appdome

No-Code Microsoft Identity in Mobile Apps

Add Microsoft Identity to any app, built in any platform.
No Coding and no dependencies

WHAT IS MICROSOFT IDENTITY?

Most enterprise IT ecosystems for the past 20+ years have been based on Microsoft. And if you've already standardized on Microsoft applications such as Office 365, you're most certainly using Microsoft Identity to authenticate to your corporate network. Microsoft offers a comprehensive collection of market leading identity, authentication and access solutions like Azure AD, Active Directory (Microsoft AD), Active Directory Authentication Library (ADAL) and more. These services and others are well integrated with Microsoft apps and other services – delivering a seamless experience to users.

THE CHALLENGE FOR MICROSOFT IDENTITY

Organizations face two closely related challenges using Microsoft Identity:

(1) mobile apps that don't support common standards like SAML, OpenID Connect (OIDC) or OAuth 2.0,

(2) non-Microsoft mobile apps. Most mobile apps don't come with Microsoft Identity built into the app.

Similarly, non-Microsoft mobile apps often don't support the proprietary Microsoft identity frameworks needed to use some Microsoft Identity services. In all cases, developers must go through the hard work that is necessary to learn, build, maintain and enable a mobile app to use Microsoft Identity services. In many cases, supporting Microsoft Identity in an app goes unfulfilled.

INDUSTRY FIRST - NO-CODE MICROSOFT IDENTITY IN MOBILE APPS

Appdome and Microsoft have teamed up to solve the tough challenge of delivering a consistent single sign-on (SSO) experience using Microsoft Identity with all mobile apps. Appdome's no-code mobile integration platform makes it easy to add Microsoft authentication, authorization and identity services to any iOS or Android app. Using Appdome, enterprises and mobile developers can add Microsoft Identity without coding in the app and without changing or upgrading the mobile app server.

To connect any mobile app to any Microsoft identity service, Appdome users simply upload an app, select the Microsoft Identity service(s) they want to integrate, and click "Fuse My App"

CUSTOMER BENEFITS

The following benefits of Appdome for No Code Microsoft Identity Services in Mobile Apps come with every implementation:

Cross App Identity: Allows mobile apps to share authentication state no matter what Microsoft Identity service is used. Signing in to one app automatically unlocks other apps in the group.

Conditional Access: Grants access to restricted resources using separate resource-level authentication and authorization no matter what Microsoft Identity services is used.

No In-App Standards Dependencies: No need to manually implement or support SAML, OAuth or OIDC in apps.

Direct ID brokering: Mobile apps authenticate directly to the Microsoft Identity service of choice, without using public identity brokers.

In-App Secure ID: Encrypts all mobile app credentials, cookies, and tokens and stores them securely in a non-shared area within the Fusion Layer of the app.

No coding: Zero coding required, ever.

APPDOME'S NO-CODE FOR MICROSOFT IDENTITY OPTIONS IN MOBILE APPS

Azure Active Directory (Azure AD)

Microsoft Azure AD is Microsoft's flagship Identity service. It combines directory services, authentication, authorization, and SSO in a single cloud-based solution. However, for a mobile app to connect to an Azure AD environment, the app must utilize the same authentication standard used in the Azure AD server (e.g. OpenID, OIDC, OAuth 2.0). The problem is mobile apps aren't built to accommodate multiple authentication standards or Azure AD tokens out of the box. Adding or changing authentication standards is not trivial. And with manual coding Azure AD to a single app, it is not possible for that app to share authentication state with other apps. With Appdome, enterprises can instantly add Azure AD to any mobile app. Outgoing connections will include the correct Azure AD tokens, and mobile apps will share authentication state.

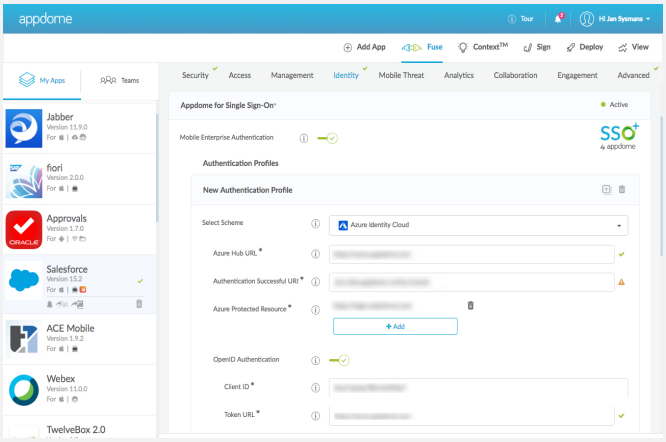

Figure 1: Appdome for Microsoft Identity - Microsoft Azure AD

Microsoft ADAL

Microsoft is a pioneer in modern authentication, including Microsoft ADAL and its support for OAuth 2.0. Designed to make secured resources available to apps via security tokens, ADAL provides a unique benefit to Microsoft customers, by enabling multiple apps to share authentication state. Most Microsoft apps use ADAL natively. While the Microsoft Authenticator App was designed to pass ADAL tokens to other apps, non-Microsoft apps don't come pre-built to use the ADAL framework. Appdome broadens the reach of Microsoft ADAL, enabling it to work with non-Microsoft apps. This means that Microsoft apps and non-Microsoft apps can share authentication state with each other (e.g., Outlook to Cisco WebEx). Using Appdome, ADAL can work in direct mode or brokering mode, and tokens can be consumed by any app or authentication gateway. Appdome users can also elect to validate accessed authorities using ADAL, offering the same Microsoft ADAL-SSO with all apps.

Active Directory (Kerberos & NTLM)

Older Microsoft Identity services such as Active Directory (including NTLM and Kerberos) rely on Windows authentication and are still pervasive in enterprises today. This poses significant challenges for most modern apps, which have their own cloud-based authentication workflows and don't have a mechanism to show the authentication portal or attach AD cookies and authorization headers to networking requests. Attempting to retrofit a mobile app to support NTLM or Kerberos can be a very complex and time-consuming undertaking, all with a non-guaranteed outcome. With Appdome, organizations can add Active Directory services to any app in minutes, without any coding at all. There is no need to add webviews at the authentication point. And Appdome also automatically overcomes compatibility and synchronization challenges. Using Appdome to add active Directory services also enables mobile apps to share authentication state among Fused apps on a device.

Microsoft Client Side Certificates

SCEP is a protocol used to provision client-side certificates to endpoints, primarily mobile devices. Appdome has extended SCEP, so that client-side certificates can persist inside mobile apps. In other words, client-side certifications can be provisioned directly to the mobile app. For Microsoft apps, customers can distribute SCEP certificates using Intune or via MS Network Device Enrollment Service (NDES). However, Non-MS mobile apps don't come with Intune built-in. On Appdome, Microsoft customers can solve this challenge quickly and easily by Fusing the Intune App SDK to any mobile app in minutes. Then they can distribute the certificates to mobile apps via Intune, providing the same automated experience enjoyed for Microsoft apps. The client side certificates can then be used to authenticate each user with a unique certificate issued specifically for him/her.

Microsoft AppProxy

Microsoft's Azure AD Application Proxy provides SSO and secure remote access for on-premise web apps. With Appdome, Microsoft AppProxy can be extended to Android and iOS apps, for controlled authentication. Enterprises can Fuse Appdome for Microsoft AppProxy, enabling Appdome-Fused mobile apps to tunnel traffic using two main modes: (1) transparent (blind) proxy and (2) reverse proxy. Transparent mode is suitable for internal resources which are not publicly resolvable. Reverse-proxy is suitable for publicly resolvable resources with a 1:1 mapping. Appdome for Microsoft AppProxy provides per-resource authentication options, as well as the ability to share authentication state between apps.

Learn more about Appdome for Microsoft Identity at **www.appdome.com** or open a free Appdome account at **fusion.appdome.com** and start fusing !

About Appdome

Appdome is the industry's first no-code platform for mobile integration. Appdome's patented* technology enables the rapid integration of multiple third-party functions to apps, shortening the deployment cycle and connecting mobile apps to other services on-demand. Appdome's codeless service allows users to complete integration projects on the final application package in seconds. No source code or development expertise is required. Likewise, no modifications to an app or SDK are required to complete integrations. The solution is currently used by the world's leading financial, healthcare and e-commerce companies to support productivity, compliance, and security for consumers and employees. For more information, visit www.appdome.com.

* Yehuda et al. Method and a system for merging several binary executables. U.S. Patent 9,934,017 B2 filed November 15, 2015, and issued April 3, 2018.