Delegation of Access Rights in Multi-Domain Service Compositions

Dr. -Ing. Ulrich Pinsdorf
European Microsoft Innovation Center
Aachen, Germany
European Microsoft Innovation Center

- Founded in May 2003
- Located in Aachen, Germany
- 40 employees, growing with projects
- Project based, collaborative, applied R&D, timeframe 3 to 6 years
- Collaborative nature allows Microsoft to share its technology expertise, to learn from and to develop stronger relationships with technology partners, universities and governments in Europe
Alice “owns“ services from various sources: Personal services

Services are operated by different vendors, but Alice manages them

Contoso and Adatum do not trust each other

Alice combines services into new composite service

Alice wants to give Bob access permissions
Examples for personal services

- Social networking
- Online calendar
- Picture gallery
- Personal location
- Shared mail folders
- Personalized news feeds
- Health information
- Web storage
Bob accessing the composite service means Bob uses Alice’s personal services.
Access control prevents Bob from doing so.
Except Alice configures each service individually.
That’s where the security mess starts...
Issues in Multi-Domain Scenarios

- Multi-Domain implies
  - No mutual trust and hence no Single-Sign-On
  - Different access control mechanisms

- Large diversity in access control
  - AC concepts and user experience
  - Representation of subjects (authentication)
  - Expression of policies (authorization)

Examples
- X.509 based Access Control List
- Google Calendar API based on Google accounts
- Claims-based authentication with XACML
Issues in Multi-Domain Scenarios

Problem #1: User experience for AC management
- Delegation means managing AC policies
- Alice needs to do that for each service
- Alice needs to understand all UI

Problem #2: Pollution of business logic with AC details
- Business logic of composite service should not be mixed with AC details
- AC unknown at design time in case of ad-hoc service composition
**Trend**

**Application-specific Delegation**
- Google calendar
- Yahoo calendar
- Exchange
- Telco location service
- Car GPS
- Groove
- Messenger
- Skype
- ...

**Principle:** delegator can delegate access to resource

**“Delegation Systems”**
- SecPal
- OAuth
- ADFS
- Liberty (SSO)
- XACML (PEP/PDP)
- Shared/cloud STS

**Principle:** resources adapt to Standardized system.

**Delegation Metasystem**
- AuthZ STS (ADFS v2)
- ACL

**Principle:** there are multiple systems → delegator has to be flexible.

**This work**
Personal services are becoming common
Service composition across trust domains will become every day life
Delegation is an essential feature
Variety of access control is a roadblock
  a) Users have to deal with multiple AC UI
  b) Ad-hoc service composition is almost impossible due to unknown AC
Standardization helps, but variety will never totally disappear
Abstract Delegation

1) Requirements
2.3) Token

2.1) Issue Token
2.2) Manages
4) Revoke

0) Owns
3) Accesses

Delegator → Delegatee → Resource
Delegation Framework

- Easy service composition
- Offers unified UI
- AC abstraction
- Personal service comes with AC type
- Plugins extend Delegation Framework

Resource abstraction
- Typed personal services
- Composite service requires service type
Delegation Plugins

- Policy manipulation ("delegation")
- Management channel
- Channel between delegator and delegatee
- Authentication mechanism
Sample Plugins

- **SecPAL**: claims based policy language, plugin creates new tokens for delegatee
- **Security Token Service**: SAML tokens based on an X.509 ACL, management via WS-Trust
- **BizTalk STS**: BizTalk Services Identity Provider, similar to above but applied on public legacy STS
- **Google Calendar API**: shows integration of non-SOAP legacy applications
- **Fingerprint**: shows applicability on non-web service resources (SOAP/REST)
Unified User Experience (1)
Unified User Experience (2)

Identities / Subjects

Quick Overview

Individual Details
Delegation

Types of delegations
- Delegatee-driven
- Delegator-driven

Delegation Mechanism
- Chain of Credentials
- Policy Manipulation
- Hybrid
Discussion

Advantages

- Allows delegation in multi-trust scenarios
- Allows various forms of delegation
- Supports ad-hoc service composition
- Unified user experience for delegation
- Deals with various subject representations

Disadvantages

- Framework on delegator’s side
- Services have to provide additional meta-data to support ad-hoc service composition
Service Centric Systems Engineering
Research project funded by EU FP6
Sep 2004 - Aug 2008
Follow-up of PRIME
EMIC‘s role: privacy aspects in service composition
Website: secse.eng.it
Enigneering, IT
CEFRIEL, IT
Centro Ricerche Fiat, IT
City Univerity London, UK
CA,
DaimlerChrysler, DE
Microsoft (EMIC), DE
European Software Institute, ES
KD Software, CZ
Lancaster University, UK
Groningen University, NL
ATOS Origin, ES
Telecom Italia, IT
Telefonica, IT
University of Sannio, IT
MIP, IT
University of Athens, GR
Foreca, FI
PrimeLife

Privacy and Identity Management in Europe for Life

Research project funded by EU FP7

Mar 2008 - Feb 2011

Follow-up of PRIME

EMIC’s role: privacy aspects in service composition

Website: www.primelife.eu

IBM Research, CH
Microsoft (EMIC), DE
SAP AG, DE
Giesecke & Devrient, DE
ULD, DE
CURE, AT
W3C (GEIE ERCIM), FR
University of Bergamo, IT
University of Karlstad, SE
University of Milano, IT
University of Frankfurt, DE
TU Dresden, DE
KU Brabant, NL
KU Leuven, NL
Brown University, US
Contact

Laurent Bussard
Anna Nano
Ulrich Pinsdorf

European Microsoft Innovation Center
Ritterstraße 23
52072 Aachen
Germany
T +49 (241) 997840
F +49 (241) 9978477
{lbussard|annaw|ulrichp}@microsoft.com