

Configuring and Deploying a Security Token Service



Kevin Dockx

@KevinDockx | <http://blog.kevindockx.com/>

Choosing a Security Token Service

- Azure Active Directory
 - <http://azure.microsoft.com/en-us/services/active-directory/>
- Active Directory Federation Services (ADFS) 3.0
 - Windows 2012 R2 (role service)
 - Only supports Authorization Code flow
- ThinkTecture Identity Server v3

ThinkTecture Identity Server v3

- Extensible OpenID Connect and OAuth 2.0 Security Token Service and Authorization Server by @leastprivilege & @brocklallen
- Part of the .NET Foundation: <http://www.dotnetfoundation.org/>
- Project site: <https://github.com/thinktecture/Thinktecture.IdentityServer.v3/>

Clients and Scopes



Client: models an OpenID Connect or OAuth2 client

- native, web, user-agent, ...

Scope: models an OpenID Connect (Identity) or OAuth2 (Resource) scope

- the **intent** of the client

Users



User: the entity that (dis)allows client/scope

- custom user store
- third-party providers (Microsoft, Google, Facebook, ...)

Hosting, Configuring and Deploying IdentityServer

Learn how to configure and deploy a security token service



Summary



ThinkTecture Identity Server v3 is a security token service that implements OAuth 2.0 & OpenID Connect 1.0

Easy to configure & easy to deploy