

Solution Overview

Zumigo Assure Authentication Solution Reduces Consumer Friction, Prevents Fraud

Zumigo Assure Authentication Solution enables seamless, secure first-time sign-ups and returning sign-ins for consumers. It prevents identity fraud and account takeover while eliminating mobile, computer and tablet authentication friction.

With Zumigo, the mobile device's phone number can be authenticated following industry FIDO-based Strong Authentication standards to:

- ❖ Facilitate frictionless authentications from an enrolled device using asymmetric key pair for device verification
- ❖ Reduce friction and user drop-off by eliminating the sign-in process entirely

How Zumigo Assure Authentication Solution works

When a consumer accesses privileged service on a mobile phone/computer/tablet for the first time, the consumer enters their mobile phone number. Zumigo authenticates that the phone number matches the assigned phone number on file and has a low risk profile. The consumer also signs in with their username and password to verify account credentials.

Upon authentication, Zumigo returns a unique QR code to displayed on their computer/tablet for the consumer to scan with the authenticated mobile device to establish trust. When scanned, the trust of the mobile number is then transferred to the computer/tablet. The consumer can access the web app without signing in with passwords.

To bypass the subsequent sign-in process, after verifying the mobile phone number over Wi-Fi,

Zumigo Strong Auth SDK generates an asymmetric key pair in the secure enclave of the device. The private key is stored in the secure enclave and the public key, now associated with the verified mobile number, is shared with the server. Subsequent logins via the same device will bypass the sign-in process, resulting in a frictionless experience.

Zumigo Assure Authentication Solution comprises several products with different capabilities, and they can be implemented separately according to specific business needs.

Do you know?

- ❖ FIDO strong authentication standards are specifications on enrolling trusted device with crypto key pair (device and server).
- ❖ Friction at sign-in is one of the top drivers for user abandonment, leading to significant revenue loss for e-commerce and other businesses that accept online payments.
- ❖ A mobile phone number can be used as a unique identifier for consumers to verify that they are a real person and not synthetic. Keeping bad actors off your platform will reduce operational expenses and improve brand reputation.

Zumigo is on the frontline of digital identity verification that helps the world's largest enterprises secure transactions, devices and accounts. [Learn more at www.zumigo.com](https://www.zumigo.com).