Microsoft
.NET Access Control Service

A Resource STS in the cloud !?

Dominick Baier

thinktecture

WhoAmI && WhyAmIHere /?

- **Why am I here?**
  - because Enno asked me to ;)

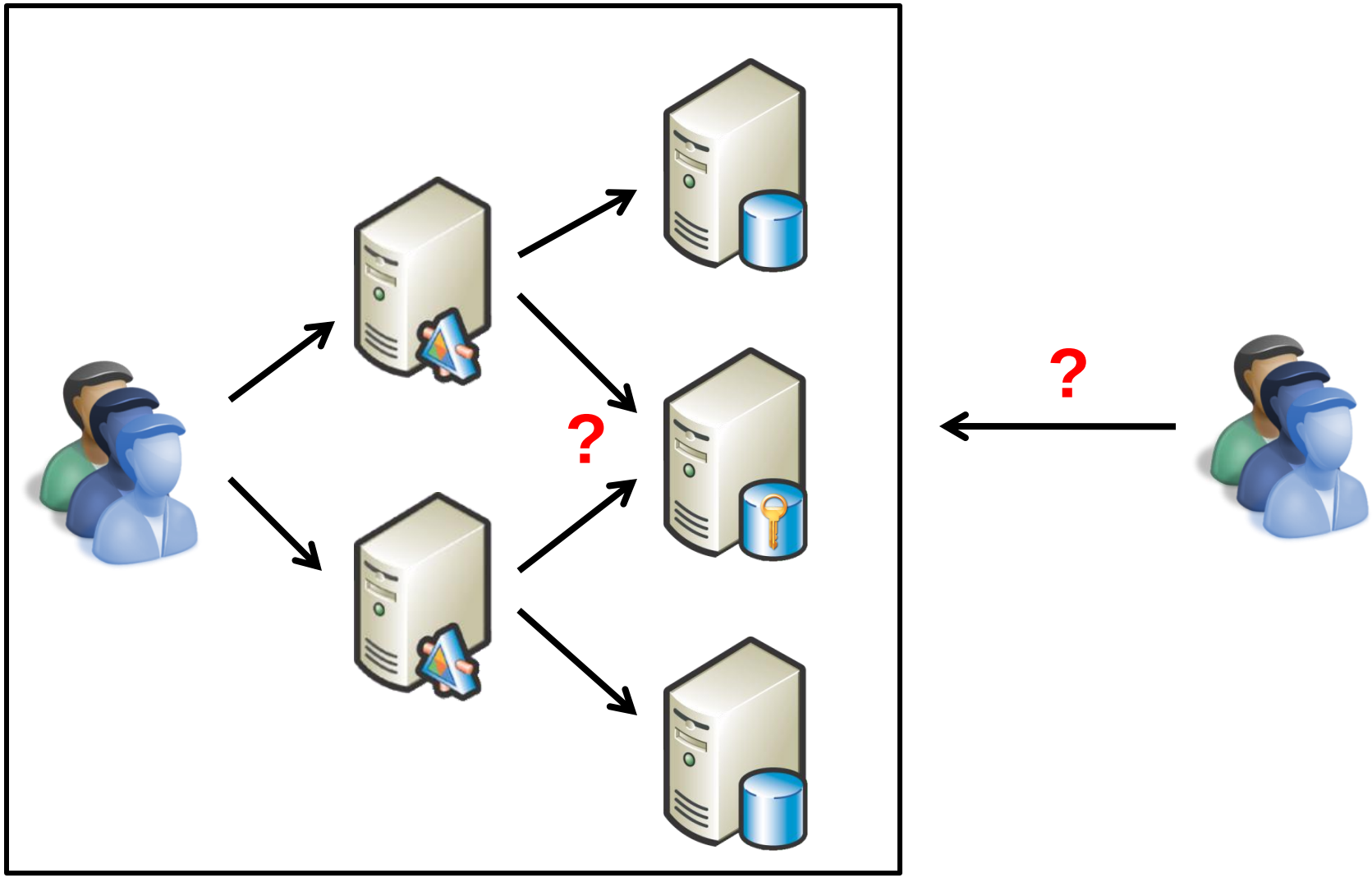
- **Who am I?**
  - former ERNW employee
  - security consultant at thinktecture
  - focus on security in distributed applications…
  - …using the Microsoft technology stack

http://www.leastprivilege.com
dominick.baier@thinktecture.com

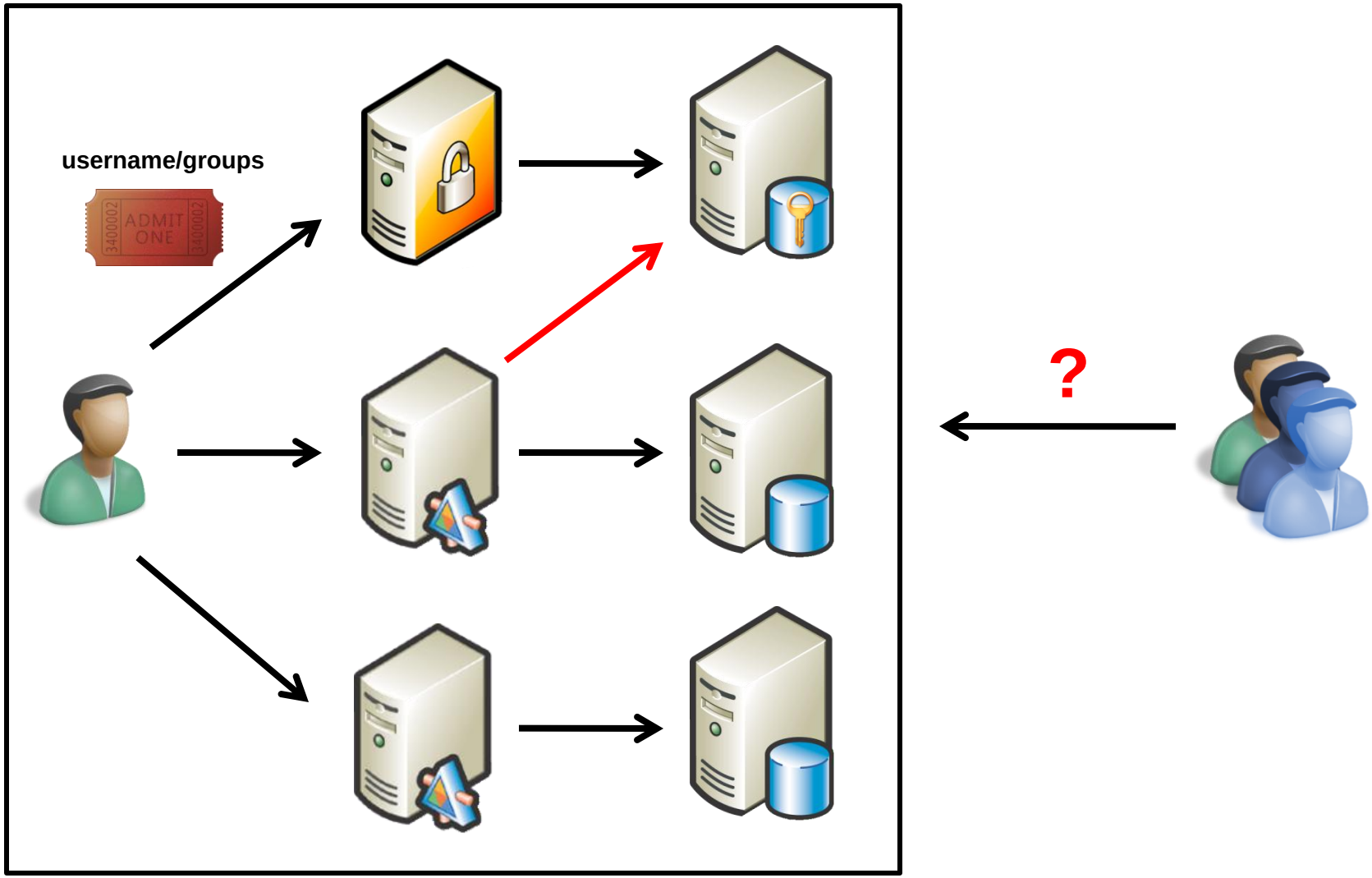
Agenda

- **Brief history of authN and authZ**
- **Technical details**
- **Demo**

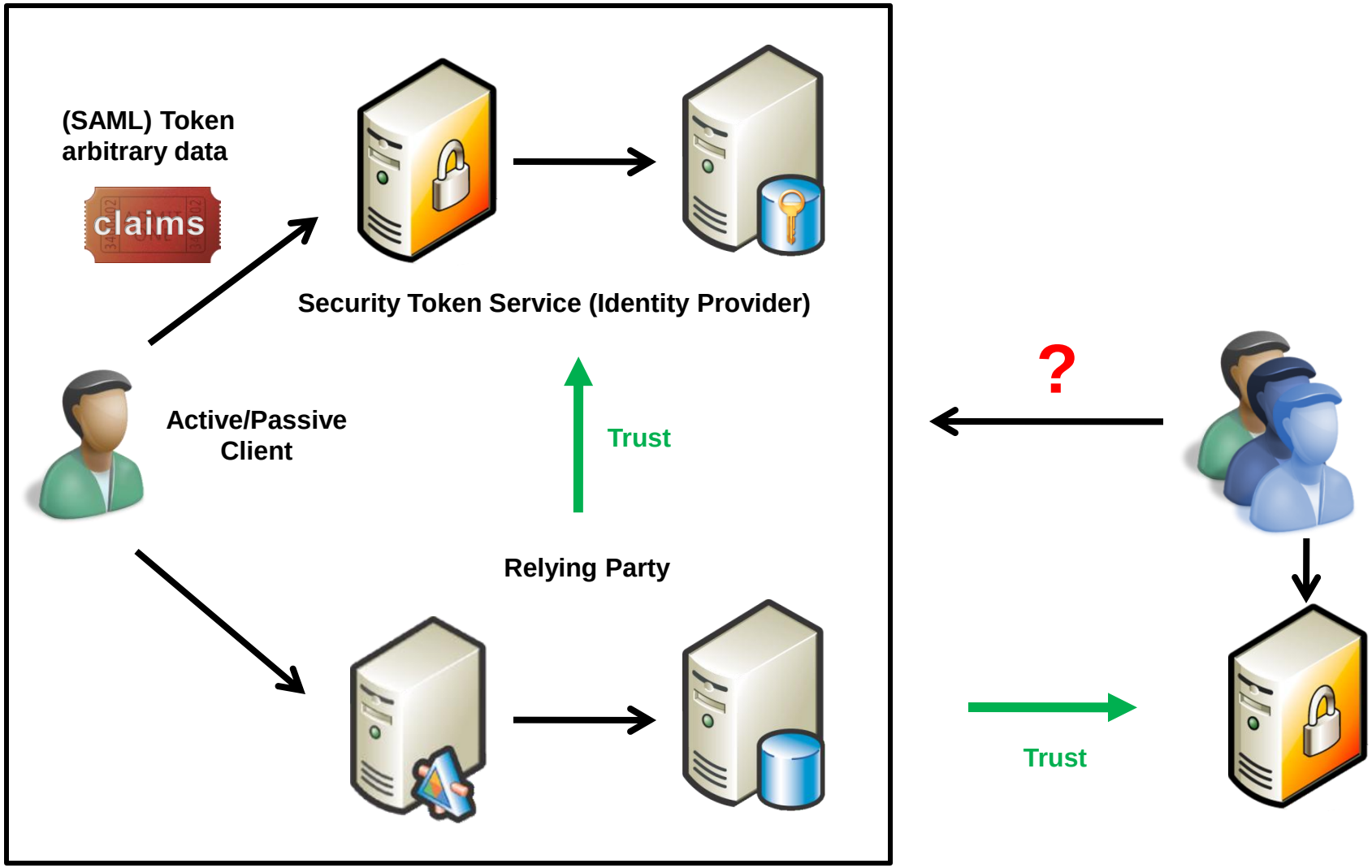
Direct authentication



Token based authentication (Kerberos)



Token based authentication (WS*)



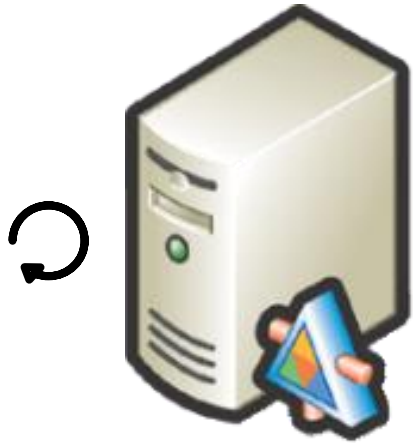
Complexity & scalability

Partner A: email, department

Customer B: email, title

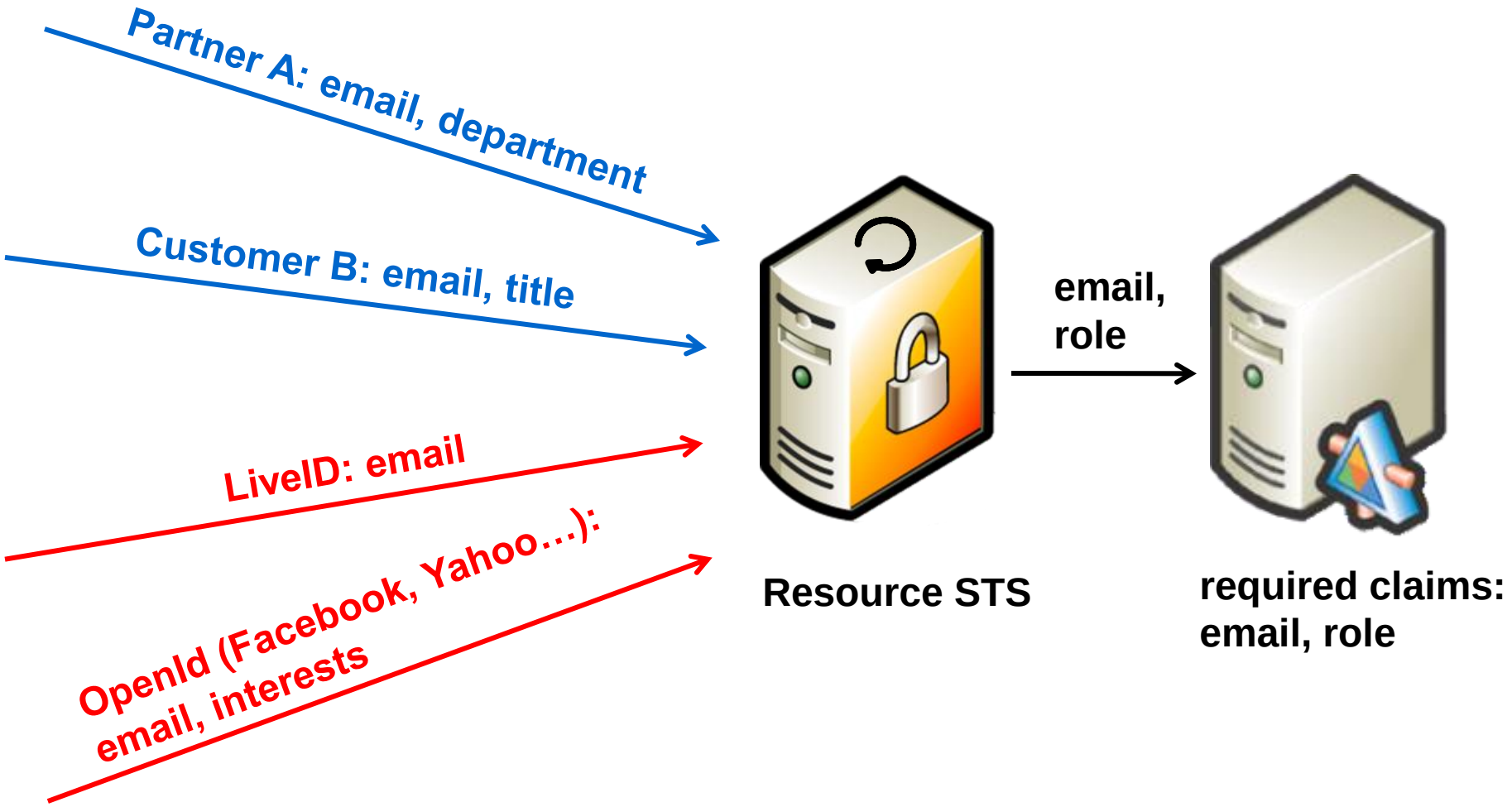
LiveID: email

OpenId (Facebook, Yahoo…):
email, interests

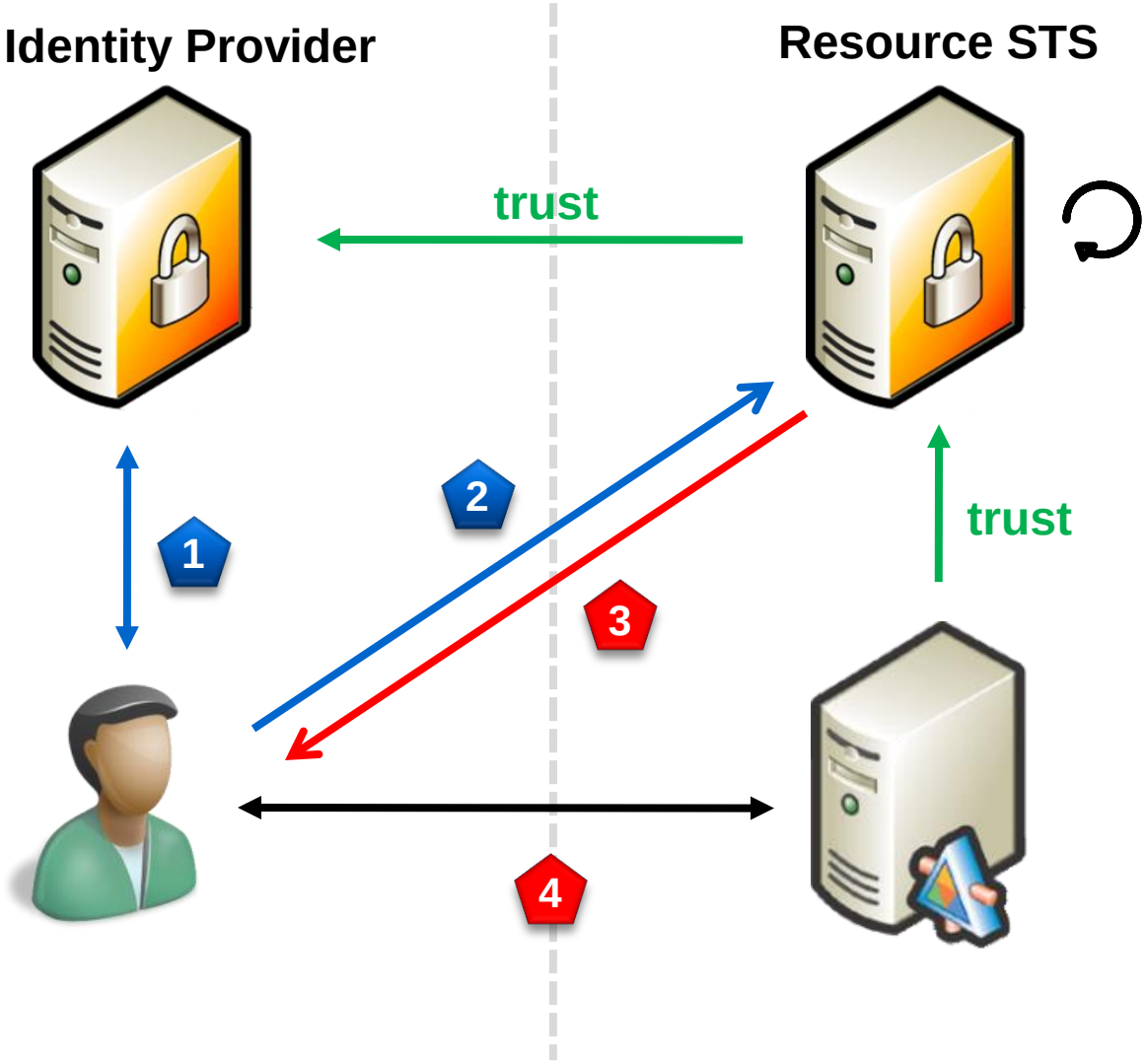


required claims:
email, role

Resource STS – conceptual model

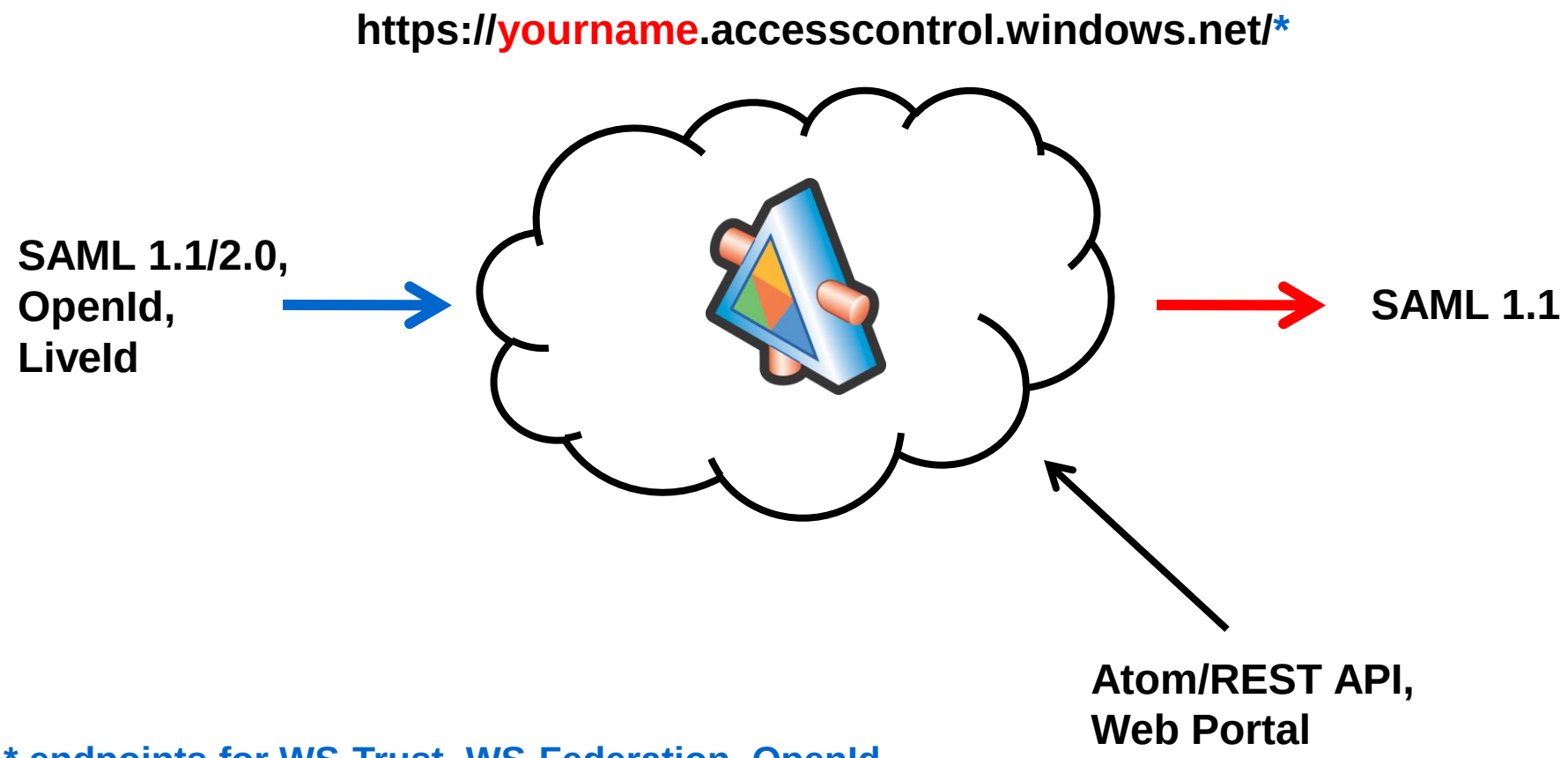


Resource STS – physical model



Azure Services Platform

Resource STS in the cloud

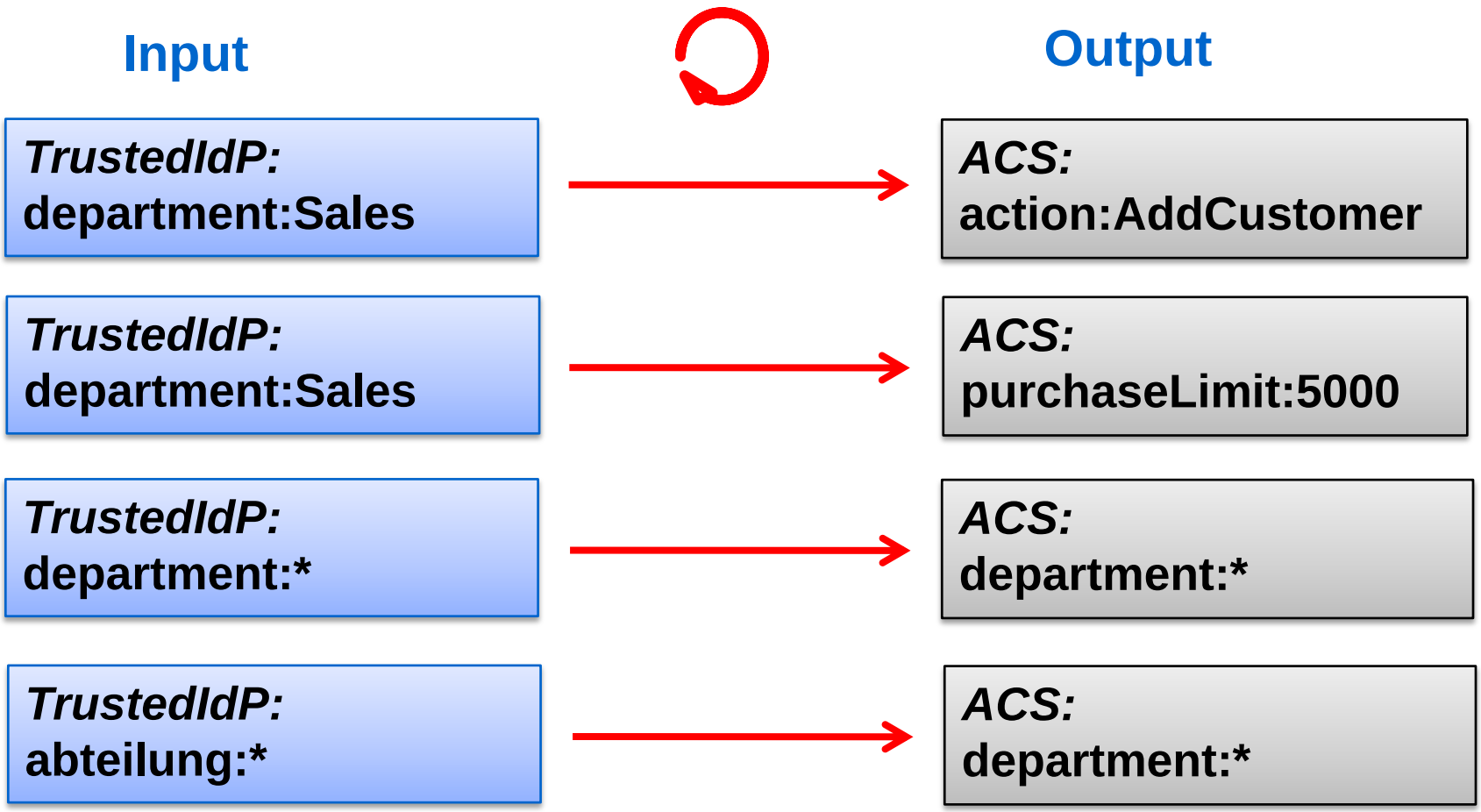


* endpoints for WS-Trust, WS-Federation, OpenId

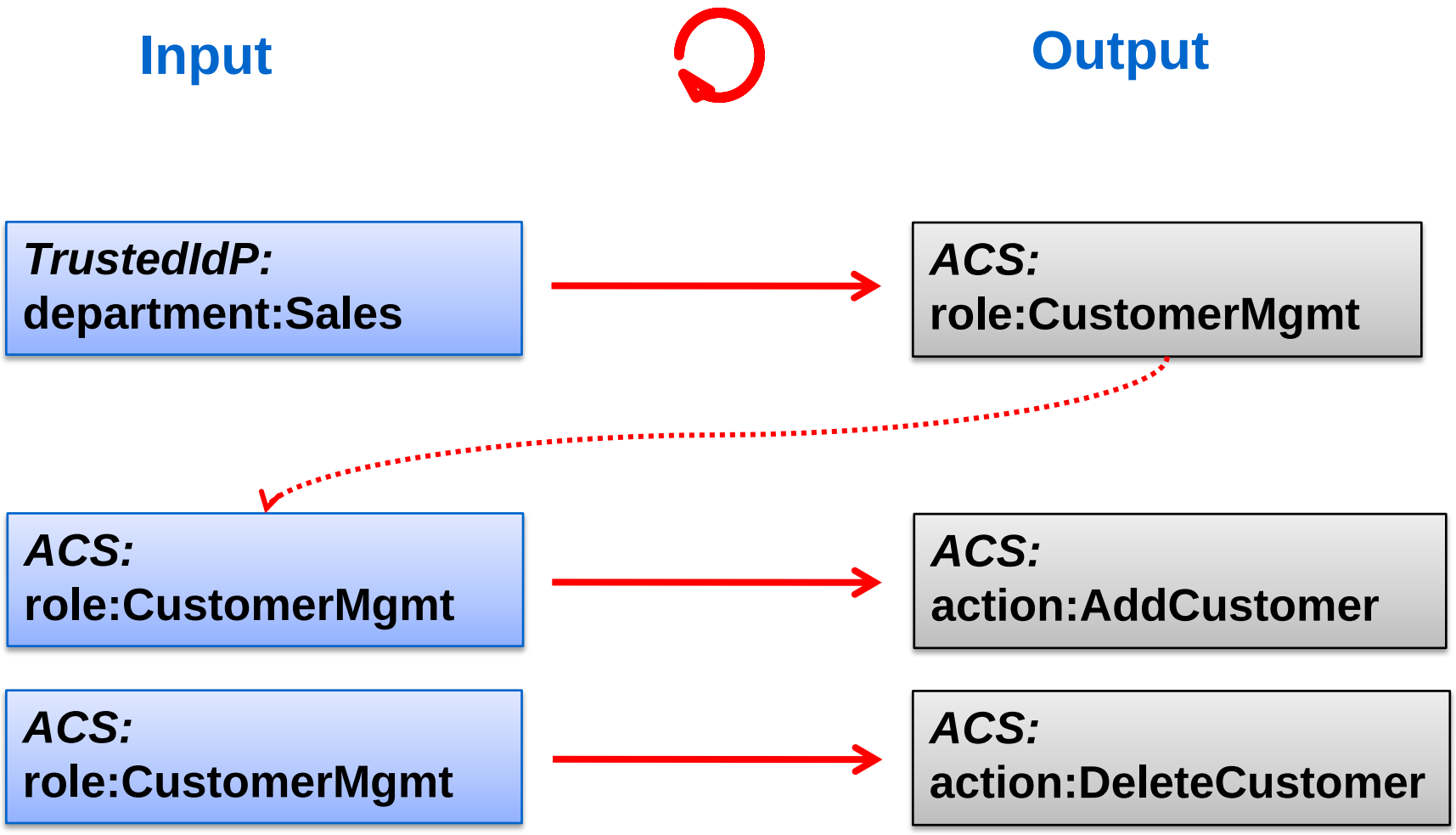
ACS concepts

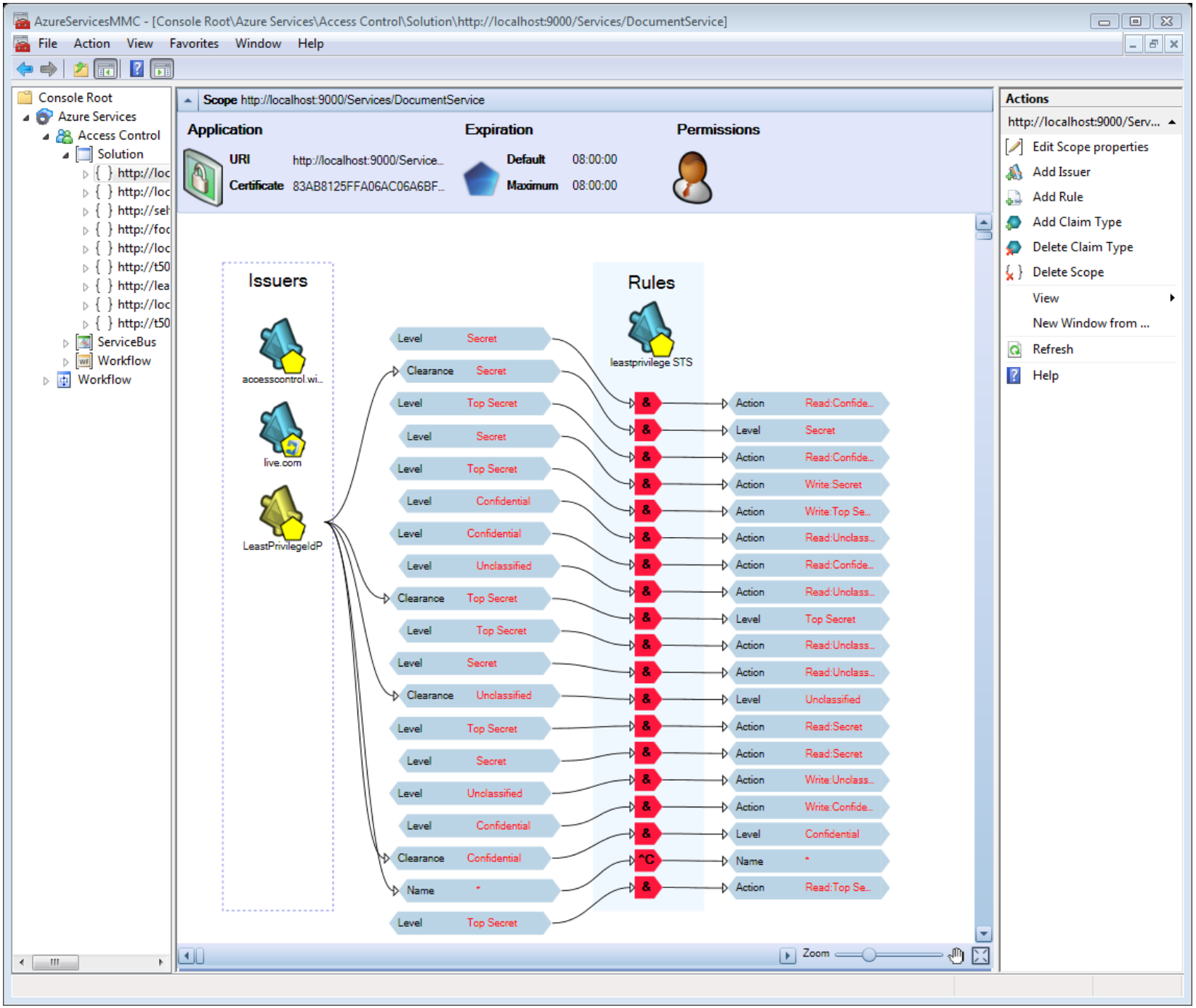
- **Scopes**
  - identifiers for applications
  - container for configuration settings
  - encryption preferences
- **Identity Providers**
  - list of trusted token issuers
  - backed by certificates
- **Rules**
  - claims transformation engine

Rules examples



Forward chaining Rules




AzureServicesMMC - [Console Root\Azure Services\Access Control\Solution\http://localhost:9000/Services/DocumentService]
File Action View Favorites Window Help
Console Root
Azure Services
Access Control
Solution
ServiceBus
Workflow
Workflow
Scope http://localhost:9000/Services/DocumentService
Application
URI http://localhost:9000/Service...
Certificate 83AB8125FFA06AC06A6BF...
Expiration
Default 08:00:00
Maximum 08:00:00
Permissions
Issuers
accesscontrol.wi...
live.com
LeastPrivilegeIdP
Rules
leastprivilege STS
Level Secret
Clearance Secret
Level Top Secret
Level Secret
Level Top Secret
Level Confidential
Level Confidential
Level Unclassified
Clearance Top Secret
Level Top Secret
Level Secret
Clearance Unclassified
Level Top Secret
Level Secret
Level Unclassified
Level Confidential
Clearance Confidential
Name *
Level Top Secret
&
^C
Action Read:Confide...
Level Secret
Action Read:Confide...
Action Write:Secret
Action Write:Top Se...
Action Read:Unclass...
Action Read:Confide...
Action Read:Unclass...
Level Top Secret
Action Read:Unclass...
Action Read:Unclass...
Level Unclassified
Action Read:Secret
Action Read:Secret
Action Write:Unclass...
Action Write:Confide...
Level Confidential
Name *
Action Read:Top Se...
Zoom
Actions
http://localhost:9000/Serv...
Edit Scope properties
Add Issuer
Add Rule
Add Claim Type
Delete Claim Type
Delete Scope
View
New Window from ...
Refresh
Help

Anatomy of an ACS SAML token

```
<saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"
  issuer="http://yourname.accesscontrol.windows.net">
  <saml:Conditions>
    NotBefore, NotOnOrAfter, ScopeName
  </saml:Conditions>
  <saml:AttributeStatement>
    <saml:Attribute AttributeName="email">
      alice@foo.com
    </saml:Attribute>
    <saml:Attribute AttributeName="purchaseLimit">
      5000
    </saml:Attribute>
  </saml:AttributeStatement>
  <Signature xmlns="http://www.w3.org/2000/09/xmldsig#" />
</saml:Assertion>
```

Summary

- **Industry-wide shift to token based authentication**
  - WS* & SAML very popular
- **Resource STS needed for more complex trust brokerage**
  - "claims adapter"
  - bridges authentication protocols
- **Resource STS is a candidate for "utility computing"**
  - Microsoft are the first this time
  - others surely to follow
  - nothing RTM'ed yet

- **Try it yourself (it is fun!)**
  - http://portal.ex.azure.microsoft.com/