A Model for Privacy Enhanced Federated Identity Management

Rainer Hörbe, EUSTIX Alliance
Privacy Issues in Federated Identity Management
Technical Privacy Controls for FIM

Standard FIM (e.g. SAML WebSSO)
• Data minimization:
  • IdPs release only required attributes, only to authorized services
• Limited unlinkability between services
  • Identifiers are targeted
• Impersonation
  • (HoK)

PE-FIM
• Limited unobservability by TTP
  • IdP/AP talks to groups of services, cannot identify service
• Limited unlinkability between services
  • Messaging, payment and delivery are pseudonymized; e.g. IdP will proxy SMTP traffic from targets email address to registered one

Rationale for enhanced privacy: scaling federation across vertical sectors
Provide and evaluate principles, techniques, and tools to support and facilitate the development and evolution of software-intensive systems.

Architectural challenge: Technical controls to enhance privacy.
Options for technical controls
- Identity escrow (zero-knowledge proof)
- Late binding (separate authN from attributes)
- Proxy pool (hub+spoke with many hubs)
- User-based IdPs (PAD, IMI)
- Pseudonym SP, targeted attributes (PE-FIM)
The Privacy-enhanced FIM Architecture (PE-FIM) model proposes an approach to federated identity management (FIM) that is privacy-friendly with respect to the requirements defined above. It is based on a 3-tier architecture that is an extended hub-and-spoke model with privacy by design principles applied to it. The hub is called the service broker (SB) in this model.

The very outset of the PE-FIM model is the introduction of a secure pseudonymous channel to support requirements R1, R2 and R3. The desired property of this bidirectional channel is that an IdP and a SP, or two SPs, can communicate about a principal, where (a) the SPs are pseudonymous to the IdPs, (b) the principal is pseudonymous to the SPs and (c) the IdP’s and SP’s identities are vouched for by the certificate authority.

![Diagram of PE-FIM architecture]

It is assumed, but not shown in the picture above, that trust has been established between SP-SB and SB-IdP, using certificates or other means. The core constructs of the proposed model are:

1. A pseudonymous secure channel, which can be used for several purposes:
   - Transmit assertions from an IdP to an SP;
   - Transmit pseudonymous data about a principal between SPs;
   - Transmit security alerts or operations-related messages from the SP to the IdP;
   - Transmit application-level messages from the SP to the principal, relayed by the IdP using SMTP or another messaging protocol.

2. The secure pseudonymous channel is implemented using a mixture of brokered trust and end-to-end encryption.
   - All messages are relayed via the service broker (SB);
   - Pseudonymous secure channel
   - One-time certificates

![Diagram of message flow]

IdP trusts CA

Certificate Authority

Service Provider

Pseudonym SP

Identity Provider

Service Broker

message flow

pseudonymous secure channel

one-time certificates

message flow
Pseudonymous SP

3-tier architecture (hub-and-spoke)

Service broker (hub) does not see user attributes

SP issues one-time encryption keys signed by CA

Group signatures would work as well

Unobservability improves with number of services per Service Broker
Targeted Attributes (e-mail)
Targeted email for SP is targeted id @ SB
Targeted email for SB is targeted id @ IdP
SB, IdP act as MTA and rewrite address
Pseudonymous Payment & Delivery
Virtual credit cards
Intermediate PO-boxes(?)
Out of scope

Display names (could be first name + number)

IP-Addresses (need overlay networks)
What else?

The model can be applied to SAML BAE, WS-Trust and OIDC as well.

A profile for SAML looks like this:
(4) /AuthnRequest/extension/pefim:SPCertEnc/ds:KeyInfo/..
(6) /Assertion/Advice/EncryptedAssertion
Project Status

Development underway for PoC using OpenAM, Shibboleth and pysaml2

Demo @ EEMA/Vienna April 2014

Pilot project: EDI-federation in Austria