FutureID - A Comprehensive Identity Management Infrastructure for Europe

Jon Shamah
FutureID
22/05/2014
FutureID - A Comprehensive Identity Management Infrastructure for Europe
FutureID – Shaping the Future of Electronic Identity

- Partially funded by EU FP7
- Collaborative Project (Large Scale Integrating Project)
- Start in Nov. 2012
- Duration of 36 month
- 19 Partners
- from 11 countries
- Coordinated by
  - Fraunhofer
Social Media: a Paradigm Shift in Identity Management

Before:
- Service Providers issue/manage identity
- Users obtain/manage one identity per service

Social Media:
- Service Providers reuse 3rd Party identities
- Users reuse their existing identity for new services
“Social Identities” have a limited Domain of Application

Legally Binding Transactions remain out of reach

Passwords

Tokens

Security

social media today

fun

social media tomorrow

Trust in Identity
Trusted and Secure Identities exist, but are locked into the old paradigm

Single service, significant effort, not worth-while!

Too costly, too small user base, maximum one type if really necessary

User

Service Provider
Trusted and Secure eIDs are also locked into the old paradigm

Few services, significant effort, not worth-while!

Too costly, Takes too long to fully deploy, maximum one type

User

eID Provider
Trusted and Secure eIDs are also locked into the old paradigm

Few services, significant effort, not worth-while!

Too costly, Takes too long to fully deploy, maximum one type

How can trusted identities be used with the new paradigm?
Objective for User

Number of necessary Credentials

old paradigm

social media

Number of Services

low trust services

high trust services

FutureID is partly funded by EU FP7 under GA n°318424
Objective for Service Provider

- The targeted user base has many different existing secure token types.
  - Example: European Marketplace of Services
    Many different national eIDs
- The cost of supporting a large number of token types must be contained.

Diagram:
- Cost vs. Number of Token Types
- Old paradigm shows an upward trend
- FutureID suggests a flat line for reduced costs
How?: ‘Traditional’ Federations match IDs to Services

most convenient token for user
How?: FutureID Transformer Component matches any ID to any Service

most convenient token for user

FutureID Infrastructure

single interfaces
Problem: BIG BROTHER IS HERE
Problem with Federations: A Centralized Infrastructure would help a Big Brother
We need Privacy Counter Measures
A Better Design: Decentralized and User-Centric

Explicit avoidance of central components / players

- Privacy
- Scalability / Availability
- Market oriented
- Flexible

ecosystem with free participation of an open number of stakeholders
The FutureID Infrastructure Overview

Free participation of an open number of stakeholders
Users
Credential Issuers (CIs)

Arbitrary credential technology:
• password
• one-time pad
• OTP device
• smart card
• privacy-ABC
• mobile
• etc.
Types of Identities

- certified by authority
- self-claimed reputation-based

Credential issuer

FutureID is partly funded by EU FP7 under GA n°318424
Users with Multiple Credentials
Service Providers (SPs)
Some SPs can directly consume user credentials

no intermediary required
Credential Transformers (CTs): Type 1: existing Identity Service Providers

- SAML
- WS-*
- OAuth
- OpenID
- ...

user credential

Session credential

CT
Authentication with existing Identity Service Provider

- IdSP transforms: user credential to session credential
- SP can directly consume session credential

SP and IdSP need to support the same federation dialect
Credential Transformers (CTs): Type 2: FutureID Brokers

- convert format
  - OAuth -> SAML
  - SAML -> WS-*
- convert semantics
  - cognome -> lastname
- filter
  - Name
  - Date of Birth
  - Address
  - SSN
- derive
  - date of B. -> age over 18
- combine attributes
  - role certificate etc.
Authentication with existing Identity Service Provider and one/several Brokers

- **IdSP transforms:**
  - user credential to session credential

- **Broker transforms:**
  - format that SP can consume
  - less privacy exposure
  - etc.

SP and IdSP need **not** support the same federation dialect

Within the limits of trust, any credential can be presented to any SP.
Who Controls Authentication Process?

Whom to trust:
• user credentials (CIs)
• CTs

Auth. Flow:
(within limits of trust)
• which user credential
• which CTs
• which attributes to disclose
Trust Scheme Authorities (TSA)
Maintaining Standards

SP/User Trust Issues:
- Difficult to determine trustworthiness
- Cumbersome to enumerate trusted entities

Trust Scheme Authorities:
- Regulation and oversight
- Certify CIs and CTs
- Define groups of CIs/CTs
  - EC qualified certificates
  - STORK level 3 credentials
  - Privacy-friendly CTs
FutureID Trust Infrastructure in Practice - solving the real operational issues

- Service Provider chooses Credential Issuers, existing Identity Service Providers and/or brokers, to rely upon
  - Enters into a number of bilateral trust relationships
  - Chooses depending on certification, reach and assurance levels
  - Can extend its market by adding more relationships directly or through FutureID brokers

- Users choose which credential and profile they wish to use from those offered by the service provider
  - Selection is dependent on what contracts the Service Provider has in place and which assurance levels are required
  - Users authenticate in their own trust domain using their token type of choice
Choice for the Citizen & Service Provider

High level visualisation - Examples Only

FutureID Broker

IdSP
Highlights of FutureID Trust Infrastructure

- Infrastructure fosters free participation of open number of stakeholders.
  - free market of “trust services”
- Interfaces almost any (trusted) credential with any SP.
- Flexible integration:
  - FutureID SPs and legacy federated SPs “as is”
  - variety of deployment options
  - Seamless integration with STORK infrastructure
  - Privacy-friendly Attribute-Based-Credentials (by ABC4Trust)
- Free from imposing any political or organizational structure; no centralized components or single point of failure.
- Privacy-friendly and (where possible) privacy-enhancing.
Contact

Jon Shamah
jshamah@ejconsultants.co.uk
www.futureid.eu