

WS-Federation in TrustCoM und BREIN

2. D-Grid Security Workshop
28. März 2007, Göttingen

Dr.-Ing. Christian Geuer-Pollmann
European Microsoft Innovation Center (EMIC)
Aachen

Agenda

- What is Microsoft EMIC?
- Security management challenges in Vos
- SAFe – A pluggable STS
- Some deployment options
- SAFe Development Overview
- Future plans

Security management challenges in virtual organizations

Security-management challenges

- We work with many partner organizations, our employee assignments to projects (VOs) may change frequently
 - We don't know all colleagues from other companies
 - identity and access mgmt is difficult to get right
- Security needs to be managed in a distributed way
 - We must ensure privacy for our employees when they access remote resources
 - We need assurance when remote users access our services

Security-related challenges (II)

- Security management – Who does it?
 - Need to find appropriate abstraction so that the I&A mgmt can be understood and done by the business owner
- Different VO membership models are possible
 - Static vs. dynamic partner sets
 - Varying infrastructure support (central repositories)

Our goals were...

- Enable people in different organizations to easily share services
- Dynamic
 - Collaborations across organizations created as necessary
 - Minimal out-of-band overhead for administrators or users
- Secure
 - Make it more secure for IT groups by making it more manageable
- Intuitive
 - Each federation is based on trust between humans

Our (EMIC) beliefs regarding collaboration

1. Trust across organizations depends on people who trust each other
2. Whoever makes a decision should have the tool to enforce that decision
3. Collaborations must be visible and manageable inside the company



The corporate STS's contact database for EPR/tokens



Scoped Federation



MS\EUROPE\chgeuer



We have a collaboration with Contoso. From our side, I (EUROPE\chgeuer) own this collaboration. The collaboration UUID is 0xdeadbeef.

Here's their STS contact.

We have a collaboration with Microsoft. From our side, I (CONTOSO\Carol) own this collaboration. The collaboration UUID is 0xdeadbeef.

Here's their STS contact.

CONTOSO\Carol

Enact collaboration inside the organizations

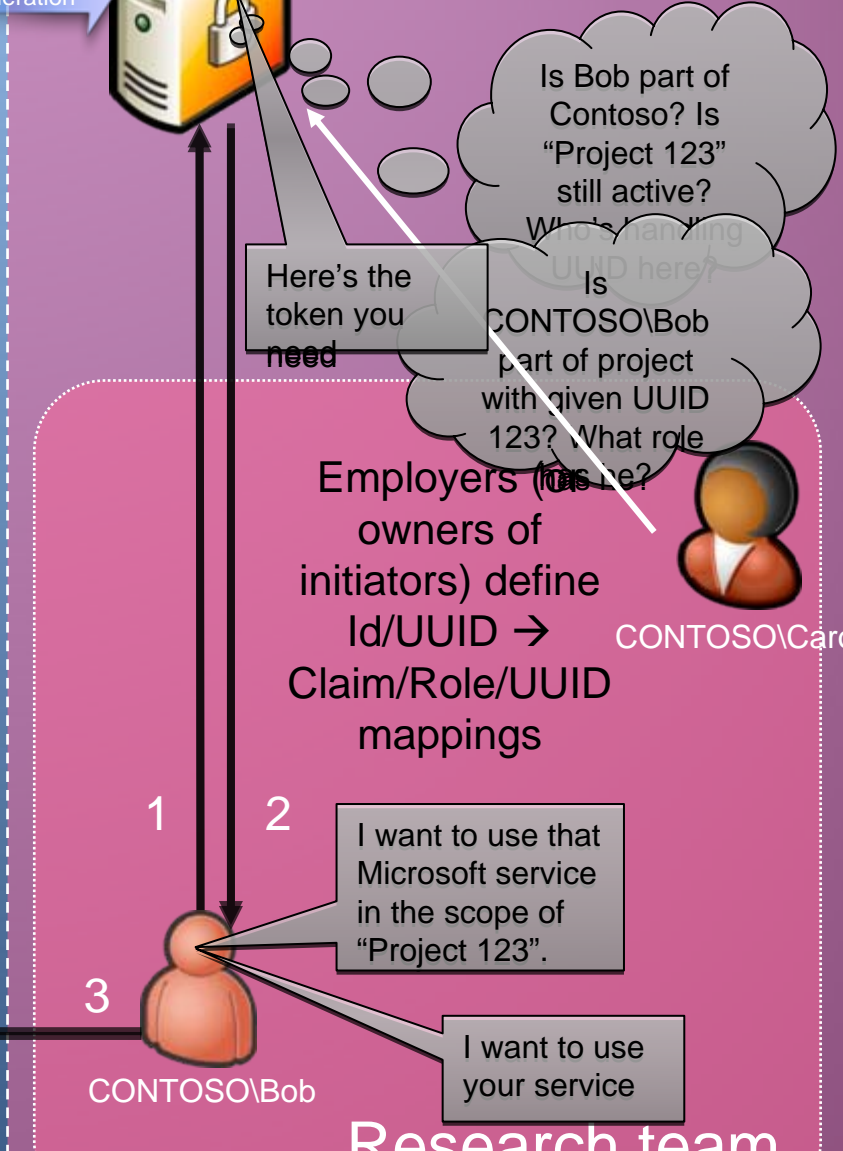
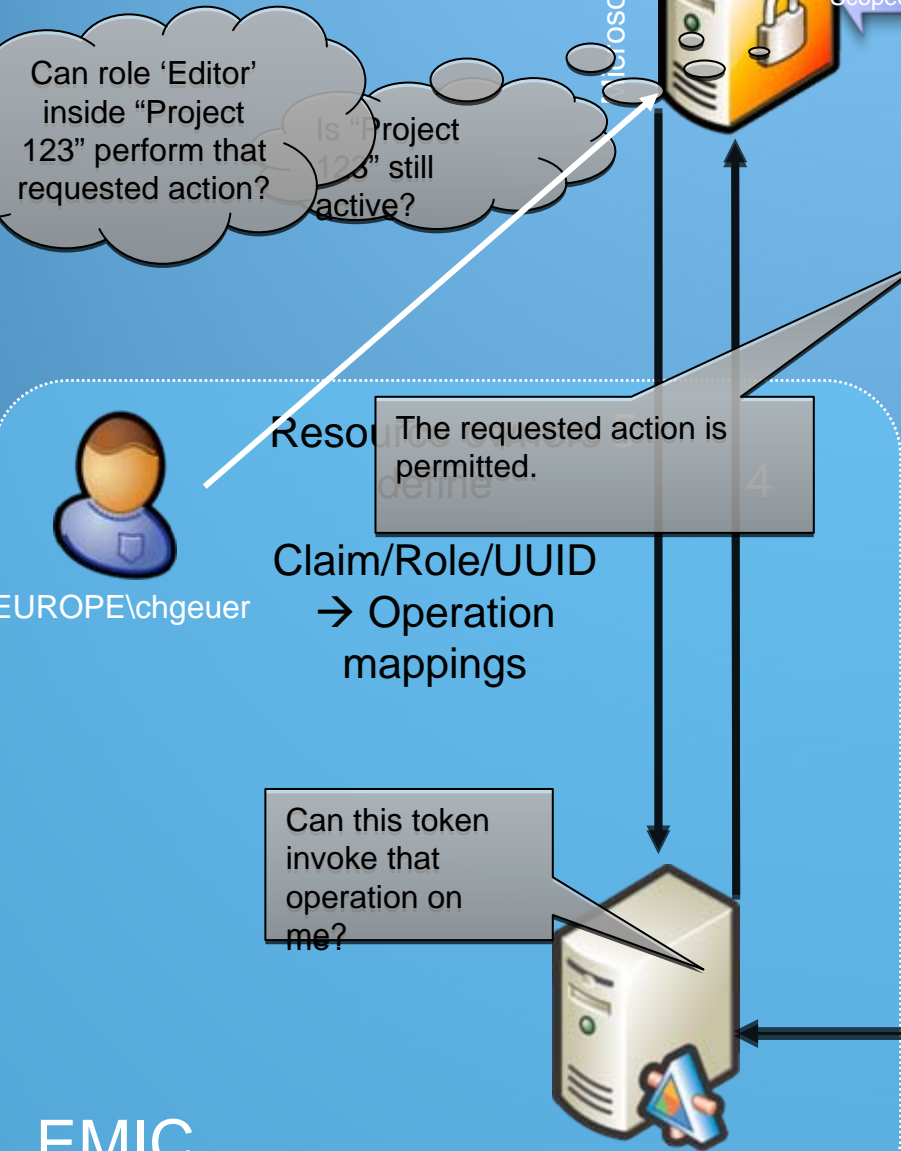
Microsoft

© 2007 European Microsoft Innovation Center

Contoso

Microsoft

Contoso



Scoped Federation

Microsoft

Contoso

Travel agency

Fabrikam



Scoped Federation

Scoped Federation

Scoped Federation



REDMOND\stevb

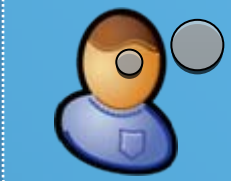


REDMONDITG

Is somebody in my organization here working together with Contoso? Hm, I see that EUROPE\chgeuer has a collaboration with them. I'll mail him what EMIC is doing there.

Fabrikam has had a virus run through their network. I'm going to stop the federation with them until we know it's safe

What Collaborations from me are still active? Hm, why are we still federated with that 'foobar' proposal? I thought we've dropped it. I have to delete that federation immediately.



EUROPE\chgeuer

EMIC

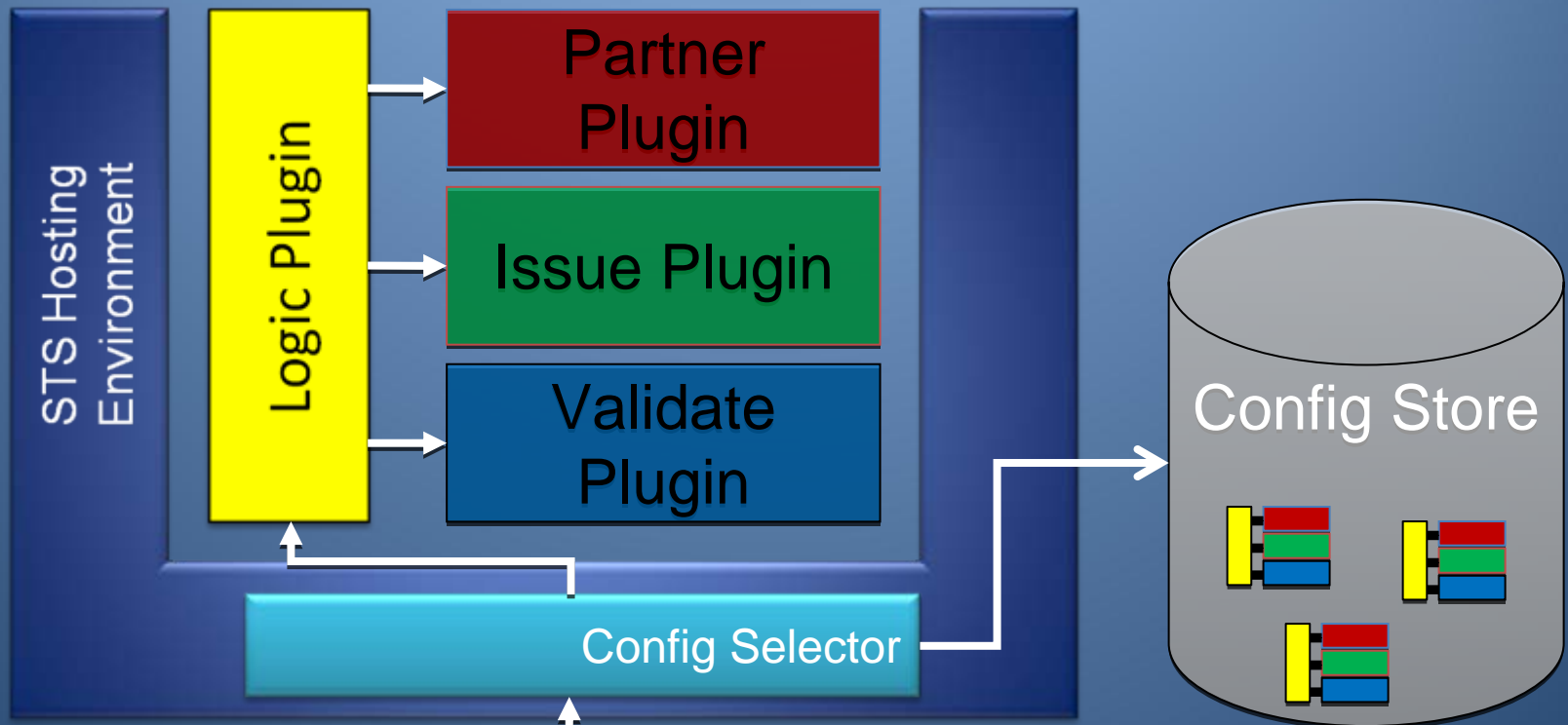
The STS is the central point of control for an organizations collaborations – the main fuse!

“Scoped” Federations

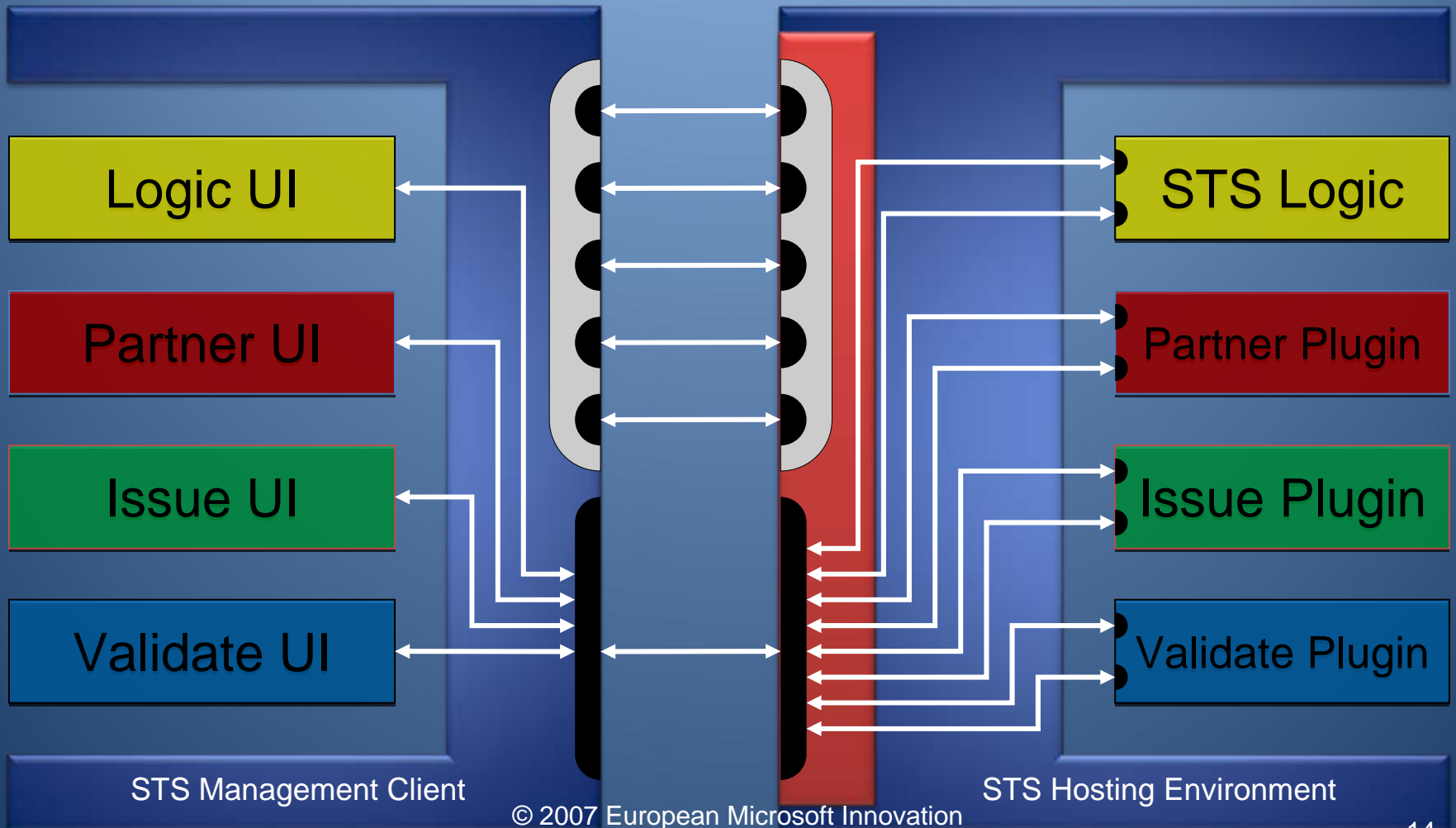
- Enable federations but scope (constrain) them to specific resources in the network
- Federations can be setup for fast situations
 - Technical support issue, sales presentations, one time interactions, etc....
- Safer for IT departments
 - Reduces the threat surface by only exposing assets in scope
 - Enables monitoring of information flow between companies
 - Puts context on information sharing, making leakage easier to detect and handle

SAFe – A pluggable STS

SAFe – A pluggable STS hosting environment



SAFe – Pluggable Manageability



Customized federation management experience

The top screenshot shows the Federation Management Client interface with the following table:

Service	Action	Worker	Manager
http://localhost/Service/Service.asmx	http://www.microsoft.com/emic/security/safe/AddThemUp	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
http://localhost/Service/Service.asmx	http://www.microsoft.com/emic/security/safe/MultiplyThem	<input checked="" type="checkbox"/>	<input type="checkbox"/>
*		<input type="checkbox"/>	<input type="checkbox"/>

The bottom screenshot shows a detailed view of a service configuration with the following table:

Service URI	Token Value	Token Type
http://localhost/Service/Service.asmx	CN=CONTOSO Service	X.509 Certificate
http://localhost/WSEServiceProxy/Service.asmx	CN=CONTOSO Service	X.509 Certificate

The policy configuration section shows the following XML snippet:

```
<cfg ClaimRequirementsPolicy>
```

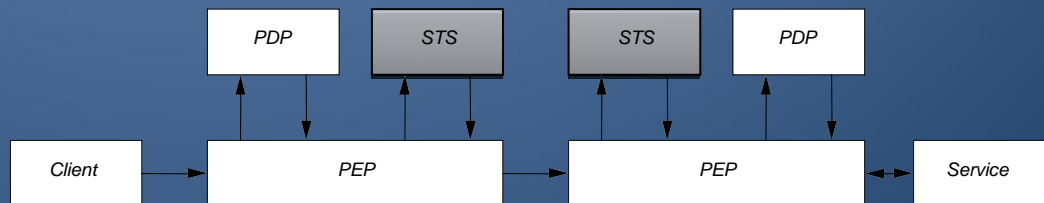
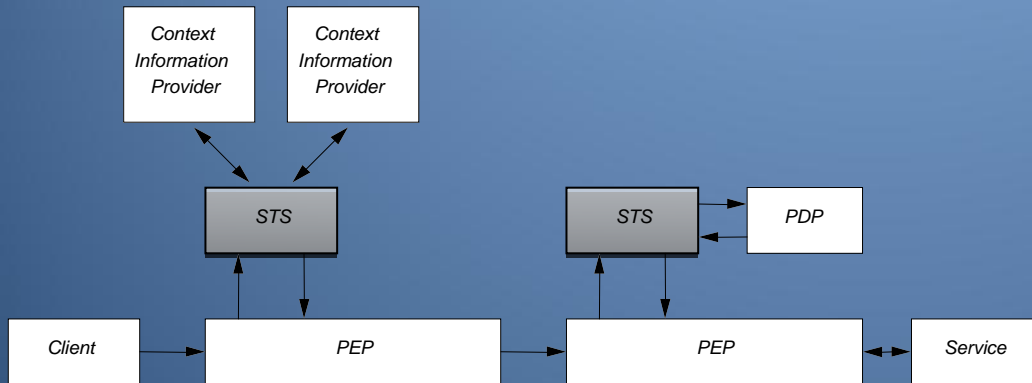
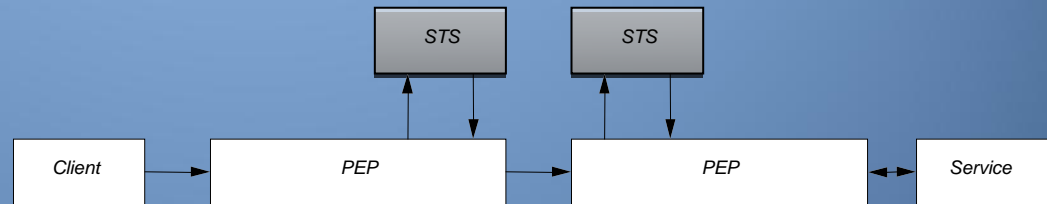
Custom UI plug-ins:

- e.g. simple, template based service mgmt
- e.g. complex, fine-grained access control

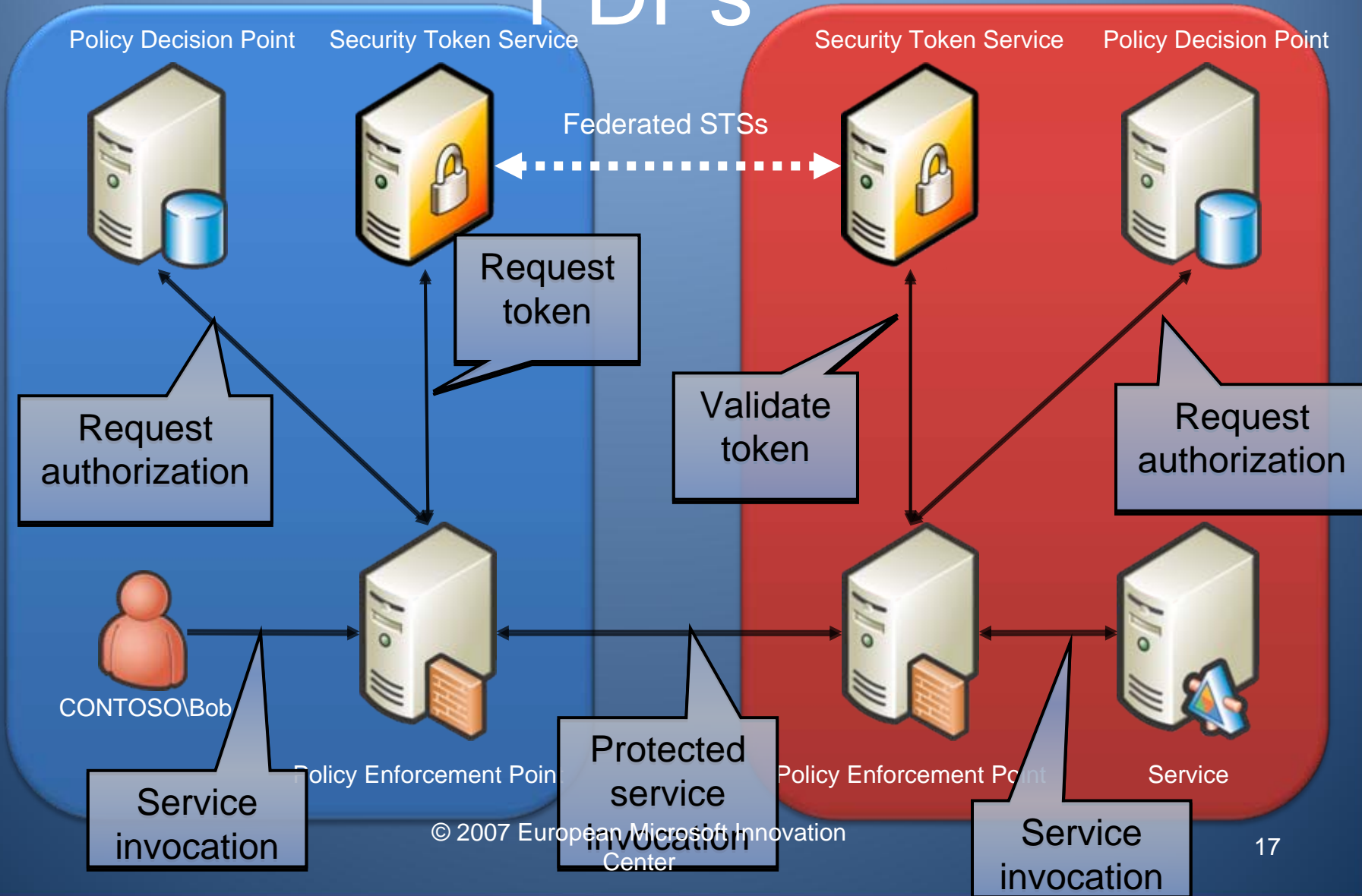
Using web services mgmt:

- application-specific “federation” mgmt
- federation mgmt operations embedded in business process

One STS – Many deployments



The TrustCoM flavor: STS and PDPs



Some architectural choices

- VO Membership
 - Manually-established partner lists (“Every partner knows every partner”)
 - VO-wide STS (WS-Trust frontend to a membership database)
- Authorization decisions
 - Dedicated PDP, STS only validates claims
 - STS running as authorization service
 - Mixed mode (TrustCoM)
 - STS validates claims and does authorization decision
 - PEP configuration specifies whether additional PDP is contacted
- Client claims
- Token formats
- ...

SAFe – Development overview

SAFe Prototype Implementation

- Prototype validation in multiple EU FP6 projects
 - TrustCoM
 - MOSQUITO
 - NextGRID
 - MYCAREVENT
- Main technologies
 - SOAP, WS-Security for communications
 - WS-Trust for token exchanges
 - SAML profile for security tokens (currently)

SAFe Prototype Implementation (II)

- Features
 - Based in .NET 2.0 / WSE3.0, will migrate soon to Indigo/WCF
 - Pluggable modules for
 - VO Partner membership providers
 - Claims implementations
 - Claims derivation providers
 - Service access authorization / claims validation modules
 - Claims-requirements policy engine
 - Proxy support to hook up legacy web services
 - Web services-based federation management

SAFe Release Plan

- SAFe Release planned for May 2007 (part of TrustCoM Reference Implementation)
- SDK based on .NET 2.0 / WSE 3.0
- SDK contains STS, management client, and sample plugins (such as the TrustCoM-specific plugins)

Plans for BREIN

- WCF (Indigo) support
- Data-centric security enforcement
- Dynamic context selection service
- (SecPAL Authorization support)

Questions?

- Contact
 - European Microsoft Innovation Center
 - Dr.-Ing. Christian Geuer-Pollmann
(chgeuer@microsoft.com)
 - <http://www.microsoft.com/emic>