

Community Days - Milano, 16 e 17 dicembre 2010

## HARDC02

# Dai ruoli ai claim: perché e come decentralizzare l'autenticazione usando Windows Identity Foundation

Raffaele Rialdi

- Email: [malta@vevy.com](mailto:malta@vevy.com)
- Articoli e codice: <http://www.iamraf.net>
- Blog: <http://blogs.ugidotnet.org/raffaele>
- Twitter: [@raffaele](https://twitter.com/raffaele)



Profilo: <https://mvp.support.microsoft.com/profile/raffaele>

[aspitalia.com](http://aspitalia.com) [www.iamraf.net](http://www.iamraf.net) [LinqItalia.com](http://www.linqitalia.com) [SmartMatrix.it](http://www.smartmatrix.it) [UGIDOTNET](http://www.ugidotnet.org) [WinFXItalia.com](http://www.winfxitalia.com) [WinPhonetalia.com](http://www.winphonetalia.com)

---

---

---

---

---

---

---

---

---

---

## Agenda

- Passato, presente e futuro della CBA
- Fatica da Ruoli?
- Il presente è già basato sui Claim
- "Claim in action" in applicazioni ASP.NET
  - WS-Federation
- "Claim in action" in servizi WCF
  - WS-Trust
- Codice, codice, codice ...

[aspitalia.com](http://aspitalia.com) [www.iamraf.net](http://www.iamraf.net) [LinqItalia.com](http://www.linqitalia.com) [SmartMatrix.it](http://www.smartmatrix.it) [UGIDOTNET](http://www.ugidotnet.org) [WinFXItalia.com](http://www.winfxitalia.com) [WinPhonetalia.com](http://www.winphonetalia.com)

---

---

---

---

---

---

---

---

---

---

## Il presente e il futuro

- In passato esistevano i Claim di WCF
  - `System.IdentityModel.Claim` è da considerare obsoleta
  - `Microsoft.IdentityModel.Claim` è parte di WIF
- Il presente è basato sui Claim
  - Windows Live è un Secure Token Service (STS)
    - Implementa WS-Federation
  - Azure Access Control Service (ACS)
  - OpenID eroga Claim
- Il futuro è basato sui Claim
  - Silverlight 5 supporterà WS-TRUST
  - OAuth2 (draft)
  - ...

[aspitalia.com](http://aspitalia.com) [www.iamraf.net](http://www.iamraf.net) [LinqItalia.com](http://www.linqitalia.com) [SmartMatrix.it](http://www.smartmatrix.it) [UGIDOTNET](http://www.ugidotnet.org) [WinFXItalia.com](http://www.winfxitalia.com) [WinPhonetalia.com](http://www.winphonetalia.com)

---

---

---

---

---

---

---

---

---

---

## I ruoli



- Rispondono solo in modo booleano
- Un livello di astrazione per evitare di gestire i permessi a livello di singolo utente
- Costo in termini di performance

aspitalia.com LINGItalia.com Smeriamata.ee UGIdoNET WinFXItalia.com WinPonItalia.com

---

---

---

---

---

---

---

---

## Disaccoppiamento



STS  
(Prefettura)



Subject  
(utente)



Token =  
lista di claim



aspitalia.com LINGItalia.com Smeriamata.ee UGIdoNET WinFXItalia.com WinPonItalia.com

---

---

---

---

---

---

---

---

## I Claim

- Hanno un valore arbitrario
- Sono "asserzioni" sul soggetto
- Un livello di astrazione per evitare di gestire i permessi nell'applicazione
- Un claim può essere il superset di un ruolo (e usato come fosse un ruolo)

aspitalia.com LINGItalia.com Smeriamata.ee UGIdoNET WinFXItalia.com WinPonItalia.com

---

---

---

---

---

---

---

---



# DEMO ROLE TO CLAIM

aspitalia.com       

---

---

---

---

---

---

---

---

## CBA nelle Web Application

- ClaimsPrincipalHttpModule converte i token tradizionali in Claim
  - Attiva i Claim anche senza STS
  - Intercetta l'evento PostAuthenticateRequest
  - Prende il token generato da un altro modulo e lo converte in claim-based
- ClaimsAuthorizationModule
  - Permette l'uso di ClaimsAuthorizationManager in applicazioni asp.net (e wcf hosted in asp.net)
  - Intercetta l'evento AuthorizeRequest
    - Se l'utente è autenticato chiama l'authorization manager
    - Se l'autorizzazione è negativa termina con 401

aspitalia.com       

---

---

---

---

---

---

---

---

CBA = Claim Based Authentication

# DEMO CBA IN ASP.NET

aspitalia.com       

---

---

---

---

---

---

---

---

# STS SECURE TOKEN SERVICES

aspitalia.com   UNQitalia.com  SIMULAMATE.ORG  UGIDENET  WINFIDITALIA.COM  WINFONETITALIA.COM

---

---

---

---

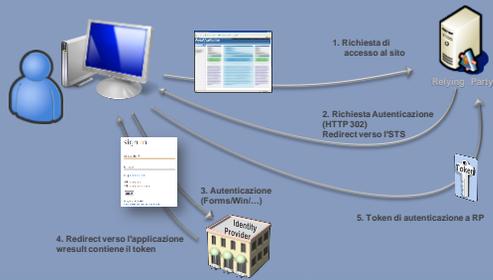
---

---

---

---

## Spostare l'autenticazione usando WS-Federation



aspitalia.com   UNQitalia.com  SIMULAMATE.ORG  UGIDENET  WINFIDITALIA.COM  WINFONETITALIA.COM

---

---

---

---

---

---

---

---

WS-Federation

## DEMO: STS PASSIVO E ASP.NET

aspitalia.com   UNQitalia.com  SIMULAMATE.ORG  UGIDENET  WINFIDITALIA.COM  WINFONETITALIA.COM

---

---

---

---

---

---

---

---

## Federation e asp.net

- Si vuole proteggere una parte del sito con il tag `<authorization />` ?
  - Usare il modulo `WSFederationAuthenticationModule`
    - Costruisce il principal con i claim
    - Alcuni eventi permettono di validare il token
  - Aggiungere il modulo `SessionAuthenticationModule` per mantenere l'autenticazione durante la navigazione
    - Usa un cookie come validazione
- Si vuole autenticare su richiesta dell'utente?
  - Il controllo `FederatedPassiveSignIn` gestisce la redirectione verso un STS gestendo i parametri
  - Il controllo `FederatedPassiveSignInStatus` ci dice se l'utente è autenticato

aspitalia.com | ... | aspitalia.com

---

---

---

---

---

---

---

---

## Spostare l'autenticazione usando WS-Trust



aspitalia.com | ... | aspitalia.com

---

---

---

---

---

---

---

---

WS-Trust

## DEMO: STS ATTIVO E WCF

aspitalia.com | ... | aspitalia.com

---

---

---

---

---

---

---

---

## WCF e Claims

- <federatedServiceHostConfiguration/> abilita WIF nei servizi WCF
- Si usa Thread.CurrentPrincipal per avere Identity e Claim
  - In precedenza si usavano ServiceSecurityContext e OperationContext
- WIF usa preferibilmente certificati nella sezione
  - <system.ServiceModel>/<behaviors>/<serviceBehavior>/<behavior>/<serviceCredentials>

aspitalia.com 

---

---

---

---

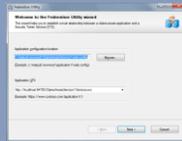
---

---

---

---

## FedUtil



- WIF ha un tool chiamato Federation Utility
  - Visual Studio lo integra nella voce "Add STS Reference"
- Può generare un STS locale (classe) o esistente
- Utilizza i metadati esposti da un STS per configurare i client attivi o le web-app

aspitalia.com 

---

---

---

---

---

---

---

---

## Hook di autenticazione e autorizzazione

- ClaimsAuthenticationManager
  - Permette la trasformazione, aggiunta e rimozione di claim. Override di Authenticate
- ClaimsAuthorizationManager
  - Intercettazione centralizzata sull'autorizzazione. Override di CheckAccess.
  - Essendo centralizzato permette di realizzare comodamente auditing

aspitalia.com 

---

---

---

---

---

---

---

---

## Scenari avanzati

- Delegation
  - La delegation di WIF conserva anche l'identity originale che è essenziale per l'auditing
- Authentication Assurance
  - È possibile scrivere nei claim quale meccanismo di autenticazione è stato usato per generare il token
  - Questo meccanismo permette di fornire certe informazioni solo, ad esempio, se è stato autenticato con smart card
- Il servizio "Claims To Windows Token" permette di generare un token Windows standard a partire da uno SAML di WIF



---

---

---

---

---

---

---

---

---

---

## Contatti



<http://blogs.ugidotnet.org/raffaele>



<http://www.iamraf.net/>



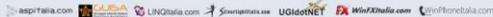
@raffaeler



malta@vevy.com



<http://www.communityring.net/>



---

---

---

---

---

---

---

---

---

---

## Slides e materiale

Nei prossimi giorni su

<http://www.communitydays.it/>

Libro su WIF  
di Vittorio Bertocci





---

---

---

---

---

---

---

---

---

---