Product Sheet

Zumigo's Silent Authentication Capability Passively Verifies Mobile Device Number

Zumigo Assure Authentication's silent authentication capability captures the phone number passively from a mobile device's cellular signal with the mobile network operator (MNO) to verify possession and ownership. It provides deterministic risk insights to help prevent fraud in transactions that occur on a mobile device. The risk insights empower businesses to decide whether to fulfill the transaction using frictionless authentication.

Once the MNO assigned mobile number has been identified from the cellular signal, it can be used to:

- Compare the mobile number provided by the consumer on other digital channels to the mobile number identified from the current session
- Determine if a mobile login is coming from the same phone that was used in the past, or the one assigned to the account
- Obtain personal identifiable information (PII) such as the name and address on file with the mobile carrier or credit bureaus to automatically pre-fill a form, an application, or a checkout experience on the mobile device so that the process is quick and easy for the consumer
- Obtain information about the mobile subscriber, account, device, and other enabled features to assess the risk of the transaction

Silent authentication works by using a process called header enrichment to automatically identify the MNO assigned phone number for the device. The overall steps are below, although some carriers have slightly different steps:

1. For silent authentication to work, the consumer has to be on the cellular network. Using an API request, Zumigo can determine whether a consumer's device is on the cellular network or Wi-Fi, based on the IP address that is allocated for the data session. If the device has Wi-Fi turned on, Zumigo informs the business so that they can instruct the consumer to disconnect from Wi-Fi.

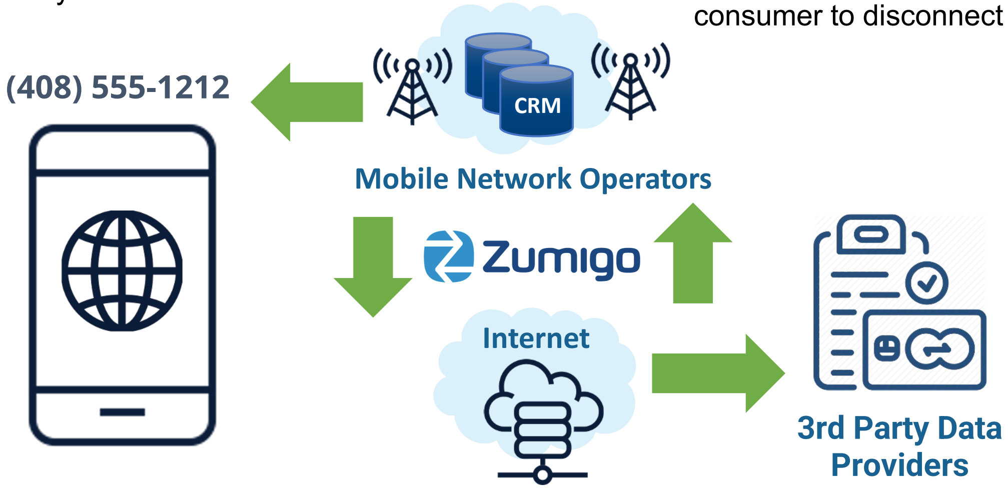

Fig 1: Zumigo Assure Authentication's silent authentication uses header enrichment to automatically verifies and authenticates a mobile number

2. When a consumer is on the business's mobile website or native app while connected to the Internet via the cellular network, the business uses an API call to request a unique, one-time session token. This token is associated with the mobile phone number for billing purposes and to facilitate header enrichment.
3. Behind the scenes, the business redirects the https request, or connects the mobile native app to an authentication URL. This process is seamless and transparent to the consumer.
4. The carrier can observe the device attempting to connect to Zumigo's authentication URL, which is whitelisted for header enrichment. When this happens, the carrier inserts a GUID (globally unique identifier) into the request header that represents the mobile phone number.
5. The device reaches Zumigo's URL where the GUID is collected from the request header, along with the one-time session token, and retained for the business.
6. The client makes a subsequent call to Zumigo's API, using the session token to verify the mobile phone number and retrieve other subscriber, account, and device information.

For consumer devices assigned to carriers that do not support silent authentication, Zumigo can send a one-time passcode (OTP) via SMS for phone number authentication.

Silent authentication can be layered with other verification and authentication methods, including strong authentication or multi-factor authentication, for more protection and risk insights to determine trustworthiness, especially for high-value transactions or accounts.

About Zumigo

Zumigo is on the frontline of digital identity verification that 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. **Learn more at www.zumigo.com**.