GDC 2026 — Meeting Report

Wallet Security Assurance: ST/PP and Convergence

Blockchain Governance Initiative Network (BGIN)
Cyber Security

3 September 2026 | 15:00–15:50 | Geneva

This record is written under the Chatham House Rule. Information may be used; other participants are not identified.

Agenda

- Opening: BGIN; ST/PP for crypto and digital-asset wallets; exchange with the digital-identity community.
- Scene-setting: key-management failures; RNG, storage, attestation, isolation, blind signing; Coldcard and Slope/Solana examples.
- Existing frameworks: Common Criteria, SSCD/QSCD, FIDO, GlobalPlatform TEE, FIPS/PCI, CSPN.
- Working frame: use cases, ToEs, and tiered PPs (non-custodial, custodial, MPC/threshold); threat mapping including PQC.
- Convergence: shared needs with ID wallets versus crypto-specific signing, smart-contract authorization, and ZK.
- Open discussion: startup-workable schemes; QSCD/WSCA; EUDI/SC 27; legal mandates; AI-driven threats.
- Close: BGIN Block 15 (Washington, D.C., October 2026); hybrid.

Session Description

Trustworthy digital-asset wallets need implementation-level security assurance, yet there is still no widely recognized protection profile for crypto wallets. Vendors who want a certified product must write their own security target. Existing schemes—Common Criteria, secure elements, HSMs, SSCD/QSCD, GlobalPlatform TEE, FIDO, FIPS, and emerging EUDI certification—are necessary building blocks, but they do not yet cover DLT-specific cryptography, blind signing of non-trivial transactions, MPC/threshold custody, or the mix of retail and institutional ToEs.

This 50-minute breakout treated wallet assurance as a gap-mapping and convergence problem, not as a rival certification scheme. It built on BGIN's Security Target / Protection Profile

work for DLT and wallet stacks, public incident patterns, and one vendor's CSPN-certified hardware-wallet security functions as a reusable starting pattern. The room was asked what is missing for identity and blockchain wallets, how a new framework can remain workable for small startups, and which use cases and assurance levels to take first, with follow-on drafting at BGIN Block 15.

Speakers

The session was conducted under the Chatham House Rule. Floor interventions may be used; neither the identity nor the affiliation of other participants is recorded here.

Speaker: Julien Bringer (BGIN Cyber Security). Presentation on failures, existing frameworks, certified-wallet security functions, use-case PPs, threats, and ID/crypto convergence; followed by a discussion starter on gaps and on making assurance workable beyond a copy-paste of heavy ISO/Common Criteria practice.

Floor discussion included QSCD / signature-activation and WSCA/WSCD architecture splits, EUDI and EUCC protection-profile work, ISO/IEC JTC 1/SC 27 and CEN/TC 224, legal requirements written into identity-wallet law, architecture-agnostic versus architecture-specific profiles, and AI-assisted building and AI-driven attacks.

Slides

Session slides were presented from a BGIN Beamer deck combining the scene-setting frames (real-world failures; Coldcard lessons; certified-wallet examples and ST security functions; use-case PPs and ToEs; core threats; ID/crypto mapping; PQC agility; candidate reference designs), discussion questions, and a Block 15 call with session, event, and registration links.
Session slides (PDF): https://bgin-global.org/documents/meeting-reports/gdc26/GDC26_Wallet_Security_Assurance_STPP_Slides.pdf

Notes & Key Points

The gap is already exploited. Digital-asset wallets have seen repeated failures around key generation, key storage, and transaction consent. Named patterns included weak or unused RNG (including firmware that sat on a certified secure-element RNG but did not consume it), seed material held on a backend, weak entropy in JavaScript wallet stacks, missing firmware/software attestation, missing isolation between apps on the same hardware, and blind signing—authorizing a transaction without a faithful account of what will execute, including non-trivial smart-contract calls. The takeaway was not that hardware is useless, but that a chip certificate is not a product certificate: users buy the integrated path, and that path is what has to be evaluated.

Coldcard as a cautionary ToE. A hardware wallet with a secure element and a certified RNG still generated weak seeds when firmware left the hardware entropy path unused. Extra user ceremonies (dice rolls, passphrases) do not repair a broken default path if they are optional and unevenly practiced. A wallet protection profile would have to test that the seed path actually consumes trusted entropy, not merely that a TRNG exists on the board.

Existing frameworks are inventory, not a finished crypto-wallet PP. Decades of smart-card and HSM evaluation (payment, e-passports), Common Criteria, SSCD/QSCD profiles for key generation, storage, lifecycle and signature consent, FIDO-style user presence, GlobalPlatform TEE protection profiles, FIPS, and PCI were presented as reusable material. Using a TEE, a secure element, or an HSM is not enough if part of the execution, key generation, or update path sits outside the evaluated boundary. The Target of Evaluation has to be drawn consistently with the claim.

One public existence proof, not a global PP. A hardware-wallet vendor defined security targets under the French CSPN scheme (Ledger Nano S from 2019, with later Nano S Plus and Nano X iterations). Functions in the ST included a true random number generator, attestation of firmware/software, end-user verification, post-issuance capability over a secure channel (remote update), and app isolation so third-party apps cannot observe or contaminate official chain apps. BGIN's proposed move is to extract that pattern, extend it for crypto-specific threats, and make it reusable as a common protection profile rather than leaving every vendor to write a one-off ST.

Use cases, ToEs, and assurance levels will not collapse into one profile. Custodial wallets (exchanges, enterprise custody; often HSM or confidential computing) differ from self-custodial hardware and mobile wallets. MPC and threshold cryptography are in production and largely without certification references for their security functions and protocols. Retail Web3 interaction and institutional custody were expected to share some functions (strong RNG) but not the same end-to-end functions or the same evaluation rigor. Candidate PP families discussed were non-custodial, custodial, and MPC/threshold. An open sequencing question was whether to start with retail wallets or with custodians.

Threats the PP must name. Weak RNG; insecure keystore; cross-app contamination; supply-chain attacks on hardware and firmware together; remote exploitation; insufficient user authentication; insecure update; side channels at higher assurance; attestation failure; post-quantum break of long-lived keys; and threshold-specific failures (quorum collusion, share reconstruction, insecure node communication). Crypto agility and a secure update channel were treated as core security functions for PQC transition, not later features. Advanced zero-knowledge constructions used in blockchain stacks sit outside many currently approved cryptographic catalogues.

Commonalities with ID wallets, and the honest remainder. Secure key generation and storage, user authentication and binding, attestation, verifiable claims, privacy, PQC, and crypto agility appear on both sides, often under different names. Crypto-wallet specificities include chain-specific signing algorithms, authorization of programmable transactions, and more complex ZK usage. Reference designs (SE-based hardware; TEE/mobile; HSM/MPC custodial) were offered as a way to stress-test a profile against realistic ToEs, with some common elements across all three: RNG validation, a secure update channel, and attestation.

Workable for small startups. Common Criteria / ISO 15408-class evaluation was described as too heavy for most blockchain wallet teams, which are small. A scheme that only large

vendors can complete will not be followed. Alignment with existing certified components was presented as the practical path: ask secure-element, TEE, and HSM providers for minimal deltas (for example one additional key-generation method or crypto scheme) so integrators can reuse already-certified products rather than forcing a full custom ST on every startup.

Architecture split, not a single hardware box. From the floor, electronic-signature practice already splits a QSCD (hardware) from a signature-activation module that may sit inside or outside that hardware; EUDI-style wallets similarly split a wallet secure cryptographic device from a wallet secure cryptographic application, including mixed mobile-plus-HSM deployments. The same split was urged for crypto wallets, especially mobile security with an HSM backend: hardware assurance and application/activation assurance are different evaluation problems.

Standards landscape. It was stated that ISO/IEC JTC 1/SC 27 does not currently have a protection profile or certification methodology dedicated to crypto wallets. European identity-wallet work (including CEN/TC 224 WG20 on the EUDI wallet, EUCC protection profiles, and QSCD / remote-signing work) is active but not a crypto-wallet project. Relationship to that work was framed as reuse: talk to the same component vendors, add only what crypto wallets need, and keep the extra effort small because crypto-wallet certification is not yet mandated at EUDI-like legal granularity.

Law is a motivator on the ID side, not yet a substitute PP on the crypto side. EUDI wallets carry legal requirements on high assurance, revocation, wallet-instance and key attestation, and registration/access certificates. Crypto-wallet protection profiles do not exist, so those legal requirements are not "already covered." Custody regulation may demand an appropriate security level without yet specifying certification. The job was still described as serving wallet providers and users first; usefulness for the Cyber Resilience Act was noted as a possible connection, not the design centre.

High-level profiles, many architectures. Identity-wallet requirements were described from the floor as needing to fit internal or external secure elements and HSMs, with WSCA/WSCD certification (including debate around EAL4+ / AVA_VAN.5-class levels) and key attestation still waiting on further ENISA clarity. The crypto-wallet side made the same claim: the PP cannot be tied to one implementation; high-level component architectures, including web wallets, have to remain in scope.

AI as a missing assurance surface. From a builder's standpoint, systems are increasingly built with AI, and recent attacks were characterized as AI-driven. A pragmatic framework would be helped by agentic harnesses that encode agreed requirements into checkable systems. The certification community was said to be still discussing how to give assurance about AI behaviour and how to anticipate AI-driven threats; additional research on AI in risk management was treated as needed before the topic is ready to lock into a PP.

BGIN's role between the wild and ISO. Block meetings are open. Stakeholders sought included wallet vendors, evaluation labs, financial and eID regulators, identity-wallet communities, and experts from FIDO / GlobalPlatform-class efforts that have already adapted existing

PPs. BGIN already holds a Category A liaison with ISO/TC 307 and is starting the same process with ISO/IEC JTC 1/SC 27, with the intent that a BGIN ST/PP deliverable can later move into the ISO document pipeline (including a PAS-style path). The reason given was that crypto wallets are often built by startups who are not in the ISO room; the intermediate community has to carry their input into a standard that labs can actually run.

Session outcomes

- A shared problem statement: there is no common protection profile for crypto wallets, so certification today means a vendor-specific security target; chip or component certificates do not evaluate the integrated seed, update, isolation, and consent path.
- A working inventory of reusable building blocks (Common Criteria, CSPN, SSCD/QSCD, GlobalPlatform TEE, FIDO, FIPS/PCI, EUDI/EUCC drafts) and an explicit non-goal: do not fork those schemes; write only the wallet/DLT gap.
- Candidate structure for BGIN ST/PP work: map use cases to threats; allow multiple ToEs and PPs (non-custodial, custodial, MPC/threshold); use tiered assurance; keep RNG, secure update, and attestation as common functions; treat PQC agility as an objective from the start.
- Distinctions the room actually used: hardware entropy present versus entropy used; QSCD/WSCD versus WSCA/activation software; legal high-assurance mandates for ID wallets versus not-yet-specified crypto-wallet certification; evaluate-able high-level architectures versus freezing one implementation.
- Floor constraint that a copy-paste of heavy Common Criteria practice will not be followed by small wallet startups; practical reuse of certified secure components, with minimal crypto-wallet deltas, is the adoption path.
- Confirmation that SC 27 has no crypto-wallet PP today, that CEN/TC 224 / EUCC identity-wallet work is adjacent rather than sufficient, and that CRA-facing usefulness is a possible later connection.
- Open research rather than a locked requirement: AI-assisted development and AI-driven attacks as an assurance surface, including agentic harnesses that encode agreed frameworks.
- A named continuation: BGIN Block 15 (15–16 October 2026, Washington, D.C.; hybrid), including Cyber: Security Target & Protection Profile (ST/PP) (16 October, 15:40–17:10).

Event: https://bgin-global.org/events/20261015-block15
Registration: https://www.eventbrite.com/e/bgin-block15-tickets-1990274282957
Session: https://bgin-global.org/events/20261015-block15/sessions/2-10