

# Sécurité: Authentification et autorisation modernes



## WorkshopPLUS

### **Public concerné :**

*Cet atelier présente un contenu de niveau 300 ciblant les rôles techniques impliqués dans le développement de logiciels tels que les architectes et les développeurs dans le but de les aider à comprendre la nouvelle approche basée sur des protocoles standards tels que OAuth2, OpenID Connect, JWT et SAML.*

### **Prérequis :**

*Les prérequis de ce cours sont les suivants :*

- *Expérience avec Visual Studio*
- *Connaissance de base de C# pour comprendre le code source utilisé dans les démos et les labs.*

## Introduction

Le développement d'applications fonctionnant dans l'environnement Internet nécessite la compréhension des options disponibles pour réaliser l'authentification et l'autorisation. Ces options incluent un ensemble de protocoles tels que OAuth2 et WS-Federation, ainsi que des outils et des environnements tels que Azure AD, AD FS et ADAL. L'objectif de cet atelier de trois jours est de former les architectes et les développeurs, au développement d'applications nécessitant une technologie d'authentification et d'autorisation adaptée au cloud. L'atelier couvre à la fois les modèles architecturaux communs, les protocoles standard de l'industrie et les outils utilisés pour les mettre en œuvre. Les aspects outils et infrastructure de cette formation sont axés sur les technologies Microsoft.

## Principales caractéristiques et avantages

Vous comprendrez comment le contrôle d'accès, l'authentification et l'autorisation doivent être adaptés lorsque les applications et / ou les utilisateurs utilisent Internet. Vous apprendrez à utiliser l'infrastructure Microsoft, Azure AD, AD FS et les outils de développement pour sécuriser vos applications en utilisant les protocoles standards de l'industrie tels que SAML, WS-federation et OAuth2.

## Plus-values techniques

Après avoir suivi cette formation, vous serez en mesure :

- De comprendre l'étendue et les limites des différents protocoles d'authentification
- De choisir le protocole approprié à votre application
- De choisir les outils nécessaires à son implémentation
- De développer des applications utilisant ces outils
- D'utiliser des protocoles d'authentification modernes pour les applications web et natives (OAuth2 / OpenID Connect)

## Programme

Ce workshop se déroule sur trois jours complets. Les participants doivent anticiper les horaires de début et de fin pour l'ensemble des journées. Partir avant la fin de la journée est déconseillé.

### **Matériel requis pour les labs :**

Les participants auront besoin d'un ordinateur tournant au moins Windows 7 avec l'infrastructure et les logiciels suivants :

- Visual Studio 2017 (édition gratuite ou supérieure)
- PDF Reader
- Une connexion Internet permettant l'accès au portail Azure et aux machines virtuelles par RDP (module AD FS uniquement)

Les participants auront également besoin d'un compte Microsoft pour se connecter à l'environnement virtuel. La salle de formation devra posséder un réseau avec un accès à Internet et une bande passante d'au moins 2 Mbps. Le port TCP 443 devra être ouvert. Nous recommandons fortement un réseau câblé dans la salle de formation.

**Module 01 : Introduction** : Ce module fournit une vue d'ensemble des problématiques d'authentification et d'autorisation des applications Internet, la raison d'être des différents protocoles (OpenIDConnect, OAuth2, SAML) et les outils Microsoft utilisés pour les prendre en charge (Azure AD, AD FS, Windows Application Proxy, OWIN et les toolkits ADAL).

**Module 02 : OAuth2 and OpenID Connect** : Ce module se penche sur les détails de ces deux protocoles. Il passe en revue les différents flux définis par OAuth2 et leur adéquation aux topologies d'application courantes. Il décrit également les menaces de sécurité qu'ils permettent d'adresser.

**Module 03 : Introduction à AD FS** : Ce module fournit une vue d'ensemble de la solution Microsoft de fédération d'applications comprenant son architecture, ses fonctions principales, sa console d'administration, ses commandes PowerShell de base et son utilisation typique pour prendre en charge les besoins d'authentification des applications.

**Module 04 : Introduction à Azure AD** : Ce module couvre l'objectif et les principales fonctionnalités d'Azure AD, en fournissant un aperçu de ses fonctionnalités B2E, B2B et B2C, de sa gestion des utilisateurs, de la configuration de ses applications et de l'utilisation de GraphAPI.

**Module 05 : Les applications basées sur des claims** : Ce module se concentre sur l'utilisation pratique des connaissances acquises dans les modules précédents pour implémenter un ensemble d'applications utilisant les protocoles OAuth2, GraphAPI et diverses autres fonctionnalités d'Azure AD (par exemple, les rôles d'application).

**Module 06 : Guide ADAL/MSAL** : Examen des API utilisées pour obtenir des jetons OAuth2 et OIDC à partir d'Azure AD ou d'AD FS.

**Module 07 : Gestionnaire du protocole OWIN** : Passage en revue des méthodes utilisées pour initier l'authentification des applications web par des protocoles passifs et prendre en charge (valider / augmenter) les jetons de sécurité reçus.

**Module 08 : Développement d'application** : Ce module détaille le développement d'un environnement complexe, constitué d'applications fournissant une interface utilisateur web, des API, des clients natifs de type "rich client" ainsi que des services communiquant et s'authentifiant mutuellement. Cet exercice peut être adapté au développement prévu du client.