EXECUTIVE BRIEF
SEPTEMBER 2018

CA Rapid App Security

Improve User and Developer Experience and Still Protect the Business

In the real world, communication is an illusion. People talk, but they don't listen. Although this is not always the case, it is probably more often than we would care to admit. In the digital world, we face a different type of illusion: Dialogue occurs between users and systems, or nothing else happens. The single biggest problem in digital communication is not whether it has taken place, but whether it has taken place with the right person.

"The single biggest problem in communication is the illusion that it has taken place."

George Bernard Shaw

Consider the most common digital communication today—authentication. Users request access and then are challenged to present login credentials. This digital dialogue occurs millions and millions of times every minute of every day around the globe and is built on one very simple principal—trust. The application is trusting that the legitimate owner is submitting these credentials. But this trust is easily compromised, as passwords can be stolen, guessed or given away.

Businesses today need a solution that provides greater assurance that users are who they claim to be. You need this not only to protect your business, but also to build and maintain trust with your customers. You require a solution that delivers:

- **Convenience.** In the application economy, users want immediate access to applications and services, and if it takes too long to deliver these, they are gone. The solution must create a native security experience that is convenient and frictionless for end users.
- **Security.** Trust is easily compromised when using security questions or passwords to verify a user's identity. Many emerging regulations are now recommending stronger authentication mechanisms. The ideal solution must address internal security policy audits and adhere to external compliance requirements.
- **Velocity.** As you attempt to balance user experience and security, you must also enable "developer velocity" so you can deliver new capabilities with speed and security. You need to make it simple to incorporate security into the app development process and make it easy for your developers to add or update apps with minimal coding, while retaining the flexibility to adapt to emerging threats or stronger security protocols.

You need CA Rapid App Security.

You need CA Rapid App Security.

Business Challenge

You are facing many barriers in getting apps to market faster.

- **Inaccessible data.** Legacy systems and data are often difficult to externalize in a safe and reliable way. Even when protected, existing methods often don't consider the risk involved and are too heavy-handed.
- **App development barriers.** Applying security within the development process can add significant time to the release cycle. Maintaining this custom-built security to address emerging threats can be difficult and costly.
- **Pervasive Internet of Things (IoT).** Mobile apps are integrating IoT devices, events and data. Developers need software development kits (SDKs) that can facilitate data exchange across devices and backends while retaining control of the data flow.
- **Regulatory compliance directives.** Many regulations and industry guidelines are recommending or requiring stronger authentication mechanisms. You need to address these requirements in your mobile apps without impacting user experience.

Solution Overview

Delivering native security integration along with a great experience is critical to digital transformation success. You need to simultaneously enhance security while improving both the user and the developer experience for each platform. CA Rapid App Security simplifies securing internal data and app infrastructure for mobile and IoT use. It delivers a lightweight mobile SDK that accelerates the development of app security, combining multiple authentication mechanisms and risk-based analysis, which can then be used to balance the appropriate security against the user experience and associated transaction risk. The solution also provides a unique trust model by identifying the user, app and device, and monitoring the relationship between the three.

CA Rapid App Security provides you with three critical capabilities:

- **Accelerate app development.** Offers common backend services in the form of SDKs/ APIs that enable an enterprise to develop, deploy and manage multiple Web, mobile and IoT apps rapidly. In addition, a combined SDK simplifies repetitive and complex app development tasks to speed time to market and enables quick support for new security protocols as they gain market adoption.
- **End-to-end security.** Enables secure consumption of backend APIs through configuration of mutual SSL between the device and gateway. It supports OAuth and OpenID Connect to enable social login and single sign-on across mobile apps and devices, maintaining a seamless user experience. The SDK can optimize UX when users access enterprise resources from multiple devices through proximity login capability. The solution provides a flexible framework for tailoring security to each use case.
- **Dynamic authentication.** Allows organizations to embed a PKI-based, two-factor authentication credential or a mobile one-time passcode (OTP) generator into the mobile app. In addition, the solution can also support other primary and secondary authentication methods such as basic (password), biometric (fingerprint), desktop OTP, FIDO Support, OATH tokens, OTP over email/SMS, push notification and risk-based authentication.

High-Level Architecture

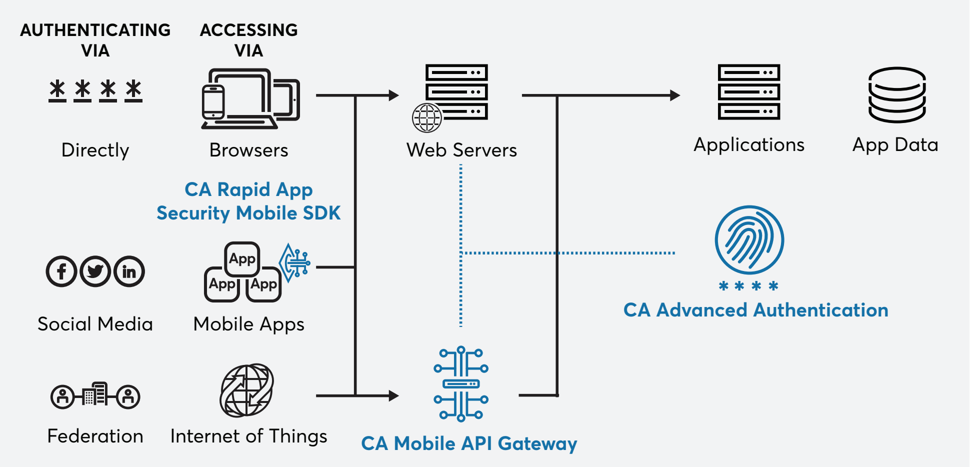
How it integrates: Authentication

There are three key components:

- **CA Advanced Authentication.** Provides a cost-effective and user-convenient way to protect mobile apps with two-factor authentication credentials and contextual risk-based authentication.
- **CA Mobile API Gateway.** Provides mobile access services including OAuth/OIDC support, mutual SSL, certificate pinning, social login, fingerprint session lock, proximity login between devices (NFC, QRCode and BLE), secure user-to-user messaging infrastructure, MQTT proxying, publish/subscribe infrastructure and secure device storage powered by APIs and SDKs.
- **CA Rapid App Security Mobile SDK.** Simplifies developer experience through a single, unified SDK that easily embeds security into a mobile app.

FIGURE 1.

High level architecture.

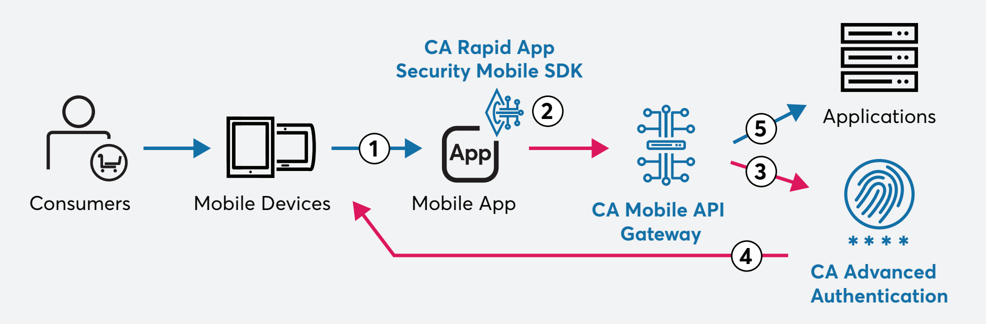


How it works: Authentication

The security begins when the user downloads and registers the mobile app. The SDK will collect data so that the solution can fingerprint the device for future comparisons. In addition, the solution will also download the CA AuthID (a 2FA PKI-based credential) into the mobile app, where it is protected by a patented concealment mechanism.

FIGURE 2.

Generic authentication process.



Generic authentication process.

When a user opens the mobile app, the authentication process is as follows:

1. User opens mobile app and enters user ID and password.
2. The password is used by the SDK to decrypt the CA AuthID private key, which is then used to sign a hidden authentication challenge. The password is never stored or transmitted.
3. The signed challenge is forwarded to the authentication server for validation. If successful, the solution can then perform an optional contextual risk analysis. In this case, the SDK will collect data from the device and forward it to the authentication server for evaluation.
4. If the risk score exceeds a specified threshold, the solution can issue a step-up challenge to the user (e.g., push notification, OTP over SMS, TouchID, etc.).
5. After successful authentication, the original request is forwarded to the application and whatever data was requested is delivered to the mobile app.

This process is generic, but could be easily adapted to support, as an example, social media login with risk analysis or step-up authentication for specific transactions/activities, etc.

The CA Rapid App Security Advantage for Authentication

CA Rapid App Security minimizes authentication and security friction for your customers by leveraging a transparent two-factor authentication credential, a transparent contextual risk-based evaluation and an easy-to-use, step-up authentication mechanism when risk is deemed too high. The solution also supports social login credentials and/or biometrics (device fingerprint), both of which can improve user experience because they are familiar to users.

It delivers increased security that allows you to build apps that provide higher value capabilities with confidence. For mobile devices, it enables trust between the user and the business by identifying the user, app and device, and by learning and tracking the relationships between the three. The solution also supports secure communications and data storage on the device.

CA Rapid App Security makes it easy to quickly build and maintain modern, frictionless and secure apps for your customers. Your developers have one easy step to rapidly integrate device security and comprehensive multifactor and risk-based authentication into their apps, eliminating dozens of complex steps typically required for coding user and device security.

For more information, please visit **ca.com**

ca technologies

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.

Connect with CA Technologies