WHITE PAPER | APRIL 2016

Speed Up Enterprise Mobile App Development With CA Mobile App Services

Table of Contents

Section 1

The Challenge: Accelerating App Development

For some time now, enterprises of all sizes have been creating mobile apps from their traditional app assets in the quest for productivity gains and improved customer satisfaction. In many cases, such mobile projects started from a specific mobile requirement originating from their line of business. Initially, the project is limited in scope but down the line, IT gets involved as the number of mobile projects and scope increases. As the complexity grows, the apps take longer to bring to market. An app is only supported on one platform, but users—employees or customers—expect the app to work on many different platforms. It's not realistic to ask users to change their devices to use the app.

Soon enough, the enterprise realizes that its existing method for executing mobile projects doesn't scale. By taking a platform approach, an enterprise can reduce the fragmentation, provide a better, unified experience across different apps and encourage more software reuse. But adopting a platform approach doesn't necessarily solve all challenges.

This white paper attempts to analyze all the developer challenges involved with mobile/Internet of Things (IoT) app development. We also offer some developer guidance and overall industry trends analysis, and go into detail about CA Mobile App Services: a very viable and flexible solution designed to help developers accelerate mobile and IoT app development.

Mobile App Challenges

There are many mobile app tools to choose from, but developing that compelling app isn't getting any easier. A developer still needs to address traditional considerations, including:

- **Enterprise apps vs. consumer apps:** First, you have to determine the target audience, because building apps for an enterprise employee is radically different than building one for a customer. With the former, you may have more tools to deploy and secure the app. For business to consumer (B2C) apps, there are all sorts of mobile platforms to be supported but fewer options in terms of adding security layers.
- **Multiple platforms:** Second, you need to determine which platforms you intend to support. Android and iOS are clear choices but if you are addressing a wider audience, you may have to support Win10 and Hybrid like Cordova. This also tends to vary with geography.
- **Data connectivity:** Third, an app that does not connect to a data source in the enterprise is most likely not a very compelling business app. Apps are a medium to connect and consume data. It's essential that the app developer leverage the tools to simplify the integration with the data sources—whether cloud services or on-premises data.

Additional challenges are inherent in many categories of mobile app development platforms, such as Mobile Backend as a Service (MbaaS), Mobile Enterprise Application Platforms (MEAPs)/Mobile Application Development Platforms (MADPs), or Mobile Application Services (with API Management).

New App Development Challenges

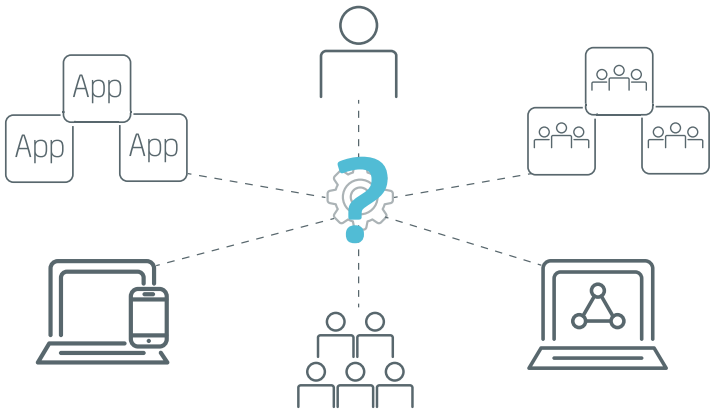
Increasingly, as users' expectations of apps change, app developers will face a new set of challenges. Today, an app needs to be intuitive. It needs to engage with the environment within which it operates; that is, the app is running on multiple devices and in the cloud. It needs to connect to other apps on other devices. It needs to monitor and control other devices. As the app interacts with the environment, it can negotiate access to other objects such as doors, TVs, cars or any other smart object that has a virtual footprint (IoT).

In many IoT use cases, the mobile app will be the provider of the user interface of the smart object. This makes sense because the user interface (UI) paradigms on mobile devices are tested and understood by the consumer. However, all of these elements represent complexity that the app developer will need to manage, including:

- **The proximity to other devices or smart objects.** A vast number of proximity-related technologies are relevant for mobile developers and a lot of innovation is happening in this area. Semiconductors are providing a steady flow of improvements and innovations; a few include Bluetooth low energy (BLE), Wi-Fi, Quasi Resonant Converter (QRC), beacons, GPS, mesh networks like ZigBee, and ultrasound. While these become cheaper and more attractive to build into or adjacent to mobile platforms, it remains a challenge for mobile developers to leverage these kind of capabilities in apps in a robust and secure manner.
- **App awareness of the identity of other entities such as users, devices and apps.** With IoT, you can add "things" to this mix. Across app and IoT use cases, there is a need to authenticate and authorize access to resources representing these entities. It's virtually impossible to define useable security policies when the identity of these entities is unknown. There is not yet an IoT-specific standard to this domain, which means one can expect proprietary solutions to flourish, thereby creating more complexity from an app developer's point of view.
- T**he reactivity of apps.** Modern apps need to be reactive in that they respond timely to events originating in other components. The developer needs to define a way of passing data and events around to the various components of the solution. Because devices, operating systems and apps are heterogeneous, it's hard to specify tight coupling between the components. There are a few notification mechanisms available but they tend to be specific to the mobile platforms. To achieve scale and robustness, a developer could implement a publish-subscribe (pub-sub) message fabric, which would enable the loose coupling desired in modern systems. The major challenge with this would be to implement a security layer with the pub-sub mechanism that can meet the vast number of use cases shared between IoT and mobile apps.
- **The engagement qualities of apps.** As an app extends its reach across devices and things, it needs to engage with users and groups of users. Not only is social login a basic necessity for easy onboarding, but in most social or collaborative apps, the developers need to classify objects such as family, employee groups, customers in a location and more. There are a number of use cases where a group classification is required. The challenge is that not all group information can be throttled down the enterprise Lightweight Directory Access Protocol (LDAP) for compliance reasons. There are also no clear and easy to use software development kits (SDKs) or application program interfaces (APIs) available to do this.
- **The importance of providing a secure messaging framework.** While the collaborative characteristics of apps are becoming far more important for the user experience, there is a significant effort in providing a secure messaging framework. Today, interactivity with another user or a group is mandatory, yet few solutions can provide a secure end-to-end messaging solution in the form of open SDKs and APIs that can provide auto encryption. Building public key infrastructure is often cumbersome because the handling of keys and certs requires care.

Figure 1

Apps, users, groups and devices create integration challenges.



The number of users, devices, and apps are growing exponentially. How do you intelligently integrate these entities?

- Users to enterprise
- Users to other users
- Users to groups
- Apps to data
- Apps to devices
- Apps to users

As businesses take a strategic approach to mobile apps, they should consider these issues as they build out a coherent platform that can drive mobile and IoT app initiatives forward.

Guiding Principles

Here are some key guiding principles that an app developer needs to look for:

- **Flexibility:** Use your own integrated development environments (IDEs) and choose open, extendable frameworks.
- **Agility:** Deliver desired functionality over time across platforms.
- **Vendor lock-in:** Avoid this by using open source frameworks where applicable.
- **Integration:** Prepare to integrate and make sure the platform is ready for integration with third-party components.
- **IoT readiness:** Use a platform that can easily work with IoT systems, whether for monitoring or control via backend or direct device-to-device functionality.
- **Message passing:** Augment Hypertext Transfer Protocol (HTTP) with a messaging pattern that offers a pub-sub paradigm to better scale apps that require asynchronous delivery of events and data.
- **Security:** Build security right into your platform to avoid worrying about security and so that apps rely on a proven platform.

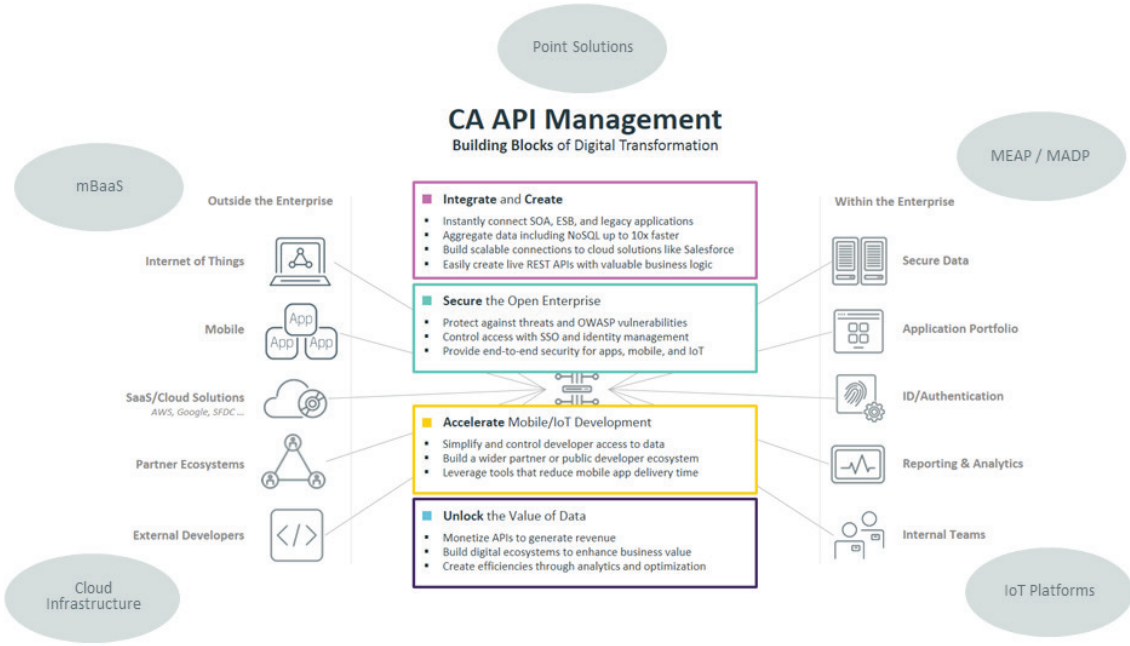
Section

Market Consolidation: Convergence of MBaaS and API Management

Today, a number of different vendors serve different purposes in the app development food chain. On the front end—the client side—you have various frameworks; some are proprietary and others are more open to help developers with the app design. On the back end, there are all kinds of services ranging from specialized push notification services, mobile middleware and MBaaS vendors. Even cloud infrastructure providers like Amazon Web Services (AWS) and Google provide an increasing number of features for mobile app developers.

Figure 2

Markets in flux



The lines between these categories are blurring with increasing overlap. In addition, API gateways are right in the middle. For some time, we've claimed that the right approach is to build a mobile offering on the back of a strong and successful API Management solution, something we did three years ago with CA Mobile API Gateway (MAG). By extending the gateway with client side SDKs, mobile developers could securely connect and consume APIs from any mobile app without having to worry about the security context. This method is also governed by the policies set on the gateway and extended to the mobile client.

API gateways play an important role in securing enterprise assets through API policies—and will be even more important now that enterprises build out solutions for IoT. (Read the article: "Why APIs Are Critical for IoT Success") Because API gateways are already the glue between various software components, they're ideally positioned, especially if they can be extended with the tooling and features that developers crave.

Section 3

CA Mobile App Services: Primary Capabilities

CA Mobile App Services sits at the convergence of various mobile platforms and stands out as a unique and powerful offering designed to help developers rapidly develop mobile and IoT apps. Let's take a look at how our capabilities enable developers to tackle the challenges of accelerating IoT and mobile app projects.

CA Mobile App Services exposes features to developers through SDKs and open APIs, giving developers a convenient method through which to access the back end. Because everything is secured through the existing Mobile API Gateway capabilities, mobile developers can take advantage of best-in-class security without the hassle of setting up security policies. Plus, we provide a set of application services for apps spanning user management, group management, pub-sub, storage and messaging services—all of which are available as SDK functionality for iOS and Android platforms.

User Management

One of the basic capabilities that apps need to deal with is user management—in many ways considered the basic building block for any enterprise app. CA Mobile App Services provide open APIs and SDKs, which feature retrieval and management of users via System for Cross-Domain Identity Management 2.0 APIs and native mobile SDKs; out-of-the-box integration with identity providers that support LDAP; and OAuth protected endpoints.

Figure 3

User attributes used in an app

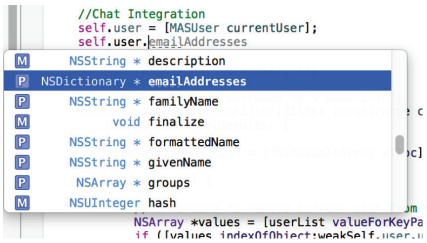
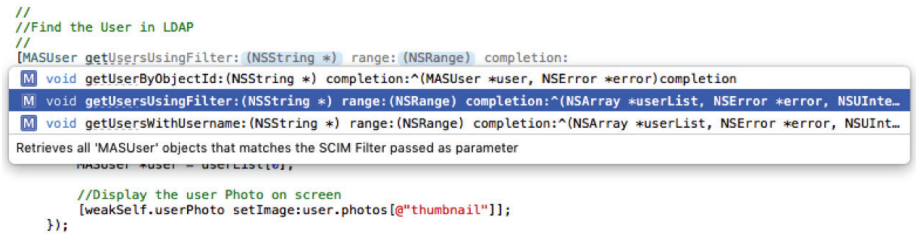


Figure 4

User filtering



Additionally, CA Mobile App Services user management capabilities:

- Allow apps to easily leverage rich user info and user lookup
- Provide basic user management to give developers what they need to allow app users to sign up and get onboarded for the app
- Offer standard-based APIs
- Include native mobile SDKs to maximize developer productivity
- Facilitate IDP-independent app development
- Enable control over the user data that gets externalized
- Provide app-level access control and real-time access revocation
- Offer limitless customization and extensibility using gateway policies

Group Management

One of the most exciting features of CA Mobile App Services is the capability to create and manage groups through SDKs. This means that an app can engage with its own group or other existing groups. The APIs on the backend follow the SCIM specification, which should ease integration and interoperability. However, key to this feature is the ability to create new groups based on application-determined criteria such as location, proximity to other objects or Internet Protocol (IP) address domain.

You can manage groups based on your app's needs via SCIM 2.0 APIs and native mobile SDKs. Support different group types and scenarios, for example, enterprise groups that map to existing IDP and ad-hoc groups that allow the app to create ephemeral groups. Take advantage of internal group store for ad-hoc groups and OAuth protected endpoints.

Additionally, use the ad-hoc group management features within CA Mobile App Services to:

- Allow developers to build more collaborative apps faster
- Enable enterprise groups to utilize the groups in the enterprise's IDP
- Allow ad-hoc groups to let developers create the groups they need for their apps without compromising existing identity store
- Permit virtual groups to address users based on criteria
- Create standards-based interfaces backed by native SDK to give easy access to mobile app developers
- Enable the development of IDP-independent apps
- Increase compliance by keeping app data separate from existing identity systems
- Provide app-level access control and real-time access revocation
- Offer limitless customization and extensibility using gateway policies

Publish-Subscribe

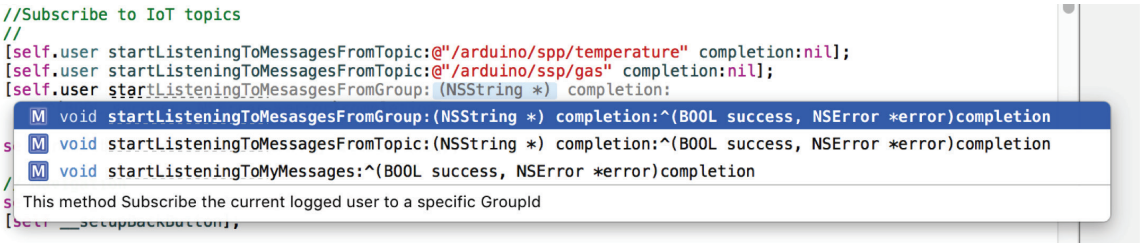
The pub-sub pattern in CA Mobile App Services is built on MQ Telemetry Transport (MQTT) 3.1.1 support. This is a huge add-on to the APIM solution in many ways. First, it allows for a messaging consumption paradigm where an app does not need to poll for data but can be notified whenever new data is available. This scales much better than the traditional request-response paradigm when the system has a high number of entities that need to consume the data. Second, pub-sub is integral to any IoT deployment where data and events will need to be propagated to other systems in near-real time. The heterogeneousness of these systems calls for a loose coupling, which is one of main benefits of pub-sub because the publisher is ignorant to who and how data is consumed. Now, from a system operator perspective, the latter is still important and needs a way to easily control who can publish and subscribe to particular topics.

Pub-sub features include:

- Messaging-based delivery of events and data to provide increased decoupling between components
- MQTT 3.1.1 support in broker proxy model
- Pub-sub via MQTT APIs and native mobile SDKs
- Protected topics for users and groups
- End-to-end security between publishers and subscribers
- Support for different QoS levels (0, 1, & 2) such as at most once—"fire and forget" or "best effort;" at least once—message stored until acknowledged by recipient; and exactly once—message stored until recipient acknowledged

Figure 5

Subscribe to messages



Additionally, use the pub-sub management features within CA Mobile App Services to:

- Leverage a ready-to-use pub-sub infrastructure
- Access an integration point to the world of IoT
- Use lightweight messaging protocol
- Enable support for different MQTT brokers
- Provide control over messages before they reach the broker and after they leave the broker
- Take advantage of Quality of Service to help app developers leverage reliable delivery
- Facilitate secure communication between publishers and subscribers
- Leverage standards-based APIs
- Use native mobile SDKs to maximize developer productivity
- Capitalize on limitless customization and extensibility using gateway policies

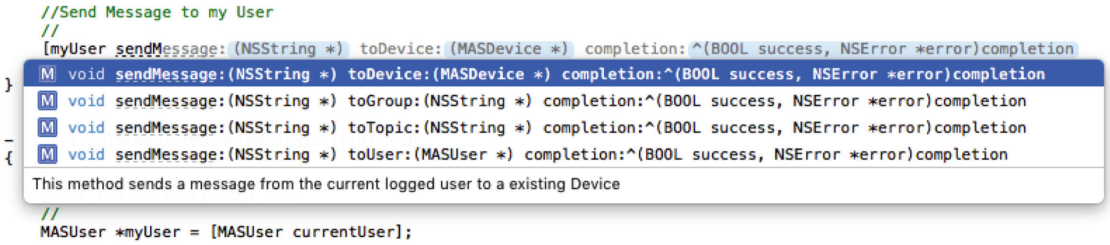
User-to-User Messaging

App developers always strive to make applications more collaborative, including through social features. But in an enterprise-type app, you would often want to be able to contact other colleagues via a quick note or a call. The user-to-user messaging component in CA Mobile App Services allows an app developer to easily build messaging into apps with a few lines of code. The app developer can do either direct user-to-user or user-to-group messaging. In the latter, all members of the group will receive the message. While there are some messaging platforms, only a few provide the simplicity that CA Mobile App Services does, and even fewer provide the advanced security layer with auto-encryption of payload so that only the recipient can decrypt the messages.

With user-to-user features, you can enable messaging to users and groups enterprise-wide via MQTT APIs and native mobile SDKs, and take advantage of end-to-end security.

Figure 6

User messaging to device, group, topic or user



With CA Mobile App Services Messaging Services, you can take advantage of:

- An easy-to-use framework that enables advanced messaging features to be added to any app
- Secure communication between users
- Standard-based APIs
- Native mobile SDKs to maximize developer productivity
- Extensive customization and extensibility using gateway policies

Storage

The ability to store data in a secure manner is fundamental to any mobile app. CA Mobile App Services offers a locally encrypted data storage service for data at rest. Depending on the app developer's preferences, secure private cloud storage can be used for off-device storage.

Storage services features include easy-to-use local and cloud data store for developers via standard-based APIs and native mobile SDKs, as well as user, group and app-level data access permissions.

Figure 7

Local encrypted storage

Additionally, you can use CA Mobile App Services storage services to:

- Enable app developers to focus on delivering business value while data persistence is handled by CA Mobile App Services
- Encrypt and store data on device
- Set up easy-to-use user, group and app-level permissions
- Leverage standard-based APIs
- Enable native mobile SDKs to maximize developer productivity
- Provide extensive customization and extensibility using gateway policies

Security

Security is one of the most important aspects of mobile applications—and one that is magnified by the introduction of more connected devices and the IoT, where enterprises have fewer options to control the data flow.

The foundation of app security is to know something about the context of the app, the user and the devices used. Only after the enterprise can identify and authenticate the various entities can it can start to discuss security. Further, the concept of authorization of access to a resource must be addressed. App developers

using CA Mobile App Services can rely on CA Mobile API Gateway to provide security frameworks using OAuth, OpenID Connect and public key infrastructure (PKI). Using a token-based system with individually issued tokens for users, apps and devices provides the most flexibility for API access policies.

Not only can CA Mobile API Gateway issue tokens but it can track the relationships between users, apps and devices. CA Mobile App Services adds to this capability by controlling the group, pub-sub and messaging policies using the underlying CA Mobile API Gateway capabilities for policy enforcement. Additional features include a CA Mobile API Gateway based platform to solve common security aspects (with OAuth, OpenID Connect and PKI); advanced authorization risk-evaluation service integration; OAuth-based permissions; and mutual Secure Sockets Layer (SSL).

With CA Mobile App Services and CA Mobile API Gateway security services, you can empower app developers to focus on building more interactive, usable and secure apps: CA Mobile API Gateway takes care of security while CA Mobile App Services address core backend functionality.

Smart SDKs and APIs Everywhere

App developers expect to find SDKs available in their preferred development environment, which means SDKs should be integrated well with XCode and Android Studio. This helps ensure maximum flexibility for CA Mobile App Services and CA Mobile API Gateway customers in continuing to use their own favorite IDE and in being able to simply extract the SDK and drop CA Mobile App Services libraries into the app projects as needed. The ability to extend the CA Mobile App Services platform through open APIs on the server side lets app developers enable easy integration and interoperability with existing systems.

Smart SDK features provide convenient methods for app developers, RESTful API endpoints and and SDKs for both the Android and iOS platforms, and extendibility through APIs and SDKs.

With CA Mobile App Services, you can speed development and get to market faster with more enterprise mobile apps, and enhance the developer experience by providing APIs everywhere.

Section 4

CA Mobile API Gateway: Features

The CA Mobile API Gateway provides a suite of security services for CA Mobile App Services developers as shown below. You benefit from best-in-class security deployed in apps that have been downloaded by millions and shipped to millions of mobile devices.

Feature	Description	Benefits
OAuth 2.0	▪ Password flow support for user authorization ▪ Client credential flow for application authorization	▪ Standards-based user- and application-level authorization
Dynamic client registration	▪ Unique per-app-instance credentials	▪ Support for multiple instances of apps deployed on different devices
OpenID Connect	▪ Token-based user authentication with JSON Web Token (JWT)	▪ Standards-based user authentication for mobile apps
PKI support	▪ Signed certificate issuance on device registration	▪ Communication channel encryption for mobile devices
Social login	▪ CA Mobile API Gateway orchestrated social login flow for SDK-based or web applications	▪ Frictionless onboarding of users in B2C apps with optional layering of additional access control parameters
Device-to-Device SSO	▪ User session sharing between adjacent devices	▪ Enhanced user experience for apps working across multiple devices
Mutual SSL	▪ Two-way authentication between clients and CA Mobile API Gateway	▪ Secure consumption of APIs through PKI-based security
Geolocation	▪ SDK can provide location parameter with requests ▪ Geolocation possible through context variables in API policy	▪ Better context for API security
Enterprise browser	▪ Access to third-party Web apps via embedded browser component with native security model	▪ Seamless access between native, hybrid and web apps
Custom login dialog	▪ Better user credentials dialog rendering control	▪ Improved developer flexibility and UX
Samsung KNOX	▪ Create or delete containers with remote commands ▪ Install or remove apps in the container ▪ Remotely wipe device or container	▪ KNOX container management for enhanced API security
Samsung Attestation	▪ Specify attestation as a condition in API policy	▪ Enhanced API security for business-to-employee (B2E) and B2C
Samsung TIMA Keystore	▪ Hardware-protected secure store for keys and tokens	▪ Improved on-device security
Advanced authorization risk evaluation integration	▪ Enable risk calculation based on API request context	▪ Stronger and more flexible security policy

Section 5

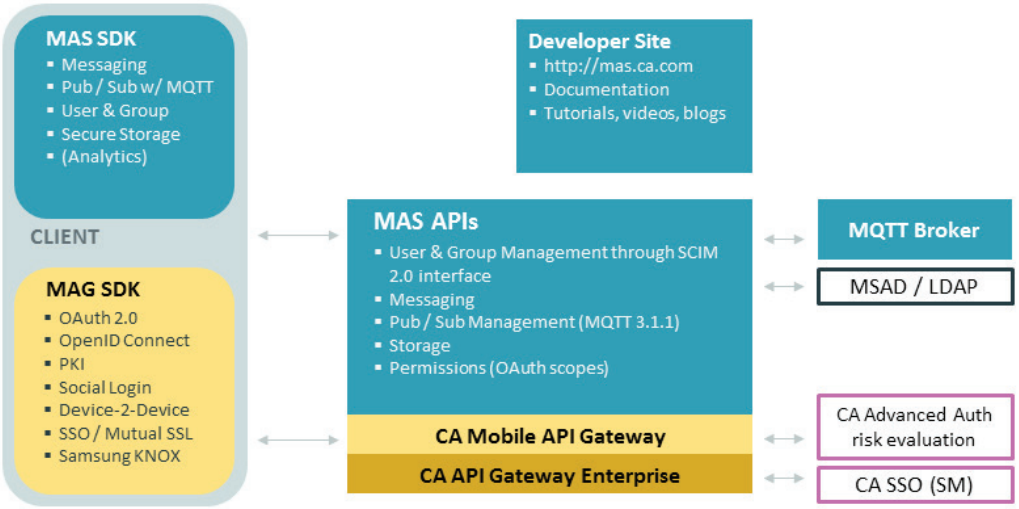
Architecture

System Overview

CA Mobile App Services builds on the CA API Management platform to extend best-in-class API integration to the enterprise and mobile user.

Figure 8

CA Mobile App Services Overview



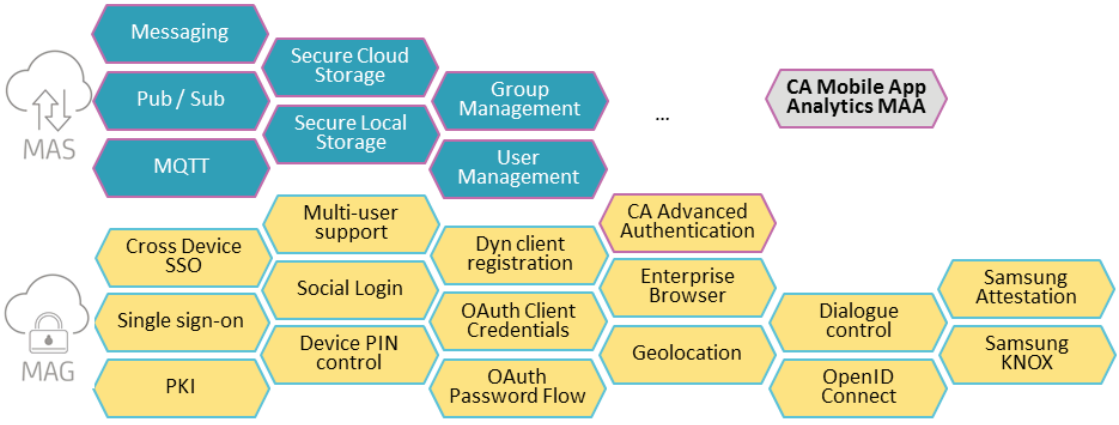
Client SDKs

System Overview

CA Mobile App Services SDKs extend the MAG SDKs, which provide the security functionality with OAuth, OpenID Connect and PKI functionality. In addition, the MAG SDK provides new security features that are required for CA Mobile App Services, such as encryption of local data and encryption of messaging payload.

Figure 9

CA Mobile App Services SDK Overview



Section 6

Business and Developer Benefits

CA Mobile App Services are essential mobile services for the enterprise developer, exposed through simple and secure SDKs and APIs. Mobile services such as user management, ad-hoc groups, pub-sub, messaging and storage are important to the modern app developer who uses them to:

- Write modern apps that can engage with the environment and nearby devices that leverage standards-based technologies
- Write reactive apps that can utilize near-real-time propagation of events and data via pub-sub capabilities while controlling message flow
- Create ad-hoc groups that can be used to enhance sharing in collaboration apps while preserving compliance in identity infrastructure
- Leverage security that's weaved into the app fabric for data at rest and in motion

Open-source SDKs provide these advantages and give the developer the flexibility to tweak the code for their own purpose. By using open and well-documented APIs, the developer can easily integrate with other systems as needed. By leveraging open standards like MQTT 3.1.1, SCIM 2.0, OAuth 2.0, OpenID Connect and PKI, developers can easily implement security and integrate with other systems.

Businesses implementing CA Mobile App Services can build their mobile and IOT app initiatives on a solid foundation. Based on best-in-class API management products, the wealth of features that address traditional API management use cases provides a unique combination for the modern app project. While security is an ongoing issue with many platforms, CA Mobile App Services leverages existing security models that have been developed for the most stringent requirements in the financial, health and military sectors.

Accelerate your mobile and IoT development projects with CA Mobile App Services. Learn more and get started by visiting http://www.ca.com/mobileapps or the developer site at http://mas.ca.com.

ca technologies

Connect with CA Technologies at ca.com

CA Technologies (NASDAQ: CA) creates software that fuels transformation for companies and enables them to seize the opportunities of the application economy. Software is at the heart of every business, in every industry. From planning to development to management and security, CA is working with companies worldwide to change the way we live, transact and communicate – across mobile, private and public cloud, distributed and mainframe environments. Learn more at **ca.com**.

CS200-183509