appdome

APPDOME FOR MFA - MOBILE MFA ANYWHERE

Add Multi-Factor Authentication to any Android and iOS app, in seconds without coding

MOBILE MFA IS A CRITICAL ENTERPRISE REQUIREMENT

Multifactor Authentication (MFA) is a security system which requires users to prove their identity from at least two independent categories of credentials before they can complete a transaction, access a protected system, or complete a sensitive action.

The three most common categories are often described as something you know (e.g. a pincode), something you have (e.g. a key fob or token) and something you are (e.g. a fingerprint scan).

MFA has quickly become a must-have tool for security and identity professionals to protect their organizations and users from an onslaught of breaches, cyberattacks, data theft, network highjacks, all of which may result from a malicious party gaining unauthorized access to private resources.

CHALLENGES WITH MOBILE MFA

MFA is a critical component of a 'Zero Trust' security posture, and the battle cry of the day has become "MFA Everywhere". In other words, all applications and all access methods should be protected by a modern MFA solution, right? However, there's a big problem when it comes to mobile. Specifically, most (if not all) mobile apps don't come with MFA capabilities built-in.

A vast majority of mobile apps still rely on static individual username/password schemes. Even if the app supports modern authentication mechanism such as SAML, OpenID Connect or OAuth, you would still need to implement a vendor specific API or SDK into the app in order to achieve MFA. And that would require access to the app's source code then modifying the code to implement the SDK manually.

An alternative to manual SDK implementation is to leverage a separate, standalone 'authenticator' app to generate random passcodes. However, your organization may not be willing to absorb the added management and configuration overhead/complexity of 'yet another app'. Further, if not implemented carefully you run the risk of introducing a single point of failure or compromise.

What if you can go the 'native', in-app route and eliminate all manual integration and add MFA to any Android and iOS app, built in any framework, instantly without coding?

ADD MFA TO ANY MOBILE APP IN SECONDS

That's exactly what Appdome for MFA delivers. Using Appdome's no-code mobile integration platform as a service, security and identity professionals can implement their choice of market-leading MFA solutions to any mobile app in seconds without coding. Using Appdome, there are no development or coding prerequisites. For example, there is no Appdome SDK, libraries, or plug-ins to implement. To add MFA to any mobile app, Appdome customers simply upload an app binary, select their favorite MFA vendor SDK, choose their deployment mode, input a few configuration fields, and click ***Build My App***. AMI, Appdome's AI-Enhanced Digital Developer completes the integration in about 30 seconds.

Appdome is 100% compatible with all Android and iOS apps, developed in any environment, no matter how the app is built. Appdome supports all native, hybrid and non-native apps. Appdome doesn't require access to source code or require any standards, SDKs or APIs to be added to the app manually. Appdome-Fused apps can be deployed through any public or private app store.

APPDOME SUPPORTS ALL LEADING MFA SERVICES

Appdome offers an instant, no-code implementation of the MFA service to any app. Appdome supports any MFA service, with all leading services available on the platform today.

Nexmo Verify

Nexmo Verify allows users to implement two factor authentication (2FA) using temporary verification codes sent to a mobile or landline over SMS and/or an automated voice call. Nexmo offers password-less authentication, allowing you to replace static passwords with single use codes sent over SMS, voice or push notifications.

OneLogin

OneLogin enables you to protect your organization against growing attacks with policy-based access control for login, and password resets based on location, application and user privilege level.

PingID

PingID enables mobile apps to use multiple authentication methods such as mobile push authentication, OTP, and facial recognition.

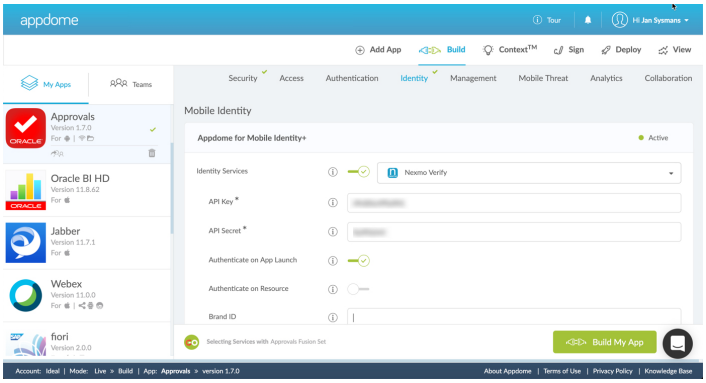

Image: no-code implementation of the Nexmo Verify service to Oracle Approvals

APPDOME IDENTITY SUITE

The Appdome Identity Suite is a collection of extensions which enables you to customize and extend any Identity service with an enriched set of functions listed below. Appdome's Identity helps you achieve a unified identity management experience for all users and all apps.

Authenticate on App Launch - In this mode, as soon as the mobile user opens a Fused app, they will receive an in-app challenge/prompt from the MFA provider's service. Upon receiving the challenge, the mobile user needs to accurately supply the required credentials in order to access the app. Otherwise, access is denied.

Authenticate on Resource - In this mode, the mobile user will receive the in-app challenge/prompt from the MFA provider's service when they attempt to access a protected server or resource (supplied during the Build process). Upon receiving the challenge, the mobile user needs to accurately supply the required credentials in order to access the protected resource. Otherwise, access is denied.

DEV-Events™ - In this mode, developers can use a standard, generic event broadcasting mechanism inside the app to trigger the in-app challenge/prompt from the MFA provider's service. Upon receiving the challenge, the mobile user needs to accurately supply the required credentials in order to access the protected resource. Otherwise, access is denied.

DynamicUI™ – When this feature is enabled, Appdome's AI technology dynamically adjusts and adapts the MFA provider's UI screens so that they adopt the look and feel of the app's native UI and branding elements. This results in a seamless and cohesive native app experience where integrated components blend naturally with the original design of the app.

Comprehensive App Security - Included with every MFA integration on Appdome is ONEShield™, a complete app-shielding solution that adds anti-tamparing, anti-debugging, anti-reversing and other app hardering mechanisms to the Fused app.

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

ABOUT APPDOME

Appdome is the industry's first no-code mobile integration platform. Appdome's patented*, Fusion technology and its AI-Digital Developer™, known as AMI, powers a self-service platform that allows anyone to complete the integration of thousands of mobile services, standards, vendors, SDKs and APIs in security, authentication, access, mobility, mobile threat, analytics and more, adding these services to any mobile app instantly. Leading financial, healthcare, government and e-commerce providers use Appdome to deliver rich mobile experiences, eliminating development complexity and accelerating mobile app lifecycles. 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.