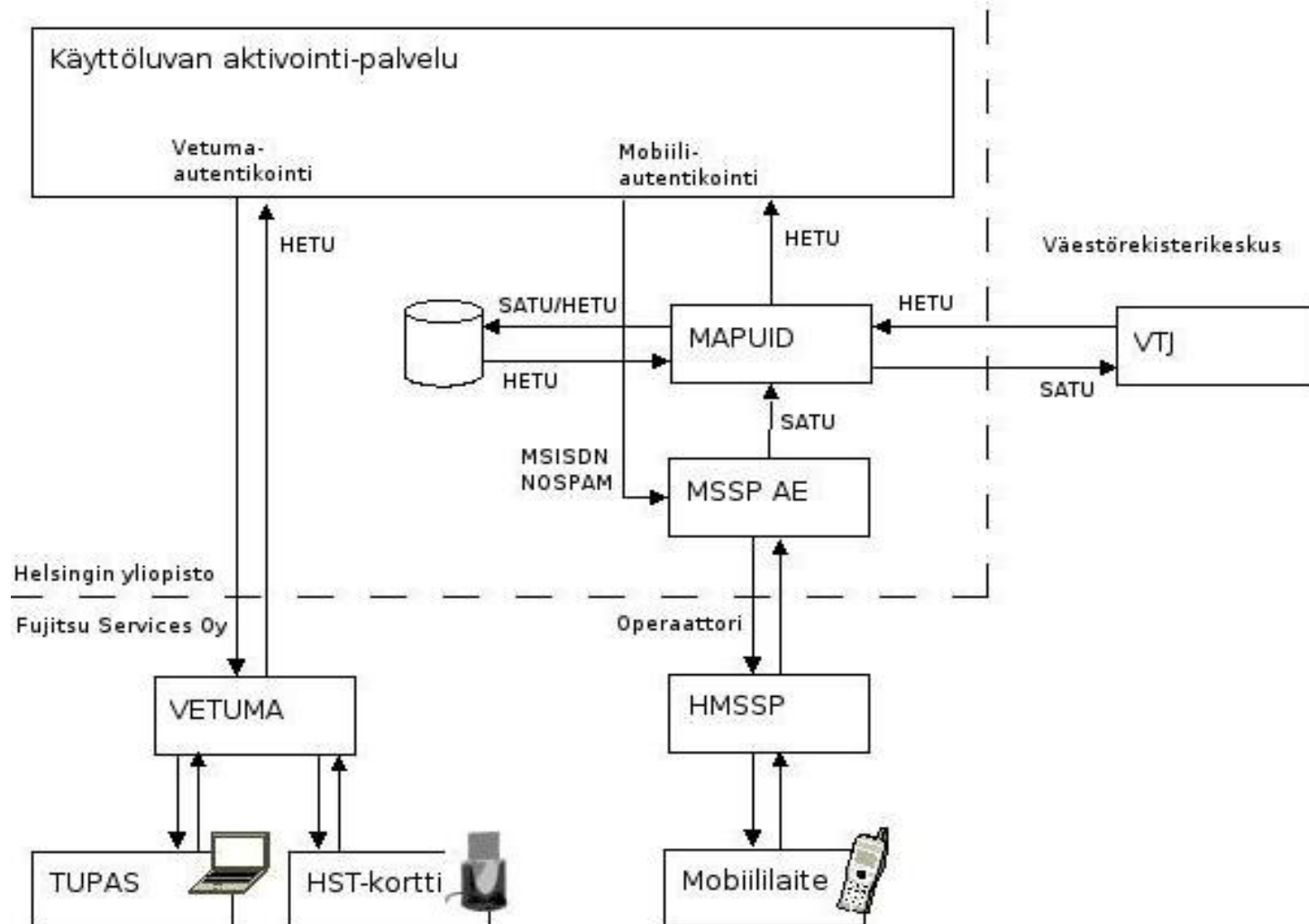


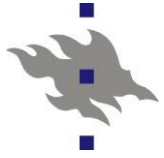
Digitaalinen allekirjoitus



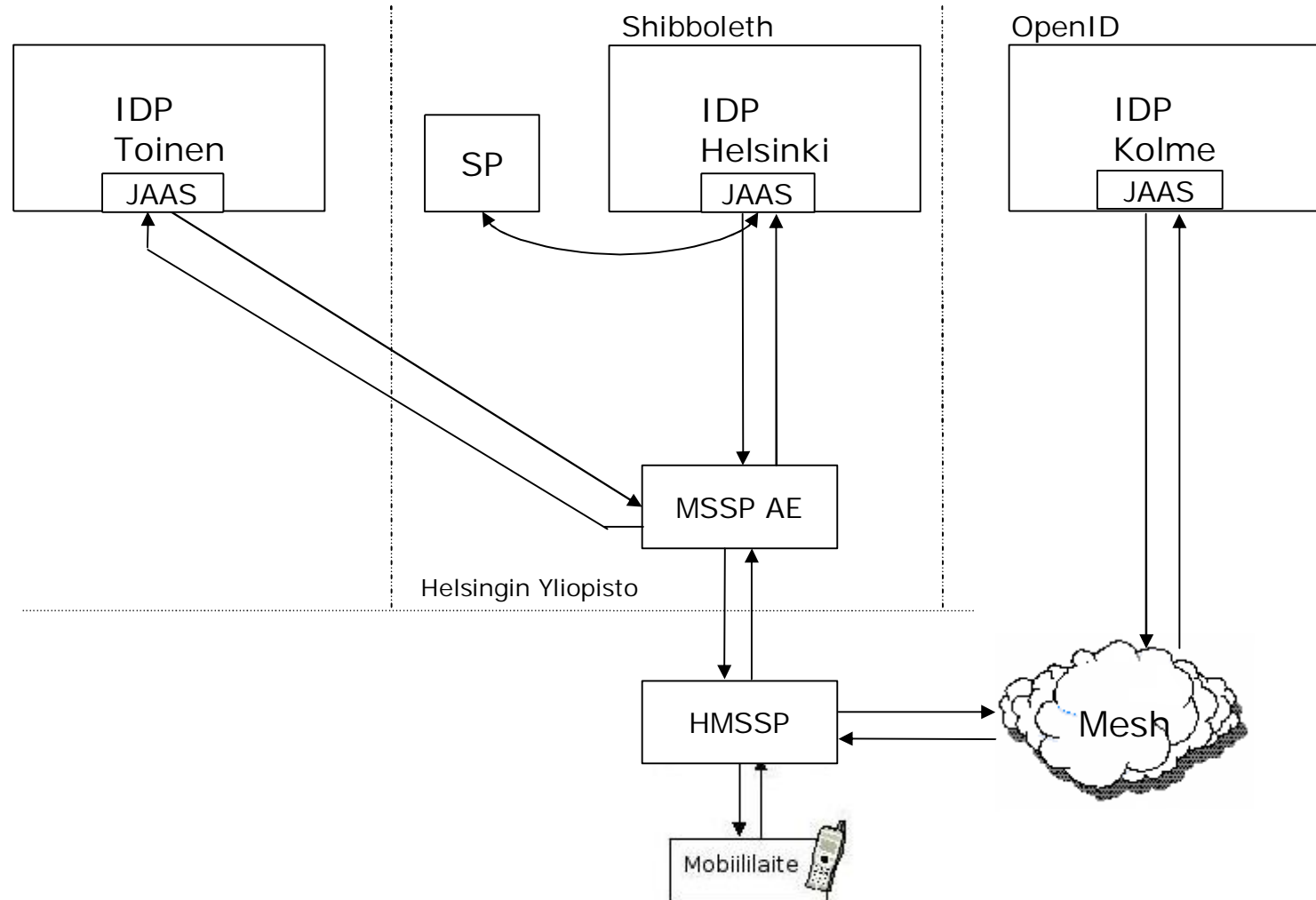


Käyttäjätilin aktivointipalvelu





Shibboleth-käyttö





Standardit ja niiden uudistaminen

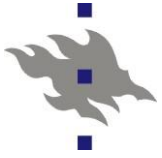
- Miten SAML2:n ja MSS voidaan liittää toisiinsa?
- Mitä hyötyjä siitä saataisiin?

- Toteutetaan SAML2:n kuljetus MSS-verkossa
 - Tavoite: Attribuuttitietoja eri teknologioiden välillä: SAML, OpenID, Oauth, IDWSF, WS-Federation
 - AttributeQuery- ja Consent-toteutukset MSSP:lle
 - Laaditaan ehdotus "SAML2 MSS Binding"
- Liitetään MSSP-palvelu Shibboleth-alustaan
 - Shibboleth 2.0 IDP:lle MSSPLogin JAAS-moduuli
 - IDP voi tarjota kaikille SP:lle mobiilivarmennepalvelun
 - IDP voi "kommunikoida" teknologiarajojen yli.



RePro =
Registering
and Profile
distribution





Johtopäätöksiä ja kysymyksiä



■ Johtopäätöksiä

- Teknologia on toimivaa, hallittavaa ja tuotteistettua
- Helppo liittää olemassa olevaan infrastruktuuriin
- Toimiva ja käyttäjälle helppo tapa tehdä vahva tunnistus
- Taloudellisesti varauksin mahdollinen
- Potentiaalinen TUPAS-tunnistamisen korvaaja.

■ Avoimia kysymyksiä

- (Kansalais)varmenteen jakelu ja käyttöönotto?
- Lainsäädännöllinen pohja
- Standardien tulevaisuus
- Hinnoittelu



HELSINGIN YLIOPISTO
HELSINGFORS UNIVERSITET
UNIVERSITY OF HELSINKI

Kiitos, kysymyksiä?

Lisätietoja:

Helsingin yliopisto:

Ville Tenhunen (ville.tenhunen@helsinki.fi)

Juha Ojaluoma (juha.ojaluoma@helsinki.fi)

Methics Oy:

Jarmo Miettinen (jarmo.miettinen@methics.fi)

Markus Lindström (markus.lindstrom@methics.fi)