RAAH
TECHNOLOGIES

PASSWORDLESS AUTHENTICATION

Groundwork, Execution, and Industry Trends

Introduction

Passwordless authentication is a strategic necessity for banking and financial institutions. Moving beyond passwords requires precise planning, technical preparation, and foresight into emerging disruptions. This whitepaper explores two critical areas for success.

INTRODUCTION

Passwordless authentication is a strategic necessity for banking and financial institutions. Moving beyond passwords requires precise planning, technical preparation, and foresight into emerging disruptions. This whitepaper explores two critical areas for success:

Groundwork for Passwordless:
End-to-end activities to prepare for and execute Passwordless authentication for B2C, B2B, B2B2C, and workforce environments.

Industry Trends & Disruptions:
Insights into global trends and paradigm shifts that influence Passwordless strategies.

1 GROUNDWORK FOR PASSWORDLESS AUTHENTICATION

Implementing Passwordless authentication involves comprehensive preparation across different environments. This section outlines the critical steps required to achieve Passwordless for B2C, B2B, B2B2C, and internal workforce applications. Many of the below items center around defining policy based on the discovery items detailed below:

User Analysis & Personas

- Identify user groups (employees, customers, contractors, partners) and their unique access needs.
- Map roles and personas to specific authentication methods (biometric, magic links, security keys).

System & Application Inventory

- Catalog all applications, services, and physical resources requiring secure access.
  - **Identify which apps support modern protocols** (WebAuthn) and flag those legacy applications that may need integration considerations or refactoring for modernization goals.
  - **Identify applications by criticality and privilege scoring metrics** to assist in driving policy for those applications as it pertains to AuthN methods and the controls therein.
  - **Assess applications in the context of Users and Personas.** This is critical to understanding how demographic data about the user population may impact the rollout of AuthN for specific scenarios.

Authentication & Access Use Cases

- Define scenarios for workforce (remote, on-site, physical access) and customers (web apps, mobile apps, call centers).
- Plan for access to buildings, physical assets (like vaults, safe rooms), and shared workspaces.

Access Control Review

- Ensure that Role-Based Access Control (RBAC) and Just-in-Time (JIT) access models are properly defined.
  - Understand user roles and permissions in services on a persona and application level, as **AuthZ** and **application context** can directly contribute to **AuthN strategies** around planning friction to fit security needs, versus using blanket strategies.
- Ensure that there are existing workflows to provide temporary, or attested and long-standing role-based elevated access (like system admins).

Technology & Infrastructure Assessment

- Identify hardware requirements (security keys, biometric readers, kiosks) and allocate necessary budgets to support those systems as needed.
- Review system readiness for protocols like FIDO2, WebAuthn, and biometric API support.

Compliance & Regulatory Requirements

- Identify hardware requirements (security keys, biometric readers, kiosks) and allocate necessary budgets to support those systems as needed.
- Review system readiness for protocols like FIDO2, WebAuthn, and biometric API support.

1.2 PROVIDER EVALUATION & SELECTION

Define Requirements

- List must-have features for workforce, B2B, B2B2C, and B2C environments.
- Prioritize support for standards like FIDO2, WebAuthn, and multi-factor authentication (MFA).

Research Solution Providers

- Identify top Passwordless authentication providers (e.g., Okta, Ping Identity, Microsoft, Duo, etc.).
- Evaluate vendor reputation, industry presence, and compatibility with banking security needs.

Feature & Capability Comparison

- Compare providers on biometric support, fallback mechanisms, integration ease, and scalability.
- Check compatibility with existing applications, SaaS solutions, and legacy infrastructure.

Vendor Demos & Trials

- Schedule live demos with vendors to review workflows, fallback processes, and end-user experiences.
- Conduct internal trials to assess operational impact and end-user satisfaction.

Risk Assessment

- Evaluate risk factors like vendor lock-in, SLA coverage, and failover processes during outages.
- Ensure providers support regulatory compliance (GDPR, PSD2) and data sovereignty needs.

Total Cost of Ownership (TCO) Analysis

- Review license fees, implementation costs, and ongoing support fees.
- Ensure support for customer service models and end-user self-service options.

Final Selection

- Rank providers based on readiness, compatibility, security posture, and TCO.
- Choose a provider that supports enterprise-wide deployment for all workforce and customer-facing environments.

1.3 PERMUTATIONS & COMBINATIONS

1. Who Needs Access?

- Internal employees, external customers, third-party vendors, and partners.

2. What Needs Access?

- Workstations, customer portals, vaults, ATMs, shared workspaces, and data repositories.

3. How is Access Granted?

- Biometrics (fingerprints, facial recognition), security keys, hardware tokens, and QR code logins.

4. Where Does Access Occur?

- Office premises, remote work environments, customer-facing mobile apps, and call centers.

5. Access Paths & Channels

- Mobile devices, desktop workstations, point-of-sale terminals, and IoT-connected devices.

By addressing every permutation, organizations ensure secure, seamless access for all users and systems.

1.4 EXECUTION & IMPLEMENTATION PATH

Discovery & Planning

- Conduct readiness assessments for apps, services, and end-user groups.
- Prepare a risk-based strategy to prioritize high-risk users, like administrators and financial executives.

Design & Architecture

- Design the Passwordless architecture, considering workforce, B2C, and B2B scenarios.
- Align authentication policies across employees, customers, and third-party users.

Pilot Implementation

- Roll out Passwordless authentication for non-critical systems or select employee groups.
- Gather user feedback and adjust before a full-scale launch.

Training & Change Management

- Conduct employee training for multi-device registration, self-service recovery, and fallback options.
- Inform customers about new login experiences and provide onboarding guides.

Full Rollout & Monitoring

- Scale Passwordless adoption to all apps, customers, and employees.
- Monitor usage, collect feedback, and refine fallback strategies.

Audit & Continuous Improvement

- Conduct audits to ensure compliance with GDPR, PSD2, and internal policies.
- Review incident logs to identify areas of improvement

2 INDUSTRY TRENDS & DISRUPTIONS

Passwordless strategies can be affected by disruptive forces, both technological and operational. Organizations must future-proof their approach to maintain resilience.

2.1 PARADIGM SHIFTS & DISRUPTIVE FORCES

Quantum Computing

- **Impact:** Quantum computers may break traditional cryptography, threatening Passwordless protocols.
- **Mitigation:** Plan for post-quantum cryptography and update algorithms as standards evolve.

Biometric Advancements

- **Impact:** New biometrics (heartbeat, gait) introduce fresh opportunities and challenges.
- **Mitigation:** Design modular systems that can support new modalities with minimal updates.

Decentralized Identity (DID)

- **Impact:** DID shifts identity ownership to individuals, requiring reimagined access models.
- **Mitigation:** Ensure the Identity Suite that is purchased or built can incorporate compatibility with decentralized identity wallets in the future when the standard for identity management could shift to focus on tokenized identity.

Regulatory Shifts

- **Impact:** GDPR, PSD2, and industry-specific compliance rules influence the design of access systems.
- **Mitigation:** Implement privacy-first access models and secure fallback channels.

2.2 TRENDS IMPACTING IMPLEMENTATION

User Experience (UX) Trends

- **Example User Expectation:** Users expect frictionless login experiences with one-tap or biometric access.
- **Solution:** Invest in user experience design to deliver "invisible" authentication.

Hybrid Workforce Models

- **Examples of Remote Work Considerations:** Hybrid work requires Passwordless access across devices, VPNs, and on-prem resources.
- **Solution:** Deploy cross-platform access with multi-device authentication and VPN-less access.

Third-Party Integrations

- **Examples of Integration Points:** Banking ecosystems rely on vendors, fintech partners, and payment gateways.
- **Solution:** Use federated access models with vendor identity verification.

Cyber Threats & Ransomware

- **Example of Threats:** Attackers target fallback options like SMS-based recovery and device loss scenarios.
- **Solution:** Use strong fallback protocols to prevent exploitation by savvy bad actors. The below comparison table should allow the framing of factors and their specific uses, as well as what you need to know about their pros and cons.

FALLBACK PROTOCOL COMPARISON TABLE

Fallback Method	Use Cases	Risk Level	Ease of Use	Security	Notes
Multi-Device Enrollment	Workforce, B2B, B2C, B2B2C	Low	High	High	Users pre-register multiple devices (e.g., phone, tablet, laptop) to ensure ongoing access if one device is lost.
Backup Authentication Methods	Workforce, B2B, B2C, B2B2C	Medium	High	High	Users register multiple biometrics (fingerprint + face) or combine with hardware tokens (e.g., FIDO2 security keys).
Emergency One-Time Passcodes (OTPs)	Workforce, B2C	Medium	High	Medium	Single-use codes are delivered via a secure app or in-session prompt (not SMS) to avoid interception risks.
Support-Driven Identity Verification	Workforce, B2C, B2B2C	Medium	Low	High	Users must verify their identity through a helpdesk or live support agent. Best for privileged or critical users.
Multi-Factor Step-Up Authentication	Workforce, B2B, B2C, B2B2C	Medium	High	High	If primary methods fail, users must provide a second factor (e.g., hardware token + biometric) for access.
Secure Self-Recovery Portal	B2C, B2B2C, Workforce	Low	High	High	Users self-recover access through a secure portal with CAPTCHA, device attestation, and risk-based logic.
Temporary Access Tokens	Workforce (Admin, IT Ops)	High	Medium	High	Time-limited tokens grant temporary access for privileged roles. Tokens are revoked after the session ends.
Risk-Based Adaptive Authentication	B2C, Workforce, B2B2C	Low	High	High	Access context (location, device, time) is evaluated, and fallback methods are triggered only for anomalous activity.
Out-of-Band Authentication (OOB)	B2C, Workforce, B2B	Low	High	High	Verification happens via push notifications or messages sent to separate secure devices, like a mobile app.
Dynamic Approval Workflows	Workforce (Privileged Access)	High	Medium	High	High-sensitivity access requires human approval (e.g., manager or security officer) before access is granted.

RAAH
TECHNOLOGIES

Follow us @RAAHTech

solutions@RAAHTech.com