BGIN Block#12 Meeting Report

- BGIN is a multi-stakeholder discussion body / distributed think tank.

Development of ST/PP

bg in

blockchain
governance
initiative
network

The Global Network for Blockchain Stakeholders™

BGIN Block#12

Development of ST/PP

Date: Monday, March 3, 2025

Location: Tokyo, Japan

Duration: Approx. 90 minutes

Summary

Establishing standardized Security Targets (ST) and Protection Profiles (PP) for blockchain and applications utilizing cryptographic key management. Identify key assets and security requirements, develop standardized STs for various application types, and create reusable PPs. This framework will address key management challenges in decentralized systems, ensuring robust security for blockchain-enabled applications. The goal of this session is to gauge the level of interest in these topics and formally adopt them as work items.

- Security Considerations in Blockchain
    - Introduces a table outlining six security aspects for blockchain systems:
        - Cryptography (e.g., ECDSA, SHA, MD signatures).
        - Backbone protocols (P2P, consensus, marketplaces).
        - Application protocols (privacy, secure transactions).
        - Application logic (smart contract scripting languages).
        - Implementation (software/hardware vulnerabilities).
        - Operations (key management, audits).
    - Highlights existing standards: NIST and ISO for cryptography, ISO/IEC 29128 for protocols, ISO/IEC 15408 (Common Criteria) for implementation, ISO/IEC 27000 for operations.
- Focus on Implementation
    - Session narrows focus to implementation security, introducing Common Criteria (CC) as an international standard for IT product security evaluation.
    - CC features seven Evaluation Assurance Levels (EAL 1-7), with higher levels requiring more effort and cost:
        - EAL 1: Functional testing.
        - EAL 7: Formal verification.
    - CC provides design guidance, documentation, and development process evaluation, recognized by over 25 countries (e.g., USA, Japan).

- Protection Profiles and Security Targets
    - Explains PP and ST as key CC documents:
    - PP: Defines security requirements for a product category (e.g., Bitcoin wallet, HSM).
    - ST: Detailed specs for a specific product, including Target of Evaluation (TOE).
    - Example: PP for a microcontroller with cryptographic units, assessing vulnerabilities and data flow.
- Certification Process
    - Describes CC certification: Applicant submits product and evidence to a certification body; labs assess based on PP/ST; certification issued if qualified.
    - Compares to NIST's FIPS 140 (Cryptographic Module Validation Program), a similar U.S.-Canada framework with a certified product list.
- Discussion Proposal
    - Proposes three discussion questions:
        - Do we need a blockchain certification program? If yes, what criteria/methodologies?
        - Should we align with existing frameworks (e.g., CC) or create a new one?
        - Suggests starting with PP/ST development, identifying use cases first.
        - Reflects on 7 years of advocating for this since 2018, urging action.
- Discussion and Q&A
    - Q1: Role of BGIN (Blockchain Governance Initiative Network)?
        - Speaker sees BEGIN creating industry-specific PP/ST for CC evaluation, not a new program or lab.
        - Example: Devices with EAL 6+ exist, but PP/ST details are unclear, necessitating blockchain-specific standards.
    - Q2: International applicability of CC?
        - CC is an ISO standard, not U.S.-centric, but not all countries adopt it due to government focus vs. global blockchain needs.
        - Alternative models (e.g., SOC 2) suggested: BEGIN sets standards, auditors verify.
    - Challenges and Alternatives
        - CC/CMVP processes are costly and heavy, potentially burdensome for startups.

        - Alternatives: Tweak existing frameworks or create a lighter blockchain-specific one, balancing cost and confidence.
        - Debate: Should startups moving funds be exempt from security standards? Speaker agrees they must manage risks.

    - BGIN's Role and Scope
        - Debate on BGIN's role: Verify certified companies (top-down) or create standards to incentivize certification (bottom-up)?
        - Suggestion: On-chain list of certified entities.
        - Comparison to C4's CCSS (key management standard): BEGIN should avoid overlap, focus on unique gaps (e.g., implementation, application logic).

    - Existing Standards
        - GBA (Government Blockchain Association) offers a maturity model for blockchain products, covering broader aspects (performance, confidentiality).
        - Request GBA link for reference, emphasizing startups' resource constraints.
        - Emerging standards: Coinbase-led group, Norse staking, tokenization frameworks, ISO TC307.

    - Prioritization and Value
        - No priority among security aspects (cryptography proven, focus on implementation/logic/operations) due to weakest-link risks.
        - Certification must be self-funding, value-driven (not cheap), offering market advantage.
        - Potential demand: Certified wallets could be recommended globally.

    - Startup Methodology
        - Startups could use PP as a checklist, while larger firms pursue certification.
        - Tiered pricing suggested for startups vs. corporations, though CC certification is external.

    - Structural Options
        - BEGIN could set standards and spin off a certification entity, maintaining independence (e.g., C4 model: auditors certify, C4 lists).
        - Debate: Focus on PP/ST only or expand to certification? Resource constraints favor the former initially.
        - BEGIN should map gaps, avoid redundancy, leverage existing work.

    - Market Fit and Stakeholders

        - Must define: What to certify (gap not covered by CCSS, e.g., implementation beyond key management)? Who benefits (insurers, VCs, regulators, consumers)?
        - CCSS success tied to marketing and insurance recognition; BEGIN needs similar strategy.
        - Naming/shaming bad actors risky; better to integrate into rating systems.

- Next Steps
    - Consensus: No strong opposition to developing standards; scope needs narrowing.
    - Proposal: Research gaps, map existing standards (e.g., PCI DSS stakeholder model), prioritize use cases.
    - Volunteers needed for research; NIST/NSA experts may contribute later.
    - Offline discussion via BEGIN's cybersecurity group recommended.

- Suggestions
    - Build a prototype to test standards (e.g., secure Web3 app), working backwards from gaps.
    - On-chain registry of standards/certifications could enhance global access, distinguishing BEGIN.
    - Matrix proposed: Technological (security) vs. Management (transparency, governance, validation) aspects.

- Conclusion
    - Agreement to analyze gaps, define scope, and assess feasibility.
    - Emphasis on value, global reach, and avoiding duplication; no final scope set yet.