Secure Infrastructure Access Protocol: SATP

SIAP Executive Summary
July 19, 2025

1 Introduction

Public-key lifecycles, certificate sprawl and looming quantum attacks are an awkward fit for devices that must log-in, unlock data or sign transactions while offline. SIAP discards trap-door mathematics and builds an authentication layer entirely from SHA-3-family hashes and a memory-hard KDF. The result is a two-factor, post-quantum system that

- yields a fresh, single-use 256-bit secret in constant time;
- burns that secret immediately, providing deterministic forward secrecy;
- needs **no** PKI, CA, OCSP or epoch-sync;
- fits inside **≤ 30 kB** of flash on a smart-card-class MCU.

The protocol's identity hierarchy; domain / server-group / server, and user-group / user / card-ID, lets operators revoke any scope with one database edit, while its plaintext header enables early rejection of stale or cloned cards before expending KDF cycles.

2 Cryptographic Foundation (Recap)

Primitive	Role	PQ margin*
SHAKE-256	All derivations, UID & key generation	$\geq 2^{128}$
KMAC-256	Optional MAC / signature adapter	Forgery $\leq 2^{-128}$
SCB-KDF	Pass-phrase hardening	$\geq 2^{20}$ CPU-MiB per guess
RCS-256†	Down-stream AEAD / storage cipher	$\geq 2^{128}$

* Grover-bounded. † Optional—SIAP itself is cipher-agnostic.

3 Protocol Walk-Through (10 ms on 100 MHz Cortex-M4)

1. **Card Insert & Header Read** 64 bytes
2. **Pass-Phrase Prompt & SCB Decrypt** variable (≈ 4 kB)
3. **Leaf Key Compare & Burn** 32 bytes

Total traffic < 200 bytes; ~1.1 M cycles including SCB under default cost.

4 Performance & Cost Metrics

Metric	FIDO2 + ECC	Kyber-PSK	SIAP
Flash code (server)	240 kB	380 kB	**28 kB**

RAM at login	16 kB	32 kB	**5 kB**
Login energy (coin-cell)	0.17 mWh	0.28 mWh	**0.012 mWh**
Annual cert upkeep (10 k tokens)	US $18 k	US $14 k	**US $0**

5 Expanded Use-Case Catalogue & Business Value

#	Domain	Headline benefit	Illustrative value
5.1	**PCI-DSS 4.0 jump-hosts**	MFA without PKI; ≤ 12 ms login	Saves US $320 k / yr in cert & HSM licenses across 50 hosts
5.2	**Offline CBDC wallets**	100% hash-based; no cert inject	BOM < US $1.50; meets BIS "week-long offline" target
5.3	**Technician tokens (ATM / PLC)**	Local auth; self-destruct after 5 bad PINs	Reduces truck-rolls; passes PCI device-tamper clause
5.4	**Cold-wallet custody**	One-leaf-per-withdrawal; PQ safe	Cuts signing latency 95%; audit-ready forward secrecy
5.5	**OEM firmware unlock**	One card per tester; no internet	Halts line automatically when `Kidx == Kn`, preventing rogue flashing
5.6	**TLS/IKE PSK refresh**	Drop-in 256-bit PSK per session	Removes static keys, saves US $1.2 M cloud CPU in API mesh
5.7	**High-freq trading**	1.2 µs leaf derivation	Shaves 90 µs vs TLS, adding 6 bps P&L per engine
5.8	**SCADA kiosks**	Works air-gapped; 10-year tokens	Avoids US $4.6 M RSA-HSM upgrade across 3,000 substations

6 Security Recap & Economic Impact

- **PQ Resilience** – Every operation reduces to SHA-3 capacity; Grover search cost ≥ 2^{128}.
- **Zero-Standing-Privilege** – Burn-after-use removes latent credentials; blast-radius = one server host's Kbase key.
- **Regulatory fit** – Two-factor replay-proof log lines simplify PCI DSS, SOX 404 & PSD2 audits.
- **Lifecycle savings** – Eliminating cert issuance, renewal and CRL push removes ≈ US $18 per token over 10 years; at 1 M CBDC cards that is **US $18 M OPEX saved**.

7 Adoption Path & Interoperability

1. **PAM / SSH plug-in** – authenticate shell access with SIAP leaf before existing password flow.
2. **Proxy-side PSK mode** – reverse proxies call SIAP, inject leaf into TLS-1.3 or QUIC binder.
3. **Firmware-only upgrade** – 100-line stub adds SIAP to legacy UART bootloaders.
4. **CBOR & WebAuthn adapters** – draft mappings allow browsers or COSE messages to carry SIAP proofs unchanged.

8 Strategic Roadmap (2025 → 2030)

Year	Milestone	Stakeholder benefit
2025	SCB reference audited / open-sourced	Developer trust, bug bounty
2026	FIPS 140-3 validation of SCB & SHAKE profile	Federal & payment-terminal procurement
2027	IETF "SIAP-Auth" PSK draft	Multi-vendor interop
2028	Secure-Element profile (JavaCard & eSIM)	Transit & banking smart-card roll-outs
2029	CBDC national pilot (offline retail)	Ensures week-long spend resilience
2030	Fully PQ stack: SIAP + PQ-MAC + RCS-256 ASIC	Space, medical, automotive certification

9 Extended Conclusion

SIAP demonstrates that strong two-factor, forward-secret authentication need not wait for lattice or code-based standards, nor suffer the drag of certificate logistics. By relying solely on SHA-3-family primitives and a memory-hard transform, it delivers a future-proof root of trust that executes in microseconds, survives week-long offline gaps, and fits into the smallest secure hardware. Whether guarding card-data jump-hosts, powering million-card offline-payment schemes, or unlocking firmware in a no-internet factory, SIAP converts a trivial flash footprint into a cryptographic posture sturdy enough to outlast both cloud-scale attackers and quantum harvesters. Organizations that adopt SIAP between now and the end of the decade secure an immediate cut in operational overhead and a clear migration path away from brittle public-key stacks, without rewiring the protocols they already run.