



# Identity Security for the Passwordless Era

A Modern Architectural Approach for Real-time, Adaptive and Flexible Verification Solutions

# Whitepaper

# Identity Security for the Passwordless Era

For decades, passwords and some portion of Personally Identifiable Information (PII) have been the cornerstone of proving a digital identity. However, beyond well-documented security vulnerabilities as well as frequency of data breaches, passwords have also become a primary source of systemic friction for both users and administrators.

Today's user is caught in a crossfire of inconsistent requirements that may paradoxically contribute to the vulnerabilities of passwords instead of the opposite. One service may demand a sixteen-character string with complex symbols, while another may insist on a password rotation every thirty days. This lack of standardization leads to *password fatigue*, causing consumers to either resort to password reuse; typing or writing them down making them easier to get stolen; or requesting for credential reset links that can be intercepted easily.

For organizations, a forgotten password is more than a nuisance; it is a significant operational drain. Every reset triggers a help desk call and a manual resolution process, requiring an increasing investment in IT operations and support systems just to maintain basic access. The cost is tangible. Commonly cited costs range from \$70 per password reset (Forrester), to comprising 20% to 50% of IT help desk calls (Gartner).

Clearly, passwords and easily obtained PII are not cutting it.

## Today's Pressures Shaping Identity Security Strategy

Operational headaches aside, the digital landscape of today has introduced five critical

pressures that make traditional credential management unsustainable:

- 1. Credential Sprawl:** In a mature digital economy, every interaction ranging from banking to utility management requires a unique account. The average user now manages hundreds of *digital selves*, creating an unmanageable attack surface for the enterprise.
- 2. The MFA Paradox:** To counter password weakness, businesses have layered on Multi-Factor Authentication (MFA). However, many of these methods introduce additional friction, forcing users to juggle disparate apps and devices to verify a single identity.
- 3. Security Architectural Misalignment:** Modern identity security frameworks, such as Zero Trust, require continuous, context-aware authentication. Static passwords that allow the service to remember the user after initial log-in do not support these dynamic security architectures.
- 4. Speed of Bot-Scaled Harvesting:** The threat landscape has shifted from individual hackers to automated botnets. PII harvesting and brute-force attacks are now accelerated by artificial intelligence, allowing attackers to test millions of stolen credentials in seconds.

- 5. Global Compliance Mandates:** From Europe's Third Payment Services Directive (PSD3) to evolving international privacy laws, mandates are becoming more stringent. Businesses now face legal and financial penalties if authentication methods fail to meet phishing-resistant standards across borders.

## The Zumigo Framework: Multi-layer Identity Verification

In response to these pressures, passwordless authentication has transitioned from a luxury, nice-to-have to a necessity in securing digital identity. While it may not entirely replace verification methods that rely on passwords, it provides an essential, low-friction, low-maintenance, high-security alternative that are flexible to deploy to address different use cases.

Zumigo passwordless authentication solution is built upon a seamless, multi-layered verification and authentication framework for businesses to create and preserve digital trust. Using multiple real-time, deterministic signals that represent a user's different identity artifacts to verify and authenticate their identity, Zumigo prevents fraudulent activities across the digital engagement journey without excessive friction. The Zumigo verification framework is architected around the following four core principles:

- 1. Strong and Adaptive Authentication:** The most common authentication method that relies on passwords and one-time passcodes (OTPs) has well-known weaknesses, including security vulnerabilities and poor user experience. Zumigo's suite of authentication solutions are minimally invasive and can address initial authentication, re-authentication, and step-up authentication use cases:

- ❖ **Mobile Network Authentication (MNA):** This is a passive, background check that verifies mobile device possession and ownership

using direct, real-time Mobile Network Operator (MNO) signals and can be achieved via two technologies: Silent Network Authentication (SNA) or SIM-Based Authentication (SBA). Both will confirm that the user is who they claim to be without slowing them down.

- ❖ **FIDO-Based Passkeys:** Zumigo facilitates the secure binding of cryptographic passkeys to the user's mobile device (leveraging the secure enclave), eliminating password vulnerability entirely while providing the strongest possible security assurance. Upon verification using MNA technology, the Zumigo SDK generates an asymmetric cryptographic key pair. The private key is stored securely within the device's hardware secure enclave (e.g., Secure Element, Trusted Execution Environment). The public key is registered and stored securely on the server, either with Zumigo or the enterprise. For future log-ins 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. The keys can be unenrolled when device changes are detected, including porting, SIM swap, de-activation and re-activation, etc., for close-looped security.
- ❖ **Trust Transfer:** Zumigo enables the ability to securely transfer verified identity trust from a mobile device to a desktop or tablet session via QR code, by authenticating the ownership using MNA or the installed passkey. This approach seamlessly maintains the Zero Trust chain across all user devices.
- ❖ **Social Authentication:** Zumigo leverages authentication using Google, Apple and Meta credentials to protect user access through MFA, device trust, biometrics, and anomaly

detection at a scale most organizations cannot replicate internally.

## 2. Ongoing Real-Time Authoritative

**Intelligence:** To build and preserve digital trust, verification and authentication must be continuous and contextual based on real-time, authoritative sources, not just a one-time event. Simple checks cannot catch sophisticated threats like SIM swap and synthetic identity fraud. Zumigo provides risk scoring based on layered verification information that do not rely on historical or outdated predictive models:

- ❖ **MNO Real-Time Signals:** Zumigo gathers authoritative, deterministic data from MNOs, including SIM swap alerts, number porting status, and deactivation status. These signals provide immediate, unforgeable context for risk assessment.
- ❖ **Data Fusion:** Zumigo aggregates MNO data with crucial intelligence on device fingerprinting, behavioral biometrics, email validity, geo location, IP listing, and payment information. This data fusion generates a single, holistic risk score that reveals threats hidden in siloed systems.
- ❖ **Contextual Risk Scores:** Real-time, multi-layered scoring is aggregated to determine the risk of various fraud threats, including Account Takeovers (ATOs) or synthetic identity, allowing the enterprise to manage risk proactively.

**3. Comprehensive Risk Signals:** No single piece of information is sufficient to confirm digital identity or prevent modern fraud. Fraudsters can compromise a single data element, but they cannot control every signal across the digital and physical layers. Zumigo assesses risk across the entire journey using information including but not limited to the following:

- ❖ Mobile number and account information
- ❖ Device fingerprinting and biometrics
- ❖ PII match and verification
- ❖ Email validity and verification
- ❖ Payment and banking
- ❖ Government-issued documents
- ❖ Network activity
- ❖ IP-Based geolocation

**4. Agile Deployment and Accessibility:** To achieve widespread adoption of seamless verification workflows, the solution must be easy for business units to deploy and manage without extensive IT support. Zumigo ensures this accessibility through flexible deployment options:

- ❖ Via API integration to Zumigo services for complex, custom use cases.
- ❖ Available on major e-commerce platforms for easy downloads and deployment to e-stores.
- ❖ Visually build, test, and deploy complex, risk-tiered workflows without relying on custom coding via the [Zumigo Identity Verification Builder](#). From the dashboard, the user can access a comprehensive set of risk signals and decisioning to build the workflows which can be hosted by Zumigo or embedded into the target website. Businesses can drastically improve agility and reduce the cost of deployment.

## Strategic Outcomes and Use Cases

By moving identity verification to the network and hardware layers, businesses can leverage the flexibility of Zumigo solutions and select the technologies that fit their specific requirements. Here are the key use cases Zumigo passwordless solution addresses:

- ❖ **Securely onboard a new consumer** and prevent fake identities from opening accounts

while preserving a seamless experience. Because of data breaches, hacking and other scams, most PII and credentials are easily accessible by career criminals. Zumigo helps businesses safely open new accounts for verified, legitimate consumers.

- ❖ **Reduce friction and streamline experience** with secure passwordless access. Using mobile network authentication, Zumigo instantly verifies consumer identities using their mobile phone number or the installed passkey with additional, layered protection using SMS or voice OTP or social log-in. Consumers can access their accounts without entering user names and passwords.
- ❖ **Enhance multi-factor authentication security** with a variety of options. Zumigo verification and authentication methods can be used individually, either as the first factor or as a second factor authentication, or together in a multi-layered approach to identity security.
- ❖ **Leverage the Trust of the Mobile Device to Access Web Accounts:** The verified trust from a mobile device via MNA or passkeys can be transferred to log into a desktop or tablet session by scanning a QR code as presented on the screen.

## Building Digital Trust with Passwordless Authentication

The flexibility of Zumigo solutions can be configured to address different adaptive and continuous verification use cases, including first step, step-up, or re-authentication. For example, if a user attempts to access sensitive financial data from a new location or exhibits unusual navigation patterns, an automated second authentication challenge can be triggered without terminating the session entirely. This approach collapses the identity attack surface, providing a

robust defense against session hijacking and automated bot attacks while reducing user friction for legitimate, low-risk interactions.

The transition to a passwordless architecture allows businesses to improve their bottom line and comply with global regulations while building lasting customer trust. By reducing identity-related fraud, lowering user friction, and improving the digital experience, Zumigo solution provides the foundation for the next era of passwordless digital interaction.

Ready to secure your digital perimeter? Contact us at [zumigo.com/contact](https://zumigo.com/contact) for a demo.

### **Additional reading:**

- ❖ [Whitepaper: Reduce Fraud with QR Code Log-in](#)
- ❖ [Technical Brief: Zumigo Assure Authentication](#)
- ❖ [Blog: Beyond Passwords: Elevating E-commerce Security with Seamless Onboarding and Authentication](#)
- ❖ [Blog: Identity Is the New Network Perimeter: Why You Need a Multi-Layered Fraud Defense](#)
- ❖ [Blog: Stop the Leak: Why Passwords Are Your Perimeter's Biggest Liability](#)

### **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](https://www.zumigo.com).