Integrating CAS and Grouper with WIF

Jean Marie THIA
Université Pierre et Marie CURIE - UPMC

Microsoft® .NET | Windows Identity Foundation

"Stop hard-coding security into applications and stop creating operating system (OS)-level accounts on servers. Consume these as services external to the application."

Neil MacDonald 13 April 2006

Gartner Group: Achieving agility: building blocks for a policy-driven, agile security services infrastructure

As an application designer or developer, imagine a world where you don't have to worry about authentication. Imagine instead that all requests to your application already include the information you need to make access control decisions and to personalize the application for the user.

Preface of Patterns a practices :

A guide to claims-based Identity and Access Control

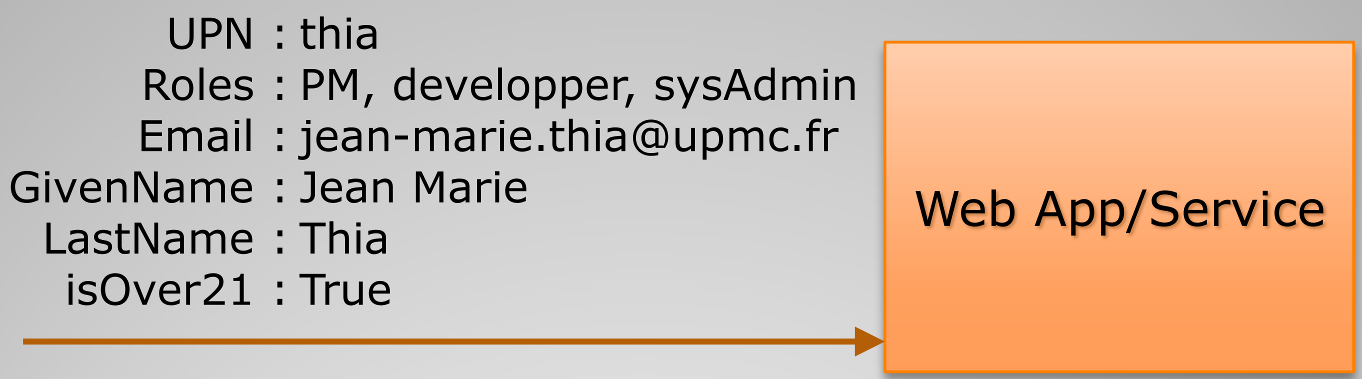
(http://msdn.microsoft.com/en-us/library/ff359103(lightweight).aspx)

Agenda

- Claim based Identity & Access Control
  - Claims
  - ADFS
  - WIF
- Integration
  - CAS Integration
  - Grouper Integration
  - To-do list
- Q&A

Claims

- A set of information



UPN : thia
Roles : PM, developper, sysAdmin
Email : jean-marie.thia@upmc.fr
GivenName : Jean Marie
LastName : Thia
isOver21 : True

Web App/Service

- Bundled in a security token
- Signed by an issuer

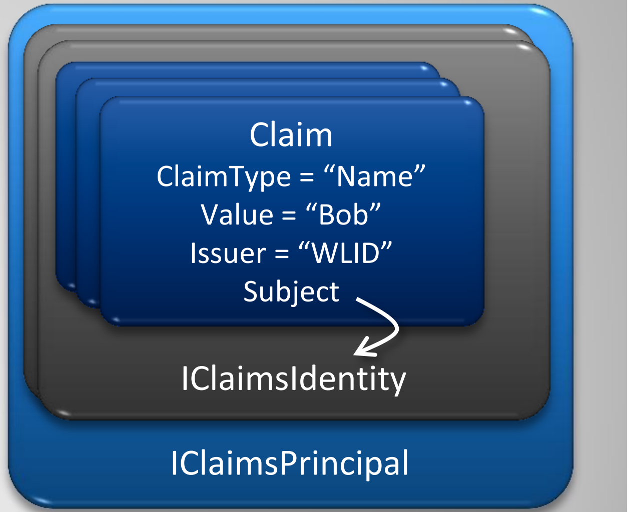
Claims

- Abstraction for
  - Authentication
  - Authorization
  - And more
- Decouple application to identity
- Allow anonymymity

- All properties are string
- ValueType indicate the value’s type

  Microsoft.IdentityModel.ClaimValueTypes contains numbers of values (date, datetime, boolean, integer, etc.)

```
public class Claim {
   // some members omitted for brevity
   public virtual string ClaimType        { get; }
   public virtual string Value            { get; }
   public virtual string ValueType        { get; }
   public virtual IDictionnary<string, string> Properties;
   public virtual string Issuer                  { get; }
   public virtual string OriginalIssuer          { get; }
   public virtual string IClaimIdentity Subject  { get; }
}
```

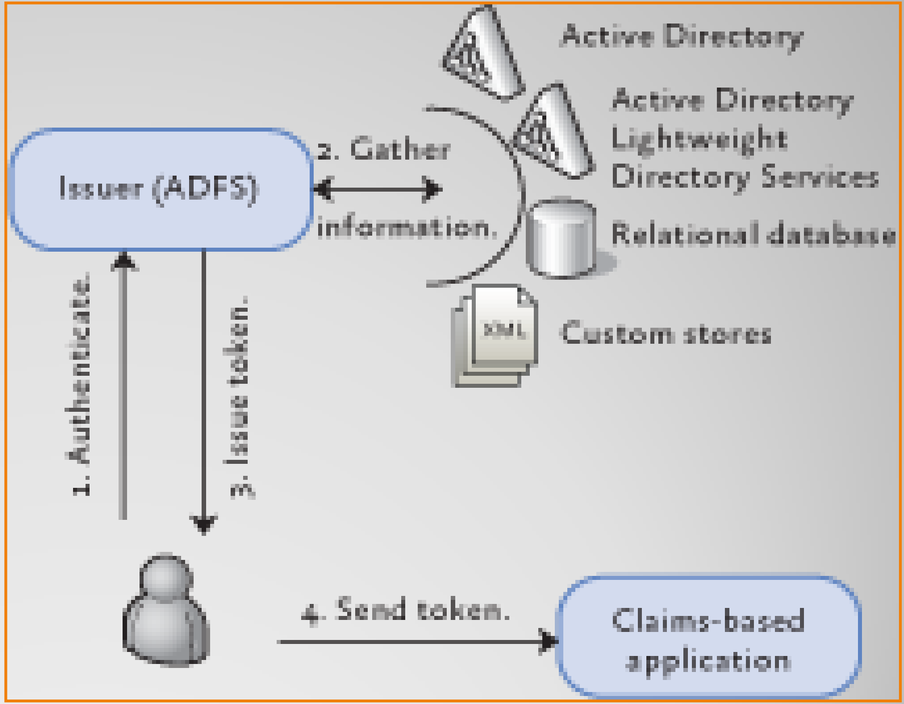


Claims : object model

Agenda

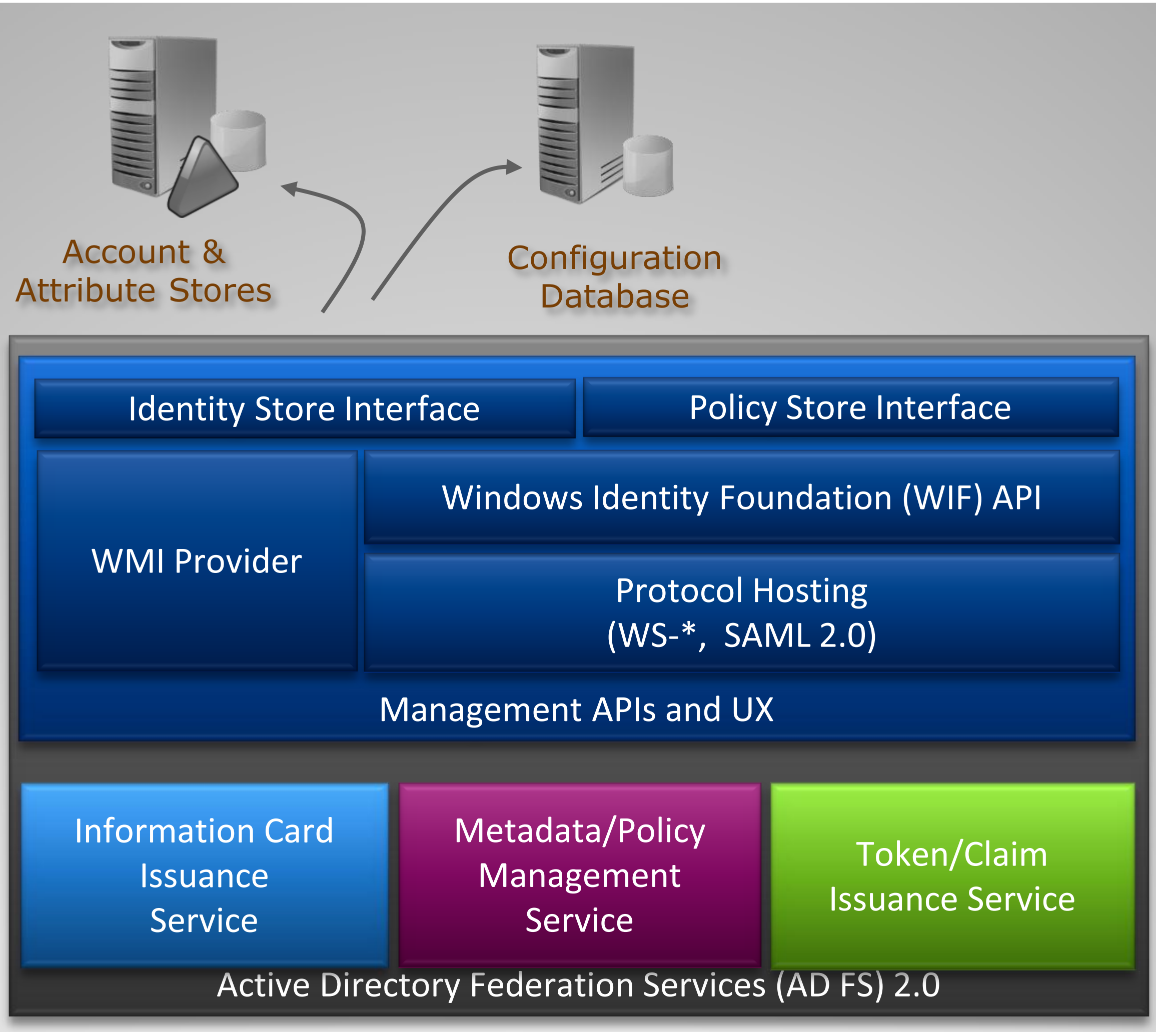
- Claim based Identity & Access Control
  - Claims
  - ADFS
  - WIF
- Integration
  - CAS Integration
  - Grouper Integration
  - To-do list
- Q&A

- A Secure Token Service for MS technologies
- Handles authentication,
- Extracts, transforms attributes
- With rule and policy engine



ADFS

ADFS : Architecture



Account & Attribute Stores

Configuration Database

Identity Store Interface

Policy Store Interface

WMI Provider

Windows Identity Foundation (WIF) API

Protocol Hosting
(WS-*, SAML 2.0)

Management APIs and UX

Information Card Issuance Service

Metadata/Policy Management Service

Token/Claim Issuance Service

Active Directory Federation Services (AD FS) 2.0

ADFS : very simplistic

- Based on WIF
- Extension points
  - Custom attribute store

- Ready for federation
- Uses SAML 2.0
- Tested with Sun, Novell and CA

- An STS starter kit on codeplex http://startersts.codeplex.com/

Agenda

- Claim based Identity & Access Control
  - Claims
  - ADFS
  - WIF
- Integration
  - CAS Integration
  - Grouper Integration
  - To-do list
- Q&A

- A framework for identity aware applications
- A unified programming model for ASP.NET and WCF
- A shield for the underlying protocol and cryptography

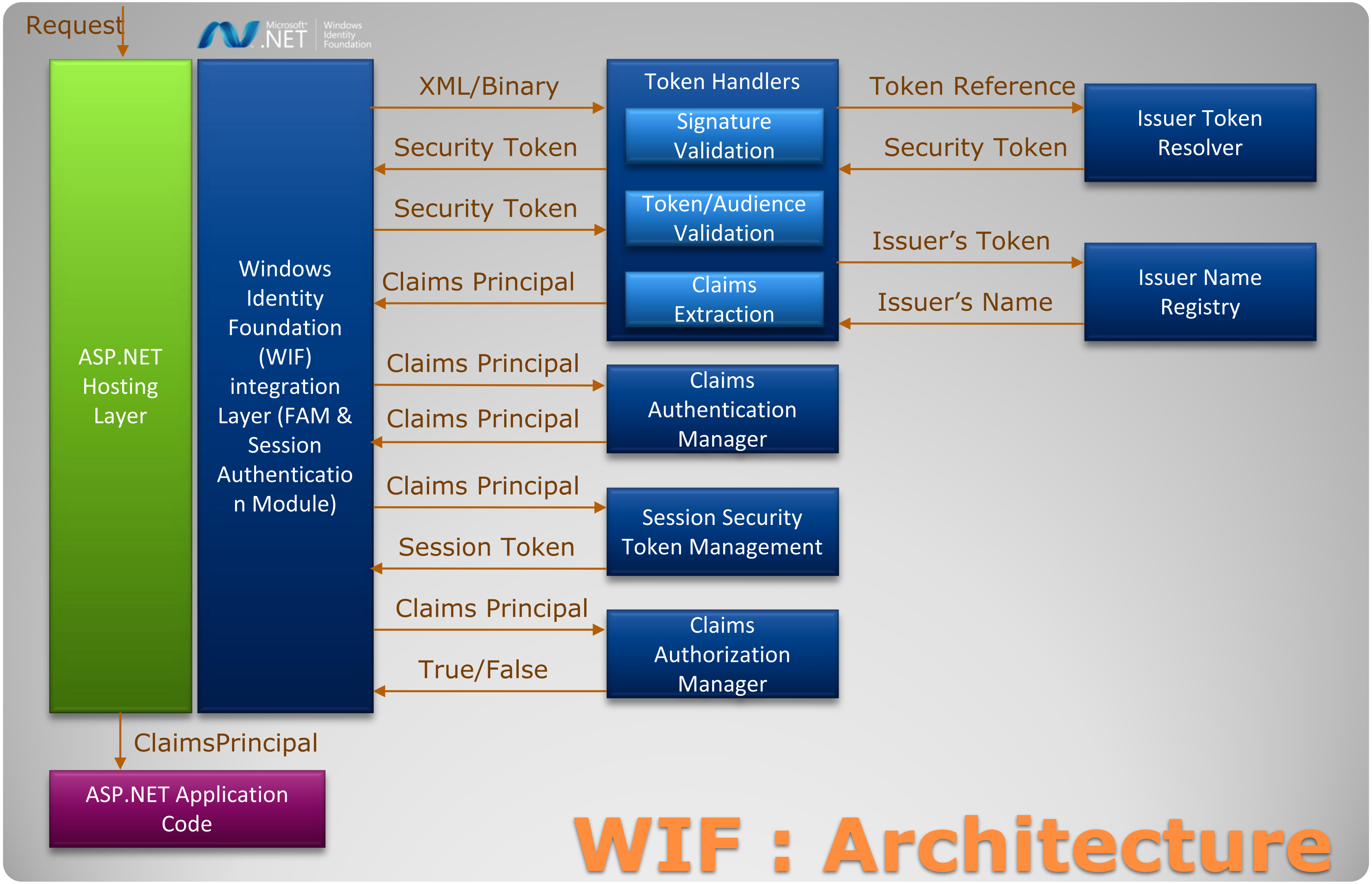
WIF : What is it ?

- Visual Studio templates for C#
- FedUtil : wizard for metadata registration
- HTTP Modules
- C2WTS : Claims to Windows Token Service
- APS.NET Controls

http://msdn.microsoft.com/en-us/library/ee748484.aspx

WIF : SDK

WIF : Architecture



WIF : Consuming claims

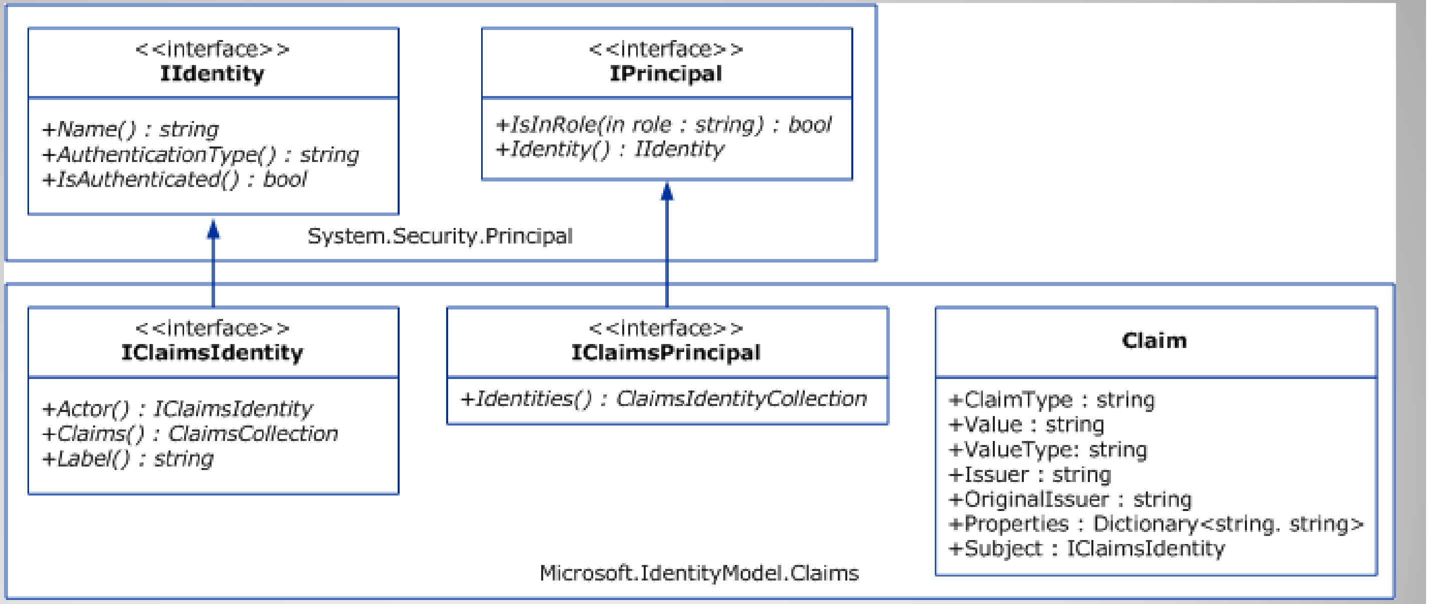
```
IClaimsIdentity id =((IClaimsPrincipal)Thread.CurrentPrincipal).Identities[0];

// you can use a simple foreach loop to find a claim...
string usersEmail = null;
foreach (Claim c in id.Claims)
{
   if (c.ClaimType == System.IdentityModel.Claims.ClaimTypes.Email)
   {
      UsersEmail = c.Value;
      break;
   }
}

// you can also use LINQ to find a claim
string usersFirstName = (from c in id.Claims
           where c.ClaimType == System.IdentityModel.Claims.ClaimTypes.GivenName
           select c).First().Value;
```

Claims : Authorization

- IsInRole still works
- The mapping is declared in web.config
- No break with non WIF application



<<interface>>
IIdentity

+Name() : string
+AuthenticationType() : string
+IsAuthenticated() : bool

<<interface>>
IPrincipal

+IsInRole(in role : string) : bool
+Identity() : IIdentity

System.Security.Principal

<<interface>>
IClaimsIdentity

+Actor() : IClaimsIdentity
+Claims() : ClaimsCollection
+Label() : string

<<interface>>
IClaimsPrincipal

+Identities() : ClaimsIdentityCollection

Claim

+ClaimType : string
+Value : string
+ValueType: string
+Issuer : string
+OriginalIssuer : string
+Properties : Dictionary<string, string>
+Subject : IClaimsIdentity

Microsoft.IdentityModel.Claims

WIF : Authorization

```
[ClaimsPrincipalPermission(SecurityAction.Demand,
              Resource = "Directory", Operation = "Browse")]
private bytes[] GetVideoFile(string path)
{}
```

- WIF can model the authorization data like
  - A ressource the subject wants to access
  - The actions the suject wants to realize on the ressource
  - This is an AuthorizationContext
- This policy can be stored in the stored in the application’s web.config file. It can be consume by the ClaimsAuthorizationManager class, a WIF extension point.
  - Hook for authorization logic
  - Define your CheckAccess implementation
- http://msdn.microsoft.com/en-us/magazine/ee335707.aspx

Integration

- Claim based Identity & Access Control
  - Claims
  - ADFS
  - WIF
- Integration
  - CAS Integration
    - Use the ‘deprecated’ membership provider
    - Tweak form authentication in the STS
    - Build a new STS
  - Grouper Integration
  - To-do list
- Q&A

Agenda

CAS : membership provider

- Just a membershib Provider
  - Reuse Cas.Net Module
- No need for WIF
- Might not be compatible with WIF

- Hook in the form based authentication
  - A post from least privilege
- Authentication provider ???

- Need more work !
- Does it make sense ?

CAS : ADFS FBA

- Should be easy
  - Thinktecture starter kit on codeplex http://startersts.codeplex.com/
  - How about rules and policy engine
- Why not use Shibboleth ?

CAS : STS

Agenda

- Claim based Identity & Access Control
  - Claims
  - ADFS
  - WIF
- Integration
  - CAS Integration
  - Grouper Integration
    - Role provider
    - Custom attribute store
  - To-do list
- Q&A

Authorization

- Is the complex part
  - Could we do RBAC ?
  - How to make delegation easy and secure
- Should be externalized
  - For treatment by business units
  - For audit
- …
- Grouper is my best choice

Grouper : Role Provider

- Just 5 methods to write
  - GetRolesForUser
  - GetUsersInRole
  - IsUserInRole
  - RoleExist
  - Initialize
- Plug into all asp.Net

Grouper : Attribute store

- Only 3 members in the interface
  - void Initialize (Dictionary<string,string> config)
  - IAsyncResult BeginExecuteQuery (string query, string[] parameters, AsyncCallback callback, Object state)
  - string[][] EndExecuteQuery (IAsyncResult result)
- Plus a few more for asynchronous calls
- A call looks like :
  - IAsyncResult result = attributeStore.BeginExecuteQuery("EmpName={0};EmpId,Age", new string[] {"Tim"}, null, null);
- A sample at connect.microsoft.com
  https://connect.microsoft.com/site642/Downloads/DownloadDetails.aspx?DownloadID=18933

- Claim based Identity & Access Control
  - Claims
  - ADFS
  - WIF
- Integration
  - CAS Integration
  - Grouper Integration
  - To-do list
- Q&A

Agenda

Future works

- RBAC with grouper in .Net
  - Use application actions as subject for roles
  - A role is a group of actions
- Grouper attribute store
- Test with Shibboleth (for ACAMP ?)
- Grouper role provider ?
- CAS STS ?

- Patterns & Practices : A guide to claims-based to Identity and Access Control http://msdn.microsoft.com/en-us/library/ff423674.aspx
- MSDN http://msdn.microsoft.com/en-us/library/ee748484.aspx http://msdn.microsoft.com/en-us/security/aa570351.aspx
- Microsoft connect https://connect.microsoft.com/site642
- Blogs
  Geneva team - http://blogs.msdn.com/card/
  Dominick Baier - http://www.leastprivilege.com
  Vittorio Bertocci - http://blogs.msdn.com/vbertocci/

links

Any question !

Thanks for listening