Blockchain Governance Initiative Network

Wallet Security Assurance: ST/PP and Convergence

BGIN – Julien Bringer & Shin'ichiro Matsuo

Global Digital Collaboration | Geneva | 2–3 September 2026

Wallet Security Assurance: ST/PP and Convergence

Toward Implementable, Interoperable, and Trustworthy Digital Asset Wallets. Needs from digital assets ecosystem & opportunities from and for digital ID ecosystem.

Co-organizers

ISO, Blockchain Group: BGIN, Blockchain Bundesverband e.V, Ethereum Climate Platform, LNet, Linux Foundation Group: OpenWallet, Trust Over IP, LF Decentralized Trust

Real-World Security Failures

The Cost of No Agreed Security Baseline...

- **Coldcard RNG flaw (recent):** Weak random number generation compromised key security — a known threat category
- **Slope/Solana wallet breach (2022):** Private key exposure via insecure seed phrase handling
- **Profanity vanity address generator (2022):** Flawed RNG → ∼$160M losses
- **BitcoinJS weak keys (CRYPTO-1 / 2023):** Entropy weakness in early JS wallet libraries

Pattern: RNG weaknesses, insecure key storage, absent attestation, no isolation guarantees → all addressable by ST/PP requirements 🔗 **Takeaway:** These are not exotic attacks — they are textbook threats that CC/CSPN evaluation would flag.

COLDCARD — Overview

A firmware bug left the hardware entropy path unused. Seeds generated on that path were guessable. This is not a break of secp256k1.

- COLDCARD is Coinkite's air-gapped Bitcoin hardware-wallet family.
- Some firmware releases generated seeds from a weak software PRNG. The hardware noise source was present; the seed path did not use it.
- Without extra user entropy — dice rolls or a strong passphrase — those seeds were attackable.
- The defect was widely publicized in late July 2026. Attackers then harvested wallets whose seeds had been generated on that path.

🔗 **Takeaway:** Users often assumed "hardware wallet" meant strong seed randomness. The sold product had left the randomness assumption that proofs rely on.

COLDCARD — Lessons

Chip entropy, open source, and a hardware form factor did not make the seed path evaluateable.

1. Entropy hardware is not entropy used. The firmware path is part of the TCB.
2. A chip certificate is not a product certificate. Users buy the whole device.
3. Published source is not a lab substitute. A fatal seed-RNG bug can sit in the open if that path is never tested.
4. Human ceremonies — dice rolls, passphrases, air-gap discipline — help, but they are unevenly practiced.
5. Shared ST/PP requirements make RNG, firmware, and update claims comparable before the next incident.

Takeaway: A wallet PP must test that the seed path actually consumes hardware entropy — not that a TRNG exists on the board.

Existing Frameworks — Rich but Fragmented

Domain	Framework	Scope	Gap for Wallets
Smart cards / HSMs	Common Criteria (CC), SSCD/QSCD PP	Hardware key protection	Not wallet-application aware
Consumer devices	FIDO Alliance (FIDO2, UAF)	Authentication	No asset/key custody scope
Mobile/TEE	GlobalPlatform TEE PP	Trusted execution	Limited to TEE boundary
Identity	OpenID4VP/VCI, EUDI Wallet	Credential issuance/ presentation	Certification schemes nascent
Financial	PCI-HSM, FIPS 140-3	Crypto modules	Cloud/enterprise focus
Hardware wallets	ANSSI CSPN (Ledger Nano S/X/S+)	Embedded HW+SW	Vendor-specific, not generalized

Learning from Certified Wallet Examples

A few examples from Ledger:

- Ledger Nano S — ANSSI-CSPN-2019-03 (first certified personal crypto wallet)
- Ledger Nano S Plus — ANSSI-CSPN-2023-13 (renewed, with Quarkslab evaluation)
- Ledger Nano X — ANSSI-CSPN-2019-12 / 2023-17

Learning from Certified Wallet Examples

- SF1 — True Random Number Generator
- SF2 — Attestation Mechanism
- SF3 — End-User Verification
- SF4 — Post-Issuance Capability over Secure Channel
- SF5 — App Isolation

BGIN's discussions: extract the pattern, extend it, and make it reusable for the ecosystem
🔗 **Takeaway:** Also note: SSCD/QSCD PPs offer reusable material for key generation, storage and lifecycle — adaptable for both SE-based wallets and server-side HSMs.

BGIN — What We Are Working on

- Use case vs threat models mapping
- Protection profiles
- Type of ToEs (HW, SW, TEE-based, HSM...)
- Possibly different PP profiles — for instance:

PP-NonCustodial

Hardware wallets, mobile wallets (self-sovereign key)

PP-Custodial

Exchange wallets, enterprise custody (HSM-backed)

PP-MPC/Threshold

Distributed key schemes, threshold signatures

From Web3 to Institutional Custody

Assurance Level	Use Cases	Key Threats	Example Controls
L1 — Basic	Web3 dApps, small wallets, NFTs	Phishing, malware, weak RNG	SW best practices, PRNG quality, basic isolation
L2 — Substantial	DeFi (?), mid-value retail, …	Remote attacks, supply chain, key extraction	TEE, secure enclave, SE, app isolation, attestation
L3 — High	Institutional custody, regulated assets, QSCD, strong self-custody	Physical attacks, side-channel, insider threat	Certified HSM/SE, FIPS 140-3 L3+, CC EAL4+, MPC

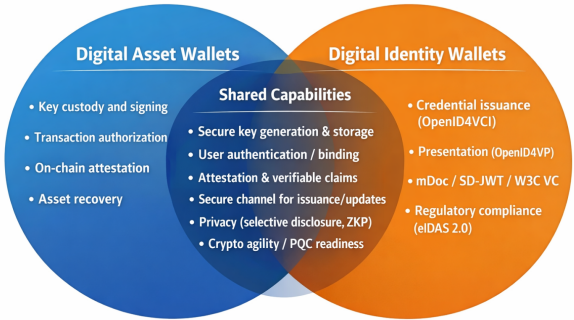
Open question for Block #15: Which use cases and levels will BGIN prioritize first?

Core Threats the PP Must Address?

- T.RNG — Weak/biased random number generation → key compromise (Coldcard, Profanity)
- T.KEYSTORE — Insecure key storage, extraction by malware or physical access
- T.ISOLATION — Lack of app/process isolation → cross-contamination
- T.SUPPLY — Supply chain attacks on hardware/firmware
- T.REMOTE — Remote exploitation via malicious transactions, RPC endpoints
- T.ACCESS — Insufficient user authentication, no lockout
- T.UPDATE — Insecure firmware update → persistent compromise
- T.SIDE_CHANNEL — Power/EM/timing leakage (relevant for L3)
- T.ATTESTATION — Inability to verify device/software authenticity
- T.PQC — Future: quantum-capable adversary breaking current crypto

MPC-specific:
T.THRESHOLD — Quorum collusion, share reconstruction attacks, insecure communication between nodes

ID Wallets and Crypto Wallets — Converging Security Needs



Avoid duplicating; maximize reuse

Convergence Map: Frameworks and Gaps

GIN PP Requirement	SSCD/QSCD	GlobalPlatform TEE	FIPS 140-3	EUDI Cert. Scheme
RNG quality	✅ (AIS20/31)	✅	✅	🔲 TBD
Key isolation	✅	✅	✅	🔲 TBD
Attestation	✅	✅		✅
User verification	⚠️	⚠️		✅
Secure update	✅ life cycle mngt	✅ OTA	⚠️ emerging	✅
MPC / threshold			⚠️	
Blind signing protection	⚠️ partial			
Zero-Knowledge Proofs (ZKP)				⚠️ emerging
Selective disclosure				✅
DLT-specific	❌	❌	❌	❌

Building Wallets Ready for the Post-Quantum Transition

- Secp256k1 (Bitcoin/Ethereum) and Ed25519
- Long-lived keys (HD wallets, institutional custody) are at greatest risk
- "Harvest now, decrypt later" threat is real for on-chain public keys

Requirements for PQC-ready wallets:

- Crypto agility: architecture must support algorithm substitution without full redesign
- Secure update channel is the enabler — firmware must be updateable to swap in PQC algorithms
- Hybrid schemes during transition (classical + PQC)
- NIST PQC standards as target algorithms

ZKP intersection: Post-quantum ZKP schemes (e.g., STARK-based, lattice-based) relevant for privacy-preserving wallets. Trust Registries and Trusted Lists will need to accommodate PQC-signed credentials. **Takeaway:** BGIN action: PP should include PQC crypto agility as a security objective from the start, not a retrofit

Should We Develop Reference Designs?

- **Non-Custodial Hardware Wallet.** Secure Element (CC EAL5+) for key storage; Verified boot + app isolation (GP TEE model); Display/button confirmation (out-of-band auth). Building on: SSCD PP, Ledger CSPN model
- **Non-Custodial Software Wallet (Mobile).** TEE/StrongBox for key protection; FIDO2 for user binding; Remote attestation for app integrity. Building on: GP TEE PP, FIDO UAF, Android/iOS secure enclave specs
- **Custodial / Institutional Wallet.** HSM backend (FIPS 140-3 L3 / CC EAL4+); MPC/Threshold for key ceremony and signing quorum; Audit log and accountability (Accountable Wallet). Building on: PKCS#11, FIPS 140-3, standards for cloud HSM

🔗 **Takeaway:** Some common elements across all three: RNG validation (AIS 20/31 equivalent); Secure channel for updates; Attestation mechanism

BGIN Roadmap: From Block #14 to Block #15 and Beyond

Block #14 (Done) ——————▶ Block #15 (Oct 2025)

Use case inventory started
LoA framework discussed
Framework mapping initiated
explored
Ledger / SSCD reference reviewed

Finalize LoA tiers
Draft PP outline
ID wallet alignment

Decisions needed at Block #15:

- Which use cases and LoA tiers to prioritize?
- Which PP profile to draft first (non-custodial hardware? mobile software?)
- MPC/threshold: in scope for first deliverable?

Stakeholders

Stakeholder	Contribution to BGIN PP Work	What They Get
Wallet vendors (HW/SW)	Input on implementation constraints, threat experience	PP-compliant design guidance, market differentiation
Evaluation labs	Methodology input, pilot evaluations	New evaluation workstream, early engagement
Financial regulators	Use case requirements, acceptance criteria	Assessable wallets for regulated contexts
eID regulators	Alignment on identity wallet overlap, national scheme input	Reduced duplication, faster scheme development
Digital Identity Wallet ecosystems (OpenID, OWF, ToIP, LFDCT)	Technical requirements from credential lifecycle, selective disclosure, ZKP, trust registries	Shared PP foundations, interoperability across DLT and ID wallet stacks
FIDO / GlobalPlatform communities	Framework input, mutual recognition discussions	Wallet extension of existing schemes
Developers / Open Source	Reference implementation feedback	Best practice guidance, L1 baseline

Summary

- **The gap is real and exploited** — RNG failures, key exposure, lack of isolation are happening now. A common PP would have helped prevent them.
- **Frameworks exist but are fragmented** — BGIN ST/PP work connects the dots across CC, FIDO, GP, FIPS, and the emerging EUDI certification landscape.
- **Tiered assurance is the right model** — From L1 (basic web3 wallet) to L3 (institutional custody), one size does not fit all.
- **PQC and crypto agility must be built in now** — Secure update channels and algorithm agility are not optional features; they are security objectives.
- **Convergence is an opportunity** — Digital asset wallets and digital identity wallets share core security needs. BGIN can help avoid duplication and accelerate trust.

🔗 **Takeaway:** Next step: Join the follow-up call / Block #15 to decide use case priorities and kick off the PP drafting process.

Why a Copy-Paste PP Will Not Evaluate This Stack

A working frame for this breakout

Blockchain Governance Initiative Network

Shin'ichiro Matsuo, Ph.D.

BGIN Co-Chair | Breakout: Wallet Security Assurance: ST/PP

Global Digital Collaboration | Geneva | 2–3 September 2026

Discussion starter

The writing problem is not a missing algorithm

CC, FIDO, GlobalPlatform TEE, FIPS, and CSPN already exist. Julien's map is the starting inventory. The BGIN job is not a rival scheme.

For DLT and wallet stacks, writing an ST/PP that a lab can actually run is hard for three stacked reasons:

Non-standard crypto

Many primitives sit outside the classical "standard crypto" lists that existing PPs assume.

Continuous novelty

New techniques appear continuously. A frozen profile goes stale before the first evaluation finishes.

Heavy customization

Deployments are customized. Profiles must stay evaluate-able without freezing innovation.

🔗 **Takeaway:** Do not fork CC, FIDO, GlobalPlatform, or OpenID. Reuse what already evaluates; write only the wallet/DLT gap — including PQC agility as an objective, not a retrofit.

Questions for this room

This 50-minute breakout is for mapping gaps and naming what Block #15 must decide — not for locking a first PP tonight.

1. Where do CC, FIDO, GlobalPlatform, OpenID, and EUDI **already cover** wallet ToEs, and where is the honest gap (DLT-specific, MPC, blind signing, customization)?
2. Which **LoA tier** and which **PP profile** (non-custodial hardware, mobile software, custodial/HSM) should BGIN draft first?
3. What must **evaluation labs** see for custodial vs. non-custodial stacks when the crypto is non-standard and the deployment is customized?
4. How should ST/PP stay evaluate-able as algorithms and wallet designs move — including the **PQC update path** Julien set as a security objective?

Join us at BGIN Block 15

15–16 October 2026 | Georgetown University, Washington, D.C. | In person (remote available). The ST/PP drafting decisions listed above continue in the Block 15 working session.

Related sessions

- 16 Oct, 15:40–17:10 (Room B). Cyber: Security Target & Protection Profile (ST/PP)
- 16 Oct, 14:00–14:45 (Room B). Cyber + IKP: Offline Key Management
- 15 Oct, 11:30–13:00 (Room A). Cyber: Governance of the Security Supply Chain

ST/PP session
bgin-global.org/.../sessions/2-10

Block 15 site
bgin-global.org/events/20261015-block15

Register
eventbrite.com/.../bgin-block15-tickets

Takeaway: Hybrid. Connection details are sent after registration. You are invited.