DATASHEET

appdome for SSO+

MOBILE AUTHENTICATION CHOICE WITHOUT CODING

SSO+ by appdome

Appdome for SSO+ makes it easy to add enterprise authentication and cloud identity services to any mobile app. Developers and non-developers can instantly add native and web-based authentication, authorization and access control services to Android and iOS apps in seconds, no code or coding required. This includes IDaaS, IAM, SSO, MFA, authorization and resource access from traditional enterprise on-premise identity systems and cloud identity providers such as Okta or Microsoft Azure AD. There is no need to code SAML, OAuth, OpenID Connect or other standards into an app.

ENTERPRISE AUTHENTICATION WITHOUT CODING

Using Appdome for SSO, enterprises can connect any mobile app to their cloud or on-premise identity system of choice, leveraging modern identity standards (eg: SAML 2.0, OAuth2, OIDC) or traditional protocols (eg: Kerberos, KCD, ADFS, or WDav). This frees enterprises, developers and ISVs from the difficult task of coding and maintaining various identity standards and/or an identity provider's API/SDK inside every app demanded by users.

Appdome eliminates the ongoing development burden required to maintaining synchronization across providers, standards, and apps. Enterprises can connect Android and iOS apps to any identity system of choice. This allows organizations to trust the identity system for authentication, authorization and access to enterprise infrastructure and resources quickly and easily.

COMPLETE AUTHENTICATION AND IDENTITY SYSTEM CHOICE

Organizations are demanding that mobile apps connect to and leverage their chosen cloud or on-premise identity solutions. Appdome for SSO supports all traditional and modern authentication, authorization and access methods, including IDaaS and IAM providers. Examples of identity systems supported by Appdome for SSO include web and SAML-based authenication portals, and cloud-first IDaaS providers such as Azure AD, Okta, OneLogin and Auth0.

Appdome for SSO ensures that the mobile app implements the full range of services from the identity system. This overcomes incompatibilities between the app and the identity system, maintaining session cookies inside the app and ensuring traffic from the app includes the relevant headers and tokens to ensure appropriate access to enteprise resources. Customers can also add standard authentication protocols in a stand-alone mode such as OIDC, Kerberos, or KCD to support specific enterprise use cases.

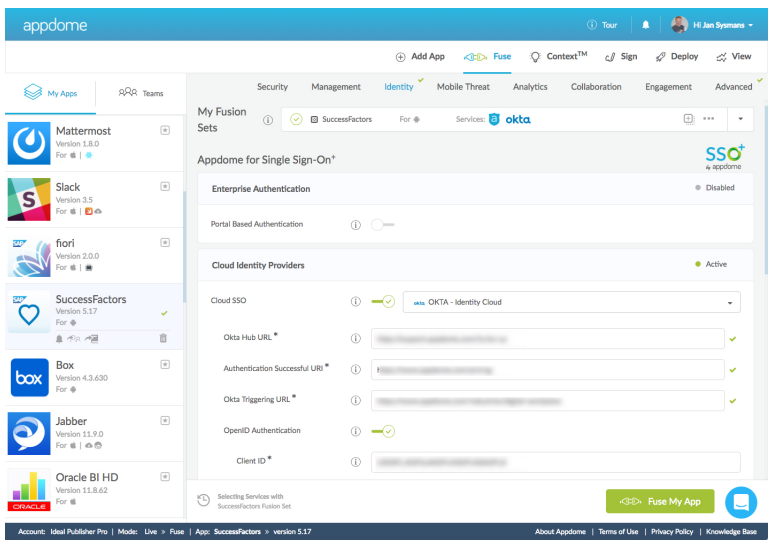

Figure 1: Fusing the Okta SSO service on the Appdome platform.

The following chart highlights some of the key capabilities that make Appdome for SSO+ a clear choice over manual SSO implementation.

THE APPDOME FOR SSO+ ADVANTAGE

Federated Authentication	Appdome's unique mobile app federation framework allows Appdome for SSO+ enabled apps to trust enterprise and cloud identity services and share valid authentication and session state among Fused apps. This allows a successful authentication to an enterprise or cloud identity service to grant access to an app (even if the app is natively coded with a basic authentication workflow) and allow an authentication event to one Appdome Fused app to unlock all Fused apps on a device.
Direct ID Brokering	Appdome for SSO+ eliminates MiTM attacks with Direct ID Brokering. Traditional SSO implementations require the mobile client to resolve the ID in the clear and utilize server-level policies to redirect the mobile client to the identity provider. This forces the mobile client to trust the redirection, opening itself to MiTM and similar attacks. Appdome identifies MiTM attacks and does not allow traffic to pass through malicious brokers. The app will either exit or transfer the event to the calling application. With Direct ID Brokering, the mobile client connects to the identity service directly, receiving its unique session credential/token from the identity service.
In-App Private ID	Appdome securely stores all mobile authentication, authorization and access credentials received by the identity service in a segmented, dedicated and encrypted area inside the Fusion layer. This prevents unauthorized services from accessing identity information. This also enables offline access after the user has authenticated sucessfully.
Smart ID Workflows	Appdome for SSO+ allows Android and iOS apps to leverage multiple identity services such as SSO, MFA, authentication and access management from any IAM or IDaaS provider inside the workflow of a single app. Appdome for SSO+ overcomes gaps between basic in-app authentication, SAML, OAuth, OpenID Connect, WebDAV and REST implementations. This results in organizations delivering apps with one of more of the target authentication services inside the app. This allows separate authentication workflows to be invoked throught the app logic without requiring the app maker to code the identity services to the app.

KEY BENEFITS OF APPDOME FOR SSO+

- **No-Code Implementation**
  Users of Appdome for SSO can implement the full range of SSO and identity services to Android and iOS apps built in any development framework, without writing code, needing developer time or requiring access to the mobile app source code.
- **Native or Web-Based SSO**
  Appdome for SSO allows organizations to add in-app authentication, authorization and access workflows to native, hybrid or web-based mobile apps. There is no need for in-app support for Webviews, embedded links, redirects to mobile websites, SAML, OAuth, OIDC or the use of a second authenticator app.
- **Leverage Existing Identity Infrastructures**
  Appdome for SSO allows organizations to leverage existing enterprise identity infrastructures inside the mobile apps they deploy to their users, all without requiring app developers (including 3rd party ISVs) to update, change or modify the apps. This allows organizations immense flexibility to deliver mobile apps that leverage existing identity services, as well as fast migrations to new indentity services without vendor lock in.
- **Multi-Vendor Implementations**
  Combine SSO services with other mobile services from another vendor to speed application delivery and gain efficiencies (eg: SSO/MFA, SSO/EMM, or SSO/MFA/EMM), all within a single fusion workflow.
- **Comprehensive App Security**
  ONEShield™ by Appdome secures the identities, the identity provider service, and the code of the app itself. ONEShield includes code obfuscation, encryption for strings and in-app preferences as well as anti-tampering, anti-debugging, anti-reversing and other app hardening mechanisms. These features prevent hackers from gaining access to sensitive resources, user credentials, user names, or discovering the structure of the app itself.

Learn more about Appdome for SSO+ 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, cloud service for mobile integration. Appdome enables the rapid integration of multiple third-party functions to apps. Appdome provides developers and others an easy-to-use cloud work-flow to complete mobile integration projects. To use Appdome, no source code, coding, or development expertise is required. Likewise, no modifications to an app or SDK are required for Appdome's technology to complete the full integration of services that are selected by users of the Appdome platform. 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.