

Product Sheet

Zumigo Assure Authentication Offers SIM-based Authentication for High-Security, Low-Friction Experience

SIM-Based Authentication (SBA) provides robust authentication with low friction via Zumigo Assure Authentication. The collaboration with mobile network operators ensures this advanced technology is widely adopted and made available to the general public.

SIM-Based Authentication (SBA), a new technology to be rolled out by the mobile network operators (MNOs), enables third-party applications like banking services to achieve robust user authentication and identity verification with less friction when compared to one-time passcodes (OTPs) or Silent Network Authentication (SNA). SBA leverages the inherent security of the mobile Subscriber Identity Module (SIM) to authenticate that the mobile number and device belong to the consumer during a session.

How It Works

SBA leverages a secure integration between mobile devices, carrier networks, and application providers to verify consumer identity against the device account and intelligence available

with the MNOs. The solution works across both Android and iOS platforms, with each utilizing native operating system capabilities to ensure security and ease of use.

Both platforms provide secure authentication in the same process but through different technical approaches. Consent is required to initiate the

authentication process.

When the consumers get to the mobile web page or app to log-in, they are asked to enter their mobile number. The consent screen is then presented. Upon agreeing, the authentication takes place in the background. In both cases, the consent is obtained either by an OS-based paradigm or by a carrier-managed app. The

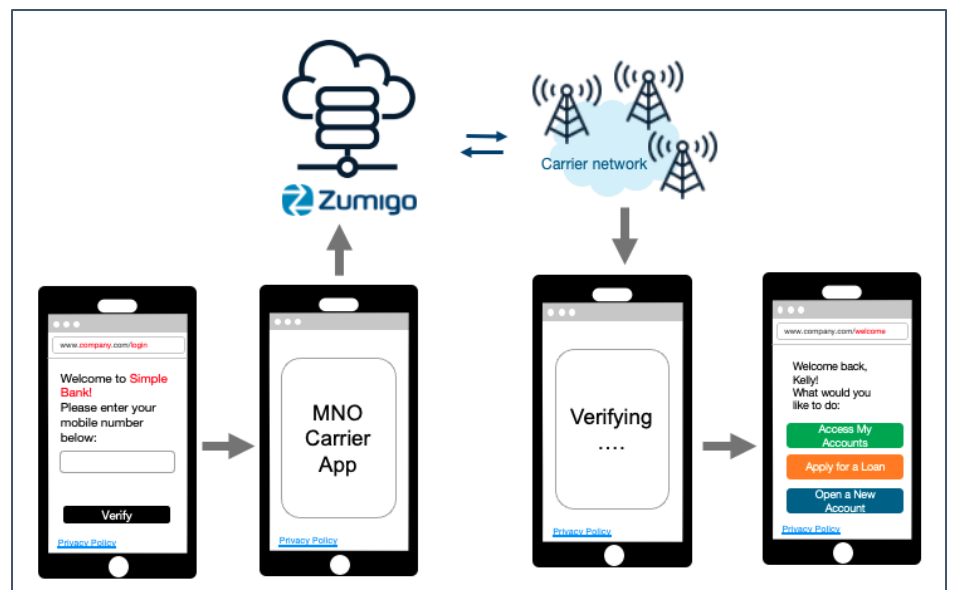


Figure 1: Consumer experience flow using SIM-based authentication with mobile phone

user interface is expected to be familiar to those who use iOS and Android often. The implementations provide equivalent security and user experience, ensuring consistent authentication quality regardless of device platform.

Why SIM-based Authentication?

Traditional authentication methods such as OTP and SNA present distinct gaps in the authentication process. OTPs, while widespread, can be intercepted or bypassed by modern hackers via phishing and SIM-swap attacks, leading to account takeovers (ATOs). Operationally, OTPs are inefficient, contributing to message delays or loss due to poor signals or roaming, and their high volume makes them costly for businesses while increasing friction for consumers.

As well, SNA requires Wi-Fi to be disabled for the network check to function correctly, and it can suffer from latency due to poor signal strength, which can slow down transaction processing and add frustrating friction to consumer experience.

Key Advantages of SBA

SBA offers a significant upgrade over traditional authentication methods like OTP and SNA in terms of security and user experience. SBA enhances security and fraud prevention efforts in the following way:

- ❖ Resists SMS interception because it uses an encrypted, secure connection within the mobile network infrastructure and does not require OTP as a second factor authentication to complete the process.

- ❖ Verification relies on cryptographic keys secured at the hardware level within the SIM, providing significantly stronger, highly resistant authentication.

Additionally, SBA can reduce consumer friction and authentication failure rates:

- ❖ By eliminating the common frustration points of SMS OTP—such as delayed, failed, or out-of-sequence codes—SBA offers a smoother experience and reduces abandonment, particularly critical for time-sensitive transactions.
- ❖ The technology works across both cellular and Wi-Fi networks, and across both iOS and Android platforms, ensuring consistent experiences regardless of connection type.

Key Use Cases

SBA can be leveraged widely where the mobile device is being used to access online services and the consumer identity needs to be verified and authenticated. The following are some key use cases:

- ❖ Securely onboard a new customer or enhance existing KYC process. By providing an initial authentication on the consumer before additional verification workflows, helping businesses safely open new accounts for legitimate consumers.
- ❖ Improve conversion rate with pre-fill forms by performing an initial authentication on the consumer with a low-friction method, to prevent abandonment due to frustration, and provide verified leads for next steps.

- ❖ Prevent ATO attacks by ensuring the consumer signing into the account is the actual owner of both the account and the device being used.
- ❖ Protect transactions by authenticating that the shoppers are the actual account owners who placed the orders.

Summary

SIM-Based Authentication combines carrier-level security with a seamless user experience. By leveraging the inherent security of the SIM card and deep mobile operating system integration, this solution addresses the critical vulnerabilities of SNA and SMS OTP while providing a reduced-friction authentication flow.

The dual platform approach ensures broad coverage across both Android and iOS devices, while working seamlessly on cellular and Wi-Fi networks. For businesses seeking to enhance security, reduce friction, and improve consumer satisfaction, SBA offers a compelling alternative to traditional authentication methods.

Zumigo will roll out SBA via a phased approach, starting in Q4 of 2025. Please contact your sales representative for additional information.

About Zumigo

Zumigo powers digital identity verification in the world's largest enterprises to protect transactions, accounts and trust, using real-time intelligence across mobile, email, device, financial, account, and other information sources. Its modernized, multi-layer approach fortifies the identity perimeter against today's complex fraud and promises a streamlined consumer journey from onboarding to transactions. Learn more at www.zumigo.com.