

Federated Identity Essentials

Federated security models and claims-based access control are key to modern distributed systems, enabling business scenarios that are very difficult to implement otherwise. Federation allows users to authenticate in their own domain while being granted access to applications and services that belong to another domain or environment. This removes the need to provision and manage duplicate accounts for a single user, reduces overall application complexity, and enables Single Sign-On (SSO) scenarios loved by all users. Claims-based access is central to a federated security model whereby applications and services authorize access to features and functionality based on claims from issuers (the STS) in trusted domains. Claims can contain information about the user, roles, or permissions – and this makes for a highly flexible authorization model. Together, federated security and claims-based access enable a range of integration scenarios across applications, departments, and partners in a wider ecosystem. Platform tools in this area have also come a long way. Windows Identity Foundation (WIF) is a feature-rich identity model framework for building claims-based applications and services, and for supporting active and passive federated security scenarios. Active Directory Federation Services (AD FS) V2 is an out-of-the-box Security Token Service (STS) that handles authentication and claims transformation for federation scenarios. Windows CardSpace V2 presents users with an easy way to select their digital identity for authentication.

During this intense, two-day class you will learn how to apply claims-based and federated identity and the relevant architectural scenarios. The class demonstrates the rich features of WIF for supporting claims-based identity and federation in your ASP.NET and WCF applications; explains how to work with AD FS V2 as the identity provider and STS in a federated scenario; provides the foundation for building custom STS with WIF for scenarios that warrant it; and discusses scenarios where managed information cards and CardSpace play a key role. By the end of this tour de force you will be well versed in the subject of claims-based and federated identity. The class offers not just the technical but also the business perspective and the practical reasons to leverage claims-based and federated identity – while utilizing numerous demonstrations that include IDesign's original tools and utilities.

Format

On top of frontal presentations this class illustrates concepts with numerous demonstrations. These demonstrations serve as a starting point for new projects and as a rich reference and samples source.

Target Audience

.NET developers, architects or technical leads who are exploring the benefits of claims-based and federated security and who are looking to understand the relevant scenarios, technology platforms, and developer tools.

Course Outline

Federated Identity Overview

- Identity challenges
- Claims-based and federated identity benefits
- Platform tools and technologies
- Terminology and protocols

Architectural Scenarios

- Active and passive federation
- Identity federation and token issuance
- Federating with multiple domains
- Home realm selection and CardSpace
- Claims transformation
- The role of a resource STS or federation provider
- Federation for REST-based web resources

Windows Identity Foundation (WIF) Overview

- WIF core features
- Enabling passive federation for ASP.NET
- Single sign-on/sign-out
- Exposing federated service endpoints
- Caching tokens
- Identity delegation
- Home realm selection

WIF and Claims-Based Access Control

- ClaimsPrincipal and ClaimsIdentity
- ClaimsAuthenticationManager and ClaimsAuthorizationManager
- Integration with .NET role-based security
- ASP.NET Login controls
- Web Forms and MVC strategies
- WCF service operations and permission demands
- Migration strategies from claims-based to federated

Security Token Services

- Security Token Service (STS) overview
- ADFS V2 platform features
- Active and passive federation scenarios
- Policy and rules configuration
- Custom STS implementations with WIF

Windows CardSpace

- CardSpace-enabled authentication for ASP.NET and WCF
- CardTile and ASP.NET
- Issuing managed information cards

Federation with the Access Control Service

- Access Control Service (ACS) overview
- Securing REST-based web resources with the Access Control Service
- Protocols support and interoperability
- Configuring claims-transformation rules for access control
- Federated security scenarios for REST-based web resources
- with the Access Control Service
- Access control key management