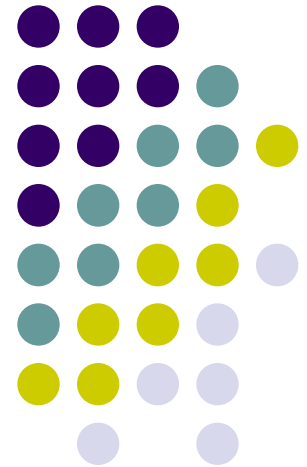


Strong Mobile Authentication in Finland (MPKI, WPKI)

Special Discussion Topic
Kantara Initiative Telco Identity Working
Group

Prepared by:
Keith Uber
Ubisecure Solutions Oy

10.3.2011

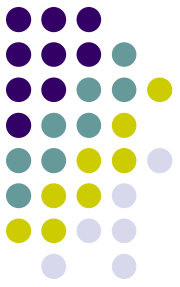


Agenda



- National ID
- Commercial Identity Providers in Finland
- Mobile ID
 - History
- Questions / Discussion

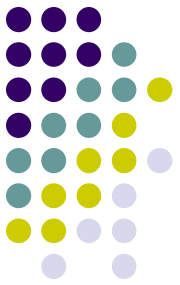
Finnish Personal Identification Number



- National ID number
- Widely used incorrectly for identification
- Format YYMMDD?123X
- Exposes both date of birth and gender

eID in Finland

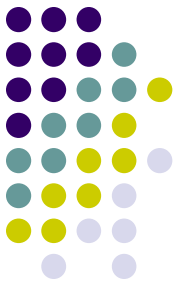
- eID card contains
 - name
 - optionally email address
 - SATU (electronic identification number)
- Not mandatory
- Price 51€
- The SATU number can be converted to a personal identity number through a web services query to the population register



eID Statistics



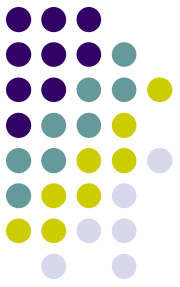
- End of November 2010
 - 341,800 certificates issued to date
 - 272,200 currently valid



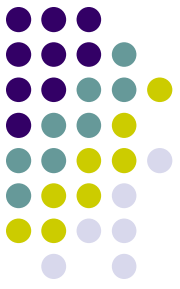
Population Registry

- Provides Web Service interface to population registry data to authorized parties (VTJKysely)
- Interface provides
 - Citizen, building and real estate information
 - Over 80 different types of attributes available
 - Web service interface authentication at connection level using client certificates

Banks as Commercial IdPs for eGov



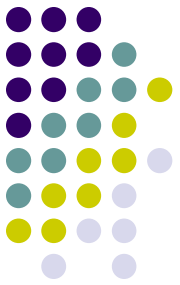
- TUPAS is a joint bank specification for electronic authentication by the Federation of Finnish Financial Services
- Proprietary protocol
- User must be strongly authenticated
- Typically PIN/TAN list
- Banks provide limited financial liability
- User approves and certifies the personal data released



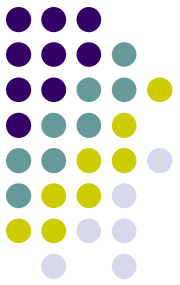
Banks as Commercial IdPs

- 10+ banks
- Commercial service
 - Contracts between SP and each bank required including typically
 - Establishment fees
 - Monthly fees
 - Transaction fees
 - Similar process to Verified By Visa etc

Familiar process




Bank authentication



Osuuspankin Tupas-tunn... x

← → ↻ <https://kultaraha.osuuspankki.fi/cgi-bin/krcgi> ☆

 **Osuuspankin Tupas-tunnistautuminen** [På svenska](#) [Suomeksi](#)

1 Tunnistautuminen **2** Key number query **3** Hyväksyminen **4** Kuittaus

Enter your username and password in the fields below and click Continue.

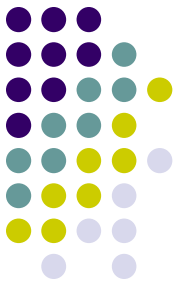
OP Internet Service uses an SSL-protected connection, making it safe to use. To use the service, make an online service agreement at your bank.

Username

Password


© OP-Pohjola Group

Indexed TAN




Osuuspankin Tupas-tunn... x

← → ↻ https://kultaraha.osuuspankki.fi/cgi-bin/krcgi?yksikas_linkki=Y=1 ☆

 **Osuuspankin Tupas-tunnistautuminen**

1 Identification **2** Key number query **3** Hyväksyminen **4** Kuittaus

 **Key number**

Find the number that corresponds to the bank number on your key number list and enter it in the input field below. The key number can be found on the right hand side of the bank number.

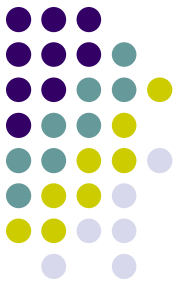
You have 100 key numbers remaining

Bank's key number: 0085

Key number:


© OP-Pohjola Group

Attribute release consent



Pohjola Bank's Internet B... x

← → ↻ https://kultaraha.osuuspankki.fi/cgi-bin/krcgi?yksikas_linkki=Y=2 ☆

 **Osuuspankin Tupas-tunnistautuminen**

1 Identification **2** Key number query **3** Hyväksyminen **4** Kuittaus

Välitettävien tietojen hyväksyminen

provider: Esittelykauppias Oy Ab

Seuraavat tiedot välitetään palveluntarjoajalle

Käyttäjän asiakastunnus: 081181-9984

Käyttäjän nimi: TESTI ANNA

© OP-Pohjola Group

Telcos as Commercial IdPs for eGov

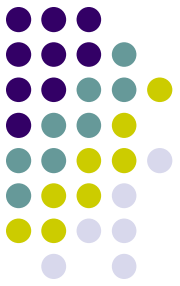


- Commercial Wireless PKI (MPKI, WPKI) service launched 30.11.2010
- Named "Mobiilivarmenne" Mobile Certificate
- http://www.mobiilivarmenne.fi/en/en_2.html
- Supported by 3 out of 4 national telcos
- Competing with TUPAS service

Telcos as Commercial IdPs



- Long history – previous studies and commercial trials commencing around 2003 to use national ID in the mobile had failed
- New business model, purely commercial
- Requires government-issued CA license with stringent auditing
- Application embedded in SIM (application toolkit application)

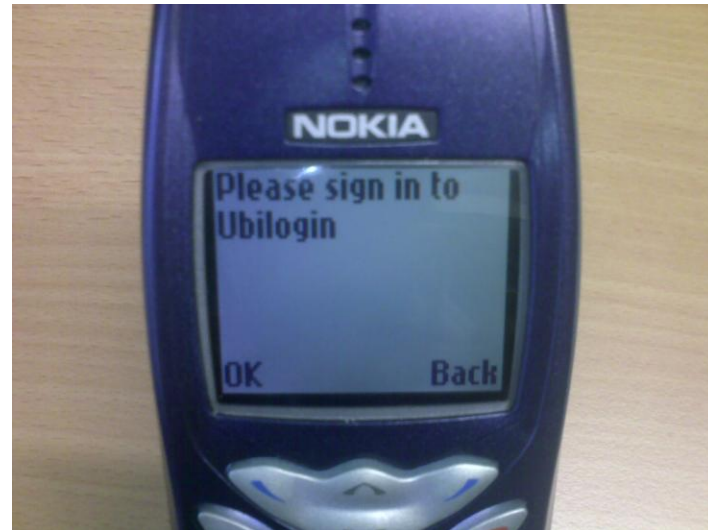


Two Profiles

- Authentication
- Signing (non-repudiation)

- Unique PIN codes for each type
- PIN codes distributed on SIM package behind scratch layer
- User can change own PINs through SIM menu

Old and new phones alike



Changing PIN codes



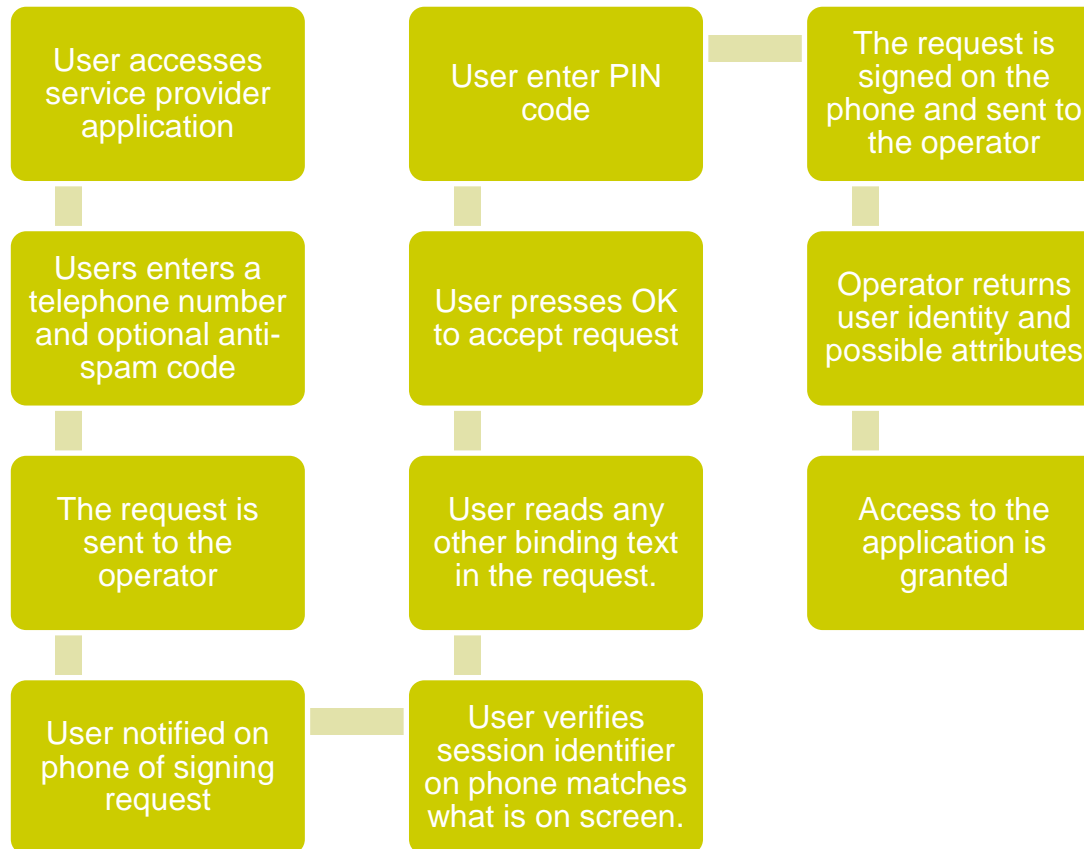
Telcos as Commercial IdPs



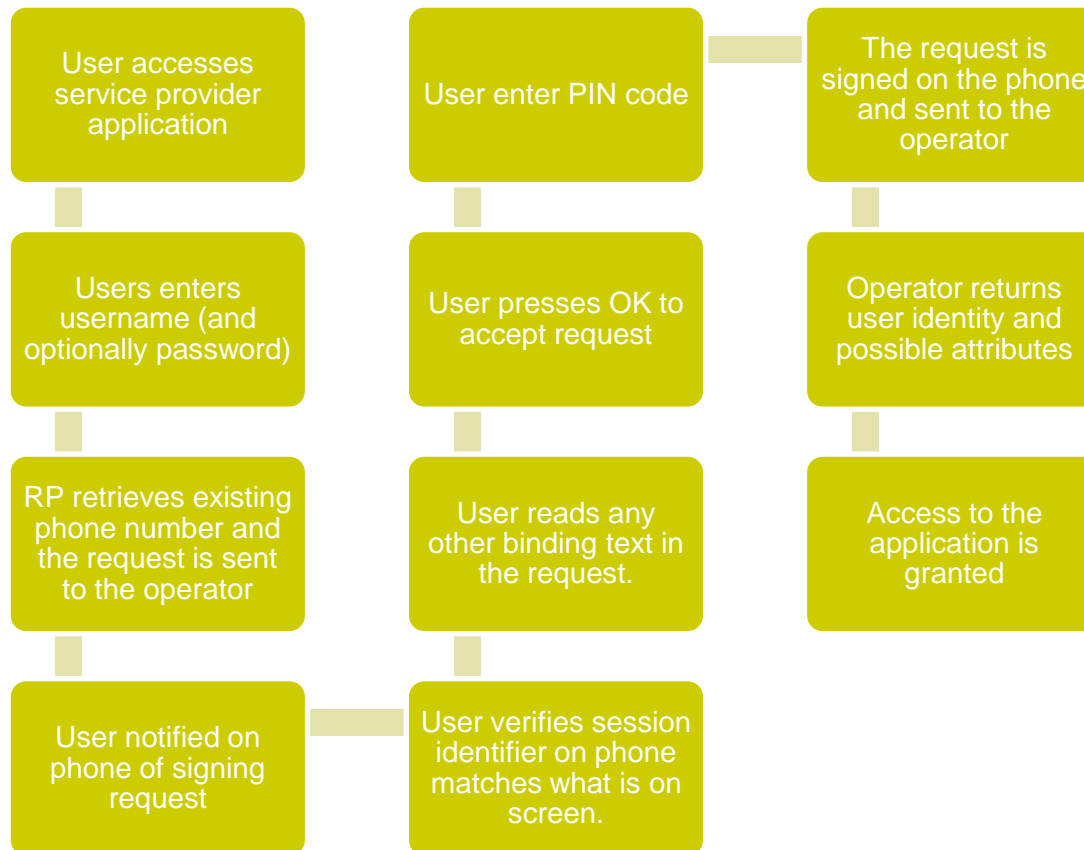
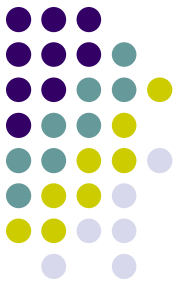
- Works while roaming (SMS based transport)
- Pricing for end users
 - Elisa: 0.09 per transaction (Free until Nov 2011)
 - Other telco pricing unknown
- Pricing for SP services
 - Unpublished
- Expected adoption for C2G services in 2011



Process Flow (A)



Process Flow (B)





MOBIILIVARMENNE
MOBIL ID

1. Lähetä tunnistuspyyntö

2. Tunnistaudu puhelimesi

3. Hyväksy tietojen lähetyks

Lähetä tunnistuspyyntö puhelimeesi

Ota puhelimesi valmiiksi esille ja poista näytön mahdollinen turvalukitus.

Olet tunnistautumassa palveluun: **palvelu.fi**

Puhelinnumerosi:

0505950550

Anna numero muodossa 0505950550

Häirinnänestokoodi:
(vapaaehtoinen)

••••

[Mitä tämä tarkoittaa?](#)

Kirjain + vähintään 2 merkkiä

Jatka

Keskeytä

[Lisätietoja mobiilivarmennteesta](#)

[Elisa Varmenne liiketoiminnan apuna](#)

[Rekisteriseloste](#)

[Anna palautetta](#)



Tunnistaudu mobiilivarmenteellasi

1. Ota puhelin esille

Saat kohta tunnistuspyynnön antamaasi numeroon **0458738428**. Pyyntö saapuu tyypillisesti alle 15 sekunnissa. Huomaa, että viesti ei ole tavallinen tekstiviesti vaan se aukeaa suoraan näytölle.

2. Varmistu viestin oikeellisuudesta

Tunnistuspyyntö
XXXXX lähettäjältä
Yritys Oy. Jatka
painamalla OK.

OK

Takaisin

Palveluntarjoajalle
välitetään: nimi,
SATU-tunniste.

OK

Peruuta

Tapahtuman tunniste on **RV22WC**. Tarkista, että puhelimeen saamassasi viestissä on sama tunniste. Näin voit varmistua tunnistuspyynnön aitoudesta. Jatka painamalla OK. Hyväksy myös, että saamme välittää tietosi palveluntarjoajalle.

Loading...

OK

Takaisin

OK

Peruuta

Tapahtuman tunniste on **RV22WC**. Tarkista, että puhelimeen saamassasi viestissä on sama tunniste. Näin voit varmistua tunnistuspyynnön aitoudesta. Jatka painamalla OK. Hyväksy myös, että saamme välittää tietosi palveluntarjoajalle.

3. Tunnistaudu tunnusluvullasi

Anna tunnusluku:

OK

Peruuta

Syötä varmenteesi salainen tunnusluku. Siirryt automaattisesti eteenpäin tunnusluvun syöttämisen jälkeen. Älä uudelleenlataa tätä sivua.

[Keskeytä](#)



Hyväksy tietojen lähetys

Nämä tietosi toimitetaan palveluntarjoajalle: **palvelu.fi**

Nimi: John Smith

Sähköinen asiointitunnus: 11111111X

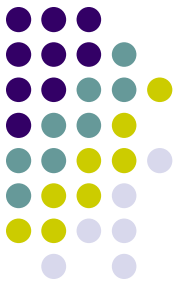
SATU on sähköinen asiointitunnus. Se on oma yksilöllinen tunnuksesi ja toimii henkilötunnuksen tavoin, mutta sen avulla ei voi päätellä ikääsi tai sukupuoltasi.

Tarkista, että tunnistetiedot ja palveluntarjoajan tiedot ovat oikein. Jos tiedoissa on virhe, keskeytä tunnistus ja ilmoita virheestä operaattorillesi.

Hyväksyn, että yllämainitut tunnistetietoni ovat oikeat ja ne välitetään yllämainitulle palveluntarjoajalle. Hyväksyn lisäksi, että operaattorin suorittama tunnistaminen ja tunnistetietojeni välittäminen palveluntarjoajalle vastaa allekirjoitustani palveluntarjoajan kanssa mahdollisesti tekemässäni oikeustoimessa.

Hyväksy

Keskeytä



Standards

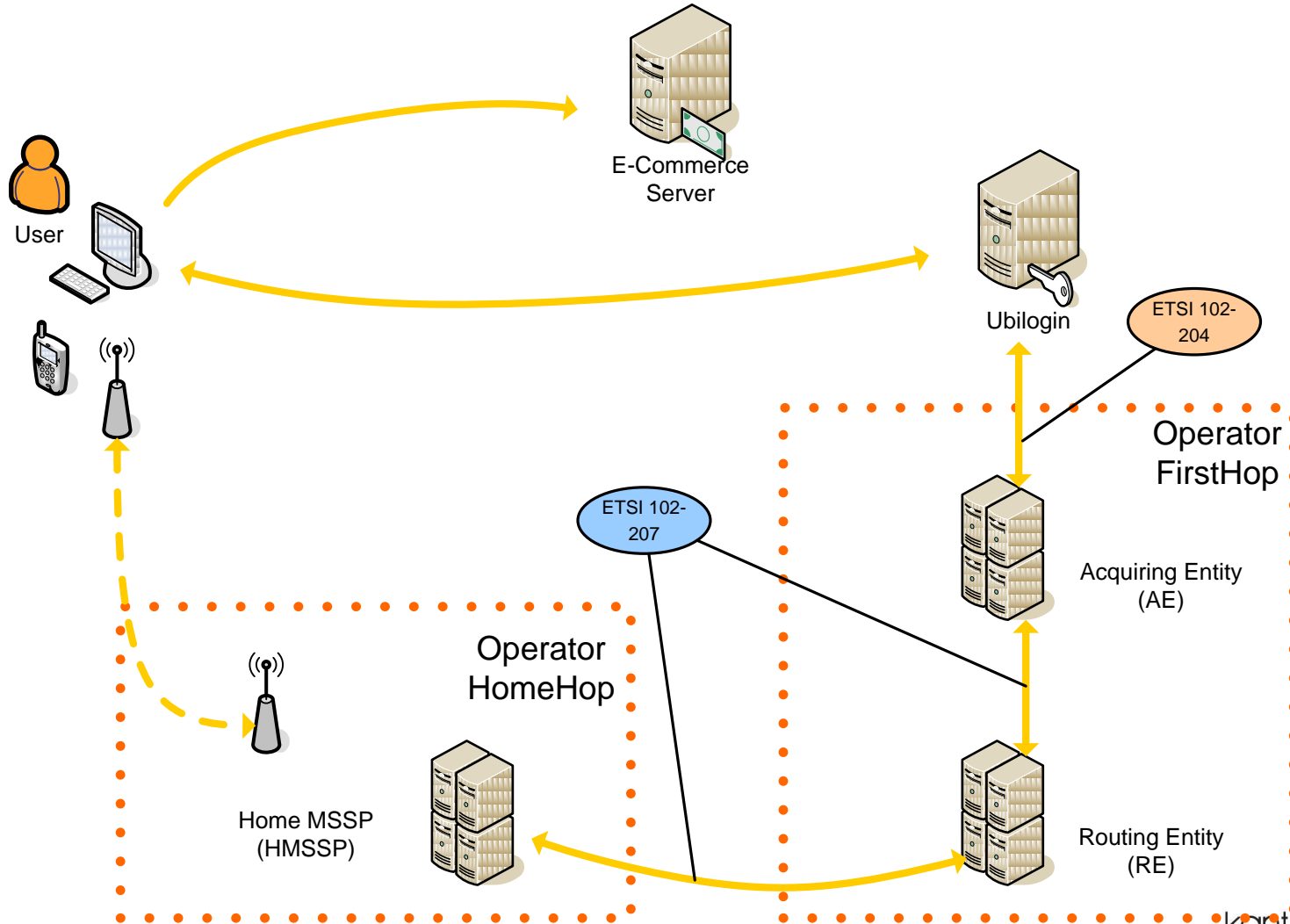
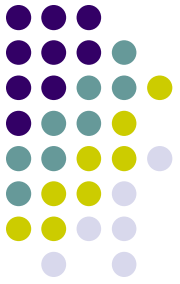
- Ficom - Finnish Federation for Communications and Teleinformatics
- ETSI MSS Mobile Signature Service
- ETSI MSS
 - TS 102 204, TR 102 206, TS 102 207

Service Provider Integration

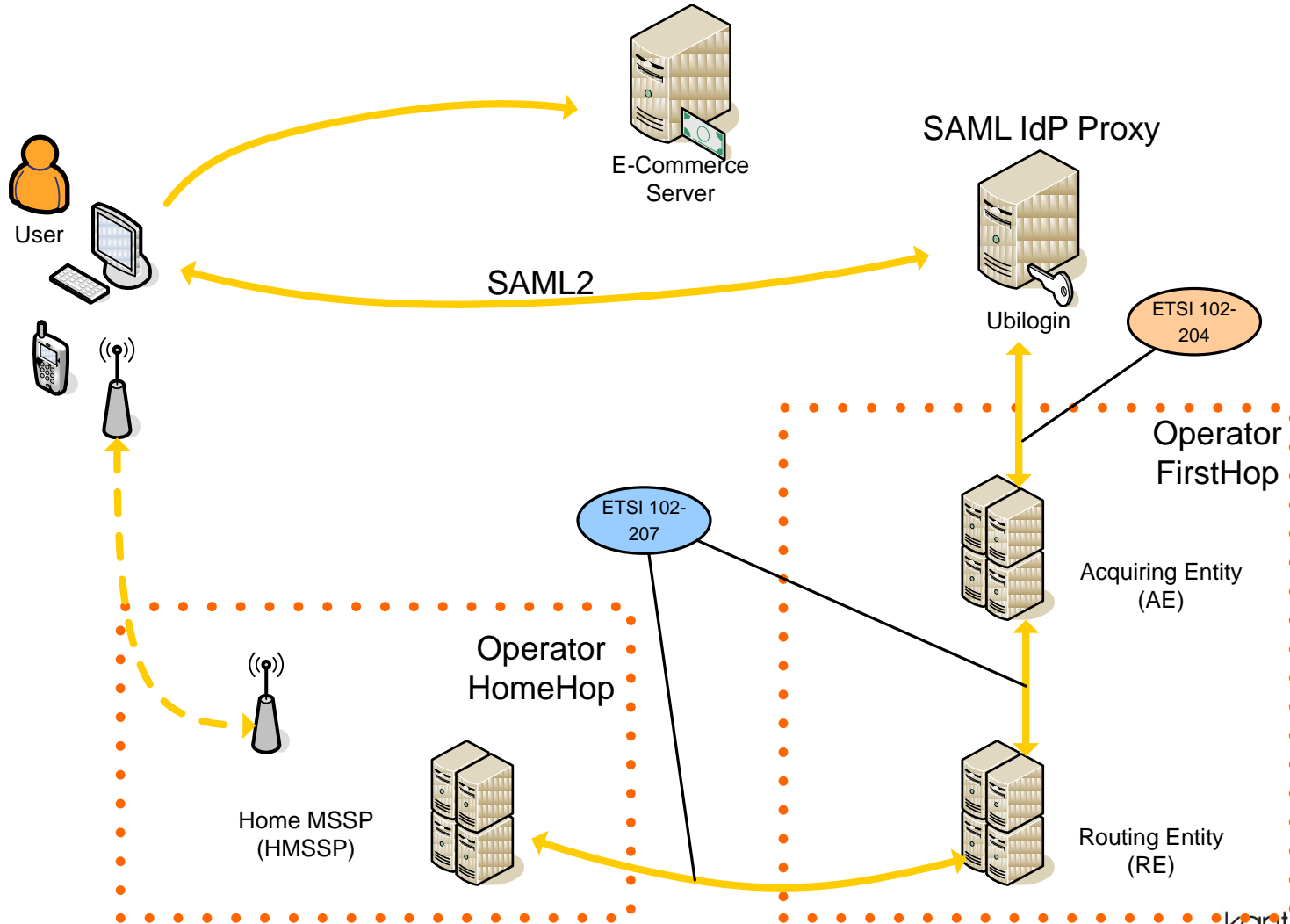
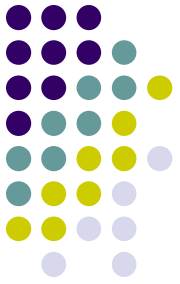


- Operator provided API
- ETSI MSS interface
- TUPAS Proxy (Emulate banking protocol)
 - Hosted by Service Provider
 - Operated by Telco
- SAML IdP Proxy
 - Hosted by Service Provider
 - Operated by Telco

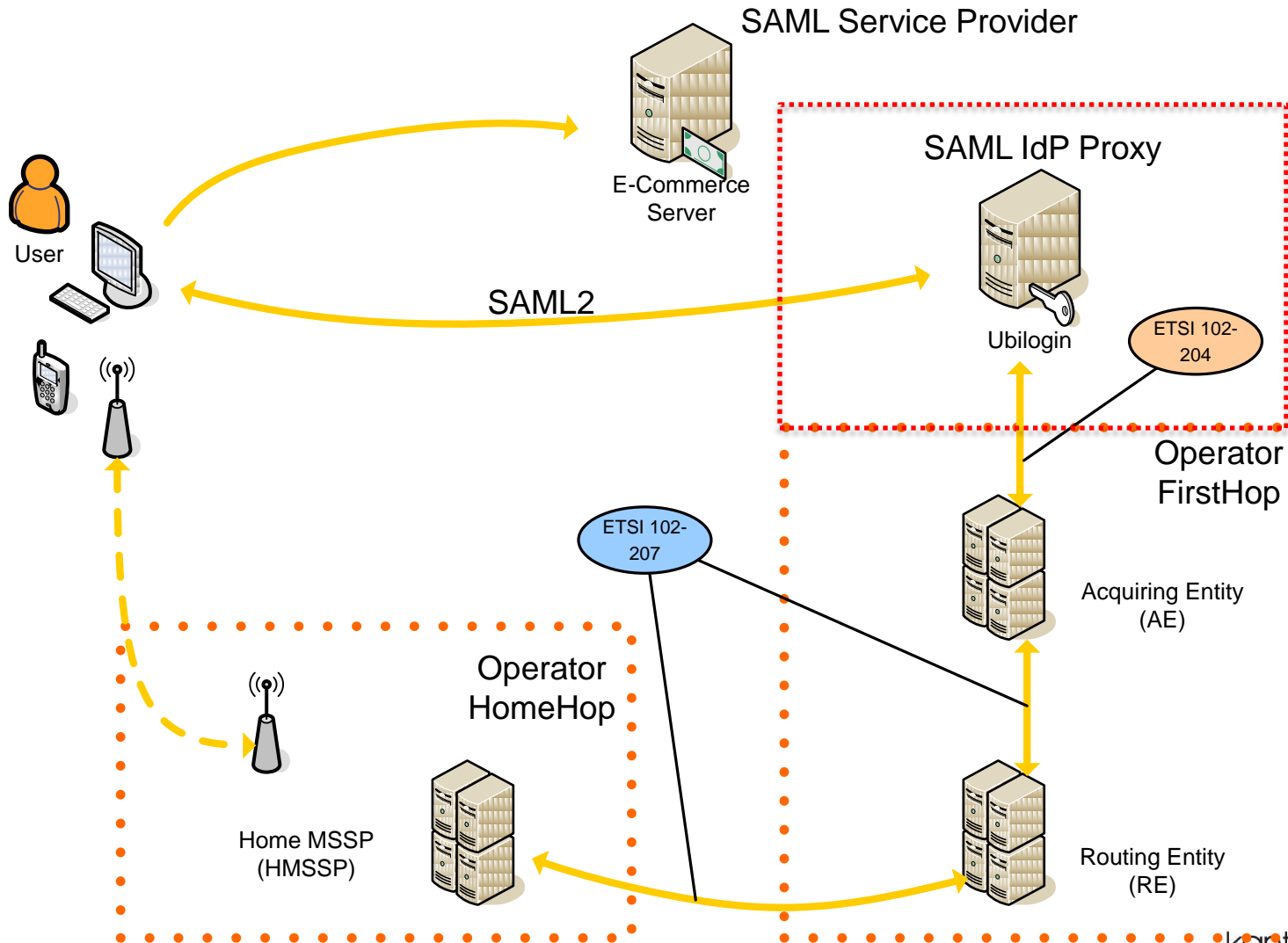
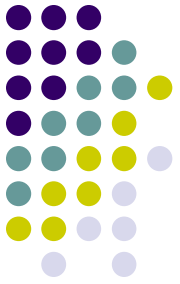
Architecture



Architecture



Architecture



Authentication during a call



- System permits a telephone operator (or automated IVR system) to perform an authentication request during a voice call
- Simtoolkit application does not interrupt call
- Eg, obtaining blood test results from a clinic

Commercial Identity Providers



Banks

TUPAS

Telcos

Mobile
Certificate

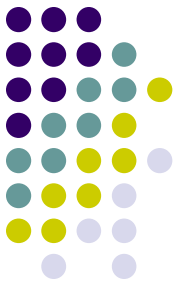
Government

eID Card

Summary



- Commercial rollout of mobile certificates has begun
- Standards-based architecture (ETSI MSS)
- "Operator roaming" thanks to federation
- One service agreement for relying party
- Leveraging existing identity value
- Ready market of existing services ready to adopt
- Competitive identity market



Questions / Discussion