Michael Stiefel
Reliable Software, Inc.
www.reliablesoftware.com

Claims Based Security

Session Code: AR 11

How can collaborative applications provide security access?

Security Access has three phases.

- Policy Determination
  - Identity is mapped to rights or privileges.
- Authentication
  - Credentials are validated. Identity established.
- Authorization / Policy Enforcement
  - Code determines if execution continues.

You do not know your users.

- Department store buyer orders merchandise from a supplier.
- National Guard needs status information from the local police in an emergency.
- Lab test results are forwarded by a doctor to an insurance company.
- Your company's CRM app has to work with your inventory management app.

Identity is complicated.

- Identities can be:
  - People
  - Organizations
  - Software processes
  - …or some combination.

Which identity technology are you going to use?

Credential Mechanisms

- Username / Password
- Smart Card
- Biometric Identifiers

Authorization Stores

- Active Directory
- AzMan
- ADAM
- Custom

Which Protocol Do You Use?

- Live Id
- Open Id
- Liberty Alliance
- Custom

Not to Mention…

- Governance Provider:
  - HP Systinet
  - Software AG Infravio
- Brokers
  - Oracle Web Services Manager

How do you interoperate with third parties?

With claims based security you don't need to know who your users are.

Claims Based Security

- A claim represents an attribute about an identity.
- Authorization is based on attributes.
- Policy represents the attributes need to permit code to execute.
- Claims can be represented in a vendor-neutral, standardized way.

Authentication Generates Claims

- A validated identity is associated with a set of claims, or claim set.
- If the software trusts the authentication mechanism, then it can trust the claims.
- The software is not required to know the identity of the user.

Benefits of Using Claims

- Removed the dependency of authorization and policy on specific authentication technologies.
- Allow software to process identities authenticated by third parties.

Requirements to Use Claims

- We need an standard to express claims.
- We need a standard to express policy
- We need a standard to identify the authenticators to determine trust.

SAML is the standard for claims.

- The **Security Assertion Markup Language** allows attributes to be expressed.
- Attributes are expressed as XML assertions.
- SAML is an OASIS standard.
- SAML profiles map to a specific technology.
- SAML is used for more than claims.

SAML Assertions

- Authentication Assertions
- Authorization Decision Assertions
- Attribute Assertions

Policy Enforcement Points

- Generic policy can be enforced in the security system infrastructure.
- Application policy must be enforced in application code.

Attributes

- Attributes can be any relevant information about an identity:
  - Age
  - Hair color
  - How authentication
  - Name
  - Role
  - …

Mapping SAML Tokens

- WS-Security puts SAML tokens in the security headers.
  - WCF ClaimSet, Claims classes
- REST uses custom headers.

  http://saml.xml.org/news/how-to-use-saml-with-rest-web-services

Basic Claims Scenario

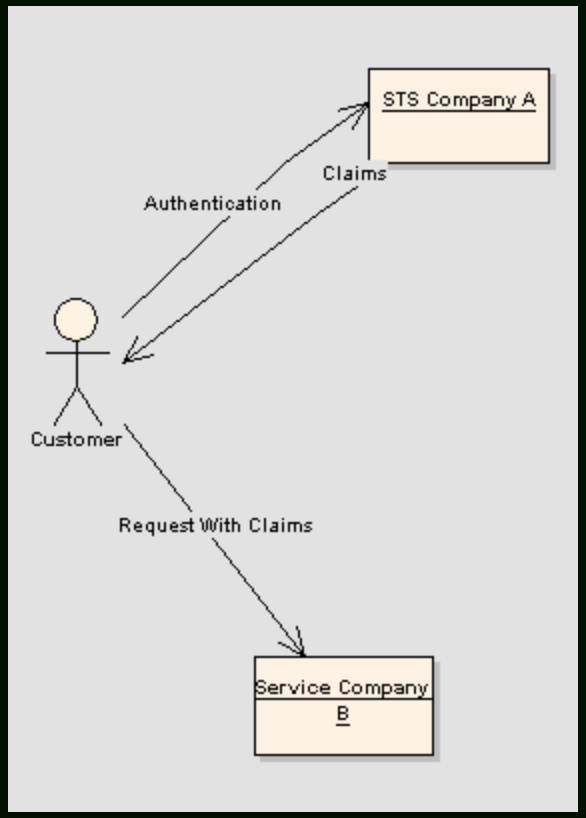
User Authenticates against Security Token Service of its own Company.

STS returns a cryptographically signed set of claims to the user based on Company B's policy.

Customer sends its request to Company B's service with its claims.

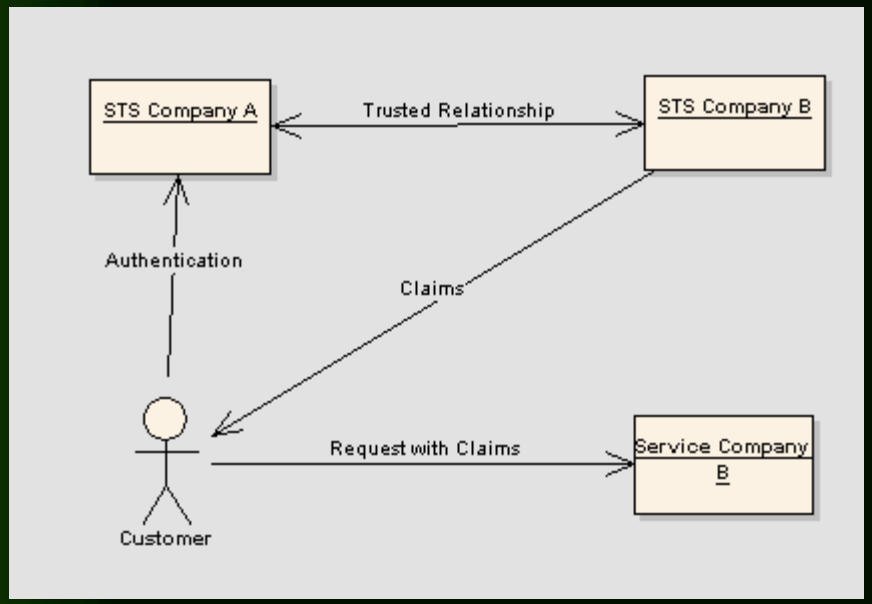
Company B evaluates whether it trusts Company A's STS.

Company B uses claims to decide whether to honor request.



Federated Claims Scenario

Instead of having to trust the STS of each client company, you can let the token services trust each other.



Standards Driven Conversation

- SAML
- WS-Trust
- WS-Federation
- WS-Secure Conversation
- WS-Security

Microsoft "Geneva"

- Geneva Framework allows you to build claims based applications.
  - Incompatible with WCF
- Geneva Server is an STS or identity provider based on Active Directory.
  - Supports both browsers and active clients.
  - Geneva Framework used to build custom STS.
- Geneva CardSpace is an identity selector.
- Currently in Beta.

How to Start to move to Claims?

- No immediate need exists for a Security Token Service.
- Have your authentication mechanism generate claims.
- Have your software make authorization decisions in terms of claims.

Demo

- Using WCF today to build a claims-based authorization mechanism.

Conclusions

- The authentication, authorization, and policy decisions can be partitioned.
- Authorization can use claims from any source, so long as they are trusted.
- Identity privacy can be protected.
- Collaborative solutions do not require knowing whom your users are.

Evaluation form

Vul je evaluatieformulier in en maak kans op een van de prachtige prijzen!!

Fill out your evaluation form and win one of the great prizes!!

Session Code: AR 11