Technology Brief

Zumigo Assure Authentication:

Providing seamless, secure access to prevent fraud

Zumigo

Technology Brief

Zumigo Assure Authentication: Providing seamless, secure access to prevent fraud

In today's digital landscape, providing legitimate consumers with seamless and secure access to services while keeping out fraudulent users is critical. Zumigo Assure Authentication solution validates the digital identity of the consumer without compromising on the frictionless user experience, preventing identity fraud and account takeover attacks.

Zumigo Assure Authentication is designed to offer first-time sign-ups and returning sign-ins without using passwords. This authentication process eases user fatigue by limiting redundant password entry while enhancing account security and reducing the associated costs. Zumigo Assure Authentication comprise the following technologies:

- **Silent Network Authentication (SNA):** Mobile device and account verification leveraging Zumigo’s direct integration with mobile network operators (MNOs). The integration provides device and account risk signals in a layered approach to authenticate the consumer.
- **Mobile Sign-in:** FIDO-compliant strong authentication SDK, leveraging the device’s secure enclaves and risk signals.
- **Desktop or Tablet Authentication:** A unique QR code-based approach that enables mobile device verification and facilitates a trust transfer from the device to the computer or tablet.
- **Multi-Factor Authentication (MFA):** Enhanced security through Zumigo’s SNA and risk signals, which can be used before and after the MFA options are employed.
- **Passkeys:** Passkey adoption support, as well as enhanced security through account and device risk signals.

Providing Frictionless Device Verification via SNA

Verifying that the user has possession and ownership of their mobile device is the first step in establishing trust. Zumigo Assure Authentication uses SNA as the core of its passwordless verification process to minimize friction.

- Zumigo utilizes SNA by leveraging direct integration with MNOs.
- When a user initiates an action requiring authentication (like first-time app use or registration), their mobile number is provided or extracted. Zumigo silently validates this number against the MNO's records associated with the active cellular session. This confirms that the device attempting the action is linked to the claimed phone number on the carrier network (see *Figure 1*).

If SNA cannot be completed, Zumigo uses a one-time passcode (OTP) to confirm possession. Zumigo checks the risk signals associated with the account and device, then sends an OTP to the

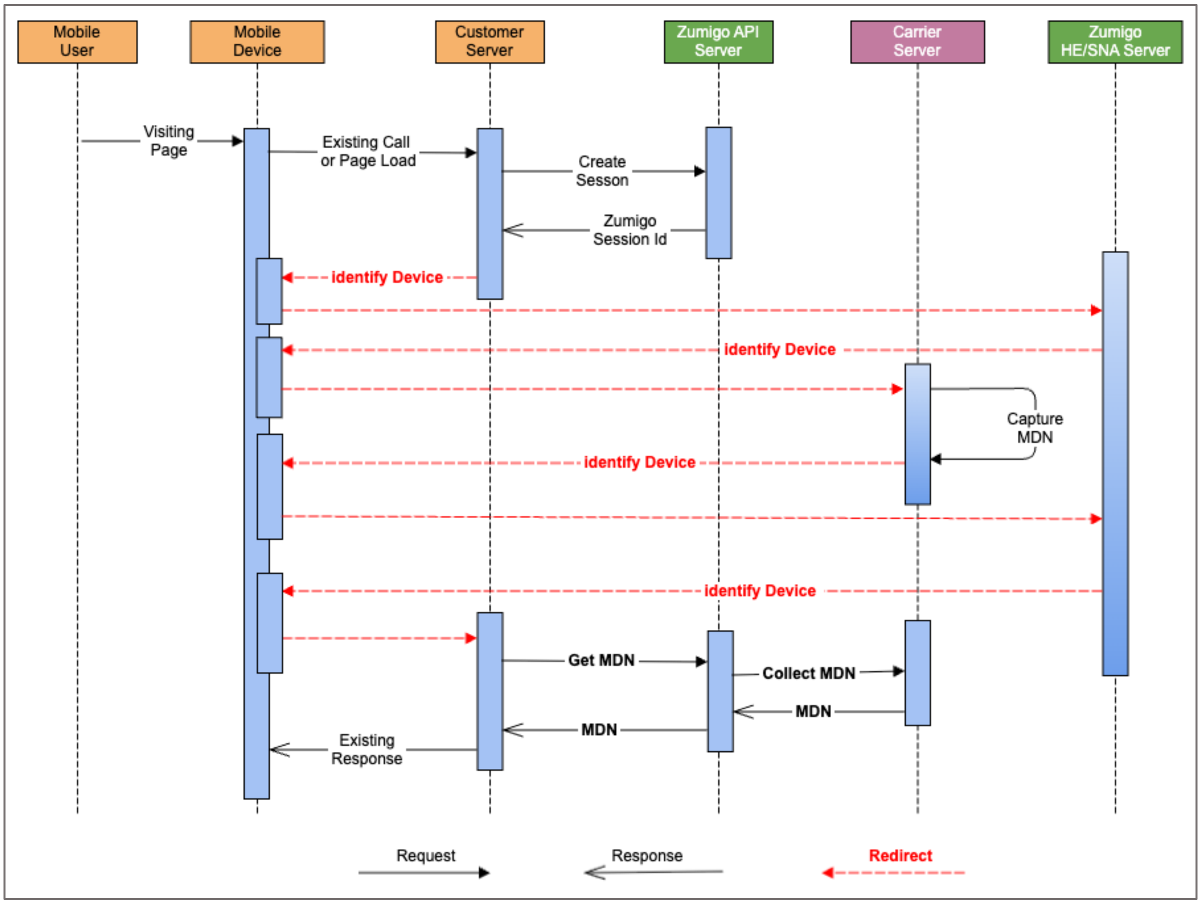

Figure 1: How Silent Network Authentication works

user's device. Once verified, the user is allowed to access the service.

The SNA technology can also be applied during voice-based transactions. When the user is in conversation with a customer service specialist, Zumigo can silently confirm that the person on the line is indeed calling from the phone number registered on the account.

Enhancing Account and Device Security

In addition to standard user authentication, Zumigo collects key signals regarding the user's account and device. This information allows Zumigo Assure Authentication to quickly assess the risk of a possible Account Takeover (ATO). Zumigo collects and analyzes the following data:

- **Porting Information**: Information on account porting across carriers, specifically when the phone number was last ported. Recency is a key risk indicator and can be used as a factor for step-up authentication.
- **SIM Information**: SIM information from carriers regarding when the most recent SIM change occurred. Like porting information, recency is a key risk indicator and can be used as a factor for step-up authentication.
- **Call Forwarding**: Account settings from carriers on the status of the Call Forwarding option. When Call Forwarding is activated, any voice-based OTP request can be re-directed to a fraudster's phone.
- **Number Deactivation:** Phone numbers that are deactivated across carriers could be

re-used by fraudsters to access accounts. The transactions originating from these accounts should be flagged for risk.

These signals allow Zumigo to monitor real-time changes and assess the trustworthiness of the account and device.

Using Strong Authentication for Passwordless Login via Secure Enclave

Once the device's link to the mobile number is verified, a secure, passwordless login experience is enabled using FIDO-based strong authentication principles. Key features of this process include:

- **Key Generation:** Post-verification (SNA or OTP), the Zumigo SDK integrated into the application generates an asymmetric cryptographic key pair:
  - The **private key** is stored securely within the device's hardware secure enclave (e.g., Secure Element, TEE). This key does not leave the device.
  - The **public key** is registered and stored securely on either the Zumigo or enterprise server. This key is associated with the verified mobile number and user account.
- **Enhanced Security:** With Zumigo’s account and device level risk signals listed in the section above, the keys can be unenrolled when changes are detected, providing enhanced security.
- **Subsequent Logins:** For future logins from the enrolled device, the application uses the stored private key to sign an authentication challenge from the server. The server verifies this signature using the corresponding registered public key.
- **User Experience:** Cryptographic verification happens seamlessly, allowing the user to bypass traditional username/password entry while providing a secure and frictionless authentication experience *(see Figure 2)*.

Transferring Trust to Other Devices

Zumigo authentication solution offers trust transfer via secure QR code login, using a trusted mobile device, for passwordless authentication during web sessions on computers and tablets. Users are prompted to enter their account username on the web interface accessed through their computer or tablet. The service provider verifies that this account exists before sending the associated mobile number to Zumigo to verify.

- **SNA Supported Login:** Zumigo determines whether the mobile number belongs to an MNO that supports SNA. If SNA is supported, Zumigo generates a unique, time-sensitive QR code which the web server displays to the user.
- **OTP Verification:** If SNA is not supported, Zumigo generates an OTP and delivers it to the phone number associated with the account. The user is prompted to enter the OTP on the screen. Zumigo verifies the OTP entered is the same OTP that was sent before generating a QR code associated with the phone number. The user then scans the QR code to access the account.
- **Using SDK and Strong Authentication:** If the user scans the QR code using an authenticated mobile device (one containing the Zumigo SDK and the associated private key), the mobile app uses the secure key/token and communicates with Zumigo via the MNO to validate the mobile number and authenticate the request.

Upon successful verification via the mobile device

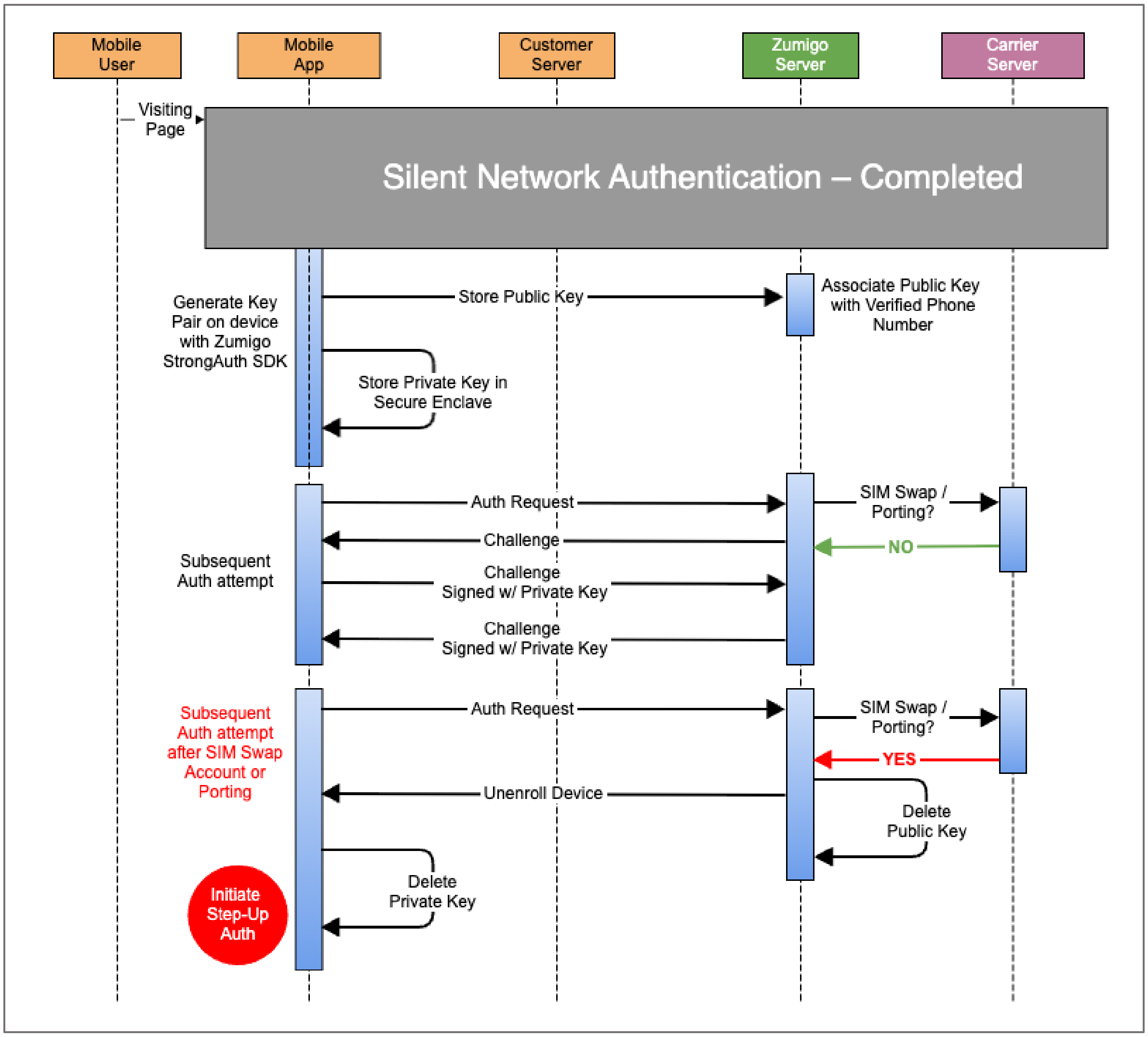
Mobile User
Mobile App
Customer Server
Zumigo Server
Carrier Server
Visiting Page
Silent Network Authentication – Completed
Generate Key Pair on device with Zumigo StrongAuth SDK
Store Public Key
Associate Public Key with Verified Phone Number
Store Private Key in Secure Enclave
Subsequent Auth attempt
Auth Request
SIM Swap / Porting?
Challenge
NO
Challenge Signed w/ Private Key
Challenge Signed w/ Private Key
Subsequent Auth attempt after SIM Swap Account or Porting
Auth Request
SIM Swap / Porting?
YES
Unenroll Device
Delete Public Key
Delete Private Key
Initiate Step-Up Auth

Figure 2: How strong authentication works with Zumigo SDK

Zumigo signals the web server to grant access, effectively transferring the trust from the authenticated mobile device to the web session. This allows the user to log into accounts on the computer or tablet without using passwords.

Strengthening Multi-Factor Authentication (MFA)

Zumigo enhances traditional MFA by incorporating device integrity checks before prompting the user for additional authentication.

- **Pre-MFA Device Check:** Before sending an MFA challenge (like an OTP or prompting for a biometric), Zumigo first verifies the device using methods such as SNA or strong authentication signature check. This ensures that the request originated from a trusted, verified, and uncompromised device *before* potentially exposing an MFA method to interception. Zumigo also checks for risk signals and events associated with the device or number, such as SIM swaps or number porting, as part of the authentication process.
- **Step-Up Authentication:** For high-risk scenarios or sensitive operations, Zumigo can orchestrate step-up challenges like Identity Document Verification (IDV) with

biometric selfie checks (including liveness detection) after the initial device verification.

- **OTP:** Zumigo can allow users secure account access using a one-time passcode provided via SMS link, email or phone audio to an authenticated mobile phone, or QR code to a laptop/tablet to be scanned by an authenticated mobile phone. This serves as an additional layer of security in the MFA process while also reducing friction.

Supporting Passkey Integration

Zumigo's strong authentication framework aligns with FIDO Passkeys and supplements their security with account and device risk signals.

- **Closing the Enrollment Gap:** While passkeys provide phishing-resistant authentication using cryptographic key pairs stored on the device, a critical step is securely enrolling or registering the device for passkey use. Zumigo's SNA and strong authentication (verifying the phone number and binding it to the device's secure enclave) provide the necessary assurance that the device belongs to the legitimate account owner before a passkey is generated and associated with the account.
- **Ease of Integration:** Generating an asymmetric key pair and storing the private key in the device's secure enclave, as used in Zumigo Strong Auth SDK, is the same basic principle behind FIDO passkeys. This correspondence helps facilitate integration and transition.
- **Enhanced Security:** By verifying device ownership and possession before passkey enrollment, Zumigo strengthens the overall security against unauthorized passkey registration on compromised or incorrect devices.

Evolution of the Technology

Zumigo Assure Authentication provides a robust layered authentication approach, starting with frictionless network-based verification, progressing to device-bound cryptographic credentials for passwordless access, offering flexible QR code options, and enhancing MFA security while aligning with modern standards like Passkeys. Additionally, with device fingerprinting, behavioral biometrics and ID Graph, Zumigo can provide optional methods to detect known devices and users, and their changes. These authentication methods can be implemented individually to augment other traditional authentication technologies.

Zumigo Assure Authentication is available as APIs that can be integrated into workflows as fully customizable solutions, or as pre-built widgets via a low-code configurator for quick deployment.

While authentication is rules-based today, Zumigo envisions autonomous agentic decisions assessing risk to adjust user authentication flows as necessary. We are actively exploring this advanced technology as we continue to enhance online security protocols.

To learn more or schedule a demonstration at zumigo.com/contact.

About Zumigo

Zumigo helps the world's largest enterprises protect transactions, devices and accounts. With a multi-layer approach, Zumigo validates users against a unique identity intelligence network that spans global carrier providers, authoritative third-party data sources, and payment information. More at **www.zumigo.com.**