Secure Collaboration in Virtual Organizations

Conference Impulse

The research leading to these results has received funding from the European Union’s Seventh Framework Programme (FP7/2007-2013) for CRYSTAL – Critical System Engineering Acceleration Joint Undertaking under grant agreement n° 332830 and from specific national programs and / or funding authorities (BMBF 01IS13001E).
Goals of CRYSTAL:

- Reduce or eliminate obstacles to working together by addressing:
  - Interoperability
  - Transport of Data
  - Security / Authentication

Problem:

- Not all parties would like to use IOS/OSLC as a mechanism to realize collaboration between companies
- The question is why?

What is slowly recognized:
It is actually the Virtual Organization (VO) that brings out the product

standardization encompasses all three
Two Views on Virtual Organizations

- **Federation of Services or Asset Space?**

**Hypothesis:** People who do not want to use OSLC/IOS take the „value asset oriented“ perspective
Virtual Organizations taking the „Federation of Services“ approach mainly intend to improve shared use of expensive resources.

- Clouds (Externalization)
- Federations

Federation of Services can contribute positively to organizational interoperability

Creates a de-facto uniform domain
Virtual Organizations taking the Value Asset perspective do care about quite different things:

- Deployment and conversion of capabilities (data and functions) onto heterogeneous IT infrastructure
- Rely on a generic channel concept (rather than TCP/IP connections) which must be safe → IT infrastructures may never touch
- Enforcement of usage rules for assets „in the wild“
- Rearranged trust relationships → requires own security concept
- Minimze need for common technical standards and legacy
- Want to detect corruption or reduced trust like „heat peaks“ in a „cooling chain“

VOs valuing their critical assets

Physical Organization

Virtual Organization

Admin +

Local Developer +

Remote Project Leader +

seek equivalence for purpose

Trust
Security in OSLC follows Federation of Services approach

- Security in OSLC relies on existing technologies
  - Physical Security
  - Transport Layer Security
  - Domain Authentication via HTTP Basic Auth, Forms or OAuth

In theory, data never leaves control of owner

In truth, data can go anywhere

OSLC requires network
OSLC Flavors, Security and Interoperability

- OSLC standardizes a tall stack of technologies:
  - TCP/IP Networks
  - Encryption Layers
  - HTTP Protocols
  - RDF/S and XML
  - LDP Specifications
  - OSLC Ontologies and Concepts
  - OAuth
  - JavaScript Features
  - Other unnamed W3C Specifications

by experience strongly glued technologies do inhibit various kinds of innovation

the taller the stack of technology to be standardized the more brittle it gets

Example: problematic authentication with OSLC
Quick Help with the OSLC/IOS Gateway

- Design of OSLC/IOS is not going to quickly change
- CRYSTAL WG on ReqIF and Security considers VO/IOS Gate

Company R

Company S

Note: type refers to some IOS service type
What could be done in the long run?

Introduce a new kind of interoperability layer that takes care of transport, transformation and VO security

Advanced Integration and Interoperability Layer for Virtual Organizations in Critical Industries

enabler technology required but OSLC is not designed for this
Thank you for your attention!

M.Sc. Aleksander Lodwich
Software Engineer at ITK Engineering AG
aleksander.lodwich@itk-engineering.de
+49 711 933157-393