Lesson 21 – REST Services Security using the Access Control Service

Service Oriented Architectures Security

Module 1 - Basic technologies

Unit 1 – Introduction

Ernesto Damiani

Università di Milano

Context

ACS 101 & Demo

ACS Entities

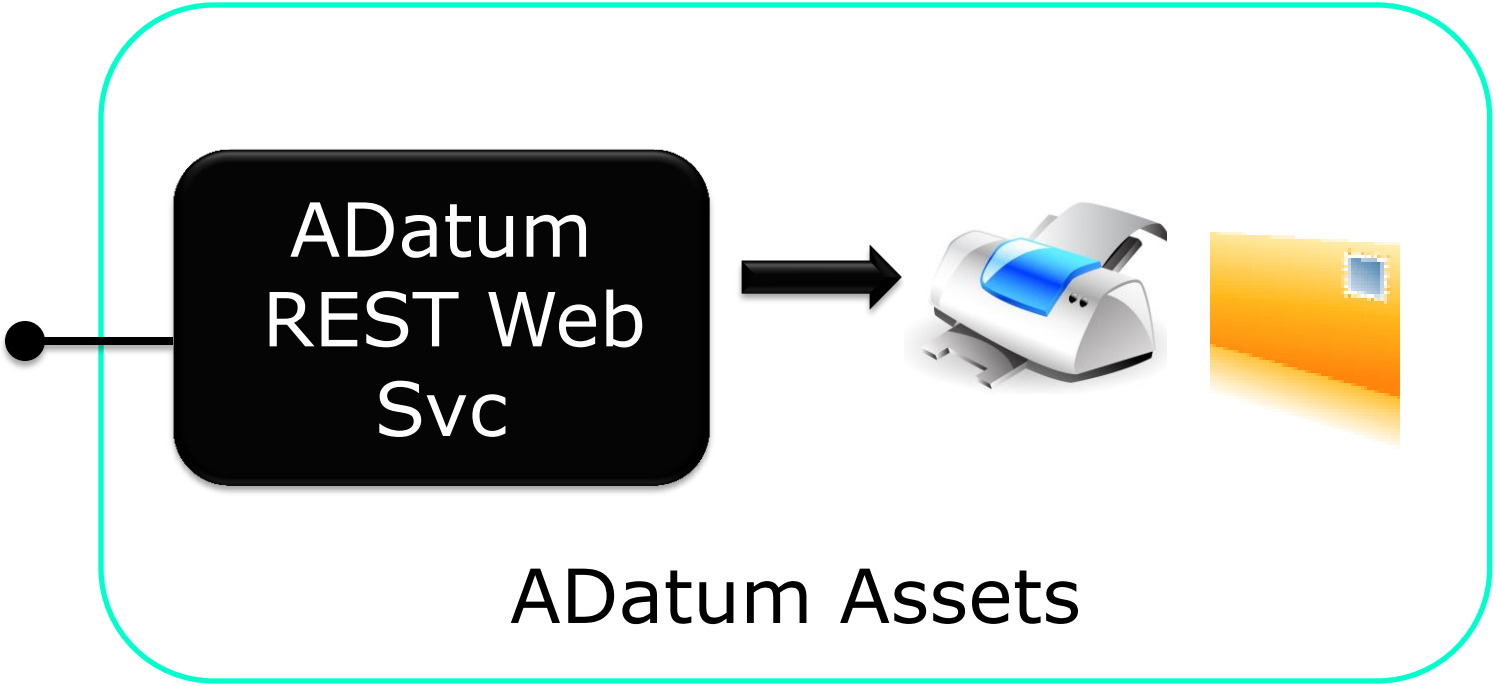
AD FS v2 Integration & Demo

Simple Delegation & Demo

Futures & Demo

ADatum Partners & Bill Print

Bill Print targets big and small companies



Role Play – ADatum Architects

- How to make it easy to onboard small companies?
- How do we integrate with enterprise directories?
- Do we need to become enterprise security wizards?
- Will we need different codebases?
- How do we allow our customers to grant others access on their behalf?
- <the list goes on…>

ACS makes it easier

ACS == claims based access control for REST web services

Key capabilities / features:

- Usable from any platform (*for real*)
- Implements OAuth WRAP & SWT
- Low-friction way to onboard new clients
- Integrates with AD FS v2
- Enables simple delegation

A web service can take advantage of these capabilities with ONE code base

Community Efforts

OAuth Profiles

- Web Resource Authorization Protocol (WRAP)
- Simple Web Tokens (SWT)

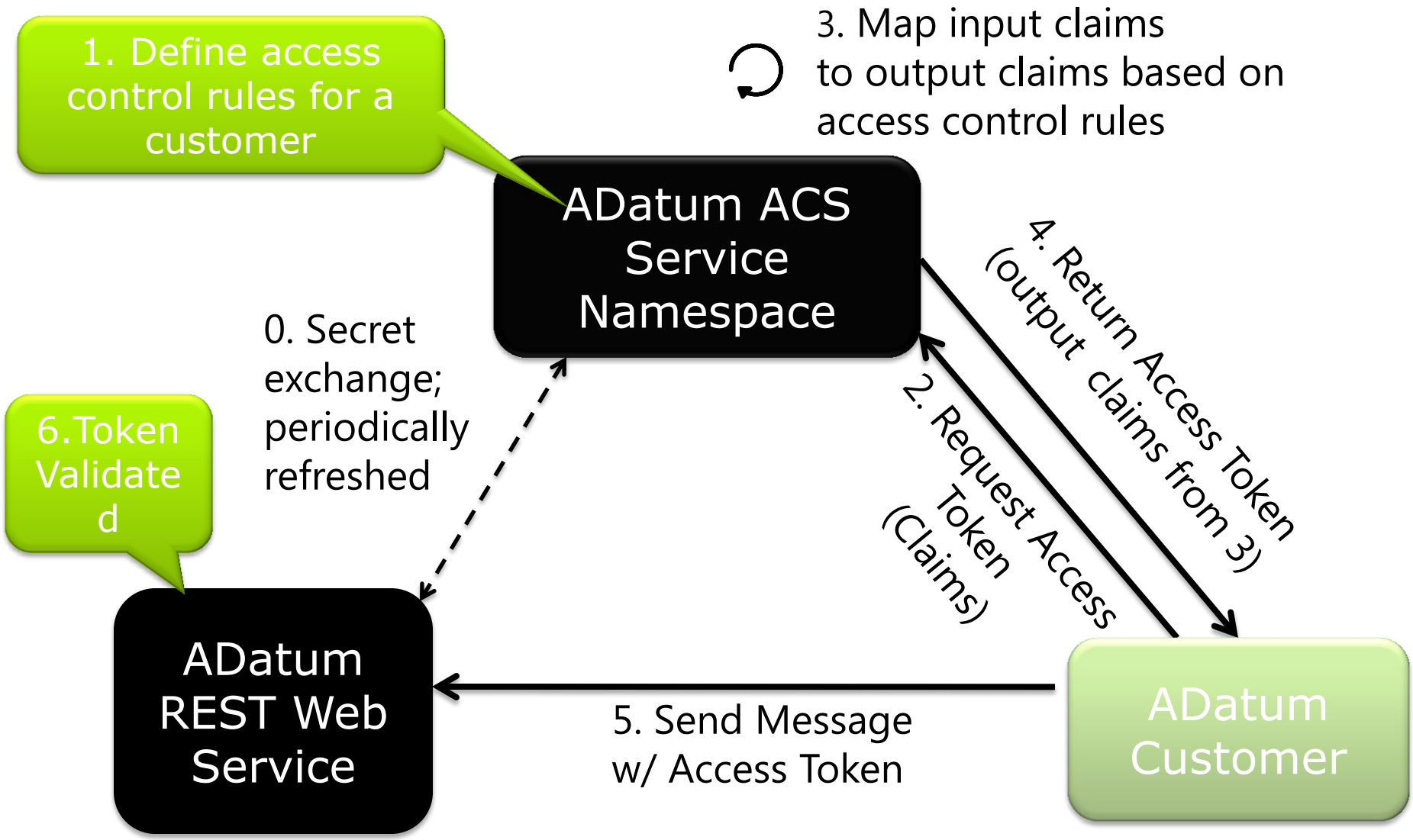
Microsoft, Yahoo!, and Google contributed

Specs, community discussion, and other information available on Google groups

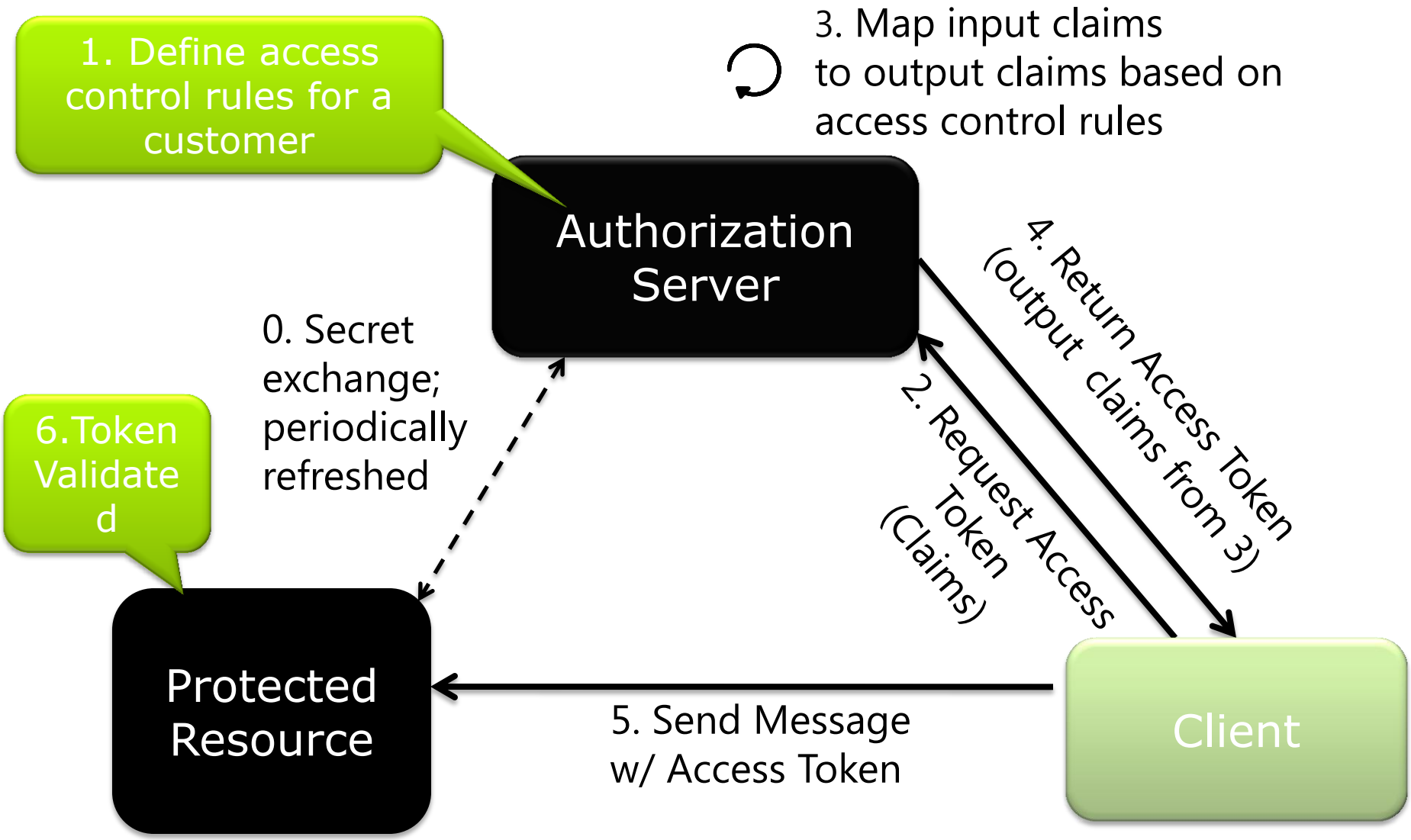
- http://groups.google.com/group/oauth-wrap-wg

Contributed to OAuth IETF working group

How It Works


1. Define access control rules for a customer
3. Map input claims to output claims based on access control rules
ADatum ACS Service Namespace
0. Secret exchange; periodically refreshed
4. Return Access Token (output claims from 3)
2. Request Access Token (Claims)
6.Token Validate d
ADatum REST Web Service
5. Send Message w/ Access Token
ADatum Customer

In OAuth WRAP terms (sec. 5.1) …



ACS Token Requests

3 ways to request a token

- Plaintext
  - –Lowest friction option, no crypto required
- Signed token
  - –Enables simple delegation, HMAC SHA 256 required
- AD FS v2 issued SAML bearer token
  - –Enables enterprise integration

ACS always returns the same kind of token (SWT)

What's a SWT?

role=Admin%2cUser&
customerName=Contoso%20Corporation&
Issuer=https%3a%2f%2fadatum.accesscontrol.windows.net%2fWRAPv0.8&
Audience=http%3a%2f%2fadatum%2fbillprint&
ExpiresOn=1255912922&
HMACSHA256=yuVO%2fwc58%2ftYP36%2fDM1mS%2fHr0hswpsGTWwgfvAbpL64%3d

How Do I Request a SWT? (Plaintext, sec. 5.1)

```
POST /WRAPv0.8/ HTTP/1.1
Host:adatum.accesscontrol.windows.net

applies_to=http%3A%2F%2Fadatum.com%2F
   services%2F&
wrap_name=adatumcustomer1&
wrap_password=5znwNTZDYC39dqhFOTDtnaik
   d1hiuRa4XaAj3Y9kJhQ%3D
```

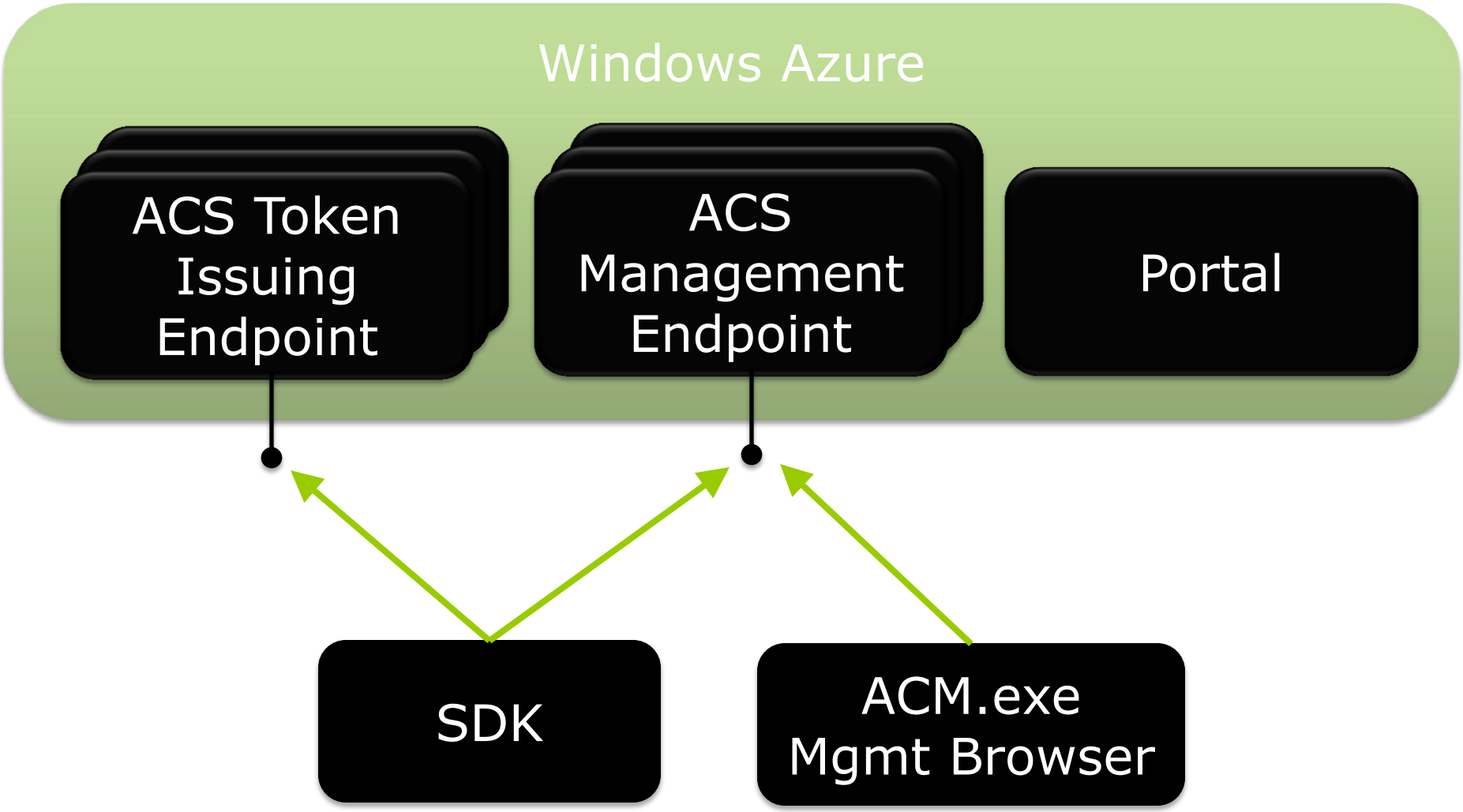
How Do I Request a SWT? (Signed Token, sec. 5.2)

```
POST /WRAPv0.8/ HTTP/1.1
Host:adatum.accesscontrol.windows.net

applies_to=http%3A%2F%2Fadatum.com%2F
   services%2F&
wrap_SWT=role%3DAdmin%252cUser%26Iss
   uer%3Dadatumcustomer1%26ExpiresOn%3
   D1255912922%26HMACSHA256%3DyuVO%
   252fwc58%252ftYP36%252fDM1mS%252fH
   r0hswpsGTWwgfvAbpL64%253d
```

How Do I Request a SWT? (SAML Token, sec. 5.2)

```
POST /WRAPv0.8/ HTTP/1.1
Host:adatum.accesscontrol.windows.net

applies_to=http%3A%2F%2Fadatum.com%2F
   services%2F&
wrap_SAML=<…SAML Bearer Token…>
```

ACS Gross Anatomy



ACS 101 Demo

ADATUM BASICS

ACS Token Issuing Behavior

ACS entities control token issuing behavior

Token Policy

- Expiration & signature key

Issuer

- Cryptographic key material (requests)

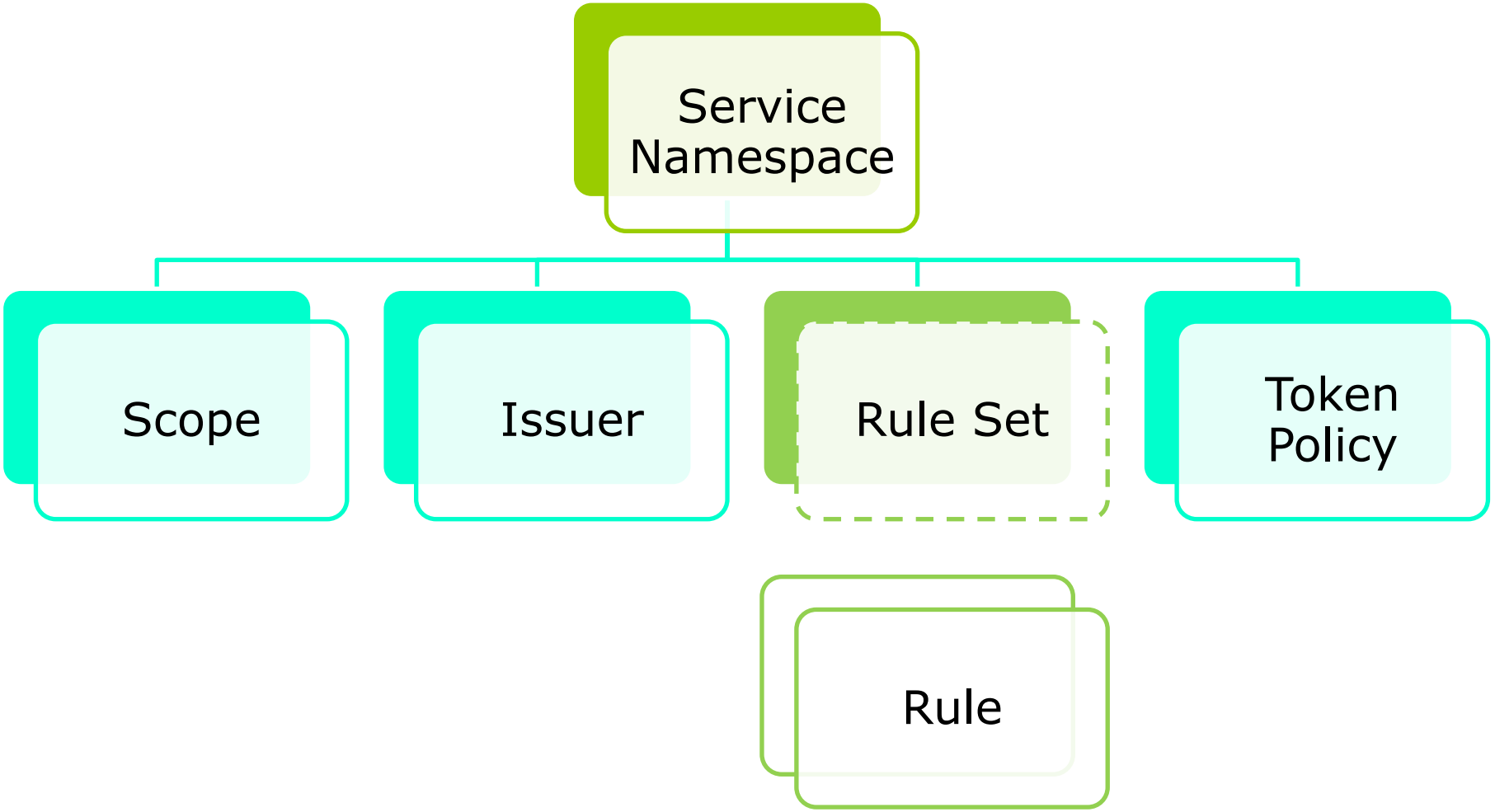
Scope

- URI that ACS uses to group Rule entities

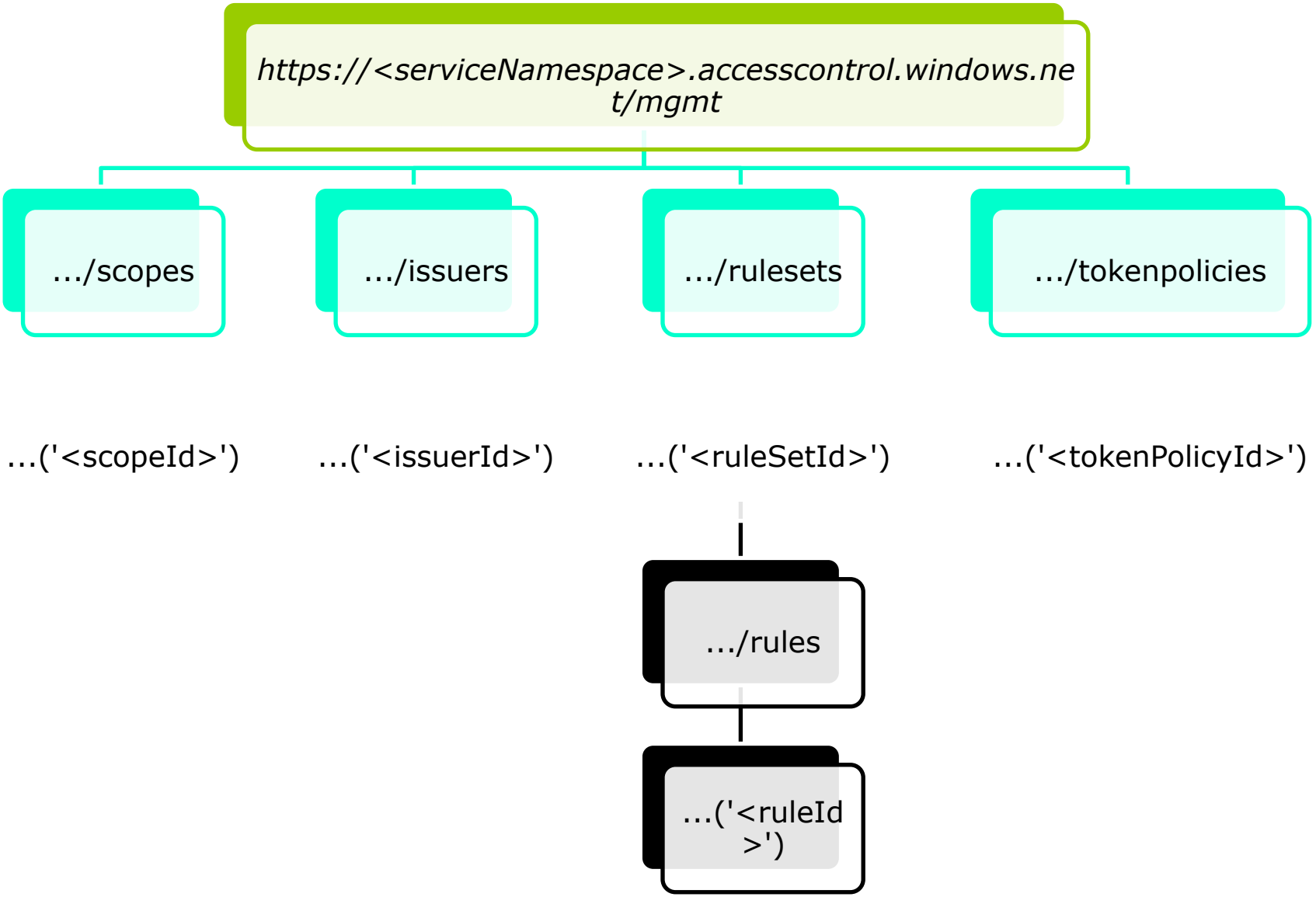
Rule Set / Rule

- Determines claims present in ACS tokens

ACS Resource Hierarchy



ACS Resource URIs



ACS & Enterprise Integration

ACS accepts signed SAML bearer tokens in token requests

- AD FS v2 can issue these

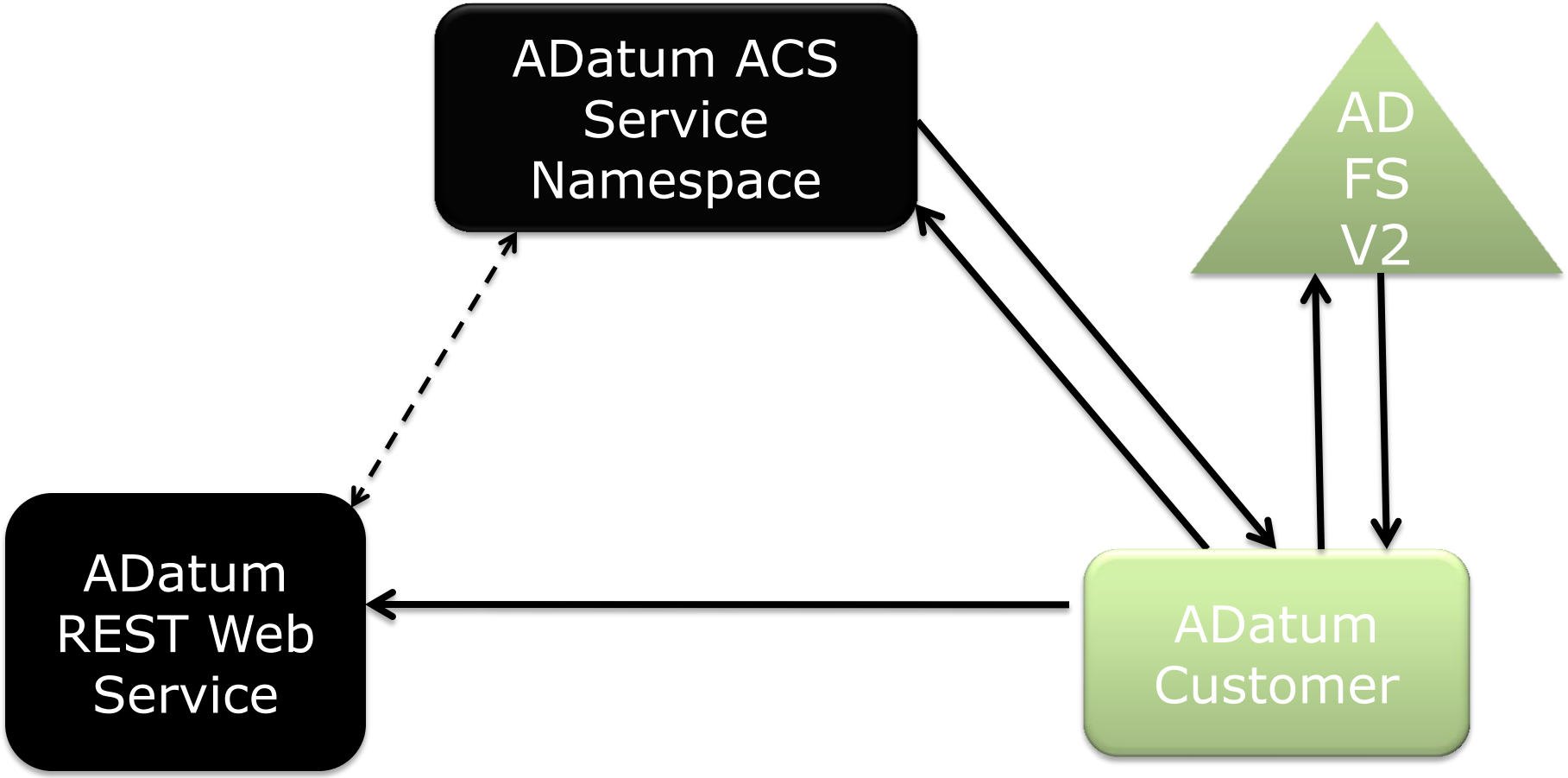
WIF is the easiest way to request a SAML token from AD FS v2

ACS must have knowledge of the signing key in order to validate the SAML token

ACS publishes and parses WS-Fed metadata

- *Automates establishing the trust relationship*

ADatum & Enterprise Integration



ACS Enterprise Integration

ADATUM & ENTERPRISE CUSTOMERS

Simple Delegation

ADatum wants to give their customers the ability to grant others access

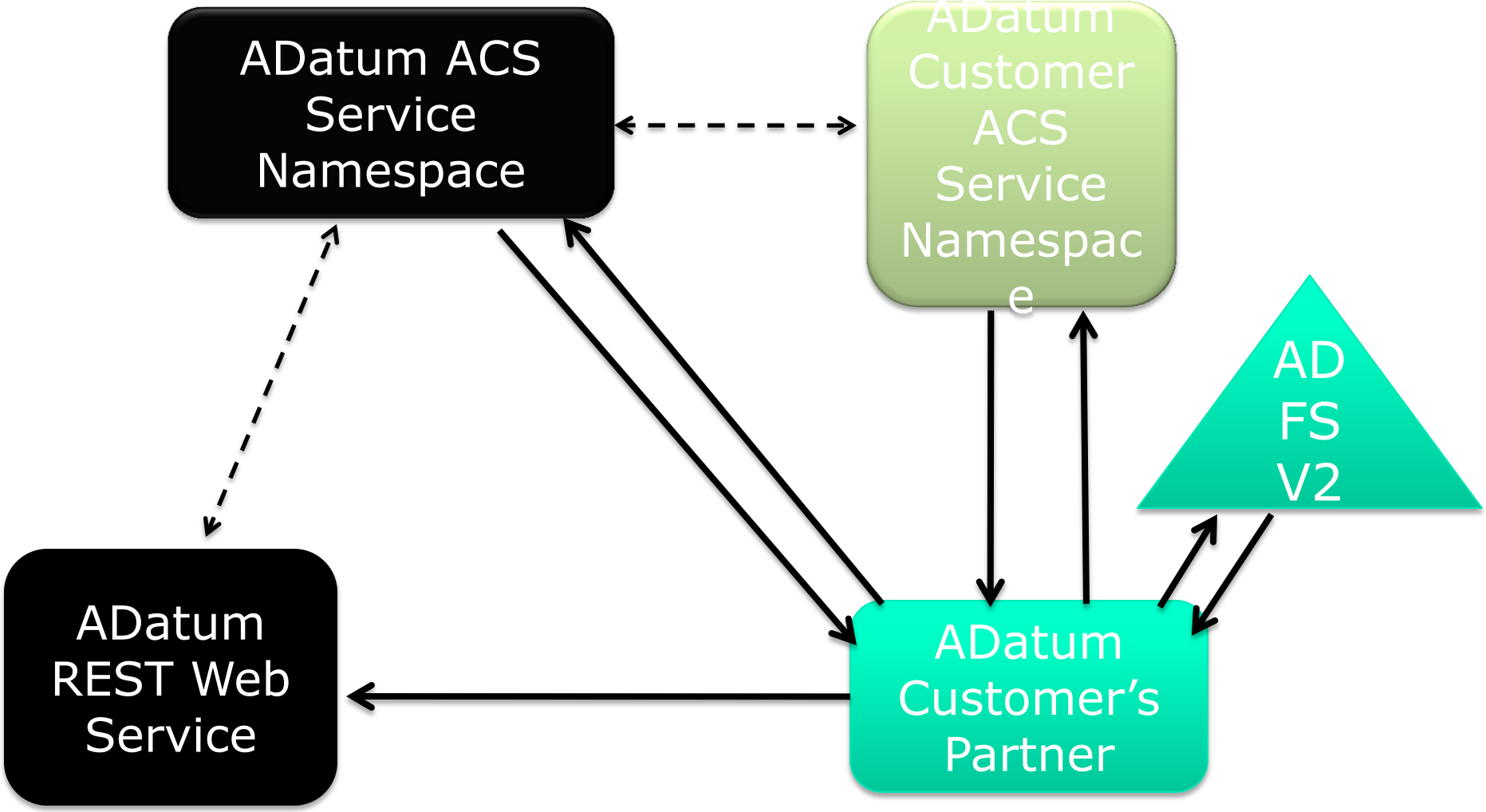
ACS service namespaces can be linked

- ACS ns1 trusts tokens issued from ACS ns2

Requires mapping token policies and issuers

- ACS ns1 contains an issuer whose key matches a token policy from ACS ns2

ADatum & Simple Delegation



ACS Simple Delegation

ADATUM & SIMPLE DELEGATION

Futures / Roadmap

Support for Web Identity Providers

- Web identity providers (Live ID, Facebook Connect, Google, Open ID, etc.)
- Enterprise identity providers

Native WS-* Support

- WS-Trust and WS-Federation
- CardSpace

ACS Futures

WEB IDENTITY DEMO

YOUR FEEDBACK IS IMPORTANT TO US!

Please fill out session evaluation forms online at MicrosoftPDC.com

Learn More On Channel 9

Expand your PDC experience through Channel 9

Explore videos, hands-on labs, sample code and demos through the new Channel 9 training courses

channel9.msdn.com/learn

Built by Developers for Developers….