OneSpan

Workforce Passkeys: From Tokens to Operational Solutions

Designing passkey deployments for real-world workforce environments

PREPARED BY MURTAZA HAFIZJI
23RD, MARCH 2026

Passkeys are moving into the workforce

- Passkeys provide phishing-resistant authentication
- Enterprise adoption is increasing

87%

of organizations are deploying passkeys for workforce access

Source: FIDO Alliance, 2025

The challenge has shifted from authentication to operations

WHAT'S WORKING

- Strong authentication security
- Improved sign-in experience
- Broad industry adoption

WHAT'S EMERGING

- Enrollment introduces friction
- Users lack a clear mental model
- Platform and UX inconsistencies
- Lifecycle and recovery gaps

Enrollment is the critical path

Most failures happen during enrollment

- Requires coordination across identity, device, and user
- Small friction → large drop-off at scale

Passkeys change the user’s role in authentication

Passwords + OTP

- User creates and enters secrets
- Familiar interaction model
- Insecure and error-prone

Passkeys

- Credentials bound to device and user
- System handles authentication
- Platform-dependent experience

One size does not fit all

Office workers
Managed devices, consistent environments

Contractors
Unmanaged devices, higher variability

Frontline / shared-device
No dedicated device, shared usage

Remote users
Multi-device access, cross-platform usage

Credential strategy requires deliberate choices

Device-bound passkeys

- **Strong control and assurance**
- Limited portability

Synced passkeys

- **Better usability across devices**
- Less enterprise control

Hardware -backed credentials

- **High assurance**
- Requires distribution and management

Where hardware security keys fit in workforce deployments

Best suited for specific workforce scenarios

High assurance scenarios

- ☑ Privileged users and sensitive access

Shared and kiosk environments

- ☑ No persistent user to device binding

Unmanaged or restricted devices

- ☑ Consistent authentication across environments

Pre-provisioning and controlled rollout

- ☑ Enables scalable, controlled environment

Platform variability introduces friction

Platform variability introduces friction

Browsers

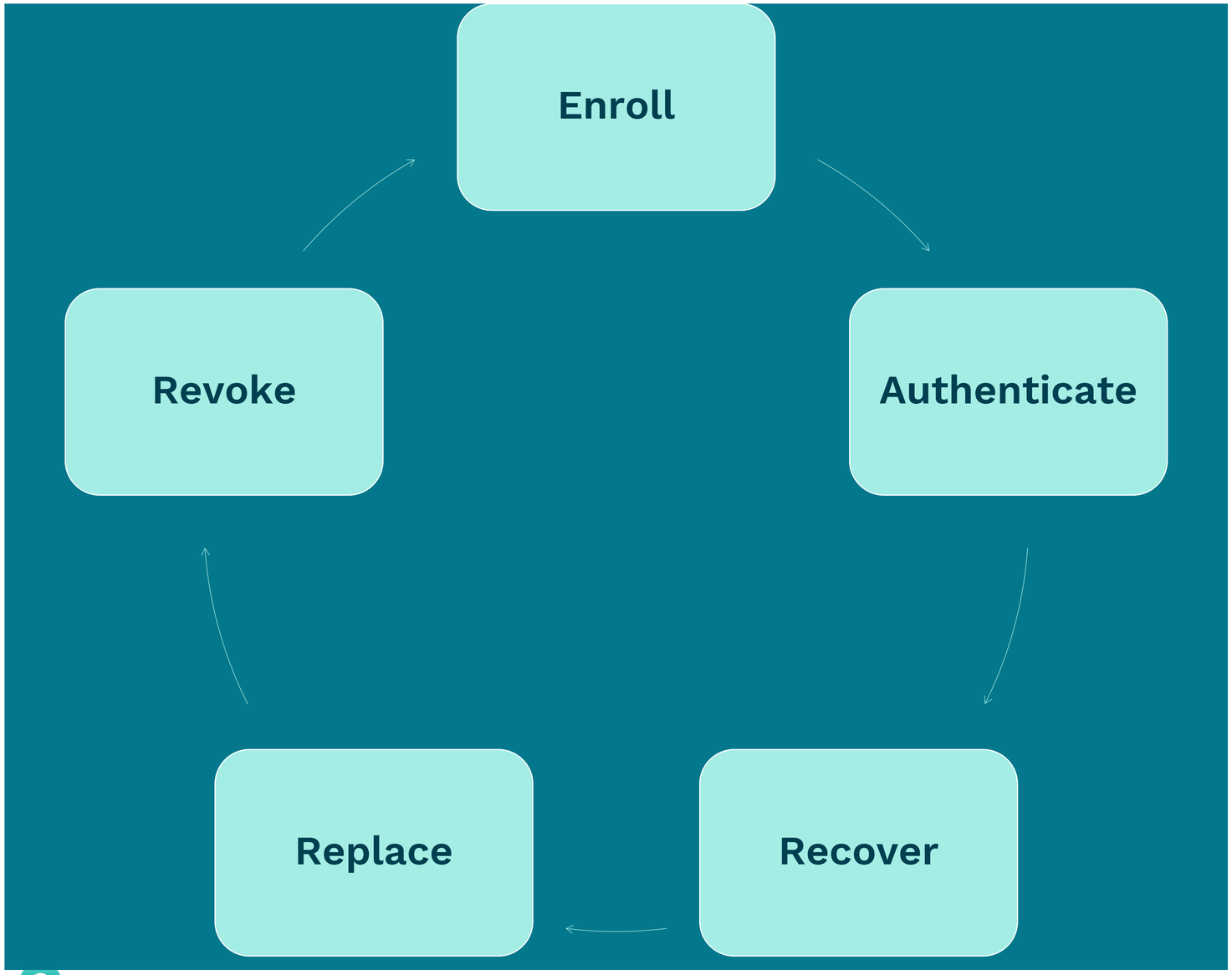
Operating systems

Credential storage

Different environments create different user experiences

Inconsistent UX impacts adoption and support

Authentication is only one part of the lifecycle



- **Authentication is improved - lifecycle and recovery are still evolving**
- Recovery and device changes are **high-risk moments**
- Operational gaps create security and usability risks

Deployment models are evolving

User -driven model

- Users enroll and manage credentials
- Experience varies by platform and device
- Higher friction and support load

Managed model

- Credentials provisioned or guided by admins
- Integrated with identity and endpoint systems
- Consistent, scalable deployment

A framework for workforce passkey deployment

Identity Binding

How identity is verified at enrollment

Credential Strategy

What credential types are allowed and where

Enrollment & Distribution

How credentials are issued and provisioned

Lifecycle Management

Recovery, revocation, and change handling

Key Takeaways

- Passkeys improve authentication security and usability
- Workforce deployments introduce operational complexity
- Success depends on how identity, credentials, and lifecycle are designed

Passkeys don’t fail — deployments do

The Authentication Company

Global — 1,000+ customers across 120+ countries with locations worldwide

NASDAQ — Publicly traded (NASDAQ:OSPN) since January 2000

Secure DNA — 30+ years of experience leading multi-factor authentication, digital transaction signing and mobile app security markets

Trust — Over 60% of the world's top-100 largest banks rely on OneSpan

Scale — 500M+ users protected worldwide

Proven — Digipass is the industry standard for strong, reliable MFA

OneSpan

Visit RSAC N # 6578

to continue the conversation...