

# Build Secure and Modern Apps Faster Using ForgeRock SDKs

ForgeRock SDK accelerates secure app development with exceptional user experiences

## Executive Summary

According to Forrester Research, a well-designed user experience can raise your conversion rates by up to 200%.<sup>1</sup> It is up to you and your team of developers to deliver an exceptional user experience without compromising security. Recent statistics underscore the importance of this approach to development. The bulk of recent breaches trace back to identity-related threat vectors, and unauthorized access was the number one attack method (40%) cybercriminals used in 2020.

Today, as more security breaches make the headlines, building secure apps has become a top business priority, but this comes with challenges. Creating identity frameworks from the ground up and incorporating them into applications increases costs, extends time to value, and requires in-house security expertise. Additionally, product teams must ensure that security doesn't compromise the user experience. After all, registration and authentication journeys play a big role in deciding how well and for how long your users engage with your apps.

The good news is that ForgeRock software development kits (SDKs) help you achieve that balance with ease. Developers can leverage ForgeRock SDKs to build native iOS, Android, and JavaScript apps with advanced access control capabilities – without excess lines of code.

ForgeRock SDKs quicken time to value of your apps in multiple ways:

### Developer ease of use

Hides the complexity of underlying protocols, simplifying integration with the ForgeRock Identity Platform.

### Security best practices

Follows industry best practices and stays current with platform-specific recommendations.

### Context-driven journeys

Enables sophisticated authentication journeys using device context information that the SDKs collect for you (example: jailbreak detection).

<sup>1</sup> "Six Steps for Justifying Better UX": <https://www.forrester.com/report/RES117708>

# Bridging the Gap Between Security and App Development

Your development team's first priority is to build business capabilities in your apps that drive revenue to your organization. In the process, integrating security best practices either ends up as an afterthought or is sacrificed to meet aggressive deadlines. At times, aggressive delivery deadlines and time-to-market urgencies force your developers to take shortcuts when they add security.

However, implementing user authentication, continued authorization, and context should not be neglected or treated as an afterthought. Shortcuts and inadequacies in access control are not acceptable either. To create secure and exceptional user journeys in your apps, developers must implement identity and access management correctly. This requirement is even more important in today's tumultuous threat landscape.

The "ForgeRock 2021 Breach Report" reveals that, in 2020, attacks involving usernames and passwords increased by a staggering 450%, compromising more than one billion records in the U.S. alone.<sup>2</sup> For the third year in a row, unauthorized access was the most reported type of breach (40%).<sup>3</sup> This data further underscores why a secure, robust identity and access management (IAM) framework is integral to your software development lifecycle (SDLC).

Apps often fall behind on security due to the extra time, cost, and effort required to implement adequate security. Embedding a powerful IAM framework in your apps from scratch can be time-consuming, as it involves sophisticated workflows. When product teams lack in-house security expertise, risks of suboptimal IAM and associated security holes and vulnerabilities increase, which hackers notoriously exploit.

A well-designed user  
experience can raise your  
conversion rates by up to  
**200%**

According to Forrester's "State of Application Security Report for 2021,"<sup>4</sup> applications are still a primary attack vector. 28% of external attacks use stolen credentials (logins or encryption keys). The report predicts that web applications will continue to be a major attack vector. Software vulnerabilities and inadequate leveraging of application security tools during SDLC are escalating this trend. Embedding security at an early stage of the SDLC is a crucial recommendation of the report.

Implementing identity and access in your applications is the last mile of protecting your enterprise. It's the key to user retention and growth because it directly impacts how easily users can engage with your app.

ForgeRock SDKs bridge the gap  
between security and your developers  
without compromising user experience  
and time-to-market.

## ForgeRock SDKs Make It Easy to Integrate Security into the Development Process

ForgeRock SDKs provide the leverage your team needs to overcome the application security challenges. The SDKs simplify adding security early in your development lifecycle. To build secure authentication journeys, your developers can quickly integrate the full capability of the ForgeRock Identity Platform. Developers do not need to write excessive lines of code or be security experts.

As a result, developers can:

- Add more features more quickly.
- Build security faster and the right way.
- Focus on accelerating new capabilities.
- Collect context for users using trusted devices and offer superior experiences.
- Introduce friction only when needed.

<sup>2</sup> 2021 ForgeRock Consumer Identity Breach Report | ForgeRock

<sup>3</sup> ibid

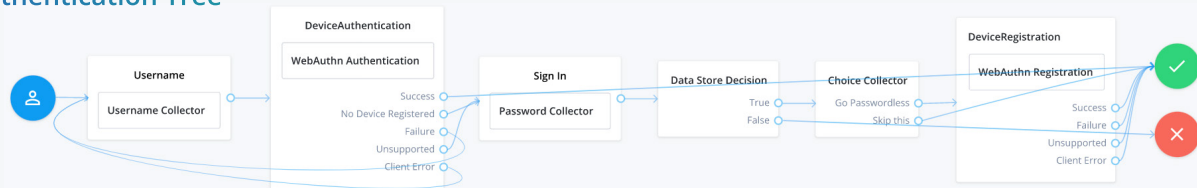
<sup>4</sup> The State Of Application Security, 2021 (forrester.com)

# A Rich Set of Identity Features at Your Fingertips

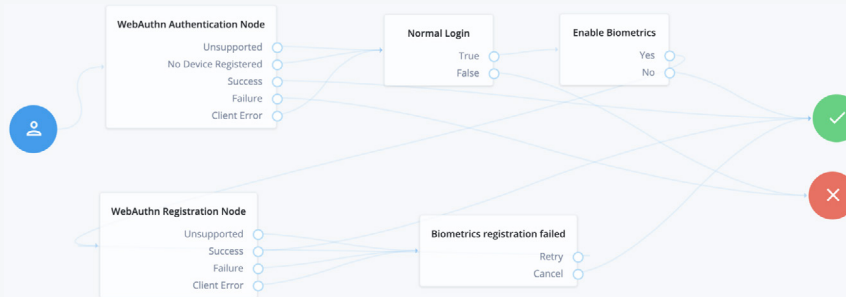
ForgeRock SDKs offer many capabilities to enable your team to quickly build secure user experiences while simplifying the delivery of identity. Our customers who already use the ForgeRock Identity platform can leverage [SDKs](#) immediately to add advanced identity features to your mobile and web experiences.

ForgeRock Intelligent Access provides out of the box user journeys to get you started quickly.

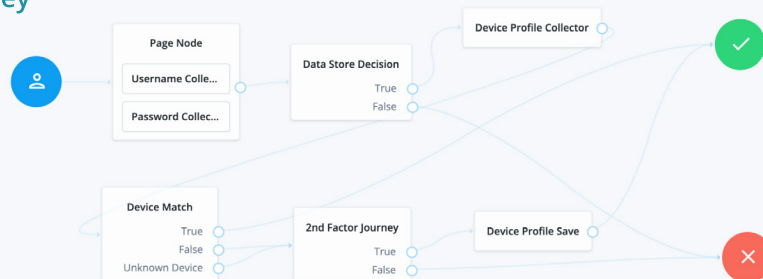
## An Authentication Tree



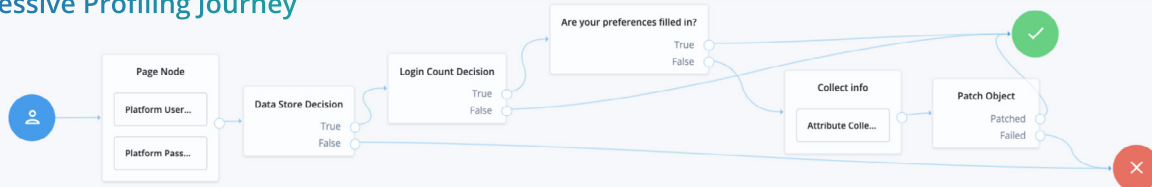
## A Mobile Biometrics Journey



## A Device Profile Journey



## A Progressive Profiling Journey



## Build Secure and Frictionless User Authentication Journeys

Customer journeys begin with authentication. A lack of relevance or too much friction in authentication flows can frustrate customers and cause them to disengage with your business. To deliver this, you have two choices: (1) embed the login to have full control over the user experience, or (2) choose a centralized login experience to ensure a single point of entry for all apps. ForgeRock SDKs enable you to decide the right approach for your organization.

**A secure, robust IAM framework is integral to the Software Development Lifecycle (SDLC) and should not be an afterthought.**

### Seamless Experience with Embedded Login

Providing seamless experiences to your customers means delivering an app that removes friction during adoption and use, such as eliminating unnecessary redirects from the app during login. Most SDKs that offer mobile login only provide a browser-based login that redirects the user to a browser (example: SFSafariViewController in iOS and the custom Chrome tab in Android). There are certain use cases where this approach is preferred. However, for customers that want a complete native application experience without browser redirects, ForgeRock SDKs offer an embedded login experience where the user always remains within the app.

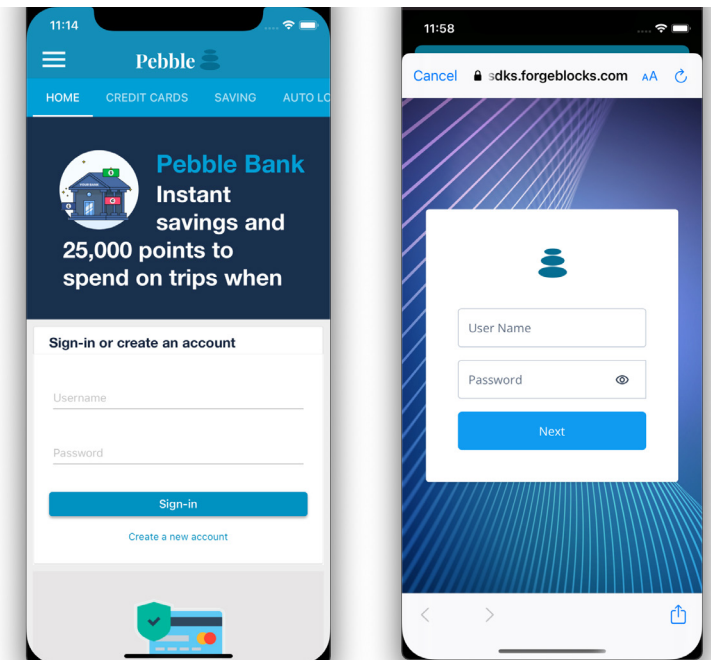
### Improve Efficiencies with Centralized Login

A centralized login or browser-based login approach is best for an organization that has multiple apps that must provide a seamless single sign-on (SSO) experience across those apps. With ForgeRock SDKs, your developers can centralize the login with an authentication user interface (UI), like [hosted pages](#), with a simple configuration switch. [Centralized login](#) allows you to easily customize and apply themes for your UI across multiple mobile and web applications. You can

still implement great user experiences without requiring your development teams to manage the theming and authentication experiences themselves for each application. This provides a consistent app experience and reduces overall app lifecycle costs.

### Simplifying Change Management

Another advantage of user registration, self-service, and authentication in a single interface is efficient change management. To change authentication flows in your application, just change the authentication journeys in the ForgeRock Identity Platform. The SDK incorporates the changes into the app. Additional work to rebuild and redeploy the application is no longer necessary. The resulting benefits quickly multiply when applied to multiple apps running across various platforms.



Embedded Login

Centralized Login

## Easily Implement Zero Trust with Intelligent Access Trees

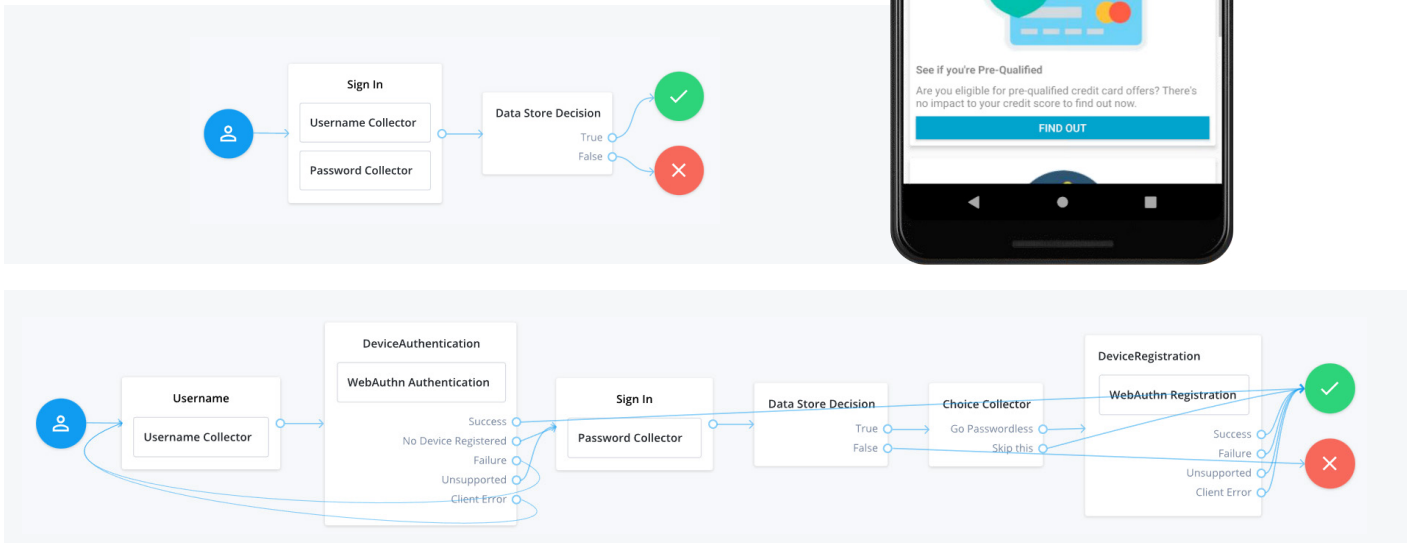
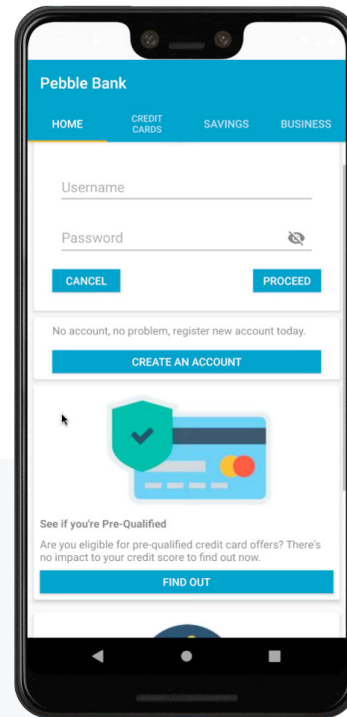
The post-pandemic surge in online users, coupled with rising cyberthreats, underscores the importance of advanced security frameworks like Zero Trust.

Zero Trust protects data and resources by granting access only on a limited basis and in the proper context. This model prevents attackers from escalating privileges, provides tighter access control, and mitigates the lateral movement of attacks in an organization's infrastructure. However, implementing Zero Trust usually adds cost and complexity.

ForgeRock SDKs simplify Zero Trust architecture in your apps by leveraging [Intelligent Access Trees](#). Your developers can access ForgeRock's intelligent authentication capability out of the box and switch user authentication behaviors dynamically based on context. The SDK empowers developers to write applications that can automatically handle the changes real time without the need to modify code or redeploy the app. This means

you can change user login behavior and security with configuration rather than coding.

Having Zero Trust capabilities out of the box is a crucial advantage in today's security and regulatory landscape. It helps you quickly achieve significant improvements in security posture and deliver frictionless user experiences. Using the ForgeRock SDKs to implement Zero Trust gives you the additional benefits of delivering ForgeRock Identity Platform's intelligent access capabilities to your mobile and web applications with minimal code.



## Simplify Authentication Journeys with Single Sign-On and Federated Identity

The unprecedented shift to remote work and online shopping since 2020 has escalated the need for easy and secure access from anywhere at scale. But the perils of password management often lead to exploits. According to the Verizon “2021 Data Breach Investigations Report,” in 2020, over 80% of data breaches involving external threat actors used brute force attacks to guess passwords or lost or stolen credentials.<sup>5</sup> Single sign-on (SSO) and federated identity management address this with open standards like OAuth 2.0, OpenID Connect (OIDC), and others. These capabilities are foundational for improved, more secure user journeys in today’s work-from-anywhere world.

ForgeRock SDKs support SSO and OAuth 2.0-based federated identity in your apps and services for any identity type. The ForgeRock SDKs support the latest standards and protocols, so your developers don’t have to. Developers are free to focus on what matters most to your business – your app’s core features and functionality.

## Passwordless and Biometric Experiences

Complex unique passwords are hard to remember, difficult to type on a mobile device, and prone to reuse. A better idea is to leverage the native biometric authentication capabilities of modern devices like fingerprint readers or Face ID (as on the iPhone). ForgeRock SDKs support passwordless and usernameless login experiences and make this easy. This reduces the risk of unauthorized credentials access and decreases help desk costs for forgotten username and password recovery.

Passwordless authentication is the hallmark of success for today’s mobile apps.

## Modernize Your Application Security

You can no longer afford to choose between security and usability for your applications. You have to elevate both and deliver strong security and exceptional user experiences. ForgeRock SDKs bring the advanced capabilities of the ForgeRock Identity Platform to your fingertips. You can raise the security bar of your apps without diminishing the user experience.

### Multi-Factor Authentication

Multi-factor authentication (MFA) is essential for improved security in mobile and web apps. ForgeRock SDKs simplify delivering MFA capabilities to your users. Developers can easily and quickly integrate push authentication or one-time password (OTP) capabilities into mobile applications.

Typically, users must download and use a dedicated authenticator app for MFA. This introduces friction in the user experience. The SDKs, by contrast, empower developers to embed native authenticator capabilities into mobile apps while maintaining a seamless, branded, and frictionless authentication experience.

ForgeRock SDK’s native Authenticator module supports

- Time-based one-time passwords (TOTP).
- HMAC-based one-time password (HOTP).
- Push notifications.

Your developers can use secure key stores for free, without additional effort.

### Secure Token and Credential Storage

Secure credential storage encrypts and protects the access artifacts like tokens from unauthorized use. ForgeRock SDKs incorporate platform-specific best practices for securely storing token material. For example, the ForgeRock iOS SDK uses Apple’s [Secure Enclave](#) for hardware-backed encryption and token storage.



## Device Profiling and Context

Device context is essential for building sophisticated authentication journeys and detecting anomalies, such as deviations in previously trusted devices, impossible travel, access from tampered devices, and more.

Our SDKs can collect contextual information from devices or browsers and seamlessly integrate with the new [Device Profile Nodes](#) of the ForgeRock Identity Platform. The SDKs automatically generate a device ID and metadata for you. Your developers can use the ID with ForgeRock to empower your app's users to manage their devices for security.

You can also easily insert device ID and associated metadata into a user's profile and set the device as "trusted." This eliminates the need for using another factor in the user authentication flow.

ForgeRock SDKs enable developers to build sophisticated authentication journeys using device context at no extra cost.

## Transactional Authorization

Your customers expect great experiences and [proper security](#) during their login and also during every transaction. ForgeRock SDKs offer the Zero Trust and CARTA models. Additionally, ForgeRock SDKs allow you to seamlessly require additional verifications when engaging in a high-risk transaction or performing an action that deviates from normal behavior. For example, to conduct high-risk transactions, users must re-authenticate by using a second factor or respond to a push notification on their mobile devices.

# Winning in the Last Mile of Identity

Implementing identity and access in your applications is the last mile of protecting your enterprise. It directly impacts how well users engage with an app and is key to user retention and growth. ForgeRock SDKs provide essential capabilities to win this last mile challenge by:

- Enabling exceptional user experiences with passwordless authentication.
- Lowering security lifecycle costs and time-to-value.
- Delivering flexible and consistent performance.

## Secure Apps Made Easy

The wait is over. If you have been exploring better ways to build advanced identity journeys without incurring skyrocketing costs, [ForgeRock SDKs](#) are the answer. ForgeRock SDKs provide a rich set of identity use cases right out of the box and at your fingertips.

ForgeRock SDKs make it easy to build secure, frictionless user authentication journeys using Intelligent Access trees. You can upgrade application security by simplifying advanced security architectures like Zero Trust and CARTA. And your developers can enable SSO and federated identity capabilities in minutes to streamline and improve authentication journeys.

ForgeRock SDKs unlock the value of robust IAM by accelerating security integration and shrinking time-to-value of your apps. There's no reason to build security from scratch. ForgeRock SDKs make it easy to create secure user journeys from A to Z with just a few lines of code and by leveraging ForgeRock's powerful identity interface. You no longer need to rebuild and redeploy each time you change authentication behavior. ForgeRock SDKs drastically reduce costs and risks across your entire application lifecycle.

Start using [ForgeRock SDKs](#) to score a win in the last mile of identity with exceptional and secure user experiences.

## About ForgeRock

ForgeRock®, (NYSE: FORG) is a global leader in digital identity that delivers modern and comprehensive identity and access management solutions for consumers, employees and things to simply and safely access the connected world. Using ForgeRock, more than 1300 global customer organizations orchestrate, manage, and secure the complete lifecycle of identities from dynamic access controls, governance, APIs, and storing authoritative data – consumable in any cloud or hybrid environment. The company is headquartered in San Francisco, California, with offices around the world. For more information and free downloads, visit [www.forgerock.com](http://www.forgerock.com).



Follow Us

