



Revolutionizing Online Security: Gold Authentication for Seamless FIDO2 Deployment

Executive Summary

In an era of escalating cyber threats, FIDO2 authentication offers robust protection against phishing and man-in-the-middle attacks. However, its adoption has been hindered by complex user onboarding, credential management challenges, and recovery issues. Gold Authentication, developed by Gold Security Corporation, builds on FIDO2's strengths while simplifying the user experience through centralized identity management and innovative features like B² Entanglement. This white paper explores the limitations of traditional FIDO2, introduces Gold Authentication as a scalable solution, and highlights its benefits for banking institutions, including reduced support costs, enhanced security, and insurance savings. With its launch at Jack Henry Connect on September 11, 2025, Gold Authentication positions banks to lead in secure, user-friendly online authentication.

The Evolving Landscape of Online Security

Cybersecurity threats, such as account takeovers and phishing, continue to plague online platforms, costing businesses billions annually. Traditional multi-factor authentication (MFA) methods, like SMS codes or authenticator apps, are vulnerable to interception and social engineering. FIDO2, a standard developed by the FIDO Alliance, addresses these vulnerabilities through public-key cryptography, enabling passwordless, phishing-resistant logins. Despite its security advantages, FIDO2's widespread adoption remains limited. As of 2025, industry reports

indicate that while awareness is growing, practical implementation faces significant hurdles, particularly in user adoption and enterprise scalability.

This white paper examines these challenges and presents Gold Authentication as a transformative enhancement to FIDO2, tailored for banking and financial services.

Challenges in Adopting Traditional FIDO2 Authentication

FIDO2's promise of secure, hardware-based authentication is undermined by practical barriers that deter users and organizations alike. Key issues include:

- **User Onboarding Friction:** Users must acquire FIDO2-certified hardware authenticators, often purchasing multiples for backup. Setting up credentials requires manual registration on each website, a time-consuming process that scales poorly for individuals with multiple accounts. Research from sources like USENIX Security highlights "friction" as a primary obstacle, with users abandoning setup due to complexity.
- **Credential Management and Proliferation:** For every site, users create unique credentials, leading to management overload. Adding backup devices doubles this effort. If a device is lost without backups, users face lockouts, exacerbated by existing MFA layers that block easy recovery.
- **Recovery and Support Burdens:** Lost authenticators trigger out-of-band recovery, often via phone support. This not only consumes user time but burdens providers with high costs—estimated at 10-30% of operational expenses in some sectors. Verification challenges during recovery open new attack vectors for hackers, as support teams struggle to confirm identities without clear protocols. Studies on FIDO2 deployability note enterprise concerns over credential lifecycle and recovery as major roadblocks.
- **Adoption Barriers:** Websites cannot mandate FIDO2 without alienating users lacking hardware. Regulatory requirements and security culture further complicate rollout, per findings from ACM and FIDO Alliance white papers.

These challenges result in slow market penetration, leaving society vulnerable to outdated authentication methods.

Introducing Gold Authentication: A Next-Generation FIDO2 Solution

Gold Authentication from Gold Security Corporation redefines FIDO2 by centralizing identity management, eliminating per-site credential creation, and enabling instant multi-device support. Built on FIDO2-certified GoldKey authenticators (available in USB and NFC formats), it maintains FIDO2's core security features—phishing resistance and cryptographic integrity—while introducing user-centric innovations.

At its heart is the Gold Identity (Gold ID), a free, user-created profile tied to a username, email, and phone number, registered in the secure Gold Security Data Center. This single identity unlocks FIDO2 access across participating sites without repetitive setups.

Gold Authentication leverages B² Entanglement, a patented technology used by the U.S. military for enhanced security. This process ensures entangled credentials across devices, providing seamless synchronization and recovery without compromising zero-knowledge principles.

How Gold Authentication Works

Gold ID Creation: Users register a free Gold ID in minutes via any supported website or directly through Gold Security. No hardware purchase is required initially—a provisional Digital GoldKey (software-based authenticator) is provided for immediate use.

1. **Site Integration:** Banks and websites display a "Sign in with GoldKey" button alongside the GoldKey Diamond logo. Users click to authenticate instantly using their Gold ID and any associated GoldKey (physical or digital).
2. **Account Linking:** For existing accounts, users log in via legacy methods once, then link to Gold Authentication. New users authenticate directly.
3. **Multi-Device Support:** Users add unlimited physical GoldKey authenticators or download Digital GoldKey authenticators to devices. All are instantly authorized across all linked sites, bypassing per-site credential creation.
4. **Credential Recovery:** Gold Security's managed recovery service prepares users in advance, using verified contact details and secure protocols. This offloads recovery from banks, reducing support calls and fraud risks.

This streamlined process accelerates FIDO2 adoption, making it accessible without hardware barriers.

Key Features and Benefits for Banking Institutions

Gold Authentication addresses FIDO2's pain points while delivering tangible value to banks:

- **Enhanced User Experience and Adoption:** Instant setup and cross-site compatibility encourage enrollment, potentially converting all online customers to FIDO2-secured MFA.
- **Cost Savings:** Banks see 10-30% reductions in liability insurance due to lowered takeover risks. Centralized recovery minimizes support expenses, as Gold Security handles lockouts.
- **Security Advantages:** Retains FIDO2's resistance to attacks, augmented by B² Entanglement for military-grade protection. Frequent use across sites reduces user forgetfulness or loss.
- **Scalability and Compliance:** Supports regulatory needs for strong authentication. Easy integration for websites via OAuth2 and OpenID Connect.
- **Credential Portability:** Users maintain access even if devices are lost, with backups ready out-of-the-box.

Participating banks can offer "unprecedented security and ease of use," differentiating in a competitive market.

Launch and Path to Adoption

Gold Authentication launches to banking institutions at Jack Henry Connect in San Diego, California, on September 11, 2025. Early adopters gain tools to enroll customers seamlessly, including API integrations and marketing resources. By embedding Gold Authentication, banks can lead the shift to universal FIDO2, mitigating societal vulnerabilities to online fraud.

Conclusion

Gold Authentication transforms FIDO2 from a niche security tool into a mainstream solution, balancing ironclad protection with effortless usability. For banks, it means fortified defenses, operational efficiencies, and delighted customers. To learn more or schedule a demo, contact Gold Security Corporation at www.goldkey.com.