Integrating cross-border and cross-sector interoperability of personal identity and attributes

STORK, yourSAM

Alberto Crespo & Nicolás Notario

21/05/2014

CYBER SECURITY & PRIVACY FORUM 2014
Business challenge

▶ Authentication and authorization across national borders or across different circles of trust (identity federations) not sufficiently efficient and secure.
▶ Current solutions for attribute aggregation are not privacy friendly.

Solution

▶ Open source and standards based, scalable architecture for attribute mgmt. and authorization in service transactions that span different “circles of trust”.
▶ Technical integration with STORK – European member state infrastructure for cross-border authentication
▶ Customizable functionalities related to policies and auditing between components.
▶ Privacy-respecting audit function re-assuring end-users by providing full traceability and usage information.

Benefits

▶ Cost saving by placing components in the cloud (IDaaS).
▶ Convenience and usability for end-users.
▶ Increased trust leads to higher use of cross-border e-services.
Efficient and secure implementation of “cross border” processes will become a critical issue in Europe.
- Such processes involve various “circles of trust” (universities, government, citizens, and private organisations)

Trust Framework + central administration = domain
Trust Framework + distributed administration = federation
yourSAM - Main features

- **Attribute names translation**
The service providers do not need to translate their attribute names for the foreign service provider destination, the system does it automatically for the service provider.

- **Attributes provisioning across domains**
Different domains (public service, universities, industry) can exchange attributes potentially bridging heterogeneous protocols.

- **Attributes discovery service**
The service provider does not need to know where the required information is previously, the WAYF (where are you from) functionality informs about the data origin address.

- **Attributes management policies definition**
The user is allowed to set-up his own attribute exchange policies at different levels.

- **List as an attribute (SAML)**
SAML extension allowing to transfer list of objects within SAML.
yourSAM - Other benefits

- **Immediate access** to many services/apps from different ‘circles’.
- Use of **open standards** & **SEMIRAMIS / STORK** results.
- **Faster deployment** of novel services with **increased Trust between all players** (time-to-market minimised).
- Higher **data quality**, known **provenance** & **integrity** help prevent ID fraud/theft.
- End-to-end **data protection & security**
- Several eID types supported (incl. mobile ID).
- Move your trust ‘anchor’ to the cloud.
- **Cloud IaaS** for **on-demand, flexible provision of IAM services**
  - Privacy-enhancing IDM & attribute exchange, e.g. proof age.
  - Dynamic availability of resources, flexible pricing, cost efficiency.
  - Composability of ID services with other cloud services
  - User-controlled trust relationships with multi-level, fine-grained access control policy management.
  - Traceability for compliance: privacy-respecting audits
yourSAM - How does it fit with IAM solutions?

- **Classical IAM Solutions**
  - Focused mainly on authentication & authorisation issues.
  - Service access control is Admin-driven.
  - IAM infrastructures centred on employee mgmt. & access.
  - Not ready for managing partial identities of same individual.
  - Not ready for well-protected, interoperable, out-of-the-box attrib. exchange.
  - Not oriented to cross-domain, cross-border process implementation.
  - No explicit trust architecture enabling scalable iop, complexity abstraction.

- **yourSAM**
  - User defines policies to govern release of attributes.
  - **Scalability** is a MUST: need to deal with many more identities (partners, customers, providers).
  - Clear duties separation with context awareness.
  - Designed from start for interop., compliance & efficient attribute exchange.
  - ‘Circles of Trust’ built on explicit mechanisms allow confidence to build process chains linking citizens, public admins & enterprise.
  - New business models can be deployed faster!
Advantages of using STORK

▶ Secure & reliable electronic identification & Authentication of customers from many European countries using recognised eID schemes fulfilling regulatory reqs.
▶ Use of reliable sources for eID data & other attributes
▶ Open Standards & Licensing: SAML 2.0, EUPL v1.1 (nearly all STORK SW) + LGPL for Industry Adopters (no copyleft!)

Benefits for the Service Provider

▶ Easy to obtain guaranteed data, possibility to simplify procedures, privacy-friendly interactions (checked with Art. 29 Data Protection Working Party)
▶ Increased quality of data, reduction of fraud possibilities, standards-based
▶ Secure cross-border authentication at very little cost
▶ Improved user perception, increased trust

Other benefits

▶ Open to integration in standard LDAP / AD solutions (or any other)
▶ User always in control: Data Type/Value Consent
▶ No storage of personal data in STORK infrastructure
STORK / STORK 2.0

https://www.eid-stork2.eu/

3 year duration
2012 - 2015

19 participating countries 58 partners
STORK 2.0 will contribute to the realization of a single European electronic identification and authentication area by:

- building on the results of STORK
- establishing interoperability of different approaches at national and EU level,
  - eID for persons
  - **eID for legal entities** (representation)
  - the facility to **mandate** Establish and transfer the eID link between.
    - principal (natural / legal person) and
    - representative (natural person)
- more active on private sector services

**4 cross-border pilots**: eAcademia, eBanking, eGov Services for Business, eHealth
STORK Breakthrough eID Interop. Model: European Federated Circle of Trust

- eID- Interop. achieved through central (PEPS) and decentral (V-IDP) components
- PEPS / V-IDP hide national specifics for other countries, guarantee Scalability & Trust
- Communication between PEPSes and V-IDPs based on common specs
- Communications with SPs, IdPs and AP’s can follow national rules
- Electronic auth. process takes place at country where eID was issued: trustworthy data sources!

STORK connects the national circles of trust to the European layer of trust.
STORK Authentication Logical Flow

1. ask for service

2. go Stork!

Estonian service provider

3. select your country

Estonian Stork gateway “S-PEPS”

4a. consent?
4b. which e-ID?

Estonian service provider

5a. authentication
5b. consent (final)

Estonian Stork gateway “S-PEPS”

Spanish citizen

Spanish Stork gateway “C-PEPS”

e-ID + attribute provider (Spanish)
STORK – Integration with IDPs/APs & SPs

1. Citizen connects to Service Provider
2. Request connection to originating country authentication provider
3. Authentication (eID card, userid/password, OTP, ...)
4. Additional attributes gathering
5. Certified identity is sent to Service Provider
6. Service open to citizen

S-PEPS  C-PEPS

Service Provider Interface

National eID interface

User Interface

Authentication Portal

Stork National PEPS

Stork National PEPS

Attributes Providers

Identity

SP Integration Package (LPGL)

MS. Int. Package (EUPL)
STORK Demo: Access of a citizen to a foreign eDelivery portal
Thank you

alberto.crespo@atos.net
nicolas.notario@atos.net

Atos, the Atos logo, Atos Consulting, Atos Sphere, Atos Cloud and Atos Worldgrid, Worldline, blueKiwi are registered trademarks of Atos Group. May 2014
© 2014 Atos. Confidential information owned by Atos, to be used by the recipient only. This document, or any part of it, may not be reproduced, copied, circulated and/or distributed nor quoted without prior written approval from Atos.

21/05/2014