Service oriented authorization

Babak Sadighi
Axiomatics AB, Sweden
Background

- Based on research project in collaboration with Ericsson Research
- Issue: How does standardized authorization management support SOA in telecom networks
  - Based on XACML
  - Both at the service and at the device configuration level
What is service oriented authorization?

- Authorization as a service to other applications and services
  - Externalized from applications
    - No need to deal with authorization logics in application code
    - Policies controlling actions on several services – covering dependencies among these services
New services from operators

- Network operators can provide base functions and infrastructure services to enable new services
  - Service providers become operators’ customers
    - Example: location based services
- The issue is that: Service providers have different requirements
  - Require different degree of control over the service
  - Different policies with respect to configuring and accessing the service data
Service Oriented Authorization

Operator services

IAM services
- Authentication & Id. Federation
- Authorization

SMS Service
Loc Service

TV Service
News Service
Parking Service
Music Service
Managing and controlling services

- **Operators** need to manage the service delivery efficiently
  - As much as possible independent of service provider
  - *Avoid micro-management of services and features on behalf of the service providers*

- **Service providers** need to control their services efficiently
  - According to their SLAs
  - Define fees
  - Manage users/user classes
  - *Natural mapping of own organization/authority structure to service management*

- **End users** need to define their constraints on the use of their services
  - Privacy control
  - Usage control
  - Parental control

- Partly an access policy issue: Control & management of a service is partly exercised by granting or denying access to service parameters and service data
Access permissions

- **End-user** access to service
- **End-user** administration of service parameters (user preferences), check status of service, history, account balance, etc.
- **End-user** management of privacy preferences, per service or for all services
- Paying party (may be **end-user**) access to service constrained by restricted usage, max charging, etc.
- **Service provider’s** application access to operator service capability
Access permissions

- **Service provider** access to end-user data (phone no., location, etc.)
- **Service provider** administration of service capability usage of its own applications
- **Service provider** administration of end-users, defining user attributes, tariffs, etc.
- **Service provider** administration of its SLAs
- **Operator** administration of SLAs with service providers
- **Operator** management of service delivery system
Example: parking service

1. Parking info?
2. Location info?
3. Location.
4. Parking info.
Example – access permission

- SP: Does the user have the right for the requested service?
  - Differentiated services based on:
    - Time
    - Type of parking
      - Fee
      - Parking company
      - Indoor/Outdoor
    - Area (Downtown)
Example – access permission

Op: Does SP has the right to know the user’s location? (privacy)

Based on:

- Time
  - Only during working hours

- Location
  - Only with the downtown area
Issues

To realize service oriented authorization we need to address the following issues:

- Policy enforcement
- Policy administration
- Attribute management
The Enforcement Issues

- Where should the various access control aspects be enforced?
  - At the service provider
  - At the operator

- The enforcement can be outsourced to the operator if the operator is trusted by the service provider.
Attribute management

- Who shall provide which attributes?
- How do we validate the provided attributes?
  - We need policies governing attribute authorities and attribute assertions.
Policy management and administration

- Who does the policy management?
  - The service provider
  - The operator
  - The end-user

- Each party shall be empowered and facilitated to manage its own policies.

- The operator shall provide a policy management tool for the other parties.
Possible architecture
Delegation profile of XACML 3.0

- **Delegation profile:**
  - XACML policies constraining creation and modification of XACML policies.

- **Delegation facilitates decentralised administration of access policies, letting consumers, service providers and operators to define and manage access policies in their own authority domains.**

- **Necessary feature**
  - To reduce the lead-time in policy administration
  - To reduce the administration overhead for operators
  - To create trust and control for each actor in the service delivery chain
Summary

- Authorisation service shall be provided by operators to service providers as a base infrastructure service and business enabler.

- XACML as a standardised authorisation language and architecture is a suitable choice.

- XACML 3.0 can play an important role to simplify policy management in a chain between the operator and the end-consumer.