The Role-ID project

Kantara meeting Munich
April 13, 2012

Mikaël Ates
Entr'ouvert

entr'ouvert

Outline

entr'ouvert

Label and funding

- Research project funded by Eureka, ITEA 2 programme.
- Started in october 2009, end in september 2012.
- French and finnish partners.
- Thanks to the French DGCIS that funds the French partners.

Partners

France

- Cassidian (EADS)
- Entr'ouvert
- Evidian (Bull)
- Ilex
- Swid
- Telecom Bretagne engineer school

Finland

- Insta DefSec Ltd
- Ubisecure
- University of Eastern Finland
- University of Oulu
- VTT Technical Research Centre of Finland

Motivations

For organisations, main issues towards identity are consisting of two points :

- They must manage a great complexity : a great number and a disparity of users, teams, divisions, enterprises, applications, services, intranet, extranet, roles, job functions, etc.
- They are changing continuously : frequent re-organisations, mergers and acquisitions ; people changing their job function ; international, European or national regulation changes ; etc.

Goal

- To address these issues, role-ID develop an organisation-oriented identity extension based on a role-centric vision.

Objectives

- Introduce an innovative concept of function in identity that will improve notions of context sharing and delegation.
- Introduce a new concept of virtual user that will allow a rich dynamic role attribution.
- Develop new means for organizations to modelling a great complexity of identities and roles.
- Adapt and improve the existing methodologies to administrate complex organisations identity database.
- Provide enhanced tools for identity provisioning that are relevant to the real life constraints.

Main concepts

Role

- Set of permissions : permission(engineer, read, access_control_manual)
- Role are assigned to users : assign(mikael, engineer)
- is_permitted(X, Y, Z) if assign(X, A) and permission(A, Y, Z)

Main concepts

Function

- Applications commonly behave relying on functionnal roles (for instance, administrator of function abc).
- These roles may have permissions externally defined and low level roles may be assigned to those functionnal roles or those functionnal roles may herit from low-level roles.
- Some users may have multiple functionnal roles and may choose which one to use.
- Some users may be able to use the application sessions of other users with the same function.
- Unknown users of third organization should be able to dynamically obtain a function.

Main concepts

Function

- Those functionnal roles are called functions.
- When a user logs in an application, the most important is its function.
- The user identifier is only used for accounting.
- The applications serve the service according to the functions and if necessary ask permissions to an access control decision point.
- Two users with the same function have the same permissions.

Use case

- Crash scene, the need to identify the victims.
- A national agency makes available to the stakeholders (firemen, medical staff, police, etc.) a web application accessible from mobile devices such as tablet PCs or smartphones.
- According to their habilitations, the stakeholders are authorized to consult or add information on victims, including for instance medical diagnosis.

Use case

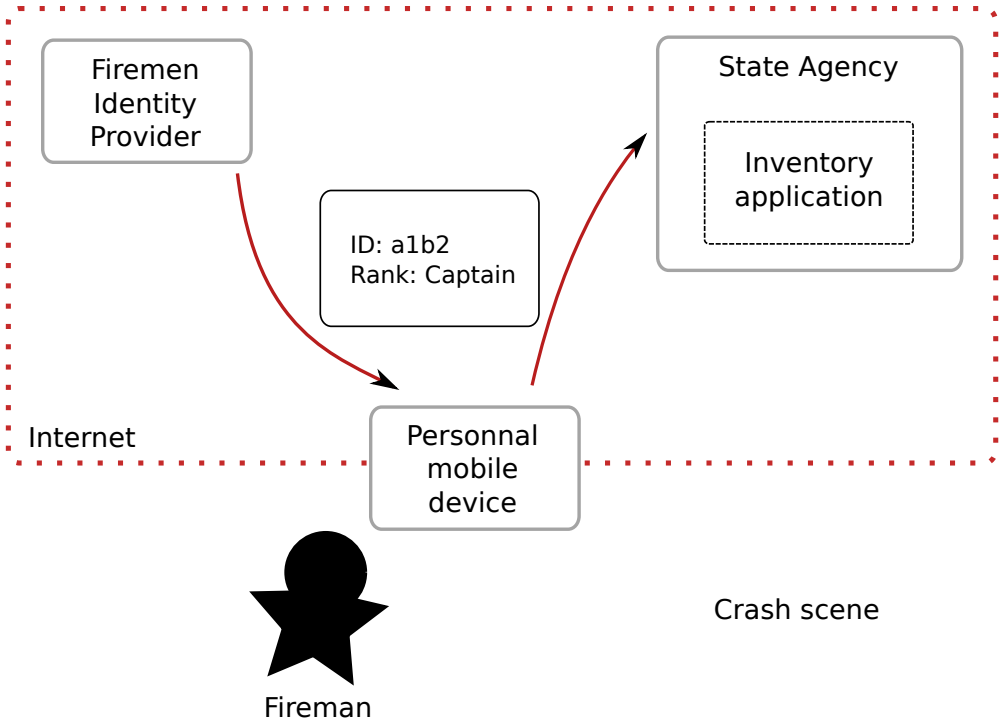

FIGURE: Identity proving on the crash scene.

Use case

The functions the public agency is able to define for the stakeholders of the use case are the following :

- Veiwer without medical clearances (VNMC) : able to look at the administrative records, without medical data, of the reported casualties.
- Viewer with medical clearance (VWMC) : able to look at the administrative and medical records of the reported casualties.
- Data entry operator without medical clearances (ONMC) : able to entry the administrative records of the reported casualties. but no medical data.
- Data entry operator with medical clearance (OWMC) : able to entry the administrative and medical records of the reported casualties.
- Medical coordinator (MC) : able to assign a victim to a hospital.
- Operations coordinator (OC) : able to generate and publish statistics.

Use case

Attribute-based user-function assignment

- $Attribute ::= organization, rank$
- $Role ::= VNMC, VWMC, ONMC, OWMC, MC, OC$
- [...]
- $Rule_i :: organization = police\ AND\ rank = officer \rightarrow ONMC$
- $Rule_{i+1} :: organization = firemen\ AND\ rank = firefighter \rightarrow ONMC$
- [...]
- $Rulej :: organization = medic\ AND\ rank = doctor \rightarrow MC$
- $Rule_{j+1} :: organization = police\ AND\ rank = captain \rightarrow OC$
- $Rule_{j+2} :: organization = firemen\ AND\ rank = manager \rightarrow OC$
- [...]

Use case

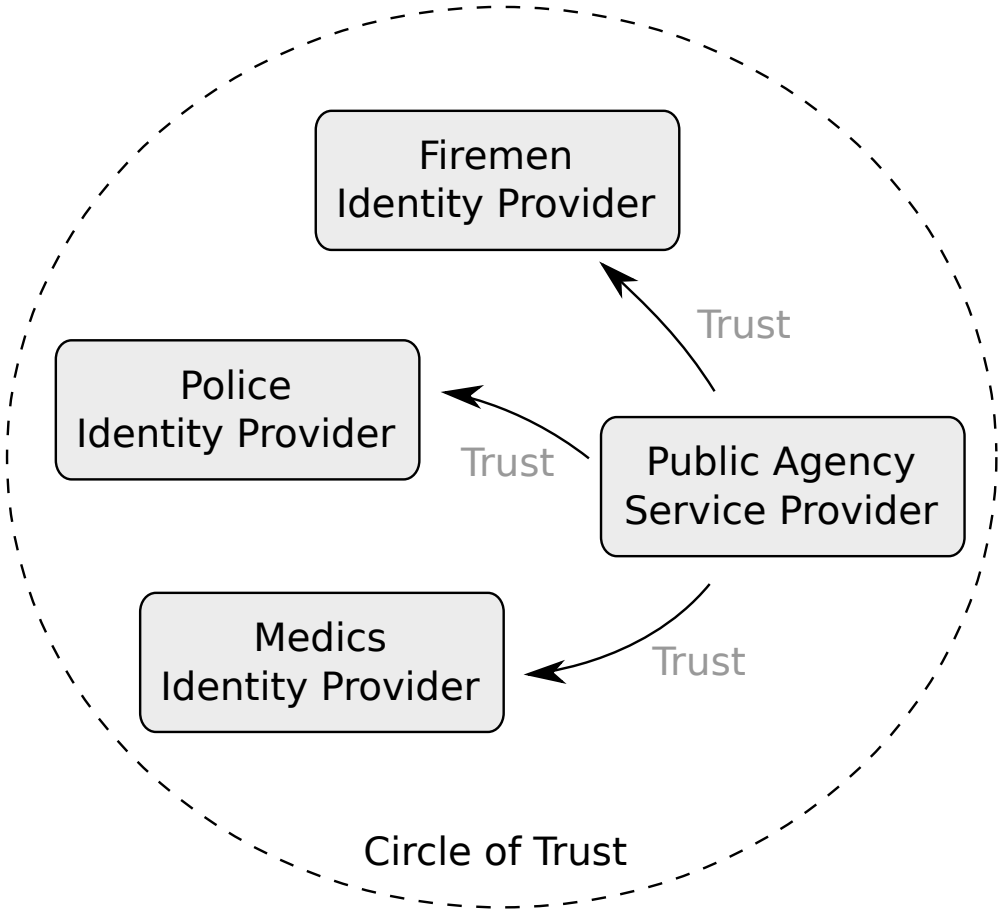

FIGURE: The use case circle of trust.

Use case

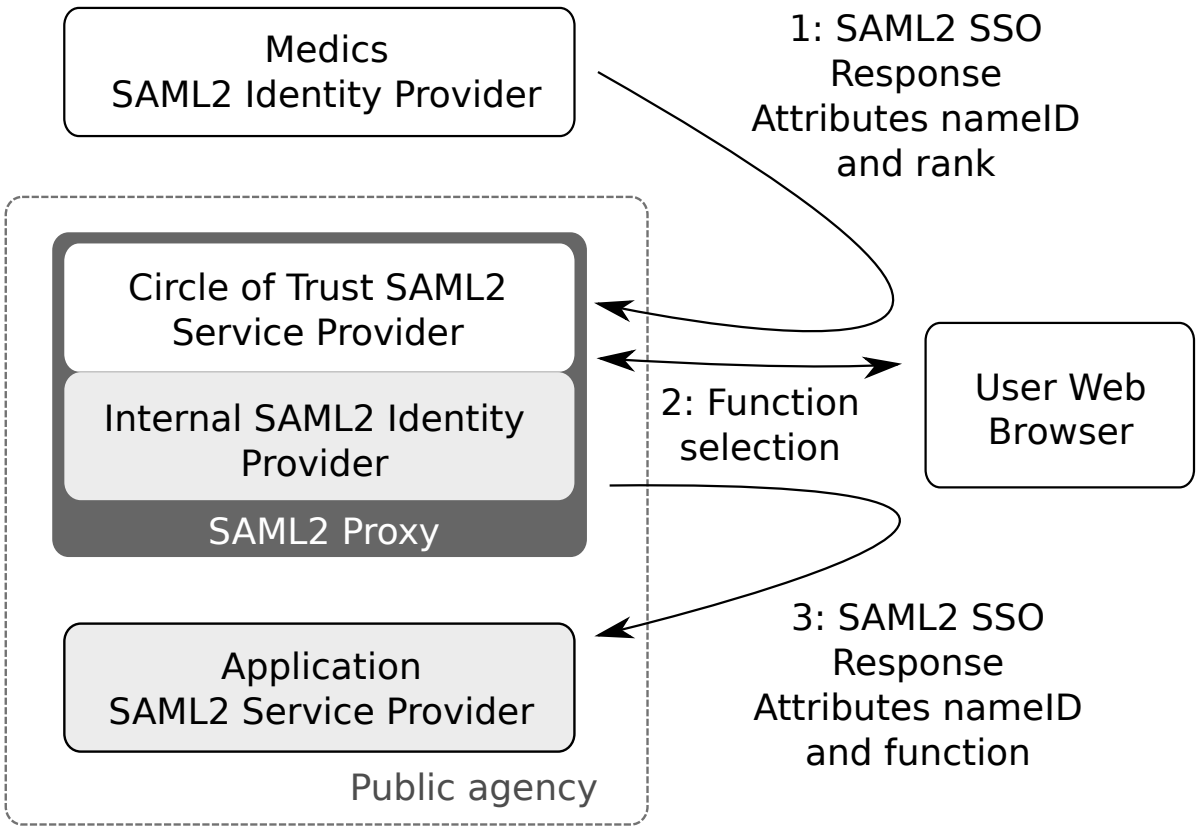

FIGURE: Technical architecture based on SAML2.

Use case

Handle user sessions capturing cookies with a reverse HTTP proxy.

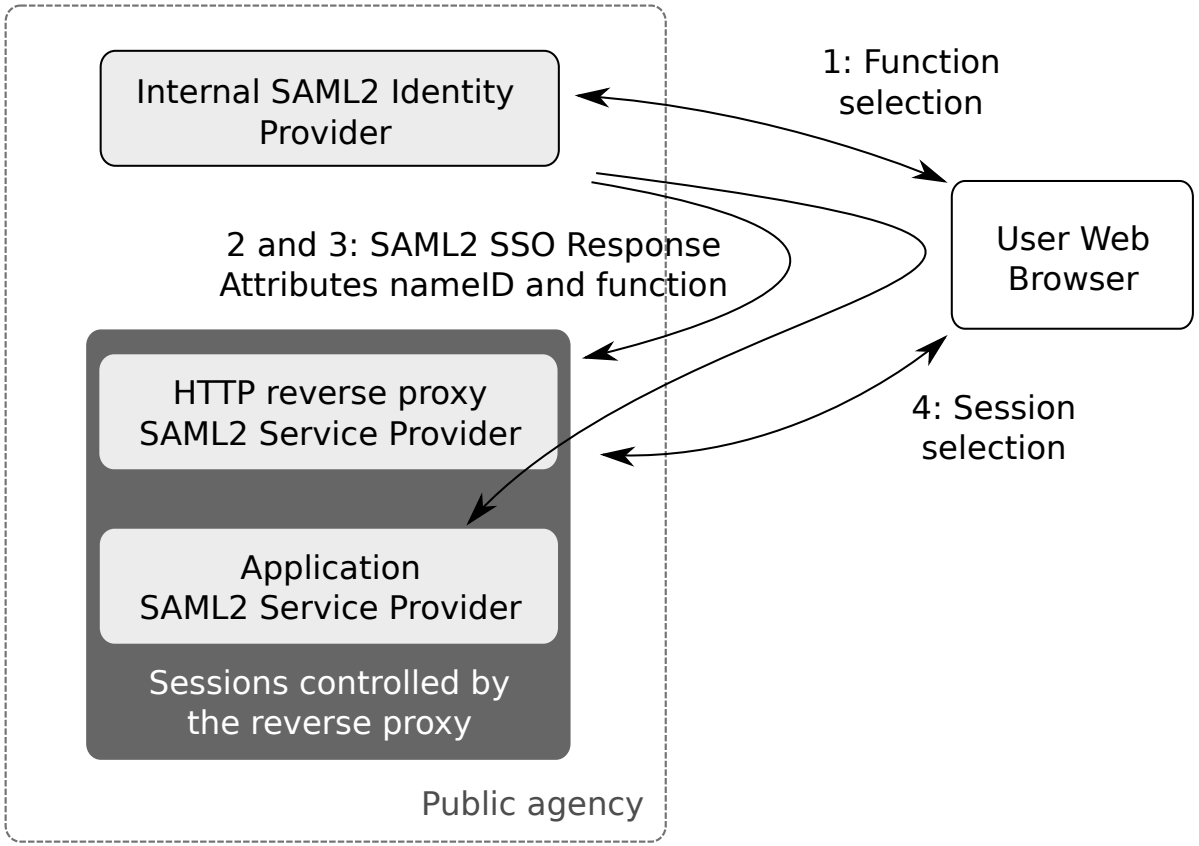

FIGURE: Handle sessions with a reverse HTTP proxy.

entr'ouvert

Use case

Provide users with a graphical interface to the mapper of the user sessions with the application sessions.

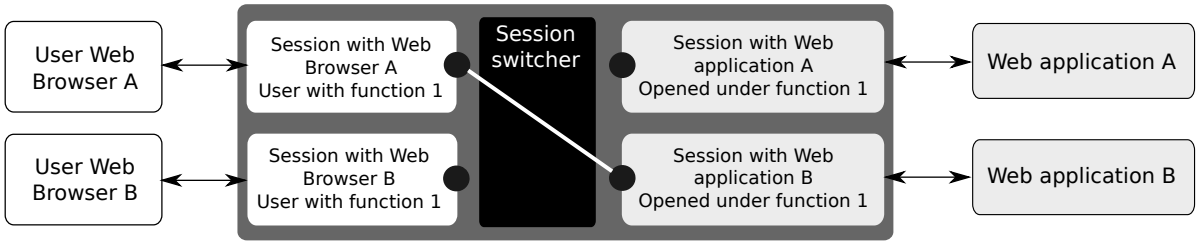

FIGURE: Handle sessions with a reverse HTTP proxy.

entr'ouvert

Platform

- Authentic 2 used for all the SAML2 identity providers and the SAML2 proxy.
- The function management module is added to Authentic 2 for the demo only.
- Mandaye is used as SAML2 reverse HTTP proxy.
- The session management module is added to Mandaye for the demo only.
- The inventory application is a quite empty Django application.

Demonstration

Go to http ://service.roleid.entrouvert.org :8000

entr'ouvert