The Add STS Reference … Visual Studio functionality (cmdline utility FedUtil) no longer exists; instead you can use the new Visual Studio extension Identity and Access Tool for Visual Studio 2012. This allows you to federate with an existing STS or use LocalSTS to test your solutions. After installing the extension you can right-click on your project and look for Identity and Access in the context menu.

claims can be used directly in existing project templates for ASP.Net, web sites, and WCF.

claims-based authorization (CBAC)

Federated Identity comprises three components: Active Directory® Federation Services (AD FS) 2.0, Windows Azure Access Control Services (ACS), and WIF.

For more information about WIF, see the Windows Identity Foundation Web site (http://go.microsoft.com/fwlink/?LinkId=149009) at the Security Developer Center on MSDN.

The framework abstracts the WS-Trust and WS-Federation protocols and presents developers with APIs for building claims-aware applications and, if needed, security token services (STS)s. Applications can use WIF to process tokens issued from STSs, such as AD FS 2.0 and ACS, and make identity-based decisions at the web application or web service.

your application is no longer responsible for the following:

Authenticating users.

Storing user accounts and passwords.

Calling to enterprise directories to look up user identity details.

Integrating with identity systems from other platforms or companies.

In this model, your application doesn’t look up user attributes in a directory. Instead, the user delivers claims to your application, and your application examines them. Each claim is made by an issuer, and you trust the claim only as much as you trust the issuer. For example, you trust a claim made by your company’s domain controller more than you trust a claim made by the user herself. WIF represents claims with a Claim type, which has an Issuer property that allows you to find out who issued the claim.

This issuing authority is a Web application or Web service that knows how to issue security tokens. It must have enough knowledge to be able to issue the proper claims given the target relying party and the user making the request, and might be responsible for interacting with user stores to look up claims and authenticate the users themselves.