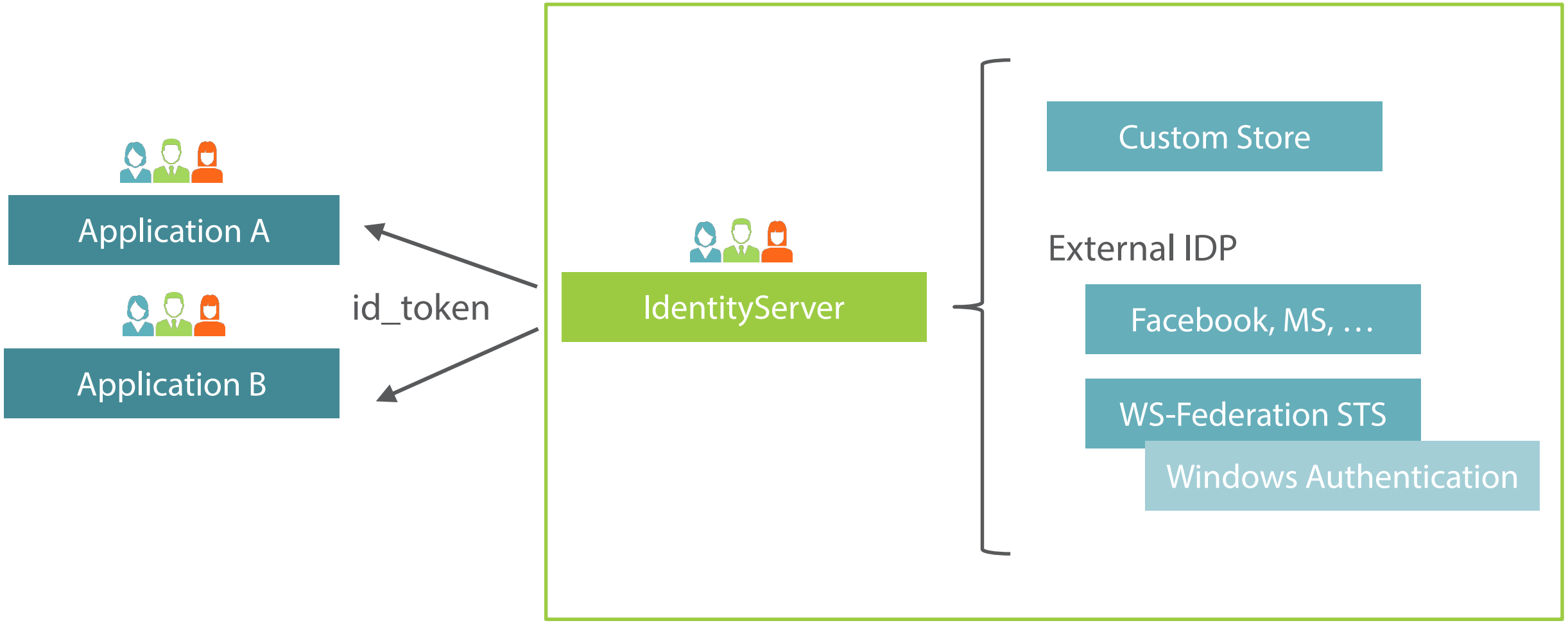
Dealing with Credentials

Kevin Dockx

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

Dealing with Credentials

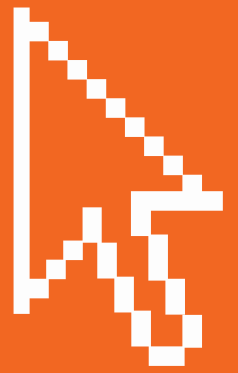


A Custom User Store

Learn how to work with credentials
that are stored in a custom user store

Creating an Account by Providing a Registration Page

Learn how to allow a user to create a new account by providing a registration page



Integrating with Third-Party Providers

Learn how to integrate with Facebook for authentication

Multiple Logins, One Account

Learn how to link an external identity provider to an existing user account

Creating an Account From an External Identity Provider

Learn how to create a new account from an external identity provider login

WS-Federation and Windows Authentication

WS-Federation + WS-Trust + WS-SecurityPolicy

(provides a basic model for federation between identity providers and relying parties)

SOAP, Windows Communication Foundation

WS-Federation and Windows Authentication

Learn how to use a WS-Federation-enabled STS, with Windows authentication enabled, as an external identity provider

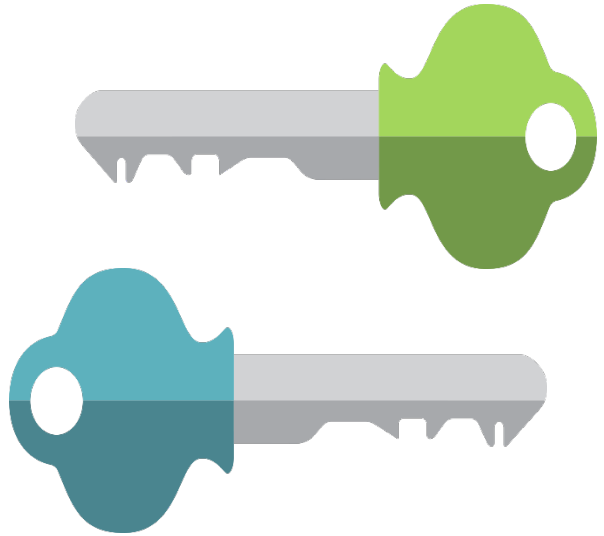
Customizing the Login Flow Through Partial Login

Learn how to customize the login flow by using the partial login functionality to ask a user for additional information

Two-Factor Authentication

2FA provides identification of users by means of the combination of two different components

(something you know, something you possess, something that's inseparable from you)



Not all applications might require 2FA

Use **acr_values** parameter (to authorization endpoint)

Two-Factor Authentication

Learn how to achieve two-factor authentication

Additional Packages and Resources

- ASP.NET Identity Support
  https://github.com/IdentityServer/IdentityServer3.AspNetIdentity

- Entity Framework Persistence Layer
  https://github.com/IdentityServer/IdentityServer3.EntityFramework

- Identity Manager
  https://github.com/IdentityManager/IdentityManager

Summary

OAuth 2.0 allows secure authorization from web, mobile and desktop applications

Grants/flows are means to achieve authorization

OpenID Connect adds authentication & identity information to OAuth 2.0

Impersonation allows us to secure the API depending on the user

Summary

Use refresh tokens for long-lived access (MVC) or a hidden iFrame to request new tokens (Angular)

Use a custom user service for working with credentials & extending authentication

You’re ready to be AWESOME!

@KevinDockx