Secure Infrastructure Access Protocol (SIAP)

Revision: 1.0
Date: July 20, 2025
Author: John G. Underhill
Document Type: Executive Summary
Keywords: SIAP, post-quantum authentication, hash-based security, two-factor, SCB, SHAKE256, KMAC256, RCS256, offline infrastructure access

1. Overview

The **Secure Infrastructure Access Protocol (SIAP)** is a lightweight, post-quantum authentication system that fuses physical token possession with a passphrase-derived cryptographic proof. It replaces vulnerable public-key infrastructures and certificate lifecycles with a compact, purely hash-based construction rooted in **SHAKE-256,** and **SCB (cost-based KDF)**. Each login produces a **unique, single-use 256-bit secret** that self-destructs after use, enforcing **forward secrecy** and **replay resistance** without depending on a network or certificate authority.

Designed for devices that must authenticate securely while offline: industrial control consoles, payment terminals, embedded IoT systems, and critical infrastructure nodes, SIAP operates within **30 kB of code**, making it deployable in **smart-card class microcontrollers** or **secure elements**. The result is a universal, post-quantum-safe access layer and authentication scheme.

2. Motivation and Strategic Rationale

Modern infrastructures remain burdened by complex certificate management, public-key renewals, and post-quantum uncertainty. As national and corporate networks confront the inevitability of quantum decryption, the operational cost and fragility of asymmetric systems are no longer sustainable.

SIAP was conceived to **eliminate reliance on asymmetric mathematics altogether**. It achieves regulatory-grade multi-factor assurance through a **removable memory token** and a **passphrase**, both bound by memory-hard key derivation. The architecture offers a practical bridge between today’s credential ecosystems and tomorrow’s post-quantum landscape, allowing critical sectors; finance, energy, government, and manufacturing, to deploy **quantum-resilient authentication immediately**, without infrastructure upheaval.

For potential acquirers or investors, SIAP represents a **disruptive cryptographic platform**: a verifiable, minimal-trust system that scales across industries, reduces compliance costs, and hardens high-value networks against both classical and quantum adversaries.

3. Architecture and Mechanism

SIAP structures identity and access around a concise, deterministic hierarchy:

- **Server Identity (Sid):** Domain → Server Group → Server Instance
- **User Identity (Uid):** Group → User → Memory Card ID
- **Key Chain:** A monotonic counter of one-time leaves, derived from a base key (Kbase) via SHAKE-256.

The **server** provisions the removable card with a time-bounded encrypted key structure (Uks) and a contiguous array of one-time keys (Kchain). Each session's secret key (Ktok) is recovered only when the correct **passphrase** and **key-index value (Kidx)** are supplied. Once authentication succeeds, the key is immediately erased and the card's state advanced, guaranteeing forward secrecy and eliminating standing credentials.

The **SCB key derivation function** enforces memory and computational hardness, raising the cost of any dictionary or GPU attack into multi-year infeasibility. The **SHAKE-only cryptographic domain** eliminates reliance on trapdoor functions, ensuring security under Grover-bounded conditions (≥128-bit post-quantum margin).

This design supports a full offline lifecycle: each server can verify identities and card states locally, without certificate validation or online time services, making SIAP ideal for **air-gapped**, **sovereign**, or **field-service** environments.

4. Security Model and Post-Quantum Posture

SIAP's security model defines adversary classes ranging from passive eavesdroppers to post-breach and quantum attackers. Against each, it demonstrates bounded, verifiable containment:

- **Two-Factor Integrity:** Access requires both possession of the card and knowledge of the passphrase; loss of either factor yields no exploitable material.
- **Forward Secrecy:** Each session burns its key leaf, producing **information-theoretic erasure** of prior secrets.

- **Replay & Rollback Resistance:** The synchronized monotonic counter between card and server detects any cloned or stale tokens before KDF execution.
- **Quantum Resistance:** All long-lived values derive from SHAKE-256 and SCB, free from lattice or code-based assumptions.
- **Offline Verifiability:** Time validity and index synchronization prevent credential reuse even when disconnected from any network.

Cryptanalytic review confirms that **no shortcut attacks** exist against the underlying sponge functions, and SCB's 64 MiB memory wall renders brute-force infeasible under modern GPU economics. The only non-recoverable compromise path; loss of a server's Kbase, is contained within its host scope, never propagating cross-domain.

5. Implementation and Integration

A complete SIAP stack fits within **28 kB of code and 5 kB of RAM**, executing a full login cycle in approximately **10 ms** on a 100 MHz Cortex-M4.

Integration requires minimal modification to host systems:

- **PAM/SSH Plug-ins** for administrative logins and jump-host access.
- **Proxy-Side PSK Injection** into existing TLS 1.3 or QUIC binders.
- **UART/Bootloader Hooks** for firmware unlock or device provisioning.
- **Secure-Element and JavaCard Profiles** for payment and transit cards.

The **server footprint** is one HSM-stored key (Kbase) and a simple identity table (Ude). SIAP thus replaces certificate servers, OCSP responders, and renewal workflows with a single deterministic derivation function.

6. Use Cases and Applications

SIAP's flexibility enables consistent deployment across industries and threat environments:

PCI-DSS 4.0 Jump-Hosts:
Two-factor administrative access without PKI; compliant with independent MFA clauses.

Offline CBDC Wallets:

Low-cost hardware tokens enabling week-long offline transactions for national digital currencies.

Technician Tokens (ATM / PLC):
Secure field access with auto-destruct after failed passphrase attempts.

Cold-Wallet Custody:
Quantum-safe signing workflows using one-time leaves for withdrawal authorization.

OEM Firmware Unlock:
On-line production control enforcing one-device-per-key activation.

TLS/IKE PSK Refresh:
Drop-in ephemeral key injection for post-quantum tunnel hardening.

High-Frequency Trading APIs:
Microsecond-scale key derivation for sub-millisecond authentication.

SCADA / HMI Kiosks:
Fully offline operation with multi-decade token lifetimes.

Each case demonstrates SIAP's capability to **replace brittle certificate infrastructures** while maintaining real-time performance and regulatory alignment.

7. Economic and Operational Value

By eliminating certificates, OCSP traffic, and asymmetric handshakes, SIAP provides immediate and measurable cost reductions:

- **Code Footprint:** 10× smaller than lattice or ECC-based systems.
- **Energy Consumption:** 15× lower login energy (0.012 mWh vs. 0.17 mWh FIDO2).
- **OPEX Reduction:** Up to **US $18 million** savings per million tokens over ten years in avoided certificate maintenance.
- **Compliance Efficiency:** Automatic audit trails satisfy PCI-DSS, SOX 404, and PSD2 without added logging frameworks.

For acquirers, SIAP represents a **commercially ready IP block**, drop-in compatible with the existing QRCS cryptographic stack (SCB, SHAKE, RCS), and suitable for rapid licensing into secure-element, banking, or government products.

8. Long-Term Security Benefit

SIAP's broader impact lies in democratizing **quantum-resilient access control**. By reducing dependence on PKI, it allows both developed and emerging regions to maintain secure digital operations even under limited network or regulatory infrastructure.

Its simplicity; deriving all security from symmetric primitives, makes it auditable, open to formal verification, and maintainable for decades. The same qualities that make it deployable in a bank's HSM can secure the firmware of a wind turbine, or enable a doctor to unlock encrypted health records offline during disaster recovery.

SIAP thus exemplifies **sustainable cryptographic engineering:** energy-efficient, hardware-portable, and independent of volatile standardization timelines.

9. Conclusion

The Secure Infrastructure Access Protocol delivers a decisive evolution in authentication architecture: **a post-quantum-ready, certificate-free, forward-secret system** designed for universal adoption. Its combination of a physical memory token, passphrase-derived key, and single-use leaf burn provides zero-standing-privilege security that rivals or exceeds contemporary asymmetric schemes.

With verifiable mathematical foundations, minimal integration cost, and proven real-world use across fintech, industrial, and embedded sectors, SIAP stands as both a **technological and strategic asset**. It extends QRCS's ecosystem of post-quantum protocols by anchoring authentication in immutable cryptographic primitives, offering investors and acquirers a platform whose simplicity, scalability, and defensibility define the next generation of infrastructure security.

Prepared by: Quantum-Resistant Cryptographic Solutions
Contact: contact@qrcscorp.ca