

STABLENOTES V1 WHITEPAPER

v 3.0.1

Owner-Bound Offline Transaction Authorization for Stablecoins and Tokenized Assets

By Alex Breton
alex.breton@printdreams.com

2024-2026 © Stablenotes™ is an EU-registered trademark of PrintDreams International AB - Reproduction of this document, or any part thereof, is prohibited without written permission.

Legal Disclaimer

This Whitepaper (including any appendices, exhibits, linked materials, updates, and revisions, the "Whitepaper") is provided by PrintDreams International AB and/or its affiliates ("PrintDreams," "we," "us," or "our") solely for informational and discussion purposes in relation to Stablenotes v1 and related software development kits (SDKs), reference implementations, and associated devices and media (collectively, the "Technology"). This Whitepaper is not intended to constitute, and does not constitute legal, tax, accounting, financial, or investment advice. You should obtain independent professional advice before acting on the basis of this Whitepaper.

No offer or solicitation; EU financial promotion and prospectus disclaimer

This Whitepaper does not constitute, and shall not be construed as, an offer to sell or a solicitation of an offer to buy any securities, transferable securities, financial instruments, crypto-assets, tokens, derivatives, or investment products in any jurisdiction, including within the European Economic Area ("EEA"). No prospectus has been approved or will be approved for the purposes of Regulation (EU) 2017/1129 (the "Prospectus Regulation") in connection with this Whitepaper, and no such prospectus is intended to be published. Any offer or distribution, if ever made, would be made only pursuant to definitive documentation and in compliance with applicable laws and regulatory requirements.

MiCA / CASP disclaimer; Technology is not a regulated crypto-asset service

Nothing in this Whitepaper is intended to constitute an offer to the public of crypto-assets, an admission to trading of crypto-assets, or the provision of crypto-asset services within the meaning of Regulation (EU) 2023/1114 (Markets in Crypto-Assets Regulation, "MiCA"). PrintDreams does not, by publishing this Whitepaper or providing the Technology, represent that it is authorized as a crypto-asset service provider ("CASP") or that the Technology is offered as a regulated crypto-asset service. Any references to blockchain networks, crypto-assets, stablecoins, wallets, or smart contracts are for technical description only.

Self-custody; no custody or control of user crypto-assets

Stablenotes v1 is designed as a self-custodial technology. Users are solely responsible for safeguarding their private keys, transaction authorization materials, devices, and credentials. PrintDreams does not take custody of, control, access, or manage user crypto-assets, private keys, or wallets and cannot recover lost keys or reverse blockchain transactions. Blockchain transactions are generally irreversible. Loss, theft, damage, compromise, or unavailability of private keys or transaction authorization materials may result in permanent loss of crypto-assets.

Third-party services (including regulated providers)

The Technology may be used in conjunction with third-party products and services, including but not limited to blockchain networks, wallets, smart contracts, decentralized applications, crypto on-/off-ramp providers, payment card programs, and other service providers ("Third-Party Services"). Third-Party Services are not controlled by PrintDreams and may be subject to separate terms, fees, eligibility requirements (including KYC/AML and sanctions screening), and regulatory authorizations. PrintDreams does not provide, and is not responsible for, Third-Party Services. Where Third-Party Services provide regulated activities (including crypto-asset services, payment services, or e-money services), such activities are provided solely by those third parties and not by PrintDreams.

PSD2 / payments disclaimer; not a payment service provider

PrintDreams is not authorized as a payment institution or electronic money institution and does not provide payment services within the meaning of Directive (EU) 2015/2366 ("PSD2") or issue electronic money. Any payment or card-related functionality described in connection with the Technology, if any, would be provided by Third-Party Services subject to their own regulatory status and terms.

Regulatory uncertainty and geographic restrictions

Laws and regulations applicable to crypto-assets, digital finance, and related technologies continue to evolve and may differ between EU Member States and other jurisdictions. The availability or functionality of the Technology may be restricted, modified, geofenced, suspended, or discontinued in certain jurisdictions to comply with applicable law or risk controls. It is your responsibility to ensure compliance with applicable laws and regulatory requirements in your jurisdiction.

Data protection (GDPR) and privacy

To the extent PrintDreams processes personal data in connection with the Technology, such processing will be governed by applicable data protection laws, including Regulation (EU) 2016/679 (the "GDPR") and any applicable Member State implementing laws. This Whitepaper does not constitute a privacy notice. Any privacy notices, data processing terms, and related disclosures will be provided separately. Where Third-Party Services process personal data (including for KYC/AML), such processing is governed by the third party's privacy documentation and legal obligations.

Security, operational resilience, and reliability risks

Use of the Technology involves material risks, including software defects, smart contract vulnerabilities, cybersecurity incidents, supply-chain compromise, device failures, printing/media degradation, tamper/counterfeit attempts, data loss, and service interruptions. PrintDreams does not guarantee that the Technology will be secure, uninterrupted, error-free, or immune from attack. Any security, durability, or survivability targets stated in this Whitepaper are objectives only and may depend on environmental conditions, user handling, third-party components, and operational controls. Nothing in this Whitepaper should be interpreted as a representation that the Technology meets any specific regulatory technical standard (including under DORA, NIS2, or other ICT/security frameworks) unless expressly stated in writing by PrintDreams.

Intellectual property; no license granted except as stated

All intellectual property rights in and to the Whitepaper and the Technology are owned by PrintDreams or its licensors. Except as expressly set out in a written agreement with PrintDreams, no license or rights are granted under any patent, copyright, trademark, trade secret, or other intellectual property right by implication, estoppel, or otherwise.

Limitation of liability

To the maximum extent permitted by applicable law, PrintDreams shall not be liable for any direct, indirect, incidental, special, consequential, exemplary, or punitive damages, or any loss of profits, revenue, goodwill, data, or crypto-assets, arising out of or related to this Whitepaper or the use of (or inability to use) the Technology, whether in contract, tort, strict liability, or otherwise, even if advised of the possibility of such

damages. Nothing in this disclaimer limits liability to the extent such liability cannot be excluded or limited under applicable law.

No reliance; forward-looking statements

The Whitepaper may contain forward-looking statements based on current expectations and assumptions. These statements are inherently uncertain and may differ materially from actual outcomes. By accessing or using this Whitepaper, you acknowledge that you have not relied on any statement or representation not expressly set out in definitive written agreements with PrintDreams.

Updates

PrintDreams may revise, update, or replace this Whitepaper at any time without notice. The version and date stated on the cover page apply only to that version of the Whitepaper.

Research and model limitation

Any empirical loss intensity, RVR, enforcement-stage probability, deterrence ratio, compromise bound or durability estimate in this Whitepaper is an identified estimand, model, target or source-derived calibration unless explicitly linked to completed independent evidence. Public sources may be incomplete, proprietary, underreported or non-comparable. No metric is a warranty, forecast, certification or representation of universal product performance.

Executive Summary

Stablenotes v1 is a non-custodial authorization architecture for stablecoins and other tokenized assets. Its target workflow combines a dedicated Secure Issuance Terminal, protected physical authorization media, a separately controlled owner factor, an isolated transaction signer and an owner-bound asset-control policy. The architecture is SDK-integrable; its security claims depend on the implementation and evidence gates in this whitepaper. A post-quantum authorization extension remains a separately gated proposed profile.

The security rationale is structural. Remote attackers can compromise an issuance dependency, manipulate the transaction shown to an operator, inject an apparently authorized command, or exploit an external verifier without extracting a private key from a secure element. Independently governed factors and an enforceable policy are intended to make compromise of an ordinary online workflow insufficient to authorize a protected transfer [R22–R27].

AI-assisted tools can increase the scale and speed of phishing, reconnaissance, malicious code development and other attack steps. The effect depends on the adversary and task; no claim is made that a particular cited incident used AI without incident-specific evidence. Defenders can also use AI to investigate and test systems, subject to independent verification.

Documented incidents reinforce the need to protect the entire authorization workflow, not only the cryptographic device. They also show why weak entropy, compromised transaction presentation and external protocol failures must be assessed separately from direct key extraction. The 29 October 2026 Binance incident illustrates this distinction: Binance estimated approximately USD 6.3 billion in unauthorized hot-wallet outflows and reported no evidence of a private-key leak in its initial investigation. The FBI later attributed the theft to North Korea's TraderTraitor. The incident illustrates a threat scenario. It should not be considered as a test of this product [R31, R35].

Another threat which is not yet a reality but that can become real is quantum computing (QC). A sufficiently capable quantum computer could compromise widely used classical public-key signatures and key-establishment schemes. Arrival timing remains uncertain. Captured ciphertext may face future decryption, while exposed classical public keys may enable future private-key derivation and signature forgery.

The resulting product requirement is clear. For custody profiles that require offline continuity, resistance to remotely scalable compromise and separation of possession from authorization, a separately controlled offline factor is not an optional convenience. It is a mandatory compensating control. Stablenotes conforms to that requirement only if possession of the note is insufficient to reconstruct the wallet secret or direct funds to an arbitrary destination.

What v1 is

1. A deployable reference architecture for provisioning, issuing, protecting and authorizing an owner-bound asset partition, integrated with an institutional wallet and security workflow.
2. A cryptographic profile that splits authorization across a physical share S1 and independent owner share S2.
3. A physical-media specification with protected S1 encoding, adjacent public verification information, a protected human-readable fallback, and qualified print and durability controls.

4. An isolated ingestion/signing workflow that accepts unsigned transaction data optically and emits only public signed-transaction data.
5. An enforceable owner-bound policy that limits permitted asset release and prevents possession-only transfer or unauthorized administrative redirection.
6. An evidence program covering issuance entropy, paired printing, secret non-retention, factor custody, firmware integrity, media survivability, transaction authorization and partner integration.

What v1 is not

7. It is not a blockchain, stablecoin, token, custodian, exchange, payment service, bearer note or cash-out network.
8. It does not make the entire wallet system unhackable. The passive physical factor has no direct network interface, while the issuance, printing, signing and underlying-chain environments retain separately assessed attack surfaces.
9. It does not satisfy AML/CFT or the FATF Travel Rule by itself; covered entities retain their own legal obligations.
10. It is not presently certified as sovereign-grade. That classification is reserved for deployments that pass additional governance, continuity and independent-assurance gates.

Production status

An SDK beta, reference wallet applications and the existing certified printer platform provide development foundations. The M5Stack Tab5 is the selected issuance-terminal platform, and the Keystone 3 Pro is the preliminary selected basis for a separate signer. The custom firmware, paired link, production factor profiles, owner-policy implementation and integrated assurance remain subject to qualification and independent evidence [R28, R29].

> **Core claim: owner-bound authorization, independent custody domains, qualified issuance, isolated transaction signing and durable media are security controls whose stated properties must be supported by deployment-specific evidence before live-value release.**

0 Document Information

0.1 Document metadata

Field	Value
Document title	Stablenotes v1 Whitepaper
Document ID	SN-WP-V1-PQC-EXT-2026-09
Version	v3.0.1
Status	Technical whitepaper; deployment assurance and approvals evidence-gated

Field	Value
Original owner	A. Breton, CEO
Main research source	The Asymmetric Attack Surface of Fiat Substitutes: A Measurement Framework and Owner-Bound Offline Custody Architecture [R1]
Reproducibility repository	github.com/printdreams/cryptoeconomic-theft-asymmetry
Public baseline commit	Public baseline: f6e87ea7cab8420504cb7f33704ace56cd48f254
Release status	Local release candidate generated and validated; public commit and any archive identifier must be verified before citation.
Integration date	2026-10-02
Additional research source	Remote Digital Asset Theft Report, 28 October 2026 [R22]; Binance incident research, 2 November 2026 [R38]

0.2 Versioning policy

MAJOR changes alter scope, trust boundaries, cryptographic profiles, security claims or Go/No-Go gates. MINOR changes clarify content without changing those properties. PATCH changes are non-substantive. Version 3.0.0 is a major document update because it specifies a separate issuance boundary, its printer interface and additional production gates. Stablenotes v1 remains the product scope.

0.3 Change log

Version	Date	Author	Summary	Sections	Evidence impact	Approval
v 0.1.0	2025-08-21	A. Breton	Initial draft structure	All	N/A	M. Kosenko
v 1.0.0	2026-03-19	A. Breton	v1 scope lock	All	v1 and v2 separation	A. Ricknell
v2.0.0	2026-08-25	A. Breton	Integrated research manuscript; corrected models and cryptography; made owner binding mandatory	All	New evidence required; prior full-key claims invalidated	M. Kosenko
v2.1.0	2026-08-27	A. Breton	Aligned to JFDA submission manuscript; removed non-identified RVR/deterrence multipliers; added exact cash calibration, mature-cohort enforcement model and repository release status	Appendix D; references	Empirical claims narrowed; product architecture retained; public-release verification still pending	M. Kosenko
v2.1.1	2026-09-16	A. Breton	Final fact checks, equations formatting and cross-references	Exec. Summary; Sec 2	None	M. Kosenko
v2.2.0	2026-10-01	A. Breton	Post-Quantum resilience addendums	Multiple	New evidence required but separated from v1 baseline	M. Kosenko

Version	Date	Author	Summary	Sections	Evidence impact	Approval
v3.0.0	2026-10-29	A. Breton	Dedicated issuance architecture, incident-derived threats and non-revealing print verification	Executive Summary; §§2–10, 12; Appendices	New issuance, print, interoperability and assurance evidence required	A. Ricknell
V3.0.1	2026-11-02	A. Breton	Reference to world's largest heist (Binance, Oct 2026)	Multiple	Dated sources; EVM abuse tests required. No new loss estimates or completed assurance.	A. Ricknell

0.4 Contents

Legal Disclaimer; Executive Summary; 0 Document Information; 1 Glossary

2 Problem Statement & Design Rationale; 3 System Overview; 4 Asset Model & Wallet Lifecycle

5 Smart Contract Specification; 6 Security and Assurance; 7 Firmware, App and Update Integrity

8 Physical Transaction Authorization Media Design; 9 Reliability & Survivability Testing; 10 Security Testing & Assurance

11 Regulatory Positioning; 12 Roadmap & Gates; Appendices A-F

1 Glossary

Purpose: eliminate ambiguity and keep technical, legal and partner terminology consistent. If a term appears in a heading, equation or critical control, it must be defined here.

Core term	Definition
ABI	Application Binary Interface
Air-gapped ingestion	A controlled transaction authorization/signing process in which secret-bearing inputs enter an isolated terminal through bounded local channels and only public signed-transaction data leaves. It does not imply zero end-to-end compromise risk.
AML	Anti-Money Laundering
API	Application Programming Interface
AQL	Acceptance Quality Limit
Asset	A blockchain-native token or coin (e.g., stablecoin) controlled via a wallet's private keys.
Batch ID	A unique identifier assigned to a manufacturing batch of transaction authorization notes; used for traceability.
Bearer instrument	A transfer mechanism where possession alone is sufficient to redeem value; out of scope for v1.
CAPA	Corrective And Preventive Actions
CFT	Countering the Financing of Terrorism

Core term	Definition
Chain-of-custody	Recorded sequence of custody handoffs for serialized media across factory, logistics, warehouse, and distribution points.
Checksum	A non-cryptographic or keyed integrity value used to detect accidental corruption. A checksum alone does not authenticate origin or prevent deliberate substitution.
Clearance outcome	A specified law-enforcement outcome for a reported incident. FBI UCR clearance is not synonymous with conviction.
Common-mode compromise	A single event or shared dependency that compromises multiple partitions or both owner-binding factors, creating positive loss correlation.
Companion app	The wallet application (e.g., Cryptocash Wallet app, Stablenotes app) providing UI for creation, verification, and transaction authorization workflows; scoped for v1.
CRC	Cyclic Redundancy Code
CSPRNG	Cryptographically Secure Pseudorandom Number Generator; used to generate high-entropy keys.
CVSS	Common Vulnerability Scoring System
Deterrence ratio (D_R^(p))	The ratio of equivalent enforcement-stage probabilities for matched offense cohorts. It is descriptive, not a complete Becker-style deterrence measure, and no cross-domain point estimate is reported without matched data.
DNS	Domain Name Service
DPA	Data Protecting Act
DPIA	Data Protection Impact Assessment (data processing)
DRBG	Deterministic Random Bit Generator
ECC (Error Correction Code):	Mechanism enabling QR transaction authorization when modules are damaged (e.g., QR ECC level).
ECDSA	Elliptic Curve Digital Signature Algorithm
Evidence artifact	A specific document or dataset (audit report, lab report, protocol) that substantiates a claim.
EVM	Ethereum Virtual Machine
Exposure-normalized loss intensity	Gross intensity $\hat{L}_{j,t}^{G}$ is gross stolen value divided by time-weighted average exposed value; net intensity $\hat{L}_{j,t}^{N}(h)$ subtracts recovery at a stated horizon. Neither is automatically a per-unit theft probability.
FPGA	Field Programmable Gate Array
GDPR	General Data Protection Regulation
Go/No-Go gate	A decision checkpoint where deployment proceeds only if defined evidence and acceptance criteria are met.
HSM	Hardware Security Module
ID	Identification Data
IDTA	International Data Transfer Agreement

Core term	Definition
IPC	Information Protection and Control
JTAG	Joint Test Action Group
Key non-retention	Requirement that private keys/secret material are not stored, logged, or transmitted beyond the workflow window.
KPI	Key Performance Indicator
KYC	Know Your Customer
MCU	Microcontroller Unit
MITM	Man In The Middle
NDA	Non-Disclosure Agreement
Note (Transaction Authorization Note):	The physical transaction authorization medium containing encoded transaction authorization material; transaction authorization instrument in v1.
Note serial number	A unique identifier printed on an individual note, enabling traceability and quarantine/recall by range.
OS	Operating System
OTA	Over The Air
Owner binding	Mechanism restricting transaction authorization so funds can only be redeemed to owner-bound destinations (address/whitelist/proof).
Owner wallet	The user's primary wallet account context that receives recovered assets.
Owner-bound substrate	Physical transaction authorization media containing an authorization factor that is insufficient, by possession alone, to reconstruct a wallet secret or transfer funds arbitrarily.
PGP	Pretty Good Privacy
PoC	Proof-of-Concept
PoS	Proof-of-Stake
Post-print verification gate	Mandatory public-key QR and back-checksum checks, linked to the qualified print process, before funding eligibility; the protected S1 encoding remains obscured.
PQC	Post-quantum cryptography
QC	Quantum Computing
QR	Quick Response
RACI	Responsible, Accountable, Consulted, Informed
Authorize / Convert	The process by which a transaction authorization happens using the physical note wallet S1 + S2 (reconstructing K).
Note wallet	The dedicated on-chain wallet or asset-control account whose assets are protected under the owner-bound profile; the physical note contains S1 rather than the wallet containing that share.

Core term	Definition
Relative Vulnerability Ratio (RVR)	The ratio of two exposure-normalized loss intensities, interpretable only when period, geography, asset/custody perimeter, event definition, transaction authorization convention, valuation, exposure and reporting coverage are materially matched.
RMA	Return Merchandise Authorization process for defective physical media or device components.
RNG	Random Number Generation
ROM	Read-Only Memory
RoPA	Records of Processing Activities (General Data Protection Regulation)
RPC	Remote Procedure Call
S1 / S2	S1 is the physical note share. S2 is the independently stored owner share. The labels describe failure domains, not possession versus a memorized biometric.
SCC	Standard Contractual Clauses
SDK	Software Development Kit
Secret share	One output of an information-theoretic or computational secret-sharing construction. A conforming share is independently protected and insufficient below the threshold.
Secret Sharing Scheme (SSS)	A scheme that divides a secret across shares; distinct from a threshold-signature scheme, which signs without reconstructing the secret key.
Secure boot	Hardware/firmware process ensuring only authenticated firmware executes on the device.
Secure element	Tamper-resistant hardware component used to store secrets and perform cryptographic operations.
SOP	Standard Operation Procedure
Sovereign-grade	A gated deployment classification requiring public-sector governance, independent assurance, continuity evidence and legal authorization; not a default product claim.
Supply-chain attack	Compromise introduced during manufacturing, provisioning, shipping, or distribution.
SWD	Serial Wire Debug
Tamper-evident	Design that provides visible evidence of opening or manipulation under defined inspection methods.
TBD	To Be Defined
TFR / Travel Rule	EU transfer-of-funds requirements extended to crypto transfers (relevant to regulated service providers; not v1 itself).
TON	The Open Network
TUF	The Update Framework
UART	Universal Asynchronous Receiver-Transmitter
UI	User Interface
URL	Universal Resource Locator
UX	User Experience
v1 (Stablenotes v1):	Physical layer with owner-bound transaction authorization; non-transactional by design.

Core term	Definition
v2 (Stablenotes v2):	Future bearer/offline transfer program; explicitly outside scope of this whitepaper.
VDP	Vulnerability Disclosure Policy
Whitelist	A permitted set of owner-bound destination addresses for transaction authorization (if implemented).
Wi-Fi	IEEE 802.11x Wireless Networking (Wireless Fidelity)
Secure Issuance Terminal (SIT)	Dedicated, restricted-connectivity appliance proposed to generate and split K, manage authorized printing, verify public media indicators and issue non-secret funding-eligibility evidence.
Isolated Signer	Separate transaction-signing appliance that validates and displays the intended action, ingests independently controlled factors, reconstructs K transiently, signs and zeroizes.
Paired printer link	Proposed authenticated local SIT-to-ATM link using per-pair credentials and TLS 1.3 PSK-DHE, subject to implementation and qualification.
Funding eligibility	A public, authenticated issuance status produced only after approved policy, public print checks and secret cleanup; it is distinct from confirmed blockchain funding and independent factor custody.
Public print verification	Non-revealing verification of the adjacent public-key QR and fallback checksum, combined with qualification of the shared print process; it is not a direct decode of the protected S1 encoding.
Class A material	K, S1, S2, seed and entropy material, readable secret encodings and secret-bearing buffers; controlled physical factors are intended outputs, while unauthorized retention is prohibited.

Glossary maintenance rule: terminology changes affecting a critical control constitute at least a MINOR version change; changes to owner binding, risk metrics or regulatory role definitions are MAJOR.

2 Problem Statement & Design Rationale

2.1 Problem Statement: stablecoin adoption is real, but custody and resilience are brittle

Stablecoins and other tokenized assets provide global reach, programmable settlement and, for fiat-referenced instruments, a unit of account that may be more stable than local currency. Those benefits do not remove custody risk. They relocate authorization into software, devices, credentials and networks whose attack surface can be reached from outside the holder's physical environment.

AI can amplify the scale and speed of cyberattacks. A sufficiently capable quantum computer could compromise vulnerable public-key cryptography; the arrival date of such a machine remains uncertain.

2.1.1 Storage safety and exposure-normalized loss

Users lose access through device loss, malware, phishing, credential failure, accidental deletion and fragile backups. The research article [R1] adds a macro lens by distinguishing gross stolen value G, net loss N(h) after post-theft recovery horizon h, and time-weighted exposed value E.

$\hat{L}^{G}_{j,t} = \frac{G_{j,t}}{E_{j,t}}, \quad and \quad \hat{L}^{N}_{j,t}(h) = \frac{N_{j,t}(h)}{E_{j,t}}$ are value-weighted loss intensities.

$RVR_{a,b} = \frac{\hat{L}^{G}_{a,t}}{\hat{L}^{G}_{b,t}}$ is meaningful only when period, geography, asset and custody perimeter, event definition, transaction authorization convention, valuation rule, exposure concept and reporting coverage are materially matched.

The exact lower-bound cash calibration is 0.080893% gross and 0.078792% net for reported U.S. currency loss in 2019 using year-end currency in circulation; reported recovery equals 2.5978% of reported gross loss. Separately, Chainalysis and TRM Labs each estimate approximately USD 2.2 billion stolen in 2024 digital-asset hacks. Because no matched stablecoin or reachable-custody exposure denominator is available, this whitepaper reports neither a digital loss intensity nor a cash-versus-digital RVR.

Binance estimated the impact at approximately USD 6.3 billion and reported approximately USD 3 billion frozen on-chain as of its 30 October 2026 update [R31]. Those amounts measure different stages: immobilization can constrain an offender's future use, but funds count as recovery only when returned to the victim under the stated recovery definition and horizon. Binance's use of its own reserves to replenish assets is separate again. The incident supplies no matched exposure denominator for a digital-loss intensity or cash-versus-digital RVR.

2.1.2 Intermittent connectivity and continuity

Unstable connectivity, constrained power, device replacement, disaster conditions and unsafe shared-device environments increase the probability that redeeming is needed when cloud or account-based methods are unavailable. Offline transaction authorization is therefore a continuity control, not merely a user-interface preference.

2.1.3 Device compromise and AI-automated attack scalability

Malicious applications, operating-system compromise, SIM or account takeover, overlays, clipboard interception and fake wallets expose authorization workflows. Drainer-as-a-Service illustrates how a reusable malicious payload and affiliate distribution can target many wallets at low marginal cost. The risk is structural: an attacker can search globally, select visible high-value targets and automate delivery without proportional physical labor.

AI-assisted tools may reduce the effort required for some reconnaissance, phishing, malware development and adaptation. Their impact varies by task and adversary, and does not eliminate the need for access, operational capability or a successful attack path.

2.1.4 Tactics, Techniques, and Attack Chains

Attack chains can combine social engineering, compromised development or security software, privileged access and transaction substitution. AI-enabled automation can assist individual stages, but a specific attribution of AI use requires evidence [R22–R27].

Automation can shorten the time available for investigation and intervention. Security controls should therefore reject unauthorized actions at the enforcement boundary, rather than relying exclusively on alerting after a transaction has been submitted.

In its analysis of the Binance incident, TRM Labs reported 50 previously signed EIP-7702 authorization tuples in one Ethereum transaction, one of which enabled delegation to attacker-controlled code. Transfers on other chains used different transaction paths. TRM assessed a signing-infrastructure compromise; Binance reported additional breach points and an ongoing investigation [R31, R32].

AI can naturally also be used for defense. It can help defenders analyze logs, identify suspicious activity, investigate incidents, test infrastructure and respond to threats. The problem is that the defender has to protect everything while the attacker only needs one weakness. This creates an asymmetry that matters.

2.1.5 The threat from Quantum computers

Modern digital infrastructure is built on public-key encryption. RSA and elliptic-curve cryptography protect among many other things, payment authorization, connected devices and secure firmware updates. A fault-tolerant quantum computer could break much of this cryptography using Shor's algorithm.

The timing of a cryptographically relevant quantum computer is uncertain. Organizations may plan migration on shorter schedules to accommodate long infrastructure lead times; a migration target is not a prediction that such a computer will exist by that date.

2.1.6 Custodial alternatives shift rather than remove risk

Hosted wallets and exchanges reduce user backup burden but introduce counterparty, insolvency, freeze, withdrawal, jurisdiction and platform-compromise risk. Self-custody and custody therefore allocate failure differently. Stablenotes addresses one narrow requirement: independent self-custody without possession-only bearer risk.

In the case of Binance, it temporarily suspended withdrawals and said it would absorb the financial impact using company resources; it reported a phased restart on 1 November 2026 [R31, R37]. Custodian replenishment can support user access but does not establish that stolen assets have been recovered.

2.1.7 Enforcement and deterrence asymmetry

Jurisdictional fragmentation, rapid transfer and reusable attack infrastructure can weaken attribution, asset recovery and sanction. Empirical deterrence analysis must nevertheless follow a mature, linked cohort through reporting, attribution, arrest, prosecution and conviction. Clearance, identified persons, complaints and convictions are different outcomes. Public sources do not provide matched cash and digital-theft cohorts, so the whitepaper treats 'deterrence deficit' as a falsifiable mechanism hypothesis and does not report a multiplier.

2.1.8 Core pain statement

> **Core problem: valuable digital-asset workflows expose software, human review, credentials and external dependencies to remote attack. A high-consequence authorization profile therefore needs independently governed physical and owner factors, a trustworthy issuance and signing process, and a destination policy enforced at the applicable asset-control boundary.**

2.2 Design Rationale: why owner-bound printed transaction authorization media exists

2.2.1 Why not hardware-only

Hardware wallets can provide strong key isolation and transaction verification. Their security also depends on entropy, firmware, supply chain, trusted display and the exact operation being signed. The passive physical factor adds an independently stored component; it does not replace qualified signing hardware or guarantee safety of the surrounding workflow [R23, R25].

2.2.2 Why not custodial transaction authorization

Custodial transaction authorization provides access through an intermediary. That can be appropriate, but it changes the control and regulatory model. Stablenotes keeps transaction authorization material under the user's independent control and is designed so PrintDreams cannot reconstruct the wallet secret or move funds.

2.2.3 Why physical media persists

11. It is passive and does not require continuous power, firmware updates or network connectivity.
12. It can be placed in a separately governed physical location and audited as an inventory item.
13. Its low unit cost can support value partitioning without one electronic device per partition.
14. Its durability, readability and tamper behavior can be tested against explicit acceptance criteria.

The medium is security-critical when its authorization factor is independently controlled and the asset policy is owner-bound. A printed complete spend key is possession-sufficient bearer material; the v1 reference profile prints S1 rather than K.

2.2.4 Tradeoffs and limitations

15. Loss or destruction of a required share can make transaction authorization impossible unless the selected threshold profile provides independent redundancy.
16. The SIT, its radio and printer path, the independent S2 domain, the isolated signer, the transaction display and the supply chain remain attack surfaces.
17. Tamper evidence indicates defined forms of access; it cannot prove that no optical copy was made.
18. Secret partitioning reduces concentration only when compromise events are not strongly correlated.
19. Material durability is a claim about the complete media stack and must be demonstrated, not inferred from a polymer datasheet.
20. Coercion resistance requires policy controls beyond secret sharing.

2.3 Design Goals and Non-Goals

2.3.1 Design goals

21. Owner-bound authorization: possession of the note alone is insufficient.
22. Remote-surface reduction: the passive physical factor has no direct network interface.
23. Independent custody domains: after issuance, S1 and S2 are held under independent controls and do not share ordinary backups, accounts or support paths. Both shares necessarily coexist transiently within the approved SIT issuance boundary and, during signing, within the isolated signer; these common boundaries require independent assurance.
24. Durable recoverability: QR and fallback remain usable under defined, tested conditions.
25. Non-retention: PrintDreams and partner backends never receive Class A material.
26. Auditable ingestion: firmware, transaction display, parsing, signing and zeroization are independently testable.

Verifiable issuance: a signed deployment profile, approved printer pairing, public post-print checks, controlled secret cleanup and independently verified funding precede release into the protected lifecycle.

27. Evidence over claims: every material proposition maps to a report, protocol, test vector or legal analysis.

2.3.2 Non-goals

28. No bearer transfer, cash replacement, payment network, operator program or cash-out rail.
29. No anonymity or mechanism designed to bypass AML/CFT controls.
30. No promise of zero end-to-end exploitability or guaranteed recovery.
31. No sovereign-grade or regulatory-certification claim without deployment-specific evidence.

3 System Overview - Architecture and Trust Boundaries

3.1 Components

3.1.1 Wallet application and SDK

32. Provides an approved institutional interface for public issuance context and transaction authorization; the production wallet or ordinary mobile app does not generate or retain K, S1 or S2.
33. Creates canonical unsigned transactions and validates signed outputs.
34. Integrates with an independently controlled S2 custodian or security domain without creating an unapproved shared backup or support path.
35. Applies interface-level checks and submits only an approved owner-bound action; the asset-control policy enforces the destination restriction independently of the online interface.
36. Never transmits Class A material to PrintDreams or partner backends.

3.1.2 Issuance terminal, paired printer and isolated signer

37. Secure Issuance Terminal (SIT): validates the signed deployment profile and operator authorization, generates K in qualified transient memory, derives the public wallet identity and splits K into S1 and S2.
38. SIT reference profile: a selected 32-byte Ed25519 seed and XOR 2-of-2 split for the initial TON profile. Canonical factor encoding, authenticity, issuance authorities and shared signer vectors must be frozen and independently reviewed before live value.
39. Cryptocash ATM: receives a bounded S1 print job over the proposed authenticated, factory-paired local link and prints the protected factor and public verification information. A separately printed S2 note is limited to an explicitly approved reference/demo profile; no job contains K or both shares.
40. Public print verification: the front public-key QR and the back checksum are checked without exposing the protected S1 areas. Their evidential relationship to the protected printing is qualified under the test program in §§6.4 and 9.3.
41. Isolated Signer: a separate transaction device validates and displays the action, accepts S1 and the independent S2, reconstructs K transiently, signs and clears secret-bearing buffers. Secure boot, updates, parsing, display and erasure are subject to independent qualification.

3.1.3 Physical transaction authorization media

42. Contains the protected S1 QR on the front and a protected human-readable S1 representation on the back, with separate public verification elements.
43. Contains format version, chain/wallet profile, note serial, and public-address verification data.
44. Uses qualified ink, substrate and two obfuscated protected areas, including tamper-evident features specified and tested for the deployment.
45. Does not contain K or a possession-sufficient spend credential in the owner-bound v1 profile.

3.1.4 Owner security domain

46. Protects S2 independently from the stored physical note and from ordinary online systems; temporary co-location in the controlled issuance and signing boundaries is explicit and assessed.
47. May be a second hardware device, institutional quorum store or separately encrypted backup.
48. Must not use the same cloud account, device backup or support path as S1.

3.1.5 Blockchain and transaction authorization -policy layer

49. Verifies chain-specific signatures and asset identifiers.
50. Enforces owner-bound destination constraints at the asset-control boundary under the applicable chain-specific policy. A signer-only restriction is not sufficient to constrain an attacker who has obtained K and can use another spend path.
51. Provides replay protection, state monotonicity and public audit events without storing secrets.

3.2 High-level workflow (v1 transaction authorization use case)

52. Ceremony 1 — Provisioning: the institution approves the deployment annex, asset and owner-destination policy, operator roles, independent S2 custody and the assigned SIT/ATM pair.
53. Ceremony 2 — Issuance: the SIT validates the approved profile and operator, creates K in qualified transient memory, derives the public wallet identity, and splits K into S1 and S2. The production profile sends S1 alone in an authenticated print job to the assigned printer; the independent S2 handoff follows its approved confidential procedure.
54. The printer produces S1 over the obfuscated front area and then, in the same front printing movement, the adjacent public-key QR. On the back, the human-readable S1 representation is printed over the second obfuscated area and the checksum immediately thereafter. Both protected areas are Class A.
55. The SIT checks the public-key QR against the approved public wallet identity and validates the back checksum without reading the protected S1 areas. These are non-revealing, process-based indicators whose reliability must be demonstrated for the complete print and media configuration. Failed, interrupted or uncertain output is held or voided; no automatic secret reprint is allowed.
56. After the public checks, approved owner-policy binding and secret cleanup, the SIT issues authenticated public funding-eligibility evidence. The institution independently verifies that evidence before funding. Confirmed chain funding and independent S1/S2 custody acknowledgements are required before the unit is marked STORED.

57. Ceremony 3 — Authorization: an isolated signer parses an unsigned transaction, displays the authoritative action and obtains confirmation before accepting the factors and reconstructing K. It signs only an action satisfying the approved policy and clears the secret buffers.
58. Ceremony 4 — Evidence and retirement: the online system independently verifies and broadcasts the signed public transaction, confirms execution and finality, records non-secret evidence and retires the used physical authorization unit under the chain-specific policy.

3.3 Architecture diagram (logical view)

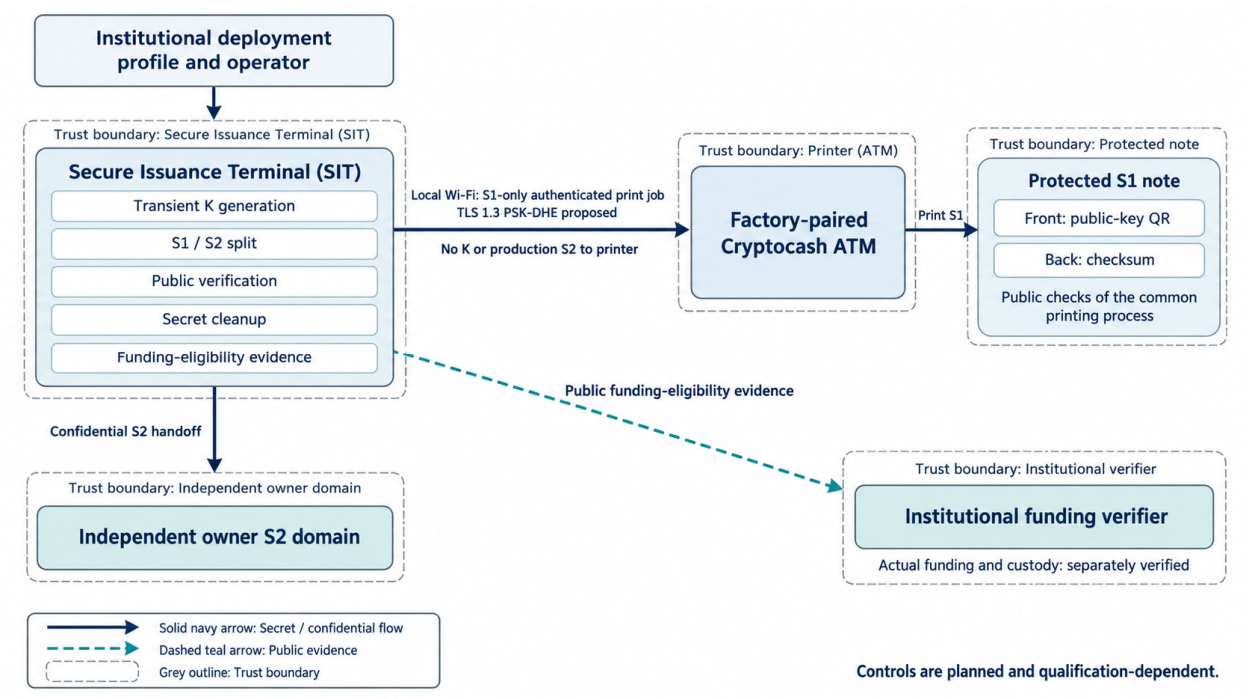


Figure 1A. Secure issuance and funding eligibility.

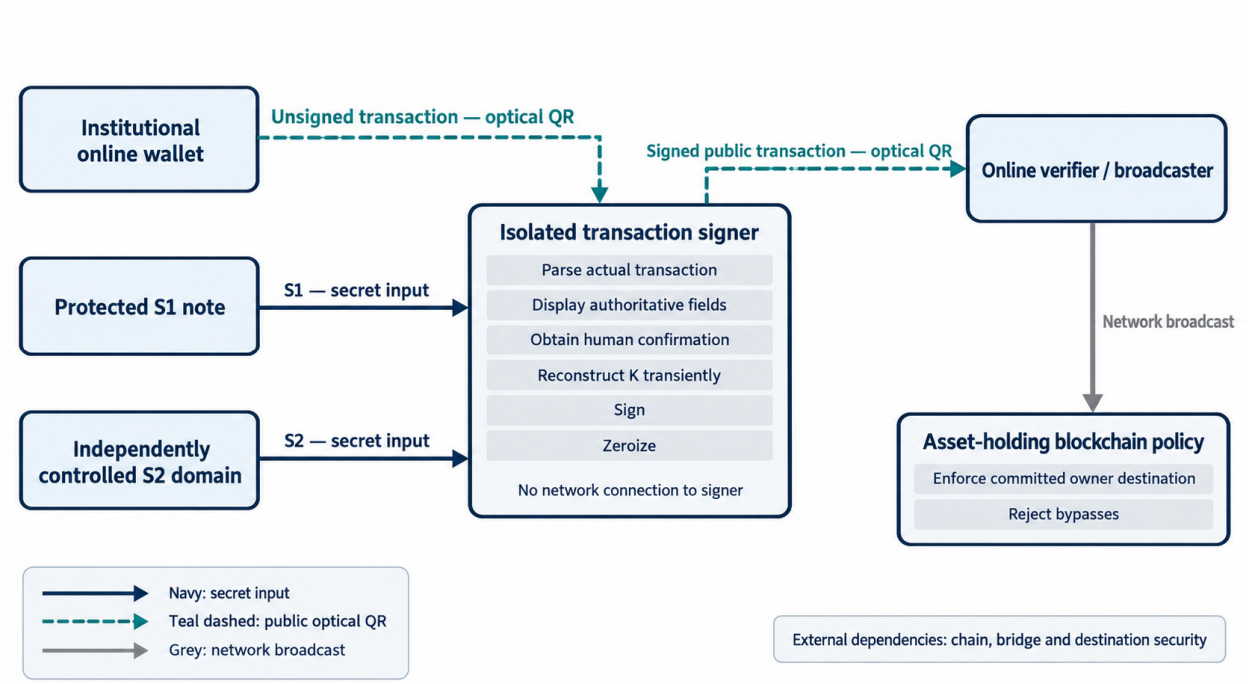


Figure 1B. Owner-bound transaction authorization.

3.4 Trust model: boundaries and assumptions

3.4.1 Trusted components

59. Entropy source and DRBG construction
60. Secret-sharing implementation and encoding
61. Owner S2 security domain
62. Isolated terminal secure boot, display, parser and signing path

SIT entropy source, approved secret memory, issuance firmware and authenticated pairing/print path are trusted only to the extent supported by configuration-specific tests and independent assurance.

63. Media qualification and post-print verification
64. Owner-destination enforcement and asset allowlist

3.4.2 Untrusted components

65. Smartphone operating environment and third-party SDKs
66. Public networks, RPC nodes and broadcast relays
67. Unverified update media and peripheral devices
68. Physical transport, retail channels and unauthorized cameras
69. User-supplied transaction QR payloads until parsed and displayed

3.4.3 Assumptions and exclusions

The security argument assumes qualified entropy, protected transient issuance and signing boundaries, independent S1/S2 custody, transaction verification and enforceable owner-bound asset control. Coercion, supply-chain compromise, consensus or bridge failure, partner modifications and common-mode incidents remain residual risks assessed in the deployment annex.

The baseline security argument assumes that its selected cryptographic primitives remain secure. Section 5.6 proposes an additional authorization boundary for deployments that must consider compromise of classical public-key signatures. This extension does not remove dependencies on the selected blockchain, token contracts or destination controls.

3.5 Threat model

Some of the following threats extend the baseline threat model to quantum-enabled attacks and cryptographic migration. Controls described as part of the post-quantum extension are proposed requirements, not claims of currently deployed capability.

Threat	Objective	Primary controls
Remote malware / phishing	Steal credentials, alter transaction or exfiltrate S2	No S1 on networked device; authenticated display; destination binding; telemetry prohibition
Physical note theft / optical copy	Obtain S1	S1 alone reveals no K; tamper evidence; independent S2
Owner-domain compromise	Obtain S2 or authorize destination	Separate S1; re-issuance; hardware-backed policy; value limits
Ingestion terminal compromise	Capture both shares or alter transaction	Secure boot; measured firmware; trusted display; red-team and side-channel review
Supply-chain compromise	Replace media/device or leak generation state	Serialization; attestation; reproducible builds; chain of custody; quarantine
Coercion	Force owner to present both factors	Quorum, delay, value caps, geographic separation and incident procedure
Common-mode process failure	Compromise many notes or both factors	Independent domains, lot diversification, transaction authorization drills and correlation stress tests

Threat	Objective	Primary controls
Quantum derivation of classical signing keys	Derive a classical private key from an exposed public key and authorize asset movement without obtaining S1 or S2.	Proposed mandatory post-quantum approval enforced by the asset-holding vault; independent PQ credentials; owner-bound destination enforcement; elimination of classical-key-only withdrawal paths.
Harvest now, decrypt later	Capture encrypted communications or archives now and later decrypt secret-bearing material or confidential operational information.	Minimize creation, transmission and retention of secrets; maintain independent S1/S2 domains and secret-free telemetry; migrate necessary channels and archives to reviewed PQ or hybrid protection.
Quantum-enabled forgery of infrastructure credentials	Forge firmware, software-update, device-authentication or administrative signatures to compromise the signing environment or alter authorization policy.	PQ-capable or appropriately constructed hybrid authentication and update verification; protected trust anchors; secure boot; rollback prevention; independently authorized policy changes.
Authorization bypass during cryptographic migration	Substitute approval keys, replace the verifier, replay approvals or exploit an upgrade, emergency or legacy path that accepts weaker authorization.	Authenticated key enrollment and rotation; transaction-bound approvals; nonces and policy versions; non-bypassable upgrade controls; downgrade prevention; fail-closed verification.
Quantum compromise of destination or underlying infrastructure	Steal assets after an authorized transfer, or undermine the blockchain or token infrastructure on which vault enforcement depends.	Qualification of destination authorization controls; documented chain, consensus, bridge and token-administrator dependencies; migration planning; explicit limits on the claimed protection boundary.
Weak or substituted issuance entropy	Derive K remotely without obtaining either factor	Qualified entropy and DRBG; compiled-binary review; failure-closed tests; affected-key migration [R25]
Transaction display or payload substitution	Induce the signer to authorize a different action	Parse signed bytes, trusted display, explicit confirmation and operation allowlist; independent policy enforcement [R23]
Forged privileged backend command or code delegation	Cause unauthorized release through an apparently legitimate instruction or a malicious account-code delegation or executor action.	Independent approval, action-bound policy, signer review, value limits and rejection of unauthorized routes [R24] EVM profile: reject unauthorized delegation signatures and executor operations; enforce asset policy independently [R31, R32, R36].
SIT–ATM impersonation, replay or printer retention	Capture S1, repeat a job or generate unauthorized media	Unique paired credentials, authenticated single-use jobs, legacy-path denial, printer non-retention and HOLD/VOID on uncertain result
External chain, bridge or verifier failure	Release or impair assets through a dependency outside the signer	Qualify chain and token dependencies, independent verification where required, circuit-breaker procedures and explicit claim boundaries [R26, R27]

3.6 Data Flows and Privacy Boundary

Class A includes K, raw entropy, coefficients, S1 and S2, readable protected encodings and all secret-bearing buffers. Class B includes public keys, addresses, note serials, approved commitments and transaction hashes. Class C includes allow-listed operational diagnostics.

Class A may exist only in defined controlled boundaries: transient SIT memory, the authorized S1 print job and protected physical output, the independent S2 handoff and custody domain, and transient signer memory. It must not enter ordinary wallet applications, partner or PrintDreams backends, telemetry, backups or support systems. Creation and authorization data flows must identify each buffer, peripheral, radio boundary, print path and crash path.

3.7 Privacy boundary (non-negotiable)

PrintDreams must not receive private keys, shares, seed material, unencrypted transaction authorization payloads, passphrases, biometric templates or identity documents from third-party ramps. Public note serialization should support inventory integrity without creating an unnecessary identity-to-balance registry.

3.9 Third-party service boundary

Regulated ramps, custodians and CASPs/VASPs act under their own permissions and data obligations. The Stablenotes SDK must exchange only the minimum public wallet and status data needed for integration. Travel Rule or KYC data belongs in the obliged entity's compliance channel, never inside the secret-share payload.

3.10 Note serialization and traceability

Serials and batch IDs are Class B. They support authenticity checks, duplicate detection, lot quarantine and incident correlation. Identity linkage is prohibited by default and requires a documented legal basis, purpose, access model and retention period.

3.11 Telemetry and diagnostics

Telemetry is allowlist-only. Permitted fields may include SDK version, coarse device model, verification pass/fail, generic error class and performance timing. QR contents, shares, addresses, screen replay, memory snapshots and sensitive crash context are prohibited.

3.12 Out of scope

The baseline privacy model does not cover user-created photographs, compelled disclosure, law-enforcement response policy, bearer-transfer v2, or AI fraud analytics. Each requires a separate legal and security review.

3.13 Implementation placeholders

70. Initial reference sharing profile: XOR 2-of-2 for TON, preliminary; production profile and independent assurance remain to be frozen.
71. Canonical factor context, authentication, encoding and signer interoperability vectors: [TBD before live-value release].
72. Independent S2 recipient, protected handoff, custody acknowledgement and loss procedure: [deployment-specific; TBD].
73. Supported chains and chain-specific signing suites [TBD]

74. SIT hardware/firmware, ATM paired link and Isolated Signer firmware and measurements: selected or proposed as described in §3.1; qualification evidence [TBD].
75. Owner-destination policy, enforcement boundary and privileged-path analysis: [chain-specific; TBD before funding].
76. Telemetry stack and third-party SDK inventory [TBD]
77. Supply-chain system of record and retention [TBD]

4 Asset Model & Wallet Lifecycle (v1 Owner-Bound transaction authorization)

The lifecycle replaces possession-sufficient key media with a two-factor owner-bound model.

4.1 Wallet model

4.1.1 Owner wallet

The Owner Wallet is the permitted owner-controlled destination. Its authorization and any S2 custody arrangements must remain independent from the physical note and ordinary support paths, subject to documented transient processing in the approved SIT and signer.

4.1.2 Note wallet

The Note Wallet holds the assets assigned to offline transaction authorization. Its secret K is never printed in full. The note represents S1; transaction authorization additionally requires S2 and satisfaction of the owner-destination policy.

4.1.3 Explicit v1 limitation

The note is not intended or designed for peer-to-peer bearer transfer. A deployment that allows possession-only redemption, arbitrary destination selection or transfer of both factors together is intended for v2 and must not use v1 security claims.

4.2 Owner binding mechanism

4.2.1 Two mandatory layers

78. Cryptographic layer: reconstruction requires the threshold of independently stored shares.
79. Policy layer: recovered value may move only to a pre-committed owner address, controlled whitelist or a destination authorized by a separately verified owner proof.

The policy layer supplements secret sharing. It does not rescue a design in which the complete spend key is printed, and it must not contain an administrative backdoor that can redirect value.

4.2.2 Approved profiles

The initial TON reference profile selects XOR 2-of-2 provisionally: the SIT generates independent K and a uniformly random S1, and S2 is K XOR S1. The final seed, factor context, authentication and shared test vectors must be frozen and reviewed. Shamir 2-of-2 or t-of-n are future profiles requiring separate normative specifications and assurance.

4.2.3 Why possession is insufficient

A conforming S1 is information-theoretically independent of K under the scheme assumptions. The thief must additionally compromise S2 and the destination policy. This changes physical theft from immediate bearer redemption to a multi-domain attack. It does not eliminate coercion, owner-device compromise, malicious ingestion or implementation defects.

If K is exposed or predictably generated, independent storage of S1 and S2 alone cannot prevent use of K. Protection against a direct bypass requires an independently enforced asset-control policy that rejects an unapproved destination or operation.

4.2.4 Residual risks

80. Loss of a required share
81. Coercion or collusion across factor holders
82. Incorrect owner destination or whitelist
83. Owner wallet compromise
84. Ingestion terminal compromise
85. Common-mode compromise of the SIT, entropy source, printer path, signer firmware, shared personnel or independent-factor custody.
86. Public-address privacy leakage

4.3 Lifecycle states

4.3.1 Created

The SIT generates and splits K, prints S1 using the paired ATM, completes the public-key QR and checksum checks, clears transient secrets and issues public funding eligibility. The S2 handoff is governed separately. Funding requires independent verification of the issuance evidence and owner policy.

4.3.2 Funded

The institution funds the approved asset-control address after validating the issuance evidence and policy. FUNDED is established from independently verified chain evidence; it is not inferred from a printer or SIT status.

4.3.3 Stored

S1 and S2 enter separate custody domains. STORED requires both independent custody acknowledgements and confirmed funding. Public balance monitoring is optional; routine scans of secret-bearing areas are prohibited unless a separately approved secure procedure exists.

4.3.4 Recovered

The Isolated Signer validates and displays the intended action, reconstructs K transiently from authorized factors, signs and zeroizes. The online system verifies and broadcasts the signed result; the asset-control policy enforces the owner-bound destination.

4.3.5 Retired

Opening exposes the physical factor but does not establish that an asset transfer succeeded. Confirm transfer finality and applicable balances independently. Retirement MUST prevent reuse in the supported workflow; it MUST NOT rely on contract destruction to prevent future deposits. Retirement must be defined chain-by-chain and include an explicit policy for accidental later deposits. The chain annex MUST define treatment of residual assets and unsolicited deposits without bypassing owner authorization or applicable PQ controls.

4.4 Deployment decisions

87. Initial TON reference: preliminary XOR 2-of-2; exact factor context, authentication, vectors and deployment annex [TBD].
88. S2 custody and replacement procedure [TBD]
89. Destination policy and enforcement layer [TBD]
90. Sweep-all versus partial transaction authorization: Sweep-all
91. Lifecycle state storage and privacy model [TBD]
92. Partition size, value cap and correlation assumptions [TBD]

5 Smart Contract Specification (Stablenotes v1)

This chapter defines the on-chain components used by Stablenotes v1. Because partner deployments may vary by chain and custody model, this chapter is written as a reference specification with explicit placeholders. Any production deployment MUST populate the placeholders and publish a chain-specific annex.

5.1 Contracts and interfaces

5.1.1 Supported chains and contract addresses

Stablenotes v1 is designed to support one or more chains where assets can be held and moved via smart contracts or standard token contracts.

Chain support (initial):

93. TON Network: [Supported]

Contract addresses (per chain):

94. TON:
95. TransAuthPolicyContract (if used): TBD at deployment
96. NoteRegistryContract (optional): TBD at deployment

97. Allowlist/TokenVerifier (optional): TBD at deployment
98. Additional chains (if any): Gnosis, Ethereum.

5.1.2 Contract roles and responsibilities (logical)

Depending on the chosen owner-binding enforcement, Stablenotes v1 may include:

99. Transaction authorization Policy Contract Enforces that any “transaction authorization” transfer from a note wallet can only be executed to an owner-bound destination (pre-committed address/whitelist/proof).
100. Note Registry Contract (optional) Stores minimal metadata about notes (e.g., note ID hash, creation timestamp, state markers).
101. Token Allowlist / Verifier (optional; chain-specific) Helps ensure the wallet interacts only with verified token contracts (e.g., verified stablecoin master contracts).

Additional logical roles for the proposed post-quantum extension

A deployment adopting the post-quantum authorization extension MUST implement the following logical responsibilities. These responsibilities may be integrated into existing contracts or implemented as separate components, subject to chain-specific review.

102. Asset-holding vault and authorization policy: Holds protected assets, or exercises exclusive contract-enforced control over their release. Enforces post-quantum approval, owner-bound destination restrictions and applicable operational limits on every asset-release path.
103. Post-quantum approval verifier: Validates an approval under the registered owner authorization policy and approved algorithm profile. Rejects invalid, stale, replayed or context-mismatched approvals. An off-chain verification result authenticated only by a classical signature is insufficient.
104. Authorization configuration and migration controls: Governs approval-key enrollment, rotation, verifier changes, algorithm versions and migration. No administrative or emergency authority may bypass the applicable owner authorization policy.

For deployments adopting this extension, these responsibilities MUST satisfy invariants PQ-1–PQ-4 in §5.2.4. The architecture and its limitations are described in §5.6.

5.1.3 ABI / interface summaries (placeholders)

Below are interface summaries in a chain-agnostic style. For TON deployments, these must be mapped into TON contract message handlers and payload formats.

A) TransAuthPolicyContract (if used)

State variables (conceptual):

105. owner_binding: one of:
106. owner_address (Pattern A)
107. whitelist (Pattern B)
108. proof_policy (Pattern C)
109. status: Active / Redeemed / Retired (optional)
110. policy_version (if upgradeable)

Functions / messages (conceptual):

111. bind_owner(note_wallet, owner_binding_params) Binds the note wallet to the owner destination policy. Called at creation time; must be immutable or tightly controlled after binding.
112. recover(note_wallet, to_owner_address, amount, proof) Executes transaction authorization transfer from note wallet to owner destination. MUST enforce owner binding.
113. set_whitelist(note_wallet, whitelist_addrs, proof) (Pattern B only) Updates whitelist under strict authorization rules.
114. retire(note_wallet, proof) Marks note wallet as retired (optional state tracking).

Events (conceptual):

115. OwnerBound(note_wallet, binding_type, binding_hash, timestamp)
116. Recovered(note_wallet, to, amount, tx_ref, timestamp)
117. Retired(note_wallet, timestamp)
118. SelfDestructed(note_wallet, timestamp)
119. WhitelistUpdated(note_wallet, whitelist_hash, timestamp) (if applicable)

Privacy note: events must not emit secret material. Binding parameters should be represented as hashes where practical.

B) NoteRegistryContract (optional)

Functions / messages:

120. register_note(note_id_hash, note_wallet, metadata_hash)
121. set_status(note_id_hash, status, proof)
122. get_note(note_id_hash) (view/query)

Events:

123. NoteRegistered(note_id_hash, note_wallet, timestamp)
124. NoteStatusChanged(note_id_hash, status, timestamp)

C) Token allowlist / verifier (optional)

Functions / messages:

125. is_verified_token(token_contract_address) -> bool
126. verify_token(token_contract_address, proof) (governance controlled)

Events:

127. TokenVerified(token_contract_address, timestamp)
128. TokenRevoked(token_contract_address, timestamp)

D) Post-quantum authorization extension — additional interface requirements

Applicability. The following requirements apply to deployments adopting §5.6. They supplement interfaces A–C and MUST satisfy invariants PQ-1–PQ-4 in §5.2.4. They describe a proposed deployment profile, not currently implemented functionality.

State variables and configuration (conceptual):

129. pq_authorization_policy: Registered owner approval keys, approval threshold where applicable, and permitted authorization operations.
130. pq_algorithm_profile: Approved signature algorithm, parameter set, encoding rules and verifier identifier.
131. policy_version: Active authorization-policy version, including its algorithm and verifier configuration.
132. replay_state: Nonces or equivalent chain-specific state preventing reuse of an approval.
133. destination_policy: Authorized owner-bound destinations and the rules governing their modification.
134. migration_state: Any authorized transition between keys, policies, verifiers or vaults, including activation conditions and invalidation of superseded permissions.

Approval payload (conceptual):

Each PQ approval MUST authenticate an unambiguous encoding of the chain identifier, vault identifier, operation type, asset identifier, amount, destination, nonce, validity conditions and policy version. For a configuration change, the approval MUST additionally bind the proposed replacement configuration. Variable-amount operations MUST define the approved amount rule explicitly.

Functions / messages (conceptual):

135. verify_pq_approval(action, approval): Verifies the approval against the registered owner policy, active algorithm profile and action context. Verification alone MUST NOT release assets or grant reusable spending authority.
136. execute_authorized_transfer(action, approval): Enforces PQ approval, owner binding, replay protection and operational limits before releasing assets.
137. rotate_pq_authorization(new_configuration, approval): Changes approval credentials only through the currently authorized transition procedure. Possession of a classical signing key alone MUST NOT authorize rotation.
138. migrate_authorized_vault(target, migration_parameters, approval): Permits migration only through an owner-authorized procedure that preserves the applicable protection policy and prevents downgrade.

These are logical interfaces. A deployment MAY incorporate them into existing handlers rather than expose separate functions. For an extension-enabled deployment, the existing `recover(...)` interface MUST enforce the same release conditions as `execute_authorized_transfer(...)`; its `proof` parameter MUST include or securely reference the required PQ approval.

Uniform enforcement. Every route capable of releasing assets or changing release authority MUST preserve PQ-1–PQ-4. This includes whitelist changes, token allowances, delegated execution, upgrades, emergency functions, retirement and contract-destruction mechanisms where supported. Unsupported routes MUST be disabled. No legacy interface may remain as a classical-signature-only alternative.

Failure and execution semantics. Missing, invalid, expired, replayed or context-mismatched approvals MUST fail closed. Verifier failure MUST NOT trigger classical-only fallback. The chain-specific annex MUST define execution and replay-state transitions, including safe retry, asynchronous execution and partial-failure handling, so that one approval cannot authorize duplicate asset release.

Events and privacy. Evidence MAY record an action identifier, policy version, verifier identifier and execution outcome. Events, logs and operational records MUST NOT contain private keys, secret shares, secret-bearing note images or material sufficient to reconstruct signing credentials. Public verification artifacts remain subject to the deployment's evidence and privacy policy.

5.2 Security properties

5.2.1 Core invariants (must hold in every deployment)

Invariant 1 — Transaction authorization only to owner-bound destinations

Redeem of assets from the note wallet MUST be restricted to the owner-bound destination defined at creation time, using one of:

139. pre-committed owner address,
140. whitelist,
141. or proof-of-ownership policy.

Requirement: Any transaction that attempts redeem to an unbound destination MUST fail deterministically.

Invariant 2 — No hidden admin drain routes

There MUST be no privileged function that allows PrintDreams, a partner, or any administrator to:

142. move user assets from note wallets,
143. override owner binding,
144. or redirect funds without the owner satisfying the transaction authorization policy.

Requirement: If any privileged keys exist (e.g., for upgrades), they must not be capable of moving user funds or altering redeem destinations in a way that enables confiscation or redirection.

Invariant 3 — Explicit upgradeability policy

The deployment MUST declare one of the following policies:

Policy A: Non-upgradeable (preferred for trust-critical contracts)

145. Contracts are immutable; fixes require deploying new contracts and migrating via explicit user action.

Policy B: Upgradeable with strong controls If upgradeability is required (e.g., chain constraints or partner requirements), the system MUST define:

146. who controls upgrades (multi-sig, governance),
147. timelocks,
148. public announcement requirements,
149. audit requirements for new versions,
150. and a rollback/disable mechanism.

Requirement: Upgrades must not introduce a pathway to break Invariant 1 or Invariant 2.

Enforcement boundary. The chain-specific annex MUST enumerate all spend-capable, delegated, upgrade, emergency and migration paths. A restriction implemented only in an app or signer does not enforce owner binding against an adversary who has obtained K and can sign through another route. Assets may be described as protected against that route only when an independent enforceable policy and adversarial tests establish the property.

For an EVM deployment, the annex MUST enumerate EIP-7702 authorization tuples, delegated code, token approvals and permits, smart-account executor or owner roles, upgrades and emergency routes. Unsupported account-code delegation, arbitrary digest signing and multi-nonce authorization batches MUST fail closed in the isolated signer before factor ingestion. An exception requires a specific approved profile, independent review and equivalent owner-bound controls [R32, R36].

A check confined to the signer cannot prevent an attacker who obtains an EOA's K from authorizing a delegation or transaction through another interface. A claim of protection against that case requires assets to be held under an independently enforceable policy that constrains all relevant release, executor, approval and administrative paths; the annex must demonstrate this property on the actual chain. PQ-1–PQ-4 continue to apply where the separate post-quantum extension is enabled.

5.2.2 Administrative roles (if any)

If any roles exist (strongly discouraged unless necessary), they MUST be defined explicitly:

151. UpgradeAdmin (multi-sig only; timelocked)
152. TokenVerifierAdmin (if allowlist exists; multi-sig)
153. EmergencyPause (optional; see below)

Emergency pause (optional): An emergency pause may be allowed only if:

154. it cannot seize funds,
155. it is narrowly scoped (e.g., pause new note registrations, not transaction authorizations),
156. it has clear criteria and expiration rules,
157. and it is disclosed to partners/users.

5.2.3 Audit and verification requirements

For any deployment using custom contracts:

158. at least one independent security review MUST be completed pre-production,
159. critical/high issues MUST be remediated and re-tested,
160. and the audit report (or executive summary) MUST be available to integration partners under NDA.

5.2.4 Additional invariants for post-quantum-enabled deployments

These invariants supplement §5.2.1 and §5.5. They are mandatory for any deployment claiming conformance with the post-quantum authorization extension; they do not describe the current implementation status of baseline v1 deployments.

Invariant	Required property
PQ-1 — No classical-signature-only release	The vault MUST NOT release protected assets on the strength of a classical signature alone. Every release MUST also satisfy the registered post-quantum owner-approval policy, destination restrictions and applicable operational limits. Missing or invalid PQ approval MUST cause rejection.
PQ-2 — No privileged bypass	Upgrades, verifier replacement, emergency actions and administrative changes capable of affecting asset release MUST preserve authorization protection at least equivalent to the active PQ policy. No such path may remove the PQ requirement, substitute an unauthorized approval key or enable asset redirection. A classical multisignature or timelock alone does not satisfy this invariant.
PQ-3 — No reconstructable signing material in evidence	Events, logs, telemetry, support records and audit artifacts MUST NOT contain private keys, secret shares, secret-bearing note images or material sufficient to reconstruct signing credentials. Public verification artifacts may be retained under a defined evidence and privacy policy. This requirement applies across contracts, devices, SDKs and operational systems.
PQ-4 — Authorized migration without downgrade	Key rotation, algorithm changes and contract migration MUST preserve owner authorization, destination binding and replay protection. They MUST NOT introduce an intermediate or fallback state permitting weaker authorization. Obsolete credentials and policy versions MUST cease to authorize actions after the defined transition; failed migration MUST leave assets subject to an enforceable protection policy.

5.3 Failure modes

This section describes expected behavior under adverse conditions. A deployment must document exact outcomes for each chain and integration model.

5.3.1 Chain congestion / high fees / delayed finality

Risk: Transactions may be delayed, fail, or become expensive.

Expected behavior:

161. Transaction authorization attempts may remain pending until included in a block.
162. Wallet UX MUST show:
163. pending state,
164. estimated fee impact,
165. and a safe retry workflow that avoids duplicate conflicting transactions.
166. If redeem is “sweep-all,” the UX MUST prevent repeated attempts that could create partial state confusion.

Mitigations:

167. Use fee estimation with conservative buffers.
168. Provide deterministic idempotency in contract logic (e.g., once recovered, subsequent recover calls fail or no-op).
169. Provide user guidance for network congestion scenarios.

5.3.2 Partial transactions / interrupted workflows

Risk: The workflow may be interrupted after some steps succeed:

170. Issuance created but not funding-eligible.
171. Premature external deposit or legacy-funded state, despite the normal funding gate.
172. Printing completed but the public verification or secret-cleanup evidence is missing.
173. transaction authorization initiated but not completed.

Expected behavior:

174. The system MUST define safe state transitions and rollback guidance:
175. If not funded and issuance is interrupted or voided: quarantine the unit and follow the approved cleanup and reissuance procedure; do not mark it STORED.
176. If an external party deposits funds prematurely or a legacy-funded print fails, treat the situation as an exceptional incident. Any transfer requires the authorized factors and policy; availability depends on a previously established valid authorization path.
177. If printing, public verification or secret cleanup fails or is uncertain: HOLD/VOID the unit, prohibit funding eligibility and reissue only under the controlled procedure.
178. Contracts (if used) SHOULD ensure state is consistent and queryable.

Mitigations:

179. The supported issuance workflow MUST NOT initiate funding before successful verification. Premature external deposits or legacy-funded states MUST be handled as exceptions under a documented procedure preserving owner authorization and applicable PQ controls.
180. Store minimal state marker in contract/registry to detect incomplete issuance.
181. Provide a support-assisted redeem procedure that never requires revealing secrets to PrintDreams, explicitly inheriting §5.3.3's prohibition on support reconstructing credentials or overriding authorization.

5.3.3 Lost note (user cannot access protection media)

Risk. Loss, destruction or unreadability of the physical note may prevent access to S1. In the owner-bound v1 profile, the note does not contain a possession-sufficient spending credential: authorized use also requires the independent owner factor and satisfaction of the applicable destination policy.

Expected behavior:

182. Loss of the note MUST NOT automatically enable asset transfer using S2, an owner-wallet signature or an administrator credential alone.
183. Where no usable, previously established redundant protection instrument exists, the required authorization may be impossible and assets may remain permanently inaccessible. This consequence MUST be disclosed before funding.
184. Support personnel MUST NOT request secret shares or signing credentials, reconstruct authorization material, or override the owner authorization policy.
185. A report of a lost note does not itself establish authority to change destinations, replace approval keys or release assets.

Mitigations:

186. Where the deployment supports redundancy, establish and verify redundant protection instruments before funding. Their storage MUST preserve separation from S2 and avoid a common compromise domain. Additional copies increase physical exposure and MUST be covered by the deployment's security policy.
187. A redundant instrument MUST satisfy the same authorization and destination requirements as the original. Its existence MUST NOT create a weaker spending path.
188. If a valid authorization path remains available and compromise is suspected, use that path to transfer assets to an authorized protected destination and complete the documented re-issuance or credential-rotation procedure. Merely printing a replacement note does not invalidate the missing note.

Fallback restrictions:

Any time-locked or other fallback procedure MUST be specified before funding, independently reviewed and consistent with the invariants in §5.2.1 and §5.5. Expiry of a waiting period, identity verification or support approval alone MUST NOT substitute for the required owner authorization factors or create an administrative drain route.

For deployments adopting §5.6, every fallback, replacement and re-issuance path MUST additionally satisfy PQ-1–PQ-4. Loss of the physical note or PQ approval capability MUST NOT enable classical-signature-only withdrawal, unauthorized approval-key replacement or downgrade of the active protection policy. Where no conforming authorization path remains, the system MUST retain the protection policy and disclose the resulting unavailability.

5.3.4 Compromised owner wallet

Risk: If the Owner Wallet is compromised, an attacker may satisfy owner-binding controls (e.g., sign proofs) or receive recovered funds.

Expected behavior:

189. Owner-binding does not protect against compromise of the owner itself.
190. If the owner wallet is compromised, transaction authorization may send funds to an attacker-controlled address.

Mitigations:

191. Partner wallets should support stronger owner security (PIN/biometrics, secure enclave signing where available, device attestation).
192. Provide user guidance: if owner wallet compromise is suspected, migrate funds and re-issue note wallets immediately.
193. Consider allowing whitelist binding to multiple owner addresses where users maintain a "backup owner" device (with strict UX and education).

5.4 Deployment placeholders (must be completed for any production release)

Each production deployment MUST publish a chain-specific annex completing the following items:

194. Deployment identity: Supported chain and network; supported assets; contract addresses; deployed code versions; and applicable SDK, firmware and note-format versions.

The deployment annex must also identify SIT and printer firmware versions and pair credentials, independent S2 custody, public print-check qualification, the signer build, the asset-control enforcement boundary, and chain, bridge, token and destination dependencies.

195. Interfaces: Final ABI or message formats, including chain-specific execution, finality, retry and failure semantics.
196. Owner binding: Enforcement mechanism, authorized destination policy, enrollment procedure and rules for destination changes.
197. Upgradeability: Immutable or upgradeable configuration; authorities; approval requirements; timelocks where applicable; and restrictions preventing administrative asset seizure or redirection. For EVM profiles, record permitted delegation and executor configurations, relevant code and permissions, and test evidence for direct-key and alternate-interface bypasses [R36].
198. Emergency and lost-factor procedures: Permitted actions, authorization requirements, operating limits and disclosed consequences where authorization factors are unavailable.
199. Assurance: Auditor, review date, report identifier, reviewed configuration and remediation status.

5.4.1 Additional requirements for the post-quantum authorization extension

Every deployment MUST state its PQ-extension status: not enabled, experimental/test-only, or production-enabled for the specified configuration. A baseline deployment MUST NOT imply conformance with §5.6.

Before production enablement, the annex MUST additionally specify:

200. Enforcement boundary: The asset-holding vault and every mechanism capable of releasing assets or changing release authority. Wallet-interface checks or off-chain approvals alone do not satisfy the extension.
201. Cryptographic profile: PQ signature algorithm, parameter set, key and signature encodings, approved verifier implementation and any intermediary verification dependencies.
202. Credential lifecycle: Generation, initial enrollment, independent protection, isolated use, rotation, revocation and erasure of PQ credentials; changes to S1/S2 handling or note formats; and evidence that disclosure of the classical signing key does not disclose or permit replacement of PQ credentials.
203. Approval and replay rules: Authenticated action fields, domain separation, nonce handling, validity conditions, policy-version enforcement and duplicate-execution prevention.
204. Migration and emergency controls: Authorized transition procedures; destination-vault qualification; invalidation of superseded permissions; failure handling; and evidence that no upgrade, emergency or fallback route permits classical-only release or downgrade.
205. Dependencies and limitations: Destination protection, blockchain and consensus assumptions, token-administrator powers, bridges where used, firmware trust anchors and communications security.
206. Operational feasibility: Signature and payload sizes, verification cost, device resource requirements, execution limits, availability risks and safe behavior when the verifier or required infrastructure is unavailable.
207. Conformance evidence: Test and review references for PQ-1–PQ-4, including classical-key-compromise, replay, unauthorized enrollment, privileged-bypass and migration-downgrade tests.

All applicable fields MUST be resolved before production enablement. An unresolved item MUST NOT be treated as an assumed security property. Any “not applicable” designation MUST include its technical justification.

5.5 Research-derived security invariants

Invariant	Required property
I-1 Possession separation	No valid redeem path accepts S1 without the threshold owner factor.
I-2 Destination binding	Transaction authorization output is restricted to the committed owner policy unless a separately authenticated rotation procedure has completed.
I-3 No administrative drain	No PrintDreams, partner or upgrade role can unilaterally redirect or seize note wallet assets.
I-4 Domain separation	Signatures and commitments bind chain ID, contract/account type, asset, note format version and transaction authorization -policy version.
I-5 Replay resistance	A transaction authorization cannot be replayed across notes, chains, states or destinations.
I-6 Monotonic state	Created -> Funded -> Stored -> Recovered -> Retired transitions cannot be reversed without a complete re-issuance process.
I-7 Fail closed	Malformed shares, ambiguous transaction display, unavailable policy state or inconsistent commitments abort before signing.
I-8 Privacy minimization	On-chain state contains no private share, plaintext identity or unnecessary serial-to-owner linkage.

Each production chain annex must translate these logical invariants into executable tests, chain-specific message formats and audit assertions.
Deployments adopting the post-quantum authorization extension must additionally satisfy PQ-1–PQ-4 in section 5.2.4.

5.6 Post-Quantum Authorization Extension

Stablenotes proposes quantum resilience as an extension of its existing owner-bound security architecture. The extension preserves physical-factor separation, independent owner authorization, isolated signing and secret-free evidence, while adding a post-quantum approval requirement to the asset-control path. It is a proposed deployment profile subject to implementation, chain-specific feasibility assessment and independent assurance.

The baseline separation of signing material into S1 and S2 reduces exposure through individual storage or processing domains. It does not prevent an adversary with a sufficiently capable quantum computer from deriving a vulnerable classical private key from its exposed public key. Consequently, protection of secret shares alone cannot establish quantum resilience where the underlying account permits asset movement using that classical key.

The proposed extension introduces a compatible smart-contract vault that enforces a post-quantum approval policy alongside the classical transaction-signing process. Protected assets MUST reside within an enforcement arrangement that cannot be bypassed through direct classical-key withdrawal, delegated spending permissions, alternate execution routes or privileged contract changes. A valid classical

transaction remains necessary where required by the selected network but is insufficient to release protected assets.

The independent authorization workflow MUST produce a PQ approval bound to the intended action. Its authenticated context MUST identify the chain, vault, asset, amount, owner-bound destination, operation type, nonce, validity conditions and applicable policy version. The vault MUST verify this approval and consume its replay protection consistently with successful execution. An off-chain approval record or a verifier response secured only by a quantum-vulnerable classical signature does not establish the required enforcement boundary.

PQ approval credentials MUST remain secure even if the classical signing key is disclosed or mathematically derived. They MUST NOT be recoverable solely from that classical key. Their generation, enrollment, physical-factor representation, independent owner-factor protection, isolated use and erasure require a separately reviewed design. Enrollment and rotation MUST prevent an adversary holding a compromised classical key from registering a replacement PQ approval key. The chain-specific annex MUST define any changes required to note formats, devices and signing workflows.

Algorithm selection SHOULD evaluate standardized post-quantum signature schemes, including ML-DSA and SLH-DSA, against device resources, signature size, verification cost and implementation risk. Selection of a standardized algorithm alone does not establish security of the complete deployment. Any intermediary proof or verification mechanism MUST be assessed for its own quantum-security assumptions.

The extension MUST satisfy PQ-1–PQ-4 in section 5.2.4. Before production use, independent review MUST test classical-key compromise, approval replay and substitution, unauthorized key enrollment, verifier failure, upgrade and emergency bypasses, and migration downgrade. The deployment annex MUST identify supported configurations, performance limits, residual risks and assurance evidence.

This extension does not make the underlying blockchain, communications infrastructure, firmware update chain or destination account quantum-resistant. Continuing protection after an owner-bound transfer requires a destination with suitable authorization controls. Claims MUST remain limited to the reviewed configuration and verified security properties. The extension retains the owner-bound, non-bearer scope of Stablenotes v1.

6 Security and Assurance

Stablenotes is a security product before it is a convenience product. The assurance case is not that physical media is universally safer than digital custody. It is that a passive, owner-bound factor can remove one authorization component from direct network reach and distribute transaction authorization across independent failure domains. That proposition is valid only when cryptography, ingestion, media and operations are evidenced together.

6.1 Security model overview

6.1.1 Security objectives

208. Unpredictable generation of K and all random sharing coefficients
209. Information-theoretic secrecy below the selected share threshold

210. Independent storage and transaction authorization of S1 and S2
211. No direct network interface on the passive substrate
212. Authenticated transaction display and chain-specific offline signing
213. No secret retention or telemetry
214. Durable, verifiable physical encoding
215. Owner-destination enforcement
216. Bounded and disclosed residual risk

The common issuance boundary is a critical security dependency: weak entropy or compromised issuance firmware can expose the reconstructed secret despite subsequent separation of the factors. Secure signing and physical custody cannot retroactively repair weak K [R25].

6.1.2 End-to-end compromise model

$$P(compromise) <= eps_{generation} + eps_{S1} + eps_{S2} + eps_{ingestion} + eps_{policy} + eps_{operation}$$

The terms are not assumed independent, and no numeric upper bound is claimed without evidence. The expression is an assurance-accounting device: each term must map to a defined threat, test method, owner and residual-risk decision.

6.1.3 v1 versus v2 assurance boundary

v1 is owner-controlled transaction authorization with possession/authorization separation. v2 bearer transfer remains future-gated and requires copy-without-open, reseal, swap, counterfeit and field-deception testing. Research-derived owner binding is a v1 requirement; bearer-transfer resilience is not.

6.2 RNG and Key Generation Assurance

6.2.1 Purpose and scope

This section defines the minimum requirements for entropy and random-bit generation used by the production Secure Issuance Terminal to create K, S1 and other security-critical random values. Any separately approved demo or partner profile must document and qualify its own entropy path.

A weak RNG invalidates the entire security model, regardless of device certification, printing quality, or tamper evidence.

6.2.2 Security objectives

The system must ensure that generated private keys are:

217. Cryptographically random (high entropy, no predictable patterns)
218. Unbiased (no systematic skew in output)
219. Non-repeating (no duplicate keys across devices/sessions)
220. Not retained (no logging, caching, or persistent storage outside intended user-controlled output)
221. Safely erased from memory after use

6.2.3 Implementation requirements

6.2.3.1 Approved entropy and DRBG. The selected SIT hardware, entropy source, health tests, DRBG construction, instantiation, reseeding and failure behavior MUST be documented and independently assessed for the exact board revision, firmware and build configuration.

222. The SIT MUST fail closed when entropy, health tests, initialization or security configuration cannot be verified; it must not fall back to a predictable software generator.
223. For separately approved mobile-only demonstrations, platform cryptographic APIs may be used only under a documented profile and must not be presented as the production SIT entropy path.

6.2.3.2 Seeding and supplemental entropy. The implementation must not:

224. seed RNGs manually using timestamps, device IDs, usernames, or any predictable values
225. accept supplemental or user-provided entropy unless its collection, combination, error handling and effect on the approved DRBG are documented and independently reviewed.
226. Isolated key-generation path. Production K and both shares are created inside qualified SIT memory without analytics, debug logging, crash payloads, clipboard use, ordinary online services or uncontrolled background handoff.

6.2.3.4 Immediate post-generation handling. After generation, key material must:

227. be used only for the intended workflow (e.g., note creation / transaction authorization media encoding)
228. pass the required public-key QR, checksum, serial and process-qualification checks before funding eligibility
229. be cleared from memory as soon as the workflow is complete or aborted

6.2.3.5 Secure erase behavior definition. The implementation must define and document:

230. which buffers may contain key material
231. how those buffers are zeroized
232. when zeroization is triggered (success, failure, cancel, crash redeem path)

Note: “Secure erase” in application memory is best-effort and platform-constrained; this limitation must be disclosed.

6.2.4 Prohibited practices

233. Predictable seeding, undocumented custom RNGs, unapproved fallback generators and build configurations that bypass the qualified entropy source.
234. Logging key material or derived secrets
235. Persisting keys in app storage “temporarily” (Temporary persistence)
236. Sending private keys to backend services
237. Running key generation in instrumented/debug builds outside controlled test protocols
238. Using clipboard for private key transport

6.2.5 Standards alignment

The RNG design and assurance process should be documented in terminology aligned with:

239. NIST SP 800-90A/B/C (DRBG, entropy source, construction)
240. FIPS 140-3 concepts for cryptographic module assurance (where applicable)
241. ISO/IEC 18031 (random bit generation)
242. BSI AIS 20/31 (RNG evaluation guidance, especially relevant in Europe)

Full certification is not required at launch, but the design should be explainable against these frameworks.

6.2.6 Validation and testing

243. Independent review of entropy-source design, boot and compiled binary, library linkage, build flags and failure paths.
244. Runtime instrumentation
245. Statistical sanity checks (supporting only)
246. Duplicate-key monitoring

6.2.7 Acceptance criteria (ship gate)

247. Ship gate: the exact production build and hardware must pass the documented entropy and DRBG assessment, health-test and fault-injection requirements, independent review and key-generation interoperability vectors. Statistical checks alone do not establish entropy.

6.2.8 Evidence artifacts

248. RNG design, code review, non-retention tests, duplicate-key SOP

Cross-references:

249. Secret handling lifecycle → 6.3
250. Partner integration controls for SDK use → 6.7.4

6.2.9 Secret-sharing entropy requirements

Entropy assurance covers K, XOR pads, Shamir coefficients, nonces and any randomness used for share authentication. NIST SP 800-90B addresses entropy sources; SP 800-90A addresses deterministic generators. A component should not be described as 'NIST-compliant' merely because it contains a physical noise source. Validation requires design documentation, health tests, entropy assessment and independent evidence.

Incident response for weak issuance entropy. If a generated K may be predictable, disable affected issuance, identify the impacted configuration and cohort, and migrate value to newly generated and verified authorization units under the approved owner policy. A firmware update alone does not repair previously generated weak keys [R25].

6.3 Key Non-Retention and Memory Hygiene

This section governs transient secret handling across the SIT, its authorized printer interface, physical outputs, the independent S2 handoff and the isolated signer. Ordinary online wallet and partner backends are outside the permitted Class A boundary.

This is a core security control. Even with strong RNG, a retained key (in logs, storage, telemetry, crash dumps, or memory remnants) can result in total fund loss.

6.3.1 Security objectives

Private keys and secret material must be handled as ephemeral data. The system must ensure that secrets are created only when needed, exist in memory for the shortest possible time, are never written to persistent storage unless explicitly required by the user-controlled security model, are never included in logs, telemetry, analytics, crash reports, or debugging tools and are zeroized or invalidated immediately after use (subject to platform constraints).

6.3.2 Threats addressed

This control mitigates accidental leakage via app logs, crash-dump leakage, telemetry/analytics exfiltration, temporary-file leakage, clipboard leakage, background task or inter-process communication (IPC) leakage and memory scraping on compromised devices (partially mitigated; not eliminated).

6.3.3 Data classification model

251. Class A (critical secrets such as private keys, mnemonics/seed phrases, raw entropy bytes, unencrypted key export buffers)
252. Class B (sensitive non-secret such as public addresses, transaction metadata and note identifiers (if not directly linkable to private keys)
253. Class C (operational such as: UI events, performance metrics, non-sensitive diagnostics)

6.3.4 Implementation requirements

No unauthorized persistence. K and transient S1/S2 copies must not be stored in files, printer job histories, caches, backups, analytics or crash artifacts. The protected printed S1 and the separately approved owner-controlled S2 custody representation are intended outputs under explicit access and retention controls.

No secret logging. The application and SDK must not log raw private keys, mnemonics, entropy, encoded key payloads, QR contents containing secrets. This applies to production logs, debug logs, analytics events, error traces and third-party SDK telemetry.

Memory minimization. Secret material must be allocated in as few buffers as possible, copied as few times as possible, kept in scope for the shortest possible duration. Developers must avoid string conversions of secrets (immutable strings are hard to sanitize), unnecessary serialization/deserialization, passing secrets through generic logging or exception wrappers

Zeroization / invalidation. Where platform/language permits, buffers containing Class A secrets must be actively cleared after use. Documentation must specify which buffers are cleared, by what method and at what lifecycle event (success, cancel, error).

Where secure zeroization is not fully guaranteed (e.g., managed runtimes), the implementation must minimize copies, use mutable buffers, reduce object lifetime and explicitly disclose residual risk.

Clipboard prohibition. Class A secrets must never be copied to or through the system clipboard in production workflows.

Background/interrupt behavior. If the app is backgrounded or interrupted during a sensitive workflow, then active secret buffers must be invalidated or cleared, sensitive screens must be redacted from app switcher previews (where supported) and the workflow must require explicit user re-entry or restart.

Crash reporting and diagnostics must use allow-listed Class C fields only; secret-bearing memory dumps, print rasters, readable S1/S2 images and sensitive context are excluded from all devices and partner services.

IPC / bridge restrictions. Secrets must not be passed through deep links, URL schemes, push notifications, webviews, JavaScript bridges and untrusted IPC channels.

6.3.5 SDK-specific partner requirements

The SDK must provide a documented "secret-safe" API surface (no APIs that encourage persistence/logging), integration guidance for partner apps on telemetry redaction and crash configuration and a compliance checklist for partners to confirm they are not retaining secrets in their own layers.

This is essential for an SDK-first option, because partner integrations can reintroduce leakage even if Stablenotes code is clean.

6.3.6 Validation and testing

Static analysis and code review. Independent review must verify that there are no secret logging paths, no persistence paths for Class A data, no clipboard or unsafe IPC use and that controlled lifecycle of secret buffers is in place.

Runtime leakage tests. Controlled test builds need to be implemented to verify secrets do not appear in local storage, caches, crash reports, analytics payloads and debug consoles.

Crash, interruption and power-loss tests must cover SIT generation and splitting, paired printing, printer buffers, S2 handoff and signer operation. Any unverified print completion remains HOLD/VOID and must not trigger an automatic secret reprint.

Background/interrupt testing. Simulation is needed for app backgrounding, incoming calls, OS task switching and low-memory events.

Third-party SDK audit. Inventory of all third-party SDKs needs to be made to verify none can capture Class A data via auto-screen capture, session replay, verbose error logging and analytics parameter scraping.

6.3.7 Acceptance criteria (ship gate)

Non-retention and memory hygiene controls are production ready only if independent review confirms no secret persistence or logging paths, runtime tests show no Class A leakage in storage, telemetry, or crash reports, interrupt/crash-path behavior is tested and documented, third-party SDK risk review is completed and any unsafe SDKs are removed or sandboxed and partner integration guidance (for SDK customers) is published

6.3.8 Evidence artifacts

254. Classification policy, code review, leakage tests, SDK guide

Cross-references:

255. RNG source and key creation → 6.2
256. Partner certification requirements → 6.7.4
257. Incident response classification → 6.7.5

6.3.9 Share non-retention and factor independence

K, S1 and S2 may coexist transiently only in the approved SIT issuance boundary and Isolated Signer reconstruction boundary. No unapproved persistence or copying is permitted in printer buffers, spool files, radio interfaces, camera caches, logs, crash reports or partner backups. The release must document and test each secret entry, transfer, deletion and residual-memory path.

6.4 Print Survivability and Key Legibility

This section defines the requirements for ensuring that printed transaction authorization media (QR code + human-readable backup text) remains readable and recoverable over the intended service life under normal handling and storage conditions.

This is a core security requirement. If a private key becomes unreadable, funds are effectively lost even if no attacker is involved. Therefore, is also extremely important that no other substrate is used except authorized notes shipped along with the device and offered as an after-market consumable.

6.4.1 Purpose and scope

Ensure printed transaction authorization media remains recoverable over intended service life and ensure that only genuine notes are used for the imprints as this narrows down the critical combination ink + substrate (ink properties can change dramatically over different substrates).

6.4.2 Security and reliability objectives

Scannable, legible, stable, creation-time verifiable, batch-consistent

6.4.3 Threats and failure modes addressed

Smudging / abrasion from handling, water damage / humidity swelling, UV fading / thermal degradation, chemical staining (sweat, sanitizer, beverages, detergents), adhesive migration from tamper stickers, low-contrast or misaligned prints, QR corruption from creases/folds, “Looks fine but won’t scan” failures (poor scan behavior), printing in other media than the authorized.

6.4.4 Media design requirements

The front contains the S1 QR over its obfuscated area followed immediately in the same printing movement by the public-key QR. The back contains the human-readable S1 representation over a second obfuscated area followed immediately by its checksum. Both S1 encodings are Class A and remain protected; the public QR and checksum support non-revealing verification of the qualified print process.

If the S1 QR is unreadable but the protected fallback is legible, the fallback supplies S1 only. Authorization still requires the independently controlled S2 factor and the applicable owner-bound policy.

QR constraints (ECC, module size, quiet zone, contrast). The QR format must define and fix error correction level (ECC), minimum module size, quiet zone margin, contrast ratio target, and placement tolerances by means of using a guidance ruler.

The QR design must be validated against a supported device matrix (camera quality + OS versions).

Fallback text constraints (checksum, readability). Fallback text must include checksum or integrity marker, typography and spacing optimized for readability, contrast and font size minimums AND rules for avoiding ambiguous characters (e.g., O/0, I/l)

Redundancy requirements. The system should implement at least one redundancy mechanism, such as duplicate QR in separate area, segmented encoding, redundant text blocks, transaction authorization code split with checksum. If no redundancy is used, the rationale and risk acceptance must be documented.

Tamper-sticker compatibility. Adhesive chemistry and sticker coating must be qualified for long-term compatibility with the ink and substrate. Adhesive migration must be characterized. The sticker must not reduce readability below acceptance thresholds over service life. Opening/removal behavior must be characterized (tearing, residue, visibility).

6.4.5 Printing process requirements

Controlled print pipeline. The printing process must define the printer model(s) and firmware versions (or approved classes), print resolution and calibration settings, media handling conditions (temperature/humidity range) and consumable specifications (inkjet cartridge lot controls, note batch controls).

Post-print verification gate. On every issued note, the SIT scans the public-key QR printed immediately after the front S1 encoding, compares it with the approved public identity and validates the note serial and job context. On the back, the operator enters the checksum printed immediately after the human-readable S1 representation; the SIT validates it against the expected issuance value. The protected S1 areas remain obscured during these checks.

These checks rely on the proximity and common printing movement of each public indicator and its protected encoding. A successful public-key scan or checksum validation verifies that indicator and its expected context; it does not independently decode S1 or cryptographically prove that every protected character was correctly printed. Before live-value release, qualification MUST demonstrate the strength of the correlation for the exact printer, media, ink, obfuscation and handling profile, including localized defects and interrupted swipes. The institution accepts the defined residual risk in its approved deployment annex.

Qualification uses controlled non-funded synthetic factors, never production secrets. Test samples compare the actual front S1 decode and back human-readable transcription against expected values after the normal print and opening process. Inject and classify partial print, nozzle dropout, local smearing, alignment, sticker, interrupted motion and serial/job substitution failures. Measure cases in which public checks pass but the protected encoding fails; predefine the maximum acceptable missed-defect rate, sampling plan, confidence level, independent reviewer and escalation procedure. A failed check, unqualified configuration or uncertain print result prevents funding eligibility.

If public verification, checksum, job completion or qualification fails, the note must be held or voided, no funding eligibility may be issued, and cleanup and reissuance must follow the controlled incident procedure.

Batch QA and rejection logging. Production and pilot printing must include batch sampling, print contrast checks, alignment checks, scan-rate checks and rejection logging by defect type.

6.4.6 Durability test program

The durability qualification program must follow as a minimum the DIN ISO 14145 Standard. It was originally developed for long-term archivability of documents (Part 2: documentary use DOC) containing

text and signatures done with roller ball pens (and corresponding refills) but it can be considered highly relevant for the purpose of qualifying the note product and imprint process.

Samples must be tested in a standard atmosphere 23/50 in accordance with DIN EN 20187, i.e. at an ambient temperature of (23 +/-1) oC and a relative humidity of (50 +/- 2) %.

Mechanical wear. Includes erasure resistance, dry rub / abrasion, repeated handling, folding / crease cycles and edge wear

Moisture / water. Test samples must be exposed to splash and wiped after moisture exposure. Test must include humidity cycling and short-duration water exposure or water resistance.

Thermal / UV aging. Includes elevated temperature exposure, temperature cycling, UV exposure / light aging and lightfastness up to level 5.

Chemical exposure. At minimum test is needed against common-contact substances: skin oils / sweat simulation, hand sanitizer, detergent/soap residue and common beverages (water, coffee, soda). Standarized DIN ISO 14145 test rounds should include ethanol resistance, hydrochloric acid resistance, ammonium hydroxide resistance and bleaching resistance.

Sticker/adhesive aging. adhesive migration, edge lift, residue formation and interaction with ink and substrate under heat/humidity aging

6.4.7 Acceptance criteria (ship gate)

The print survivability system is production ready only if all following conditions are met:

Creation-time verification pass. Every note must pass the public-key QR identity/serial check and back-checksum check. The protected S1 areas remain obscured; the associated print process and its false-acceptance rate must be independently qualified before live-value use.

Post-stress QR readability threshold. After durability tests, QR scan success must meet a defined threshold across a supported device matrix (e.g., threshold set by product requirements and test protocol).

Post-stress fallback legibility threshold. After durability tests, fallback text must remain legible and checksum-valid at the defined threshold.

Batch consistency. QA sampling demonstrates print quality remains within tolerance across lots and devices.

Sticker compatibility threshold. No adhesive or tamper component may reduce readability below threshold during the claimed service life.

6.4.8 Supported device matrix

The supported verification matrix must cover the actual SIT camera for public indicators, the Isolated Signer camera for protected-factor use, approved verifier equipment and environmental conditions. Mobile devices are included only for an explicitly approved profile.

258. SIT public-QR camera and exact software build
259. Isolated Signer camera and factor-decoding build
260. Approved mobile devices and OS versions only where the profile permits them

261. typical lighting conditions

The matrix must be reviewed periodically and updated as devices/OS versions change.

6.4.9 User handling guidance and replacement policy

The product includes plain-language guidance covering:

262. why to avoid printing in substrates other than the supplied notes
263. how to store the note
264. what to avoid (moisture, direct heat, chemicals, abrasion)
265. what to do immediately if damage occurs
266. how to verify readability periodically (optional recommended check)
267. when to replace/re-issue the transaction authorization media

On top of the handling guidance, a replacement policy must be clearly defined and documented:

268. replacement procedure for damaged but still-recoverable notes
269. support process for partial legibility failures
270. escalation path for “unreadable note” incidents
271. whether any warranty applies (and its limits)

This policy is part of product safety, not just customer support.

6.4.10 Validation and testing evidence

Independent lab report. An external lab must test the defined matrix and report conditions, sample sizes, failure rates, scan/legibility outcomes, pass/fail against acceptance criteria and requirements met or not met.

Internal QA validation. Internal QA must demonstrate repeatable print quality across batches, defect classification plus rejection workflow and traceability of materials and consumables

Field validation cohort (recommended before scale-up). A controlled field cohort must be executed to capture real handling behavior, scan failures by device model, environmental failure patterns and replacement rates.

6.4.11 Evidence artifacts

272. Media spec, durability protocol, lab report, QA report, user guide

Cross-references:

273. Tamper-layer compatibility → 6.5.4
274. Partner support responsibilities → 6.7.3 and 6.7.5

6.4.12 Research-derived durability qualification

BoPET and ink-receptive coatings are candidate materials, not evidence of a specific service life. Claims such as -50 C to +180 C operation, complete moisture impermeability or complete UV shielding are excluded until the complete ink/substrate/adhesive/encoding stack passes a defined protocol. Accelerated aging must state its correlation model to real-time aging and report uncertainty.

6.5 Tamper Evidence and Adversarial Access

6.5.1 Purpose and scope

This section defines the requirements for tamper evidence and resistance to adversarial access attempts against printed transaction authorization media and any tamper-evident resource (e.g., security sticker).

The goal is to clearly separate:

275. v1 (Cold Storage): minimum credible tamper-evidence claims for owner-controlled transaction authorization media
276. v2 (Bearer/Transfer use): much stronger adversarial-transfer claims required before any transactional/bearer product launch

This prevents over-claiming in v1 while preserving a rigorous path to v2.

The use of a tamper-evident security sticker already during v1 (Cold Storage) might be considered overkill since the transaction authorization media is fully owner-controlled. However, the introduction of a security sticker already during v1 fulfils two main objectives:

277. Opening or tamper evidence indicates that a physical factor may have been exposed; it does not prove a transfer occurred or that the wallet is empty. Settlement and balances must be independently verified before retirement.
278. It enables the deployment and testing of tamper-evident characteristics of the security sticker under real life conditions and on a bigger scale before moving forward to a transactional product (v2).

The scope applies to printed transaction authorization media carrying secret material (QR and/or text), tamper-evident overlays (security sticker that includes VOID features and obfuscation layers), user verification cues (visual indicators, border text, tear evidence), packaging and handling steps that affect tamper evidence, adversarial testing protocols and acceptance thresholds

The scope covers unauthorized viewing attempts, partial opening / resealing, label replacement / swap, stamp off secret material to other surface (boiled egg attack), optical extraction attempts, residue and edge-lift attacks and counterfeit visual mimicry (v2 scope primarily).

6.5.2 Security objectives

The tamper system must provide defined, testable tamper evidence, not vague “anti-counterfeit” claims. At a minimum (v1), it must aim to ensure that secret material is not plainly readable before intended opening, that opening causes visible, irreversible evidence under normal inspection, that tamper evidence remains functional over the expected service life and that users can follow a simple verification checklist before transaction authorization.

For v2 (future), the bar is higher:

279. Practical read-without-open and reseal attacks are not feasible at meaningful rates
280. Field users can detect tampered notes reliably using simple procedures

6.5.3 v1 vs v2 claim boundary (critical)

v1 is owner-controlled transaction authorization media, not a bearer instrument. Tamper evidence in v1 supports owner confidence, not anonymous circulation.

281. v1 allowed claims: tamper-evident, obscures secret until opened, visible opening evidence under defined conditions.

282. v1 prohibited claims: counterfeit-proof, unforgeable, safe for bearer transfer, prevent all copying.

v2 — Bearer / Transfer (future-gated). v2 requires materially stronger claims and independent adversarial testing against hostile transfer scenarios. These claims should not appear in v1 marketing or deployment materials until validated.

283. v2 claims: only after adversarial testing and field validation

6.5.4 Threat model (tamper-specific)

The system design and tests must consider the following attacker classes:

A) Casual attacker

Attempts basic peeling, edge lifting, steaming, or light-based viewing using consumer tools.

B) Skilled attacker

Uses magnification, controlled heating, solvents, optical enhancement, micro-lifting, and resealing attempts.

C) Organized attacker (v2-critical)

Performs repeated tests with specialized tools, custom labels, and counterfeit reproduction workflows.

6.5.5 Material and design requirements (v1)

Obfuscation effectiveness (pre-open). When the sticker is used, the secret payload must be visually obscured or obfuscated prior to opening under normal viewing conditions. The design must define viewing conditions (lighting, angle), acceptable visibility threshold and prohibited leak-through (e.g., characters visible through obfuscation).

Irreversible opening evidence. Opening the tamper layer must create visible, irreversible evidence such as VOID pattern, edge text disclosure, delamination pattern and substrate damage / residue pattern. The evidence must be observable without specialized tools.

User verification cues. The product must include a simple “before opening” and “after opening” visual checklist including intact border alignment, intact tamper marks, no edge lift / bubbles / residue anomalies and expected opened-state pattern visible after opening.

Shelf-life compatibility. Tamper-evident behavior must remain functional over the claimed storage life so that the sticker must not self-lift, the obfuscation must not degrade and reveal text and so that the adhesive must not destroy print readability during normal aging.

Opening workflow guidance. The transaction authorization workflow must assume the note becomes higher-risk after opening: user should recover funds promptly, opened notes should be treated as

compromised for future long-term storage, guidance must instruct users not to re-store opened notes as "secure" and segregate them from closed notes.

6.5.6 v1 test program (mandatory pre-launch)

The v1 program must test edge lifting attempts (using manual tools), peel attempts under normal conditions, oblique-light viewing attempts, basic heat/humidity exposure impact on tamper behavior, adhesive aging and residue patterns, user inspection clarity (can normal users tell opened vs intact?).

The output should establish a baseline tamper-evidence claim only.

6.5.7 v2 adversarial test program (future-gated)

The v2 program must include independent red-team rounds covering controlled optical extraction attempts, chemical/thermal opening and reseal attempts, counterfeit sticker reproduction, note/sticker swap scenarios and field deception tests against actual user/agent SOP.

Before any bearer/transfer product launch, the system must additionally demonstrate:

Read-without-open resistance. Attackers cannot practically recover the secret without triggering visible tamper evidence.

Reseal resistance. Attackers cannot open, copy, and reseal in a way that passes field inspection at meaningful rates.

Counterfeit and swap resistance must be measured against a predefined acceptance threshold and test population; testing cannot establish that substitution is impossible in every circumstance.

Field deception tests against lay SOP. Non-expert users (or agents) can detect tamper/counterfeit indicators reliably using a short checklist.

6.5.8 Acceptance criteria

284. v1 ship gate: baseline tamper evidence consistency + usability
285. v2 gate: independent adversarial success rates below threshold

6.5.9 User guidance requirements

The product must include tamper guidance:

286. How to inspect the note before opening
287. What "opened/tampered" looks like
288. What to do if tamper is suspected
289. Why opened notes should not be stored long-term
290. How to safely proceed with redeeming after opening

This reduces support burden and prevents misuse.

6.5.10 Validation and evidence artifacts

Material compatibility report. Confirms sticker/adhesive/ink/substrate compatibility over aging and environmental conditions.

Tamper baseline test report (mandatory for v1). Documents attack methods attempted, sample sizes, visible outcomes, consistency of opening evidence and observed failure modes.

User inspection usability test report (mandatory for v1). Confirms users can identify intact vs opened samples using the provided checklist.

Independent adversarial red-team reports (mandatory for v2 only). Required before any bearer/transactional claims or pilots.

Cross-references:

291. Print/adhesive compatibility → 6.4.4 and 6.4.6
292. v2 roadmap gates → Chapter 12
293. Partner support scripts and claims control → 6.7.5 and 6.7.7

6.5.11 Coercion and possession-only theft

A stolen S1 yields no reconstruction advantage under a correct scheme, but a thief may coerce the owner or compromise S2. Higher-value profiles therefore require a policy package: value caps, delayed transaction authorization, geographic or organizational quorum, destination allowlists, incident escalation and a tested duress procedure. These are defense-in-depth controls, not cryptographic proofs.

6.6 Serialized Note/Device Supply Chain and Distribution Assurance

It should include:

294. serialization requirements
295. manifest and chain-of-custody controls
296. warehouse and retail controls
297. exception management
298. audit evidence

6.6.1 Purpose

Define a traceable, tamper-evident, low-complexity supply chain for Stablenotes note media (as an aftermarket consumable) and Mobile ATM device from factory → warehouse → distribution points → retail issuance.

The goal is not to copy a central bank. The goal is to borrow the useful parts such as serialization, chain-of-custody, tamper-evident packaging, reconciliation and exception handling.

That materially improves security without creating an unscalable cost structure.

6.6.2 Security objectives

This supply chain should support five concrete objectives:

299. Authenticity Only genuine Stablenotes media and devices enters partner channels.
300. Traceability Every note/device and every batch can be traced by serial number and batch ID.
301. Tamper detection Any carton/pallet opening, substitution, or missing inventory is detectable quickly.

302. Containment If a batch is compromised, stolen, or defective, it can be quarantined by serial range.
303. Operational accountability Every custody handoff is attributable to a person/entity and timestamped.

6.6.3 Asset classes

It is important for risk and cost to differentiate notes and devices.

Class N — Serialized blank transaction authorization media (default v1)

304. Pre-printed note media with unique serials
305. No stored value at shipment
306. Primary risk: counterfeit stock, quality drift, unauthorized substitution
307. First to scale

Class V — Serialized vouchers / pre-funded samples / Mobile ATM devices (higher risk)

308. Notes carrying promotional value (e.g., small USDT voucher)
309. Mobile ATM devices with starter-packs of blank notes inside
310. Primary risk: theft, fraud, abuse, consumer disputes
311. Requires tighter controls than Class N
312. Tightly controlled marketing pilot lane only

6.6.4 Simplified “banknote-like” supply chain model

6.6.4.1 Factories (Approved printing house and device manufacturing facility)

Required controls for notes

313. Each note gets a unique note serial, a batch serial and an optional lot code for security sticker.
314. Printing house generates a digital batch manifest containing a batch ID, note serial range(s), production timestamp, material lots used and operator line / machine ID.
315. Manifest is signed (digitally) and transmitted to PrintDreams.
316. Defective/rejected notes are logged and destroyed with count reconciliation.

Packaging rules for notes

317. Notes packed into serialized inner packs (e.g., 25/50/100)
318. Inner packs packed into serialized cartons
319. Cartons sealed with tamper-evident tape/label
320. Pallets (if used) get pallet ID and pallet manifest

Required controls for devices

321. The printer platform uses a read-only device identifier for traceability. The SIT and signer require their own qualified device identities and provisioning records; an identifier or serial number is not, by itself, cryptographic authentication.
322. Device manufacturing facility generates an entry into a device database containing MCU ID, production timestamp and operator ID.

323. PrintDreams has authorized access to device database and can use it for device traceability throughout the supply chain

Factory provisioning must bind the intended SIT and ATM using unique per-pair credentials, record device identities and qualified firmware, disable unapproved printer paths and establish authenticated replacement and credential-revocation procedures. Pairing and printer controls remain subject to hardware-in-the-loop evidence.

Packaging rules for devices

324. A serialized note starter-pack (25 pcs) is packed into a serialized device pack
325. Individual device packs packed into serialized cartons (8 pcs each)
326. Cartons and device packs are sealed with tamper-evident tape/label
327. Pallets get pallet ID and pallet manifest

Why this helps security: If counterfeit or defect issues emerge, isolation is possible by MCU ID, note serial range, batch, material lot and machine line.

6.6.4.2 Factory → central warehouse transport

Required controls

328. Shipment created against a digital manifest (carton IDs + batch IDs)
329. Handoff scan at origin (carton/pallet serials)
330. Sealed transport (tamper-evident seal ID recorded)
331. Handoff scan at destination
332. Seal integrity check at receipt
333. Exception workflow for seal mismatch, missing or damaged carton and manifest mismatch

“Simplified banknote-like” rule

Armored cars for Class N are not necessary. Instead, serialized scanning, seal verification and exception logging should be implemented.

For Class V vouchers and devices, tighter transport controls (insured courier, higher verification, smaller consignments) should be implemented.

6.6.4.3 Central warehouse (vault-lite, not central bank)

This is the core control point for the entire Stablenotes supply chain.

Required controls

334. Segregated storage zones for Class N stock, Class V stock, quarantined stock and returned stock
335. Access control: limited authorized staff, role-based access and entry logs
336. Inventory system tracks: note serial range by location, carton status (received / picked / shipped / quarantined), batch and lot metadata
337. Cycle counts: daily (high-value / Class V), weekly (Class N active SKUs), monthly full reconciliation
338. CCTV coverage for receiving, picking, packing, quarantine

Dual control (should be kept simple)

Dual sign-off will be enforced only for: opening factory cartons, repacking stock, handling Class V voucher stock/devices and quarantine releases.

No need to dual-control every pick for blank media.

6.6.4.4 Warehouse → distribution points (partner DCs / field distributors)

Distribution points can be partner-operated warehouses, regional distributor hubs, authorized retail resupply points or remittance partner back offices

Required controls

339. Ship by serialized carton/pack only (avoid loose notes)
340. Scan-out at warehouse, scan-in at destination
341. Destination acknowledges might include MCU IDs, carton IDs, tamper status and quantity
342. Stock state transitions recorded: In Warehouse → In Transit → At Distribution Point

Exception handling: Any missing MCU IDs, serials or opened cartons would trigger immediate quarantine of affected batch, investigation ticket and hold on further shipment of same batch until cleared (if needed)

6.6.4.5 Distribution point → retail point / end channel

This is where most sloppy supply chain systems fail.

Required controls

343. Retail receives sealed packs, not loose notes or devices
344. Retail scans pack serial(s) and device MCU IDs into inventory
345. Packs are opened only at issuance point (or controlled prep station)
346. Unsold stock remains in sealed packs where possible
347. End-of-day reconciliation must include MCU IDs, issued serials, remaining serials and damaged/voided serials

Critical rule: No “informal” stock transfers between retail points. All transfers must be scanned and recorded.

6.6.5 Retail distribution strategy

Following an SDK-strategy first, retail should be partner-led and controlled, not mass shelf or open-shelf retail at launch.

6.6.5.1 Phase 1 retail strategy

Channel type

Use authorized counter distribution through partners:

348. exchange storefronts / partner service points
349. remittance agent locations
350. electronics/mobile shops with trained staff
351. partner branches (where applicable)

Why counter distribution first

352. better staff control and stock reconciliation
353. fewer theft/substitution incidents
354. easier user education (handling + tamper checks)

6.6.5.2 What is sold at retail

For v1 (Class N)

Devices and sealed serialized refill note packs (larger quantities for repeat users):

Optionally co-branded partner packaging (if partner-integrated)

For Class V vouchers (if used)

They should be treated as a separate SKU with tighter controls and kept as a marketing experiment, not core distribution.

355. very small denominations
356. short expiry dates
357. one-time redemption rules
358. stricter issuance logging

6.6.5.3 Point-of-sale process (simple but controlled)

At retail issuance:

359. Staff scans pack serial / note serial
360. Inventory system marks note as Issued
361. User receives handling/tamper guidance
362. (Optional) App/SDK can validate note serial authenticity on first use

This gives end-to-end traceability: Factory batch → warehouse → retail point → issued note serial

6.6.5.4 Returns and damaged stock

A formal loop is needed, or fraud will fill the gap.

Return categories

363. Unopened sealed pack → return to stock after inspection
364. Opened but unused note → quarantine or controlled resale (policy-defined)
365. Damaged note media → mark serial Void, quarantine, destroy with record
366. Suspected counterfeit → quarantine + incident escalation

Every destroyed note serial should be logged as Destroyed with reason code.

6.6.6 How distribution assurance fortifies Stablenotes security objectives

The serialized note/device supply chain and distribution assurance is not just an operations process. It directly improves security:

A) Anti-counterfeit and anti-substitution

Serial and batch traceability makes it harder to inject fake notes or fake devices unnoticed.

B) Faster incident response

If one batch of notes has print defects, adhesive drift, or tamper-layer issues, exact serial ranges can be quarantined. The same thing is valid for batch of devices.

C) Better partner trust

Partners will integrate faster if the following can be proved:

367. where stock came from
368. who handled it
369. and what happens when something goes wrong

D) Better forensic capability

If a user reports a problem, several things can be traced including batch, retail point, shipment and material lot. That's how Stablenotes' supply chain can move from anecdotes to root-cause analysis.

E) Lower warranty and support cost

Most "mystery failures" become inventory/handling exceptions that can actually be diagnosed.

6.7 Partner Integration Security Boundary and Liability Model

This section defines the security boundary, operational responsibilities, and liability allocation model for SDK-first deployments of Stablenotes technology.

This is essential for an SDK-first model, the core technical risk is not only Stablenotes code — it is also how partners integrate it. A clean boundary prevents:

370. security regressions caused by partner implementation choices,
371. compliance ambiguity,
372. and endless blame-shifting after incidents.

Core principle

Stablenotes is provided as a security and transaction authorization infrastructure layer.

In an SDK-first deployment:

373. Stablenotes owns the security and reliability of its SDK/device/media components.
374. Partner owns the regulated financial service relationship (where applicable), app UX decisions outside the SDK boundary, and customer operations.
375. User owns self-custody decisions and handling of transaction authorization media, subject to disclosed limitations.

This must be reflected consistently in contracts, product docs, and support scripts.

6.7.1 Purpose and scope

376. Define responsibilities, shared-risk interfaces, and liability allocation for SDK deployments

6.7.2 Security boundary definition

377. Stablenotes-controlled components. Stablenotes is responsible for the security of:

378. SDK code and documented APIs
379. Device firmware and secure update chain
380. Print workflow inside the Stablenotes-controlled path
381. Media specifications (QR format, fallback encoding, survivability requirements)
382. Tamper-evidence design (v1 claim scope)
383. Reference implementation used for integration validation
384. Partner integration guidance and security requirements

These areas require integration certification before production deployment.

6.7.3 Responsibility model (RACI)

385. Stablenotes obligations (SDK security, docs, advisories, evidence)
386. Partner obligations (integration correctness, telemetry controls, support training, patching)

The institution approves the owner policy and issuance request, independently verifies funding eligibility, and assigns distinct S1 and S2 custodians. PrintDreams and integration partners define and maintain the qualified SIT, printer and signer boundaries according to their contractual responsibilities; incident ownership and evidence access must be recorded in the deployment RACI.

6.7.4 Integration security requirements (production gate)

387. Golden path requirement
388. Telemetry/logging controls
389. Version and patching SLAs
390. Integration certification (functional + security + ops)

6.7.5 Incident response model

391. Incident categories (Stablenotes / Partner / Shared)
392. Notification and triage SLAs
393. Kill-switch / containment procedures
394. Customer communications ownership

6.7.6 Liability allocation framework

395. Liability follows control
396. Warranty scope and exclusions
397. Liability caps and carve-outs
398. Consumer-loss policy framework (no blanket guarantee)

6.7.7 Evidence sharing and audit rights

399. Evidence package obligations
400. Partner attestations
401. Audit/review rights

6.7.8 Branding and claims control

402. Approved v1 claims
403. Prohibited claims (cash equivalent, unhackable, guaranteed recovery)

6.7.9 Production readiness checklist (partner launch gate)

404. Certification complete
405. Logging controls verified
406. Runbooks approved
407. Contracts executed
408. SDK version current
409. KPI rollback thresholds agreed

6.7.10 Evidence artifacts

410. Boundary spec, RACI, certification checklist, incident runbook, liability framework

Cross-references:

411. Secret handling requirements for partner apps → 6.3.6
412. Print/tamper support guidance → 6.4.9 and 6.5.8
413. Regulatory boundary → Chapter 11

6.8 Security and Assurance Ship Gates Summary

6.8.1 v1 production ship gates (consolidated)

A v1 deployment may proceed only after the documented pass/fail requirements for the following controls have been met:

414. 6.2 RNG
415. 6.3 non-retention
416. 6.4 survivability
417. 6.5 v1 tamper evidence
418. 6.6 supply-chain assurance and 6.7 partner integration

SIT hardware, entropy and firmware qualification; authenticated paired printer link and printer non-retention.

Public-key QR and checksum verification with qualified protected-print correlation; independent funding verification, S2 custody and signer interoperability.

Chain-specific owner-policy enforcement, privileged-path testing and independent integrated security assessment. Unexecuted tests remain pending and do not establish production readiness.

6.8.2 v2 future gates (separate, non-blocking for v1)

419. Adversarial tamper testing
420. Bearer-transfer field SOP validation

421. Additional liability/reserve and compliance gating

Cross-references:

422. Detailed acceptance criteria in each subsection
423. Roadmap sequencing in Chapter 12

6.8.3 Post-quantum extension activation gate

Production enablement of the post-quantum extension requires configuration-specific evidence demonstrating compliance with PQ-1–PQ-4 and the applicable hardware, firmware and update requirements in Chapter 7. Evidence MUST include independent review, resolution and re-testing of critical/high findings, and documented operational limitations. Unverified capabilities MUST remain identified as planned or experimental. These gates apply to extension-enabled deployments; changes affecting shared baseline components also require regression assessment under §6.9.3.

6.9 Claims-to-Evidence Mapping and Document Control

6.9.1 Claims-to-evidence matrix reference

424. Link to the master matrix (spreadsheet/data room)
425. State versioning and update cadence

6.9.2 Evidence artifact index

426. Pointer list to all reports/documents referenced in 6.2–6.6 and relevant requirements in chapters 3, 5 and 7

6.9.3 Change control

427. Any change affecting security claims, print specs, or SDK integration requirements requires:
428. version bump
429. regression review
430. partner notification (if applicable)

6.10 Cryptographic profile specification

6.10.1 XOR 2-of-2

$$S_1 \xleftarrow{\$} \{0,1\}^{256}, \qquad S_2 = K \oplus S_1; \quad \text{Reconstruction is:} \quad K = S_1 \oplus S_2$$

Use only when strict 2-of-2 transaction authorization is acceptable. The pad must be uniform, independent, never reused and authenticated through the payload commitment.

6.10.2 Shamir t-of-n

$$f(x) = K + \sum_{j=1}^{t-1} a_j\, x^j, \qquad a_j \xleftarrow{\$} \mathbb{F}$$

The field definition, representation, coefficients, x-coordinates, interpolation, encoding and malformed-share behavior are normative. The locally validated reproducibility package uses $prime521 - v1$ over $p =$

$2^{521} - 1$ for deterministic conformance tests; that implementation choice is not a production Stablenotes field profile unless separately approved and independently reviewed.

6.10.3 Share payload authentication

Each share payload binds format version, scheme, threshold, share index, chain/wallet profile, public-key commitment, note serial commitment and integrity data. A checksum detects transcription errors; it is not a cryptographic authenticity control. Substitution resistance requires an authenticated commitment or signature rooted in the issuance workflow.

6.10.4 Post-Quantum Cryptography Standards for surrounding infrastructure

Stablenotes operates in an environment where blockchains and wallets have their own cryptography solutions. Stablenotes cannot offer direct protection against protocol-level failure. Also, the suggested split-secret controls in this whitepaper do not stop mathematical key recovery so, for deployments claiming conformance with the post-quantum extension, mandatory PQ authorization is required in the asset-control path.

The overall infrastructure around Stablenotes needs to become quantum-safe, which is a migration effort. The relevant governing documents presented only as guidance with defined applicability are:

- NIST IR 8547, Transition to Post-Quantum Cryptography Standards (initial public draft), proposes that quantum-vulnerable configurations with 112-bit classical security strength are deprecated after 2030 and disallowed after 2035. Listed configurations with at least 128-bit strength are proposed for disallowance after 2035; the same 2030 deprecation is not specified for that tier. Applicability depends on the algorithm, parameters and final guidance [R30].
- NSA CNSA 2.0 — mandates ML-KEM-1024 and ML-DSA-87 (Category 5 parameters only) for US national security systems, with its own timeline.
- OMB M-23-02 and NSM-10 — US federal inventory and migration requirements.
- NCCoE SP 1800-38 — practical migration guidance.
- Protocol-level work still in flux: TLS hybrid key exchange (X25519MLKEM768, widely deployed), IETF LAMPS profiles for X.509/CMS, SSH, IKEv2.

In addition to the above external guidance, special attention needs to be given to the PQ deployment's cryptographic profile which includes the items specified in §5.4.1. (algorithms, parameters, key lifecycle, encoding and verification dependencies).

6.11 Cryptoeconomic risk model

$$G_{j,t} = \sum_{e \in \mathcal{E}_{j,t}} g_e\,, \qquad N_{j,t}(h) = \sum_{e \in \mathcal{E}_{j,t}} [g_e - r_e(h)]$$

$$E_{j,t} = \frac{1}{T} \int_t^{t+T} V_j\,(u)\,du$$

$$\hat{L}^G_{j,t} = \frac{G_{j,t}}{E_{j,t}}, \qquad \hat{L}^N_{j,t}(h) = \frac{N_{j,t}(h)}{E_{j,t}}$$

$RVR_{a,b} = \frac{\hat{L}^G_{a,t}}{\hat{L}^G_{b,t}}$ and $DR^{(p)}_{c,d} = \frac{p_c}{p_d}$, are conditional estimands. Production claims require the research article's metadata match and mature-cohort rules. Current public data supports neither cross-domain point estimate.

For equal partitions, $L = \frac{W}{N}\sum_{i=1}^{N} X_i$, $\mathbb{E}[L] = pW$; $\mathrm{Var}(L) = W^2 p(1-p)\left[\frac{1}{N} + \rho\frac{N-1}{N}\right]$

With common-mode probability q, $\Pr(L = W) = q + (1-q)p^N$. Portfolio design should minimize expected loss plus a tail-risk term and operational cost subject to transaction authorization constraints; the resulting objective is a decision framework, not an empirical optimum.

The multi-wallet Binance incident is a relevant common-mode scenario: shared or correlated operational dependencies can expose multiple nominal partitions to one attack campaign. In the tail-event expression above, q denotes the common-mode probability (q_c), and p is the per-partition compromise probability conditional on no such event. The p^N term also assumes equal and conditionally independent partition risks; residual correlation requires a joint model. The incident does not identify either parameter or prove a reduction from this proposed architecture; the actual dependency and control effectiveness require deployment-specific evidence [R31, R32].

7 Firmware, App, and Update Integrity (Stablenotes v1)

This chapter defines the minimum security architecture and operational controls for the printer unit firmware, its update mechanism, and the reference wallet companion app within Stablenotes v1. The intent is to meet “high assurance” expectations commonly applied to security-critical devices and software supply chains, including platform firmware resiliency guidance (NIST SP 800-193), secure software development practices (NIST SSDF), and supply chain risk management principles (NIST SP 800-161). (NIST Computer Security Resource Center)

Scope note: This chapter applies to the Stablenotes v1 printing device and v1 companion app role. Any consumer “banking-like” features (buy/sell/swap/card) are showcased in the v1 companion app just as pure reference for v1 partner deployments, particularly neobank partners which might want to see a fully integrated reference deployment.

Three device boundaries apply: the SIT generates and splits the issuance secret; the paired ATM prints an authorized share; the separate Isolated Signer handles transaction authorization. Each requires its own hardware, firmware, update and non-retention evidence.

7.1 Firmware architecture

Quantum-readiness scope. Stablenotes plans to extend its hardware and firmware security architecture to support post-quantum migration. The additional requirements below define the target profile for this extension; they do not establish current implementation or certification. They apply to relevant printer components and any separate isolated signing terminal. Deployment documentation MUST distinguish implemented, planned and unsupported capabilities.

7.1.1 Hardware components (reference architecture)

The printer unit SHOULD be treated as a security appliance. A typical secure architecture includes:

431. Hardware root of trust: immutable boot ROM / secure bootloader.
432. Secure element or equivalent protected execution/key-storage component; PQ capabilities and migration limitations to be verified for the selected configuration.
433. Main MCU/FPGA: runs device firmware and print orchestration.
434. Non-volatile storage: firmware slots + configuration (encrypted/verified).
435. Print engine: printer controller, gyro, accelerometer and navigation sensors.
436. Connectivity: the existing printer supports Wi-Fi and USB-C charging. In the target production issuance profile Wi-Fi is limited to the assigned SIT/ATM pair and approved protocol; ATM firmware must deny legacy or unauthenticated secret-print routes. The SIT local link is not an air gap, and the transaction signer remains a separate isolated device.
437. Physical debug interfaces: JTAG/SWD/UART (must be locked/disabled in production)
438. Device identity: unique device 96 bits MCU ID etched on silicon and provisioned at manufacture. It is an immutable serial identification used to assign a specific device to a named operator (authorized officer).
439. Formats that accommodate larger, variable-length keys, signatures and certificates, with bounded parsing and measured memory requirements.

Post-quantum readiness. Hardware selection SHOULD provide sufficient processing capacity, RAM, firmware storage and update-package capacity for the selected post-quantum algorithms, verified through representative benchmarks. The design MUST document cryptographic capabilities and migration constraints across the boot ROM, secure element, main processor and device-identity mechanism.

A secure element does not establish quantum resistance unless its relevant algorithms and interfaces support the intended protection. Where an immutable trust anchor cannot support a secure transition, the deployment roadmap MUST identify hardware replacement rather than assume that a firmware update can resolve the limitation.

7.1.2 Secure boot and chain of trust (MUST)

The device MUST implement a full chain of trust from immutable hardware to the running firmware image:

440. Security-critical peripheral firmware, FPGA bitstreams and authenticated maintenance/debug paths within the assessed chain of trust.
441. Boot ROM verifies the first-stage bootloader using a vendor root key.
442. Bootloader verifies the firmware image signature (and optionally a measured hash).
443. Firmware verifies critical configuration and any loaded modules before use.

This “verify-next-stage-before-executing” model aligns with platform secure boot chains used in modern ecosystems (e.g., Apple secure boot chain of trust; Android Verified Boot). (Apple Support).

For the post-quantum extension, boot authentication MUST preserve a quantum-resistant verification path from the hardware trust anchor through all security-critical executable stages. Adding a PQ verifier to application firmware alone is insufficient if an attacker can replace that verifier through a vulnerable earlier boot stage.

Where a hybrid classical/PQ signature policy is adopted, both required signatures MUST validate and bind the same image and security metadata. Missing or invalid PQ verification MUST NOT trigger classical-only fallback. Trust-anchor changes MUST use an authenticated, downgrade-resistant transition procedure.

7.1.3 Firmware resiliency (MUST)

Firmware MUST be designed for protect / detect / recover behavior consistent with platform firmware resiliency guidelines: (NIST Computer Security Resource Center)

444. Protect: prevent unauthorized modification (signed firmware, locked storage, debug disablement).
445. Detect: detect corruption/unauthorized changes (signature validation; measured boot optional).
446. Recover: support recovery to a known-good state (A/B slots, recovery partition, or factory-safe mode).

Firmware restoration MUST preserve the active cryptographic security policy. Alternate boot slots, restoration images and factory-safe modes MUST NOT re-enable revoked keys, obsolete verification policies or classical-only authentication after PQ enforcement is activated. Interrupted updates MUST leave either a verifiable operating image or a restricted restoration path that cannot process signing secrets. Tests MUST cover power interruption, corrupted images, invalid signatures and attempted security-policy rollback.

7.1.4 Secrets handling in firmware (MUST)

447. Private key material and sensitive payloads MUST be treated as ephemeral unless explicitly required (e.g., device identity keys in secure element).
448. Firmware MUST NOT log or persist private keys or printed transaction authorization payloads.
449. Sensitive buffers MUST be zeroized after use where feasible.
450. Debug logs MUST be compiled out or restricted to non-sensitive operational codes in production builds.
451. Extend zeroization to temporary stack and heap buffers, and protect cryptographic working memory from unauthorized DMA, debug access and crash dumps.

The same secret-handling restrictions MUST cover PQ private keys, seeds, shares and temporary cryptographic buffers. Implementations MUST maintain separation between owner-authorization credentials, device-identity keys and firmware-update signing authority. Devices require update-verification public keys, not private release-signing keys.

PQ operations MUST undergo review for random-number quality, side-channel leakage, fault handling and effective zeroization. Introducing PQ algorithms MUST NOT cause S1 and S2 to be retained together or weaken their existing isolation boundaries.

SIT and printer secret handling must additionally cover the P4-to-radio boundary, TLS buffers, print raster, job queue, preview, internal RAM, PSRAM, flash, crash and reset behavior. K never travels to the ATM. Production S1 is sent only in an authorized bounded job; a reference S2 print is a separately approved job and requires explicit common-printer risk controls.

7.1.5 Production hardening (MUST)

452. Debug interfaces MUST be disabled or locked (fuses/secure element policy) for production units.

453. Factory test modes MUST require authenticated entry and be disabled post-provisioning.
454. Device must implement rate limits / lockouts for any privileged maintenance commands.

7.2 Updates

7.2.1 Signed updates (MUST)

All firmware updates MUST be cryptographically signed and verified on-device before installation.

Minimum requirements:

455. Signature verification occurs before writing to the active boot slot.
456. Update packages are authenticated and integrity-checked end-to-end.
457. Update signing keys are protected by an HSM-backed process and role separation.

7.2.2 Key management and signing hierarchy (MUST)

Stablenotes SHOULD adopt a structured update signing model similar in spirit to modern update security frameworks (e.g., TUF concepts: separation of roles, survivability under partial key compromise). (TUF)

Minimum key management requirements:

458. Root key(s): offline storage (HSM or air-gapped), used only for key rotations and critical policy updates.
459. Release signing key(s): used for routine firmware releases; protected by HSM; rotated on schedule.
460. Threshold policy: for high-risk releases, require M-of-N approvals (two-person integrity).
461. Key ceremony: documented creation, rotation, revocation, and incident response procedures.

7.2.3 Rollback protection (MUST)

The device MUST protect against downgrade attacks.

462. Maintain a minimum allowed firmware version (monotonic counter or secure element-backed anti-rollback).
463. Block installation of firmware below the minimum version.
464. Permit rollback only to a known-good version within an approved window (if required for safety), never to a vulnerable baseline.

Android Verified Boot explicitly supports rollback protection concepts; the device should meet an equivalent standard appropriate to its platform. (Android Open Source Project)

7.2.4 Reproducible builds and provenance (SHOULD; target high assurance)

For partner and auditor trust, firmware and companion software SHOULD be built with strong supply chain provenance:

465. Reproducible or verifiable builds (documented build pipeline, deterministic artifacts where feasible).
466. Build provenance attestation targeting SLSA-style controls (e.g., tamper-resistant build service, signed provenance). (SLSA)
467. SBOM generated for each release and retained (with dependency risk tracking).

468. Secure SDLC aligned to NIST SSDF practices. (NIST Computer Security Resource Center)

7.2.5 Update rollout controls (MUST)

469. Staged rollout (canary → limited → full) with measurable health signals.
470. Emergency pause mechanism for failed releases.
471. Mandatory update path for critical security fixes within defined SLA.

7.2.6 Supply chain integrity and manufacturing controls (high level; MUST)

Manufacturing and provisioning MUST implement baseline cybersecurity supply chain risk controls consistent with established C-SCRM guidance. (NIST Computer Security Resource Center)

At a minimum:

472. Secure provisioning stations (access controlled, audited).
473. Unique device identity provisioned per unit; keys injected only under controlled procedures.
474. Firmware loaded only via authenticated process; prohibit “side-loading” in factory.
475. Chain-of-custody for devices and critical components (secure element lots, MCU lots).
476. Factory-to-warehouse tamper evidence and reconciliation (see Chapter 6 supply chain assurance).

Evidence artifacts (examples):

477. Firmware_Architecture_Spec_v1.pdf
478. SecureBoot_and_AntiRollback_Design.pdf
479. Update_Signing_Key_Management_Policy.pdf
480. SLSA_Provenance_Attestation_v1.json (or equivalent)
481. Firmware_SBOM_<version>.spdx.json
482. Manufacturing_Security_Provisioning_SOP.pdf

7.2.7 Post-quantum migration readiness

The proposed extension supplements the signed-update, key-management and rollback requirements in §§7.2.1–7.2.3.

483. Cryptographic inventory and agility: Maintain an inventory of algorithms, trust anchors, certificates and dependencies used for boot, updates, device authentication and communications. Version cryptographic policies explicitly and restrict selection to approved algorithms and parameter sets.
484. Authenticated migration: Define enrollment, rotation and revocation procedures for PQ verification keys. Establish the new trust path before retiring the previous one; a transition authenticated solely by an already-compromised classical key is insufficient.
485. Protected update metadata: Authenticate the firmware digest, target hardware, firmware version, algorithm identifiers and minimum security-policy version. Rollback protection MUST cover cryptographic policy as well as firmware version.
486. Communications readiness: Assess provisioning and maintenance channels for PQ or hybrid protection appropriate to their authentication and confidentiality needs. This does not relax prohibitions on transmitting signing secrets.

487. Evidence before activation: Verify performance, boot continuity, key rotation, interruption handling and rejection of downgrade attempts on the selected hardware. Record results and residual limitations in the deployment annex before claiming PQ-enabled firmware protection.

These measures complement the asset-authorization controls in §5.6; neither layer substitutes for the other.

7.2.8 Authenticated issuance printer link

TR-SPL-1 is the proposed local interface between one factory-paired SIT and ATM. The target is per-pair Wi-Fi credentials plus a distinct high-entropy external TLS credential, TLS 1.3 PSK-DHE, no 0-RTT, no plaintext or legacy secret-print fallback, bounded single-use jobs and authenticated job context. Exact platform and ATM firmware support, cipher suite and credential lifecycle require qualification.

A wrong-pair request, replay, malformed job, authentication failure, printer-bypass route or uncertain completion MUST fail closed. UNKNOWN print completion enters HOLD/VOID or quarantine; it must not automatically reprint a secret. Independent hardware-in-the-loop and memory-forensic evidence is required before live-value issuance.

7.3 Companion app (Reference Wallet apps) — v1 role and boundaries

7.3.1 Minimal v1 role (recommended for partner deployments)

The companion app is an online institutional interface for public transaction construction, verification, monitoring and broadcast. It may initiate an approved issuance request but does not generate K or secret shares, render production secret print jobs or act as the production isolated signer.

Recommended minimal responsibilities:

488. Initiate an approved issuance request and receive public status from the SIT.
489. Display public verification and funding-eligibility results; the SIT performs the public-key QR and checksum checks under the approved issuance profile.
490. Display handling and storage guidance
491. Provide read-only monitoring of public address state (optional)
492. Provide transaction authorization/import workflow when needed

7.3.2 What v1 explicitly does NOT do (non-negotiable for v1 scope)

In v1 deployments, the companion app and the Stablenotes SDK integration MUST NOT:

493. Provide custody, hosted accounts, or key escrow
494. Provide exchange execution, brokerage, or market-making
495. Provide buy/sell/swap functionality as a PrintDreams-provided service
496. Present itself as a bank, neobank, payment institution, or e-money provider
497. Operate a cash-out network, operator program, or any “bearer note” transfer system

If buy/sell/swap/card functionality exists in a reference wallet for demonstration purposes, it must be clearly segmented as a third-party regulated service and treated as outside the v1 assurance scope. Partner

deployments should default to disabling such features unless explicitly approved and contractually structured.

7.3.3 App integrity controls (MUST)

To support the security model in Chapter 6:

498. The app and SDK must not receive or retain production K, S1, S2 or readable secret print material; approved transaction metadata remains subject to data-minimization controls.
499. Disable session replay / screen recording in sensitive flows.
500. Restrict third-party analytics SDKs on key-handling screens.
501. Implement hardened crash reporting (no memory dumps, redaction on sensitive flows).

7.3.4 OS trust anchoring (SHOULD)

When feasible, partner deployments SHOULD leverage platform security primitives:

502. iOS secure boot chain of trust (baseline device integrity) (Apple Support)
503. Android Verified Boot / integrity checks for supported devices (Android Open Source Project)

7.3.5 Implementation placeholders to complete before production

504. Printer platform and SIT/ATM pairing profile: selected hardware and proposed interface; exact firmware compatibility and security evidence [TBD].
505. Secure element model and policy: [TBD]
506. Secure boot key hierarchy + custody model: [TBD]
507. Anti-rollback mechanism: [TBD]
508. Update distribution model (direct OTA / partner-managed): [TBD]
509. Companion app telemetry stack and allowed fields: [TBD]
510. Partner integration certification checklist for app hardening: [TBD]

Evidence artifacts (examples):

511. App_DataFlow_and_NonRetention_Test_Report.pdf
512. ThirdPartySDK_Inventory_and_RiskReview.pdf
513. SensitiveScreen_Redaction_and_NoReplay_Config.pdf
514. Release_Signing_and_Distribution_SOP.pdf

7.4 Air-gapped ingestion and transaction integrity

7.4.1 Interface constraints

515. No enabled Wi-Fi, cellular, Bluetooth, NFC or general-purpose USB data path during transaction authorization signing.
516. Optical input accepts only a bounded, versioned unsigned-transaction format.
517. Parser implementation is memory-safe where practicable and fuzz-tested with malformed and adversarial payloads.

518. Updates use authenticated artifacts and a documented offline verification ceremony.

7.4.2 Trusted transaction display

The isolated signer displays the chain, source, asset, amount, destination, fees, nonce and policy constraints derived from the parsed transaction, not an untrusted label. The operator verifies the action against the approved request and confirms it before S2 acceptance or reconstruction. Unsupported or ambiguous operations abort. An EVM signing profile must additionally identify EIP-7702 type-0x04 transactions and independently signed authorization tuples; unexpected delegated-code changes, executor/owner changes, unlimited approvals, arbitrary-hash requests and nonce batches are rejected unless explicitly authorized by an independently reviewed deployment profile. This signer check does not replace the asset-holding policy [R36].

7.4.3 Reconstruction, signing and zeroization

Reconstruction occurs inside the approved isolated signer boundary. K, S1, S2 and intermediates are held only as long as needed, excluded from logs and persistent storage, and cleared on success, failure and interruption. The signed public transaction returns optically to an online verifier for independent checks and broadcast.

7.4.4 Residual attack surface

The terminal remains exposed to compromised manufacturing, malicious firmware, optical capture, display substitution, fault injection, power/EM side channels and operator error. Secure boot and attestation reduce these risks but do not prove their absence. Vendor-specific security-element properties may be claimed only when the exact component and firmware configuration are verified.

8 Physical Transaction Authorization Media Design

The v1 note is a physical encoding of S1 and associated non-secret metadata. Its objective is durable owner-bound transaction authorization, not transfer by possession. A complete private key, seed or possession-sufficient encrypted record is not permitted in the reference owner-bound profile.

8.1 Encoding format

8.1.1 Authenticated share payload

519. format_version
520. scheme_id and field/profile identifier
521. threshold t and share count n
522. share_index and x-coordinate where applicable
523. share value S1
524. chain_id and wallet/signature profile
525. public-key or address commitment
526. note serial commitment and issuance nonce
527. integrity checksum plus cryptographic authenticity data

The payload uses a canonical binary encoding with deterministic field order, length limits and rejection behavior. CBOR with a deterministic profile or another compact canonical format may be used after parser and interoperability review. Human-readable labels must not be parsed as authoritative transaction or cryptographic data.

8.1.2 QR specification

528. QR Code Model 2 with a fixed version-selection rule
529. Error correction selected from payload size and validated damage profile; Level H is a candidate, not an automatic guarantee
530. Minimum module size and quiet zone qualified across the supported camera matrix
531. No placement across folds, perforations, adhesive boundaries or high-glare areas
532. Every note must pass the public-key QR identity/serial check and the back-checksum check before funding eligibility. The protected S1 QR is not decoded during this non-revealing per-note check; its print-process correlation must pass the qualification requirements in §§6.4 and 9.3.

ISO/IEC 15415 is relevant to print quality grading. ISO/IEC 29158 applies to direct part marking and should be cited only if the production method fits its scope. The final test plan must identify the normative standard and verifier configuration.

8.1.3 Human-readable fallback

The protected fallback encodes the same S1 payload or a formally specified authorization representation. It is printed over the second obfuscated area, followed immediately by the checksum. The checksum supports non-revealing process verification and detects transcription errors; it does not authenticate the issuer or independently prove each protected character is readable.

8.2 Redundancy

8.2.1 Physical redundancy versus cryptographic threshold

Two identical QRs on one note improve resistance to localized print damage but do not create an independent cryptographic share. A Shamir t-of-n profile can create independent transaction authorization shares, but co-locating them on the same note defeats threshold separation. The specification must state whether redundancy protects encoding, media loss or factor availability.

8.2.2 Recommended v1 physical encoding

533. Primary S1 QR in a protected secret area
534. Second S1 encoding only if its additional copy risk is accepted and both are protected by the same owner-bound threshold
535. Human-readable S1 fallback with full-payload checksum
536. Public address and note commitment in an unprotected verification area
537. No production S2 data or S2 secret hint appears on the S1 note. Any separately printed S2 reference note has its own approved job and independent custody controls.

8.3 Tamper evidence

The tamper layer should obscure S1 under defined ordinary viewing conditions and produce visible evidence when opened. It must not be described as copy-proof, counterfeit-proof or proof that no prior access occurred. After opening, the user should complete transaction authorization promptly and retire the note.

8.3.1 Required tests

538. Oblique and transmitted-light viewing
539. High-resolution photography and image enhancement
540. Peel, lift, heat, humidity, solvent and reseal attempts
541. Adhesive migration and post-aging opening
542. User ability to distinguish intact, opened and suspicious samples
543. QR and fallback readability after intended opening

8.4 Substrate engineering and environmental claims

BoPET, cotton-banknote paper and hybrid composites are candidate substrates. Ink-receptive acrylic/silica/cationic coatings are candidate print systems. Material selection is governed by measured optical contrast, adhesion, abrasion, chemical resistance, dimensional stability, tamper-layer compatibility and decode performance. Supplier datasheets do not establish multi-decade system life.

8.5 Implementation placeholders

544. Final payload schema and canonical encoding [TBD]
545. Preliminary first TON profile: XOR 2-of-2; production profile, authentication and interoperability approval [TBD].
546. Share authentication/commitment mechanism [TBD]
547. QR version, ECC, module size, contrast and quiet zone [TBD after lab study]
548. Fallback alphabet, grouping and checksum [TBD]
549. Substrate/ink/adhesive stack and suppliers [TBD]
550. Tamper-evidence claim and acceptance threshold [TBD]

9 Reliability & Survivability Testing (Pre-Launch Gate)

This chapter defines the pre-launch reliability qualification program for Stablenotes v1 transaction authorization media and associated tamper layers. In v1, survivability is not a quality preference, it is a fund-loss risk control. An unreadable key is functionally equivalent to stolen funds.

The program is designed to be (i) testable, (ii) repeatable across production lots, and (iii) defensible to integration partners and auditors.

9.1 Service-life targets

The source draft contains conflicting candidate targets (12 versus 24 months carry-life and 5-10 versus 20 years storage-life). No target is normative until resolved by product requirements and evidence. The production specification must define one carry-life, one storage-life, environmental assumptions, replacement interval and statistical confidence level.

9.1.1 Carry-life profile

Defines handling frequency, folding, abrasion, sweat/moisture, light and temperature exposure. The acceptance test must reproduce or conservatively bound the profile.

9.1.2 Storage-life profile

Defines protective sleeve, UV dose, humidity and temperature range, chemical exclusions, inspection interval and accelerated-aging correlation. A multi-decade claim requires both accelerated evidence and a continuing real-time aging program.

9.2 Test matrix

The test program must cover both baseline qualification (design validation) and ongoing QC sampling (lot acceptance). It must also cover the complete media stack: ink + substrate + overlays (security sticker).

QR print-quality testing should identify the applicable edition and measurement configuration of ISO/IEC 15415. ISO/IEC 29158 concerns direct part marking and is relevant only if the qualified production method falls within its scope. The selected verifier and measurement conditions must be documented.

9.2.1 Key Parameters for QR Code Readability

Standard verification software assesses these parameters to assign an overall grade (usually A through F or 4.0 through 0.0):

551. Symbol Contrast (SC): Measures the difference between the highest and lowest reflectance values. High contrast between black modules and the white background is essential.
552. Modulation (MOD): Evaluates the uniformity of reflectance across the code. Low modulation occurs when some "dark" modules are too light or "light" modules are too dark, confusing the scanner.
553. Reflectance Margin (RM): Determines how well each module can be distinguished as light or dark relative to a global threshold.
554. Fixed Pattern Damage (FPD): Assesses the integrity of the "Finder Patterns" (the three large squares in the corners) and "Alignment Patterns." If these are damaged, the scanner cannot "locate" the code.
555. Axial Non-uniformity (ANU): Measures if the code is stretched or scaled differently on one axis versus the other.
556. Grid Non-uniformity (GNU): Evaluates how well the modules align with an ideal grid. Significant deviation suggests printing distortion.

557. Unused Error Correction (UEC): QR codes have built-in redundancy (Reed-Solomon). This parameter measures how much of that "safety net" is still available. If this is low, the code is "barely" readable.

9.2.2 Mechanical tests (mandatory)

Purpose: simulate daily handling and physical wear that can destroy QR modules or characters.

Minimum tests:

558. Abrasion / rub tests
559. dry rub cycles with controlled pressure
560. wet rub cycles (light moisture)
561. Fold cycles
562. repeated folding along defined fold lines
563. crease stress with compression
564. Edge wear
565. repeated insertion/removal from sleeve or wallet pocket
566. Smudge resistance
567. finger rub and cloth rub tests

9.2.3 Water and humidity tests (mandatory)

Purpose: determine whether accidental exposure causes unrecoverable damage.

Minimum tests:

568. Splash exposure
569. water droplets + wipe
570. Immersion (short duration)
571. e.g., 5–30 seconds immersion, followed by air-dry
572. Humidity cycling
573. high humidity exposure (e.g., 85% RH) and return to ambient
574. Condensation simulation
575. cold-to-warm transition

9.2.4 Chemical exposure tests (mandatory)

Purpose: reflect common real-world contamination that destroys readability.

Minimum substances:

576. Sweat / skin oil simulation
577. Hand sanitizer (alcohol-based)
578. Detergent/soap residue
579. Beverages: water, coffee/tea, soda (sugar + acid exposure)

580. Household cleaner (mild) — optional depending on target market

Procedure concept:

581. controlled application → dwell time → wipe/dry → scan and legibility test.

9.2.5 Aging tests (mandatory)

Purpose: accelerated aging to estimate service life under storage conditions.

Minimum tests:

582. UV exposure
583. defined spectrum and dose
584. Heat aging
585. elevated temperature exposure (e.g., 60–80°C for defined hours)
586. Cold cycling
587. low temperature + return to ambient
588. Thermal cycling
589. repeated hot/cold transitions

9.2.6 Sticker aging and adhesive interaction (mandatory if sticker used)

Purpose: ensure the tamper layer does not degrade recoverability.

Minimum tests:

590. Adhesive migration
591. observe bleed-through, residue, ghosting over time
592. Edge lifting
593. humidity/heat to test peel behavior
594. Residue and delamination behavior
595. post-aging opening test

9.3 Acceptance criteria

Acceptance criteria must be defined to support:

596. binary ship gate decisions,
597. partner diligence,
598. ongoing QC acceptance,
599. and incident root-cause analysis.

9.3.1 Scan success thresholds (QR)

Use calibrated barcode-verifier equipment and the actual SIT and isolated-signer camera/build combinations under the documented production profile. A controlled non-funded sample permits direct testing of the protected encoding after the normal opening procedure; per-note public checks remain non-revealing.

600. SIT camera and software for the public-key QR
601. Isolated Signer camera and software for protected S1 after authorized opening
602. in typical indoor and low-light conditions

Core metrics (mandatory):

603. Post-stress QR scan success: at least 98.5% under the applicable qualified test condition, unless a stricter approved deployment profile applies.
604. The test protocol must state the population, confidence level, lot structure and pass/fail calculation before testing; it must not infer a per-note guarantee from a batch average.
605. Time-to-scan target: median at most 2 seconds and 95th percentile at most 5 seconds, measured under the approved conditions.
606. Any change to these targets requires documented risk acceptance and requalification.
607. Failure classification: every failure must be categorized (contrast, blur, distortion, quiet zone damage, camera limitations).

Hard stop criteria (suggested):

608. Any single stress category causing scan success < 90.0% triggers design review.
609. Any repeatable failure mode across lots triggers batch hold and investigation.

9.3.2 Human-readable fallback legibility thresholds

Fallback text must remain readable when QR fails.

Core metrics:

610. Fallback legibility target: at least 99.9% under the approved test conditions and statistically justified sample plan.
611. A small sample with no observed failures is not sufficient by itself to establish a 99.9% success rate; confidence, clustering and sample size must be stated.
612. Checksum validation: 100% of transcribed fallbacks must pass checksum where legible.
613. Ambiguity rate: misread characters must be below a defined threshold (e.g., ≤ 0.1%) by design (font/encoding selection).

9.3.3 Sample sizes and QA acceptance rules

Two layers:

A) Design validation (pre-launch qualification)

614. Initial minimum: 200 non-funded synthetic notes per media configuration and condition; increase the sample where required by the target confidence level and expected failure rate.
615. The sample plan must quantify confidence in both print readability and the probability that public checks pass when the protected encoding is defective. Zero failures in 200 samples do not establish a 99.9% reliability claim.
616. Test across at least 3 production lots to ensure repeatability.
617. Independent lab required for baseline qualification report.

B) Ongoing production QC (lot acceptance)

618. Each manufactured lot must have:
619. sampling plan (AQL-based or risk-based)
620. print contrast check
621. Serial QR scan check
622. fallback checksum verification
623. Lot acceptance: lot passes only if all sampled notes meet thresholds; otherwise, lot held or reworked per SOP.

9.4 Replacement and support policy

This policy is part of the safety case. It defines what happens when survivability fails in practice.

9.4.1 User-facing support outcomes (required)

When users report damage/unreadable media, the support process must route into one of these outcomes:

624. Recoverable note with degraded QR
625. If fallback text is readable and checksum-valid:
626. guide user through transaction authorization using fallback input.
627. encourage immediate migration of funds and re-issuance.
628. Partially readable note
629. Provide structured guidance:
630. attempt scan under varied lighting / camera settings
631. attempt fallback using partial blocks + checksum logic (if supported)
632. if not recoverable: communicate clearly that self-custody loss may be irreversible.
633. Unreadable note
634. If both QR and fallback are unreadable:
635. classify as potential unrecoverable loss event.
636. log incident with batch/serial details for investigation.
637. provide disclaimers and best-effort remediation steps (but no false guarantees).

9.4.2 Replacement policy (operational)

Stablenotes should define a replacement policy by product class:

638. Blank transaction authorization media (Class N):
639. replacement available for defective media within warranty window, subject to verification.
640. Funded note wallets (user value at risk):
641. replacement of media does not redeem funds; only transaction authorization does.
642. support focuses on enabling transaction authorization and immediate migration.

9.4.3 Disclaimers (required; must align with legal posture)

643. Printed transaction authorization media is a self-custody backup tool.
644. Damage, loss, or exposure may cause permanent loss of funds.
645. Users are responsible for safe storage and handling.
646. Survivability targets assume defined environmental conditions.

9.4.4 Recommended user best practices (optional but strongly recommended)

Provide clear guidance:

647. Store notes in protective sleeves (provided or recommended spec).
648. Avoid moisture, direct sunlight, and chemicals.
649. Avoid repeated folding; store flat when possible.
650. Verify readability periodically (optional; guidance to avoid exposing secrets).
651. If tamper layer is opened, recover promptly and re-issue; do not re-store opened notes.

9.4.5 Operational feedback loop (required)

Every survivability incident should:

652. record note serial + batch (if available),
653. capture failure mode and photos (user opt-in),
654. map to lot/material traceability,
655. feed into corrective action (CAPA) process:
656. lot hold/quarantine if systemic
657. supplier/material change if recurring
658. design updates if needed.

9.4.6 Implementation placeholders to finalize for production

659. Carry-life duration: [TBD]
660. Storage-life duration: [TBD]
661. Test protocol references (lab + internal): [TBD]
662. Device scanning matrix list: [TBD]
663. Final acceptance thresholds (QR pass rate, time-to-scan, legibility): [TBD]
664. Sampling plan (n, lots, AQL): [TBD]
665. Warranty/replacement terms and support scripts: [TBD]

9.5 Research-derived qualification additions

9.5.1 Share integrity after stress

Post-stress testing must verify exact share bytes, format version, commitment and public-address derivation, not merely that a QR scanner returns some data. Silent corruption and parser divergence are security failures.

9.5.2 Common-mode media failure

Test across independent production lots, printers, cartridges, adhesives, storage sleeves and environmental chambers. The program must estimate whether a single supplier defect or process drift could compromise a large partition set simultaneously.

9.5.3 Optical confidentiality

In addition to readability, the tamper stack must be assessed for unintended S1 disclosure through transmission, infrared/UV response, photography, enhancement and partial delamination. S1 exposure alone should not authorize funds, but it reduces the system to the security of S2 and must be treated as a compromise event.

10 Security Testing & Assurance (Pre-Launch vs Future)

This chapter defines the security assurance program for Stablenotes. It separates what is mandatory before any v1 production deployment from what is explicitly future-gated and out of scope for v1. The goal is to prevent “security theater”: every claim must map to an evidence artifact, and every future claim must be gated behind specific tests and pass criteria.

Scope note: v1 is an owner-bound transaction-authorization layer, not a bearer-transfer product. Mandatory assurance covers the SIT, paired printer and print verification, independent factor custody, isolated signer, chain-specific owner policy, partner interfaces and media survivability.

10.1 Pre-launch mandatory audits (v1 ship gates)

Before live-value v1 deployment, independent review MUST cover issuance entropy and non-retention; SIT, paired printer and signer firmware and updates; public-print verification qualification; owner-policy enforcement; signer interoperability; and partner integration.

10.1.1 Key generation and non-retention audit (mandatory)

Purpose: Prevent catastrophic loss from weak randomness, key leakage, or secret retention.

Scope (minimum):

666. RNG correctness
667. Verify the qualified SIT entropy source and DRBG, exact build flags and linked binaries, health tests, secure failure behavior and absence of unapproved fallback generators.
668. Verify no insecure fallback RNG providers.
669. Verify uniqueness controls (no repeated keys).
670. Key lifecycle and memory hygiene
671. Identify all buffers and objects that may contain secrets.
672. Review secret handling for copies, string conversions, serialization, caching.
673. Verify zeroization/invalidation procedures (best-effort per platform).
674. Non-retention proof
675. Confirm secrets are not written to persistent storage (files, databases, preferences).

676. Confirm secrets are not present in logs, analytics, crash reports, or telemetry.
677. Confirm K is never transmitted to the printer or ordinary online systems; S1 may leave the SIT only through an authorized bounded print job and intended protected output, and S2 only through the approved independent custody handoff or separately controlled reference profile.
678. Crash/interrupt paths
679. Validate behavior under app kill, device restart, backgrounding, low-memory.
680. Confirm sensitive UI redaction where applicable.
681. Confirm no residual secret material appears in crash artifacts.
682. Print-flow verification gate
683. Confirm every note passes the public-key QR and checksum checks, the public indicators bind to the correct serial and issuance context, and the protected encoding is covered by an independently qualified correlation protocol.
684. Confirm any failures lead to safe abort and do not create “half-issued” dangerous states.

Deliverables (evidence artifacts):

685. Keygen_RNG_Independent_Audit.pdf
686. Non-Retention_Runtime_Test_Report.pdf
687. Crash_Interrupt_Path_Review.pdf
688. Sensitive_Flow_Verification_Gate_Test_Report.pdf

Acceptance criteria (ship gate):

689. No Critical/High findings open at launch.
690. No evidence of unauthorized Class A persistence, logging, leakage or exposure outside the explicitly approved issuance, printing, S2-custody and signing boundaries in tested builds.
691. Verified approved seeding, entropy health tests and no insecure RNG fallback in the exact production build.

10.1.2 Firmware and update chain audit (mandatory)

Purpose: prevent subversion of the SIT, paired printer or Isolated Signer through firmware compromise, downgrade, unauthorized print routes or supply-chain injection.

Scope (minimum):

692. Secure boot and chain-of-trust
693. Verify secure boot implementation, signature verification, and enforcement.
694. Verify debug interfaces locked/disabled in production.
695. Firmware attack surface review
696. Review connectivity interfaces (USB/BLE/Wi-Fi) and privileged commands.
697. Verify authentication/authorization for maintenance modes.
698. Confirm sensitive payloads are not logged/persisted.
699. Update security

700. Review signed update flow: verification-before-install.
701. Validate key hierarchy and signing key custody (HSM policy, role separation).
702. Validate anti-rollback controls.
703. Validate staged rollout + emergency pause procedures.
704. Supply chain / provisioning controls (high level)
705. Verify only signed firmware can be loaded at factory.
706. Verify device identity provisioning controls and traceability.

Deliverables (evidence artifacts):

707. Firmware_Secure_Boot_Update_Chain_Audit.pdf
708. Anti_Rollback_Downgrade_Attack_TestReport.pdf
709. Provisioning, per-pair credential custody and SIT/ATM hardware-in-the-loop security assessment for v1.
710. Debug_Interface_Lockdown_Verification_Report.pdf

Acceptance criteria (ship gate):

711. Secure boot enforced; unsigned firmware cannot run.
712. Downgrade attacks fail; anti-rollback is effective.
713. Update signing process has documented key custody and two-person integrity for release.
714. Factory provisioning process prevents firmware side-loading.

10.1.3 Companion app review (mandatory)

Purpose: Reduce the risk that the “untrusted phone” leaks secrets, misleads users, or compromises the v1 security posture.

Scope (minimum):

715. Scope enforcement
716. Verify v1 mode: verification/ transaction authorization only.
717. Confirm prohibited v1 features are not enabled (no custody, no “bank-like” claims).
718. Third-party SDK inventory and risk
719. Identify analytics/crash/reporting SDKs and disable session replay on sensitive screens.
720. Confirm privacy disclosures match reality.
721. Transaction safety and UI integrity
722. Verify warnings for irreversible actions and secret-handling steps.
723. Confirm safe error handling and retry behavior.
724. Data flow boundary review
725. Confirm no KYC artifacts or identity data handled by the app when third-party ramps are integrated (if applicable).

Deliverables (evidence artifacts):

726. App_Security_Review.pdf
727. Third-PartySDK_Inventory_and_Risk_Review.pdf
728. Sensitive_Screen_No-Replay_Redaction_Evidence.pdf
729. Data_Flow_Privacy_Boundary_Assessment.pdf

Acceptance criteria (ship gate):

730. No Critical/High findings open.
731. No session replay or sensitive telemetry on key-handling screens.
732. No contradictions between app-store privacy declarations and actual data handling (if applicable).

10.2 Future work (v2) explicitly gated (NOT shipped in v1)

This section exists to prevent accidental scope creep and over-claiming. The following tests are v2-only and are not required for v1 shipping but MUST be passed before any product is marketed or deployed as bearer-transfer/offline transactional.

10.2.1 Required v2 adversarial-transfer tests (examples)

733. Copy-without-open
734. Attempt to read/photograph/extract secret through sticker without visible tamper evidence.
735. Test across lighting, angles, optics, and common enhancement techniques.
736. Open-and-reseal
737. Attempt to peel, open, copy, and reseal such that normal inspection cannot detect prior opening.
738. Swap attack
739. Replace a genuine sticker with a counterfeit or swapped sticker/overlay.
740. Replace genuine note with a counterfeit note carrying attacker-controlled secrets.
741. Counterfeit replication
742. Produce counterfeit notes/stickers that pass lay inspection and initial validation procedures.
743. Field deception test
744. Evaluate whether non-expert agents/users can reliably detect tamper/counterfeit using the provided SOP.

v2 gating statement (mandatory):

745. These v2 tests are not shipped in v1.
746. No bearer-transfer product may be launched, marketed, or piloted until:
747. independent adversarial testing confirms success rates below defined thresholds, and
748. field detection procedures meet acceptable false-accept/false-reject rates.

10.3 Disclosure & bounty policy

A security product must assume vulnerabilities will be found. The question is whether the organization can detect, respond, and remediate with discipline.

10.3.1 Vulnerability reporting policy (VDP)

Stablenotes MUST maintain a published vulnerability disclosure policy that includes:

749. a dedicated security contact (email + PGP key or HackerOne)
750. scope of systems covered (SDK, app, firmware, smart contracts, media workflows)
751. safe-harbor language for good-faith research
752. reporting format expectations (PoC, logs, affected versions)
753. acknowledgment and response timelines

10.3.2 Bug bounty program (recommended; phased)

A bug bounty SHOULD be implemented in phases:

754. Phase 1 (private bounty): invite vetted researchers prior to launch.
755. Phase 2 (public bounty): expand scope post-launch once triage capacity is proven.

Bounty scope should explicitly include:

756. key generation and non-retention failures,
757. device update chain compromise,
758. app telemetry leakage,
759. smart contract vulnerabilities,
760. supply-chain/media integrity issues (where researchers can test safely).

10.3.3 Patch and remediation SLAs (mandatory)

Define and publish internal SLAs for:

761. critical vulnerabilities (e.g., 7–14 days)
762. high severity (e.g., 30 days)
763. medium/low (scheduled)

For firmware, define staged rollout and emergency pause procedures (see Chapter 7).

10.3.4 Post-launch monitoring commitments (mandatory)

At minimum, Stablenotes MUST maintain:

764. release monitoring and incident logging
765. anomaly detection for duplicate keys/public addresses (privacy-safe)
766. monitoring of failure rates in printing verification and scan success (field telemetry allowlist)
767. partner integration certification refresh checks (for SDK deployments)
768. periodic security reviews for third-party SDK changes

10.3.5 Public communication policy (mandatory)

Security communications must be controlled and factual:

769. publish security advisories when users/partners need to act

770. avoid ambiguous claims or minimization
771. provide clear remediation instructions and upgrade requirements

10.3.6 Implementation placeholders to be resolved prior to v1 production

772. Selected auditors and scope sign-off: [TBD]
773. Audit schedule and gating dates: [TBD]
774. Bug bounty platform and rules: [TBD]
775. Severity scoring model (CVSS + product-specific impact): [TBD]
776. Monitoring telemetry allowlist and retention: [TBD]
777. Partner certification refresh cadence: [TBD]

10.4 Mandatory cryptographic and ingestion audits

Audit domain	Minimum test	Gate
Secret-sharing implementation	Known-answer vectors; malformed/duplicate x coordinates; threshold behavior; field arithmetic; constant-time review	No mismatch across independent implementations; no critical/high findings
Entropy and coefficient generation	SP 800-90B-style source assessment; DRBG instantiation; health tests; fault behavior	Documented entropy claim and independent review
Factor independence	Trace S1/S2 across device, backups, logs, support and crash paths	Independent custody and support paths; transient SIT/signer co-location explicitly bounded and tested.
Optical parser	Fuzzing; oversized payloads; malicious metadata; image parser vulnerabilities	Fail closed; no secret disclosure or code execution
Transaction display	Destination/amount/asset/fee substitution and UI confusion tests	Displayed fields match signed canonical bytes
Zeroization	Success, cancel, timeout, crash, power loss and watchdog reset	No recoverable Class A material in defined tests
Side channels / fault injection	Power, EM, timing and fault review proportionate to deployment risk	Residual risk documented; critical paths remediated
Common-mode recovery	Compromise one firmware build, S2 provider, print lot or operator process	Blast radius within approved limits
SIT entropy and compiled build	Exact board and binary; entropy faults, compiler/link flags, RNG fallback and reproducible build	Independent review; health failures abort issuance
Paired printer link	Wrong pair, replay, downgrade, legacy secret path and uncertain print completion	Reject unauthorized job; UNKNOWN enters HOLD/VOID
Print-check correlation	Synthetic known S1; compare public indicators with both protected encodings; inject localized defects	Predeclared missed-defect bound and confidence met
Asset-policy bypass	Attacker has K; try alternate destination, delegation, upgrade and emergency paths; EVM: EIP-7702 authorizations, delegated calls, token approvals, executor roles and use of K outside the signer	Enforced policy rejects unauthorized release; all applicable alternate paths preserve owner binding

Audit domain	Minimum test	Gate
Incident-derived transaction substitution	Mutate target, amount, operation and calldata against displayed and signed bytes; EIP-7702 tuples, arbitrary-digest requests and multiple nonce authorizations in applicable EVM profiles	Mismatch or unsupported operation aborts before signing; unapproved delegation and unsupported signing domains fail closed

Before an empirical result is cited externally, the reproducibility release candidate must be committed and pushed, all 21 equation scripts and CSV outputs reconciled to the clean submission manuscript, and any archive identifier verified against its contents. The current package has been generated and validated locally; it is not yet treated here as a public archival record.

11 Regulatory Positioning (EU-Primary)

This chapter is a technical-policy analysis and must be read with the Legal Disclaimer. Regulatory classification depends on actual functions, roles, control and jurisdiction, not on product labels.

11.1 v1 functional boundary

778. Non-custodial: PrintDreams does not possess a threshold of shares, control owner destinations or move user assets.
779. Transaction authorization -only: v1 does not provide merchant acceptance, bearer transfer, payment initiation, exchange, brokerage, remittance or cash-out.
780. Third-party separation: regulated ramps, custodians or CASPs/VASPs provide their own services under separate terms and controls.
781. No identity on the secret medium by default: AML/CFT and Travel Rule data are handled by obliged entities through separate channels.

11.2 MiCA and EU transfer-of-funds context

MiCA states in its recitals that providers of non-custodial hardware or software wallets should not fall within the Regulation merely for that activity. This does not pre-determine the classification of a deployment that performs regulated services professionally. Regulation (EU) 2023/1113 separately establishes information requirements for certain transfers of crypto-assets, including transfers involving self-hosted addresses and CASPs.

Every production partner must complete a function-by-function legal assessment: who holds keys or sufficient shares; who executes an order; who controls smart-contract administration; who supplies transfer information; who performs KYC/sanctions screening; and who is responsible for self-hosted-address checks.

11.3 FATF Travel Rule and AML/CFT alignment

Owner binding can reduce anonymous possession-only transfer and can support destination controls. It does not satisfy the FATF Travel Rule by itself. Where a VASP/CASP participates in a covered transfer, that

entity remains responsible for collecting, holding and transmitting required originator and beneficiary information and applying risk-based controls.

11.4 Privacy and traceability

Public addresses and serials can create linkability. The design should separate inventory authenticity from user identity, minimize off-chain retention, restrict access, define deletion periods and avoid publishing balance-linked identity. A DPIA or equivalent assessment may be required where deployments systematically link notes, wallets and individuals.

11.5 Institutional and sovereign deployment

A sovereign or regulated-institution deployment requires additional authority, governance and resilience evidence. Offline reserve shares should be geographically distributed, subject to dual control or quorum, reconciled to public balances, tested under network and power failure, and integrated into incident, audit and legal-accounting procedures. Stablenotes is not an offline CBDC payment mechanism under v1.

Institutional deployment documentation must identify who approves issuance, holds each factor, validates funding evidence, administers the policy, handles device incidents and verifies retirement. These records support governance but do not by themselves establish regulatory authorization.

11.6 Regulatory evidence artifacts

782. Deployment-specific MiCA/CASP and payments analysis
783. Regulation (EU) 2023/1113 transfer-data flow and self-hosted-address procedure
784. FATF Travel Rule responsibility matrix
785. AML/CFT and sanctions control mapping for each partner
786. GDPR controller/processor matrix, RoPA and DPIA triggers
787. Sovereign/institutional mandate, audit and liability framework where applicable

12 Roadmap & Gates

This chapter sets out a two-track roadmap with explicit Go/No-Go gates and kill criteria. The intent is to (i) keep Stablenotes v1 deployable and investable as an SDK-first transaction authorization layer, and (ii) prevent v2 ambitions from contaminating v1 scope, compliance posture, or security claims.

Rule: Track A (v1) ships only on evidence. Track B (v2) proceeds only if Track A proves viability and Track B gates are passed.

12.1 Track A (v1): SDK-First transaction authorization Layer (Production Path)

12.1.1 Milestones and required evidence artifacts

Below is the recommended milestone sequence. Each milestone is paired with required evidence artifacts. All “TBD” fields must be completed with owners and dates prior to execution.

Milestone A0 — Scope lock and partner posture (TBD: Date)

Objective: Freeze v1 scope as transaction authorization -only and ensure partner-facing posture is consistent.

Required artifacts:

788. V1_Scope_Definition.pdf (explicit non-goals)
789. Marketing_Claims_Policy_v1.pdf
790. Partner_Integration_Boundary_Spec_v1.pdf

Gate: No v1 deployment proceeds if v1 copy/UX implies cash-like transfer or bearer usage.

Milestone A1 — Integration readiness (TBD: Date)

Objective: SDK and reference implementation support core lifecycle flows.

Required artifacts:

791. SDK_API_Spec_v1.md + sample integration
792. Partner_Integration_Certification_Checklist_v1.pdf
793. Reference_Wallet_Release_Notes_<ver>.pdf (placeholder)

Gate: “Hello world” integration must be achievable in ≤ [TBD] engineering days using the “golden path.”

Milestone A2 — Security baseline audits complete (TBD: Date)

Objective: establish v1 security fundamentals across SIT entropy and secret memory, authenticated printing and printer non-retention, signer integrity, owner-policy enforcement and integrated testing.

Required artifacts (minimum):

794. Keygen_RNG_Independent_Audit.pdf
795. Non-Retention_Runtime_Test_Report.pdf
796. Firmware_Secure_Boot_Update_Chain_Audit.pdf
797. Anti-Rollback_Downgrade_Attack_Test_Report.pdf
798. Third-Party_SDK_Inventory_and_Risk_Review.pdf
799. SIT_Entropy_and_Firmware_Independent_Assessment
800. Paired_Printer_Link_and_NonRetention_Report
801. Public_Print_Check_Correlation_Report
802. Signer_Interoperability_and_Policy_Bypass_Report.

Gate: No open Critical/High findings; remediation verified.

Milestone A3 — Durability qualification complete (TBD: Date)

Objective: Prove printed transaction authorization media survivability under defined service-life targets.

Required artifacts (minimum):

803. Durability_Test_Protocol_v1.pdf
804. Independent_Durability_Lab_Report.pdf
805. Sticker_Adhesive_Compatibility_Report.pdf

806. Supported_Device_Matrix_v1.pdf

Gate: QR scan success and fallback legibility meet thresholds in Chapter 9/Appendix

Milestone A4 — Supply chain integrity and traceability operational (TBD: Date)

Objective: Establish banknote-like traceability controls for media production and distribution.

Required artifacts:

807. Serialized_Note_Spec_v1.pdf
808. Batch_Manifest_Format_v1.pdf
809. ChainOfCustody_SOP_v1.pdf
810. Quarantine_Recall_SOP_OnePager.pdf
811. Quarantine drill: Quarantine_Drill_Report_<date>.pdf

Gate: Quarantine-by-serial-range drill meets SLA: quarantine initiated ≤ [TBD] hours and propagated ≤ [TBD] hours.

Milestone A5 — Controlled production pilot with design partner (TBD: Date)

Objective: Deploy v1 with a design partner under caps to generate field evidence.

Required artifacts:

812. Pilot_Spec_<partner>_v1.pdf (caps, geos, assets, support model)
813. Incident_Response_Runbook_Joint_v1.pdf
814. Pilot_Metrics_Dashboard_<period>.pdf

Gate: Pilot KPIs meet thresholds (below) with no critical incidents.

Milestone A6 — Production launch (TBD: Date)

Objective: Scale to production partner deployment(s) using the certified integration program.

Required artifacts:

815. Evidence_Pack_Index_v1.pdf (claims-to-evidence mapping)
816. Release_Governance_and_Change_Control_SOP.pdf
817. Partner_Production_Readiness_Sign-off_<partner>.pdf

Gate: All ship-gate controls are GREEN; partner operations trained; ongoing monitoring operational.

12.1.2 Go/No-Go conditions (v1)

A v1 deployment is GO only if all are true:

Security gates (must-pass):

818. Independent audits confirm RNG correctness and non-retention (Chapter 10).
819. Secure boot, signed updates, and rollback protection verified (Chapter 7).
820. No unresolved critical/high issues.

Reliability gates (must-pass):

821. Durability lab results meet scan success + legibility thresholds (Chapter 9).
822. Every note passes the approved public-key QR and checksum checks; the protected print correlation, approved media configuration and verification protocol have passed independent qualification.

Operational gates (must-pass):

823. Supply chain traceability operational; quarantine drill passed (Chapter 6 supply chain).
824. Partner integration certified and support runbooks in place.
825. SIT/ATM unique pairing and legacy-path denial, printer non-retention, unknown-job handling, independent S2 custody, shared factor vectors and asset-policy bypass tests are verified on the exact production configuration.

No-Go triggers (immediate):

826. Evidence of key leakage or secret retention in production builds.
827. Systemic unreadable-media incidents above threshold.
828. Firmware/update integrity compromise.
829. Partner refuses required boundary controls or claims discipline.
830. Unqualified SIT entropy, bypassable or unauthenticated printer path, missed-defect performance beyond the approved bound, forged funding evidence, or a spend-capable route that defeats the owner policy.

12.1.3 v1 kill criteria (hard)

If any of the following occurs, Track A should be paused or terminated unless remediated with verified evidence:

831. Catastrophic key compromise (RNG failure, non-retention breach, firmware compromise) with credible exploit path.
832. Unrecoverable loss rate exceeding [TBD threshold] under normal use (unreadable QR/fallback without viable transaction authorization).
833. Support burden indicates the product is unsafe for non-expert users at scale (e.g., critical user error rate above [TBD]).
834. Partner adoption stalls: no additional partners move from LOI → integration within [TBD 6–9 months] despite evidence pack completion.

12.2 Track B (v2): Separate Program (Future-Gated)

Track B is a separate program that explores bearer-transfer/offline transactional use cases. It is not part of v1 and must not be implied by v1 claims, marketing, or partner deployments.

12.2.1 Entry criteria (v2 cannot start until these are met)

Track B may proceed only if:

835. Track A proves viability
836. at least [TBD: 1–2] production partner deployments OR equivalent traction signal

837. durability and incident rates within target thresholds for [TBD: 3–6 months]
838. Security maturity is proven
839. v1 evidence pack is complete and maintained
840. security operations (VDP/bounty/IR) functioning in practice
841. Regulatory and liability pathway exists
842. credible sponsor/authorization strategy in the target pilot geo(s) (placeholder)
843. preliminary liability/reserve framework is economically viable (placeholder)

12.2.2 v2 kill criteria (hard)

Track B must be killed (or paused indefinitely) if any occur:

844. Adversarial transfer cannot be secured
845. independent red-team testing shows practical copy-without-open or reseal success rates above acceptable thresholds.
846. Field detectability fails
847. non-expert detection SOP produces unacceptable false-accept rates (tampered/counterfeit notes pass inspection).
848. Regulatory pathway is not credible
849. no viable sponsor/authorization path within [TBD timeframe] despite sustained effort, or requirements make the business uneconomic.
850. Loss/fraud economics are untenable
851. required reserves/insurance or expected loss rates make unit economics non-viable.
852. v2 contaminates v1
853. if v2 work causes v1 to drift into “cash replacement” positioning, increases compliance exposure, or jeopardizes key partners.

12.2.3 Placeholders to finalize

854. Target dates per milestone: [TBD]
855. Partner names and pilot caps: [TBD]
856. Audit firms and lab vendors: [TBD]
857. Quantitative thresholds (unrecoverable loss rate, scan success, support burden): [TBD]
858. v2 security thresholds and red-team rounds: [TBD]

12.3 Research-integration gates

Gate	Required evidence
R0 Reproducibility release	Reconcile all 21 equation scripts, inputs, outputs, notebook and tests to the clean submission manuscript; commit and push; verify any archive identifier and record the public commit hash.
R1 Data identification	Build stablecoin- and custody-segment event datasets with time-weighted reachable exposure, recovery horizons and matched metadata before estimating digital intensity or RVR.

Gate	Required evidence
R2 Cryptographic profile	Select XOR or Shamir; freeze field/encoding; publish test vectors; complete independent review.
R3 Factor independence	Demonstrate independent S1/S2 custody and support paths, with documented and assessed transient co-location inside the approved SIT and signer boundaries.
R4 Ingestion assurance	Pass secure-boot, parser, display, signing, zeroization, side-channel and malicious-input testing.
R5 Correlation stress	Model and test common-mode compromise across lots, firmware, S2 stores and operational personnel.
R6 Policy validation	Complete EU/FATF and deployment-specific legal analysis; verify product behavior against stated boundary.
R7 Sovereign-grade gate	Only after R0-R6 plus continuity exercises, governance approval and public-sector assurance may that classification be used.
R8 Issuance and print verification	Qualify SIT entropy, paired link, printer non-retention, non-revealing public-check correlation, signer vectors and independently authenticated funding eligibility.

12.4 Additional kill criteria

859. Any production profile prints or exports a possession-sufficient complete spend key while claiming owner binding.
860. Independent implementations disagree on share reconstruction or field arithmetic.
861. A partner backend, analytics SDK or support path receives Class A material.
862. Transaction display can be made to differ from signed bytes in a plausible attack.
863. A common-mode defect makes the assumed $1/N$ or p^N risk reduction materially false at the deployed partition scale.
864. Empirical RVR or deterrence claims are published without aligned data, limitations and reproducibility evidence.
865. Regulatory or sovereign-grade claims exceed the documented function and evidence boundary.
866. An unauthorized print path, unbounded secret retention, unqualified public-check correlation, forged funding eligibility or owner-policy bypass is demonstrated in the production configuration.

Appendices (Evidence-first)

Every material security, reliability, economic or regulatory claim in the main body must map to an owned artifact with acceptance criteria and status. Defined models as per research article and product-derived evidence remain separate evidence classes.

Appendix A - Claims-to-Evidence Matrix

Claim ID	Claim	Class	Evidence	Acceptance	Status
C-OWN-01	Possession of S1 alone cannot reconstruct K	Cryptographic	Scheme proof + implementation vectors + factor-independence audit	No unauthorized shared custody, backup or support path; transient SIT/signer co-location documented and assessed.	Pending
C-AIR-01	Passive substrate has no direct network interface	Architecture	Hardware/interface inspection + threat model	No enabled network/data interface on substrate	Design
C-AIR-02	End-to-end compromise is bounded but nonzero	Assurance	Attack-path register + red-team report	All critical/high paths resolved or remediated	Pending
C-DUR-01	S1 remains recoverable for claimed service life	Reliability	Independent lab + real-time aging + device matrix	Pass stated decode/legibility thresholds	Pending
C-RISK-01	All 21 manuscript equations and stated empirical calibrations reproduce from versioned code and data	Research	Scripts + CSV inputs/outputs + unified notebook + tests + public commit/archive manifest	Exact arithmetic; documented provenance, precision, hashes and no unsupported cross-domain estimates	Local candidate validated; public release pending
C-POL-01	Owner binding supports non-bearer transaction authorization	Policy	Functional legal analysis + product behavior test	No possession-only or arbitrary-destination path	Pending
C-SOV-01	Deployment qualifies as sovereign-grade	Governance	Independent assurance + continuity drills + legal mandate	All sovereign gates passed	Not claimed
C-PQ-01	No classical-signature-only release	Post-Quantum	Smart contract audit shows that protected assets are not released on the strength of a classical signature alone	Missing/invalid PQ approval causes rejection	Pending
C-PQ-02	No privileged bypass	Post-Quantum	Independent test showing that special paths are incapable of removing PQ requirement, substitute keys or enable asset redirection	Active PQ policy governs anything capable of affecting asset release	Pending
C-PQ-03	No reconstructable signing material in evidence	Post-Quantum	Inspection of events, logs, telemetry, etc. shows no secret shares	Public verification artifacts may be retained under a defined evidence and privacy policy	Pending
C-PQ-04	Authorized migration without downgrade	Post-Quantum	Owner authorization intact during key rotation, algorithm changes and contract migration	Authorization does not weaken due to fallback or intermediate states.	Pending
C-SIT-01	SIT issuance entropy and memory handling	Assurance	Independent board/build and entropy review	Qualified entropy; fail closed; no unauthorized residuals	Pending

Claim ID	Claim	Class	Evidence	Acceptance	Status
C-PRT-01	Only approved paired printer jobs accepted	Assurance	HIL tests; printer memory and route audit	Wrong pair, replay, legacy route and uncertain retry rejected	Pending
C-VRF-01	Public checks predict protected print quality	Reliability	Synthetic note correlation and fault-injection report	Missed-defect rate and confidence meet approved plan	Pending
C-POL-02	Owner policy resists direct K-based bypass	Policy	Chain-specific adversarial audit and test vectors	Unauthorized destination and privileged routes rejected	Pending
C-INT-01	SIT factors interoperate with signer	Cryptographic	Frozen shared vectors and end-to-end tests	Exact context, signature and reconstruction agreement	Pending

Appendix B - Chain and Contract Annex Requirements

867. Deployment chain, network ID and verified asset identifiers
868. Transaction authorization -policy contract address and code hash
869. Message schema / ABI / TL-B definitions
870. Owner-destination commitment format and rotation rules
871. Replay-protection domain and nonce semantics
872. Upgradeability, administrative roles, timelock and no-drain proof
873. Events, error codes, failure behavior and audit reference
874. Post-quantum authorization extension status.
875. When status above is enabled, the annex MUST additionally specify enforcement boundary, cryptographic profile, credential lifecycle, approval & replay rules, migration & emergency controls, dependencies & limitations, operational feasibility and conformance evidence.
876. Issuance and signing profiles: exact SIT, printer and signer builds; per-pair link; public print-check protocol and evidence; approved S2 handoff; independently verified funding and custody; and handling for chain, token, bridge and destination dependencies.

Appendix C - Test Protocol Index

Protocol	Domain	Minimum scope
C.1	Entropy and DRBG validation	K, pads, Shamir coefficients, nonces, health tests
C.2	Secret-sharing interoperability	Known-answer vectors, thresholds, malformed shares, field arithmetic
C.3	Non-retention and memory hygiene	Logs, storage, crash, cancel, power loss, camera/printer buffers
C.4	Ingestion terminal	Boot, update, parser fuzzing, display, signing, zeroization, side channels
C.5	Media durability	Mechanical, water/humidity, chemical, UV/thermal, adhesive, decode

Protocol	Domain	Minimum scope
C.6	Tamper evidence	Optical viewing, peel/reseal, counterfeit, user detection
C.7	Smart contract / wallet policy	Destination binding, replay, states, admin roles, fail-closed behavior
C.8	Common-mode and continuity	Lot, firmware, S2 store, operator, site and network failures
C.9	Partner integration	Data-flow, telemetry, third-party SDKs, incident RACI and liability
C.10	PQ Extension	Classical-key compromise, unauthorized enrollment, privileged bypass, migration downgrade and PQ boot/update failure
C.11	SIT and paired printer	Hardware entropy, firmware build, mutual authentication, legacy bypass, replay, HOLD/VOID and print-memory forensics
C.12	Public print-check correlation	Synthetic known S1; front/back public indicators; actual protected encoding; localized and interrupted-print defects; predefined statistical acceptance
C.13	Incident-derived authorization	Malicious transaction presentation, forged commands, direct K-based bypass, external verifier failure and owner-policy rejection; Binance-style EVM delegation and multi-nonce requests, compromised signer orchestration and independent asset-policy enforcement [R31, R32, R36]

Appendix D – Research Article Integration and Reproducibility

D.1 Source and research questions

Primary integration source: Alex Breton, The Asymmetric Attack Surface of Fiat Substitutes: A Measurement Framework and Owner-Bound Offline Custody Architecture. The article asks:

877. RQ1: Under what conditions can exposure-normalized loss intensities be compared across physical cash and USDC or USDT in a specified custody configuration?
878. RQ2: How do remote reach, automation, common-mode compromise, transfer speed, and enforcement friction enter an offender's expected payoff?
879. RQ3: Which attack paths are reduced by an owner-bound passive substrate, and which remain in the end-to-end custody system?
880. RQ4: How does value partitioning affect expected loss, variance, and catastrophic-loss probability when compromise events are correlated?

D.2 Measurement framework and empirical calibration

$$G_{j,t} = \sum_{e \in \mathcal{E}_{j,t}} g_e\,, \qquad N_{j,t}(h) = \sum_{e \in \mathcal{E}_{j,t}} [g_e - r_e(h)]; \quad E_{j,t} = \frac{1}{T}\int_t^{t+T} V_j\,(u)\,du.$$

$$\hat{L}^G_{j,t} = \frac{G_{j,t}}{E_{j,t}}, \qquad \hat{L}^N_{j,t}(h) = \frac{N_{j,t}(h)}{E_{j,t}}$$

These are value-weighted gross and net loss intensities, not per-unit theft probabilities.

$RVR_{a,b} = \frac{\hat{L}^G_{a,t}}{\hat{L}^G_{b,t}}$ is reportable only after matching period, geography, asset and custody perimeter, event definition, gross/net convention, valuation rule, exposure concept and reporting coverage. No cross-domain point estimate is reported.

2019 U.S. reported currency gross intensity = 1,423,559,757 / 1,759,800,000,000 = **0.080893%.**

Reported recovery share = 36,980,933 / 1,423,559,757 = **2.5978%**;

Net reported intensity = (1,423,559,757 - 36,980,933) / 1,759,800,000,000 = **0.078792%**.

The calibration is a lower bound and uses year-end currency in circulation, including notes abroad. Approximately USD 2.2 billion of 2024 digital-asset theft is triangulated by Chainalysis and TRM Labs, but no matched exposure denominator is available.

The Binance incident provides a dated event-level example and should not be considered a population risk estimate: its approximate USD 6.3 billion gross impact, approximately USD 3 billion frozen on-chain as reported by Binance on 30 October, any later victim recovery, and corporate replenishment are distinct measures. Amounts must be matched by asset, valuation time and recovery horizon; immobilized assets are not automatically recovered funds [R31, R34].

D.3 Enforcement pipeline and deterrence

For a cohort of eligible events, the observable transition rate is: $\hat{\theta}_k = \frac{n_k}{n_{k-1}}, \quad k = 1, \dots, K$ and the cohort probability of reaching the final recorded stage is $\hat{p}_{0\to K} = \prod_{k=1}^{K} \hat{\theta}_k = \frac{n_K}{n_0}$

These equalities require consistent event linkage and a sufficiently mature cohort.

$DR_{c,d}^{(p)} = \frac{p_c}{p_d}, \qquad p_d > 0$ is descriptive only for matched cohorts and equivalent final outcomes. Clearance, persons identified, complaints, prosecution and conviction cannot be substituted for one another; no cross-domain deterrence point estimate is reported.

D.4 Offender-choice and partition-risk models

Risk-neutral offender payoff: $\pi_j = q_j G_j - c_j - q_j p_j (F_j + R_j).$

A custody control may lower technical success q_j, transferable gain G_j, or common-mode reach; increase cost c_j; or improve recovery R_j and enforceable sanction p_j.

For N equal partitions, $L = \frac{W}{N}\sum_{i=1}^{N} X_i, \qquad \mathbb{E}[L] = pW;$

$\mathrm{Var}(L) = W^2 p(1-p)\left[\frac{1}{N} + \rho\frac{N-1}{N}\right]$ Partitioning reduces concentration under independence but does not reduce expected loss when ρ is unchanged.

With common-mode probability q, $\Pr(L = W) = q + (1-q)p^N$.

A portfolio objective may combine $\min_N \mathbb{E}[L_N] + \lambda\,\mathrm{CVaR}_\alpha(L_N) + C(N)$, subject to recovery and governance constraints. This is a decision framework and cannot be treated as an empirical optimum.

Issuer freezing can affect an offender's attainable gain, but its value cannot automatically be subtracted from that gain or treated as victim recovery: legal control, prior conversion, valuation time, later release and actual return all matter. Multi-chain outflows can indicate common operational exposure; neither the common-mode probability nor this product's risk reduction is estimated from the Binance incident [R31, R32, R34].

D.5 Repository and data-availability status

The public baseline is https://github.com/printdreams/cryptoeconomic-theft-asymmetry at commit f6e87ea7cab8420504cb7f33704ace56cd48f254. A local reproducibility release candidate has been generated and validated with 21 numbered-equation scripts, input and output CSV files, a unified reproduce_report_figures.ipynb notebook, tests, continuous-integration configuration and documentation. The release candidate must be committed and pushed before the whitepaper cites a new public commit; any DOI or archive identifier must be verified after deposit.

D.6 Methodological limitations

881. No public source supplies a global event-level stablecoin-theft numerator matched to average reachable exposure and followed through a comparable enforcement pipeline.
882. Commercial blockchain-intelligence datasets are useful but proprietary, updateable and sensitive to taxonomy, valuation, recovery and incident-linkage rules.
883. The 2019 cash calibration is U.S.-specific, reporting-dependent and based on year-end currency stock that includes notes abroad rather than time-weighted theft-exposed value.
884. Gross stolen value and net loss after recovery are different estimands; recovery horizon and valuation convention must be stated.
885. Right-censoring, jurisdictional transfer, multiple defendants and missing outcomes can bias enforcement-stage estimates.
886. Partition independence may fail through common firmware, process, storage, operator, site or coercion events; positive dependence and common-mode probability must be modeled.
887. Cryptographic correctness does not establish end-to-end security. Parser, firmware, supply-chain, side-channel, coercion, human-factors and environmental performance remain engineering evidence obligations.

D.7 Remote theft incidents and security scenarios

The Remote Digital Asset Theft Report [R22] compiles publicly reported incidents and distinguishes gross movement, returned value and net loss. These cases guide threat modeling and test selection; they are not a representative sample from which a per-unit theft probability or cross-domain vulnerability ratio can be inferred.

Signing workflow: the 2025 Bybit incident illustrates transaction manipulation through a compromised wallet interface. A corresponding deployment test must compare the signer's authoritative display with the actual signed action and reject unauthorized operations; physical media alone is not proof of that property [R23].

Forged commands: the September 2026 Bitget incident illustrates compromise of a third-party security product followed by fraudulent wallet-backend instructions. The corresponding test submits a plausible privileged command without valid independent approval and confirms rejection at the relevant enforcement boundary [R24].

Binance signing and account delegation: Following the 29 October 2026 attack, Binance estimated an approximately USD 6.3 billion hot-wallet impact. Its initial investigation cited a possible compromised endpoint and unauthorized withdrawal submissions; it later identified additional breach points and

reported no evidence of a wallet-private-key leak [R31]. TRM Labs identified a batch of 50 signed EIP-7702 authorizations affecting an Ethereum hot wallet, alongside transfers on other chains [R32]. Protocol C.13 and §10.4 test unauthorized delegation, direct-key and executor bypass, and signer display; they do not demonstrate that the proposed architecture would have prevented this incident.

Weak entropy: the 2026 COLDCARD disclosure illustrates how incorrectly generated seed material can permit remote key regeneration even when a device was not remotely accessed. Tests must cover the exact production entropy path and compiled image; previously affected keys require migration rather than a firmware update alone [R25].

External dependencies: the Kelp DAO and Liquid Network incidents illustrate respectively a compromised external verification path and a protocol validation defect. Deployment evaluation must identify bridge, consensus, token-administrator and destination dependencies; the physical authorization factor cannot by itself repair those failures [R26, R27].

Source discipline: incident value, recovery, attribution and loss horizon can change. Use dated primary disclosures and distinguish gross movement from net loss; no incident example is evidence that this product prevented the event or that all digital assets share one measured loss rate.

D.8 Future research

888. Post-quantum share commitments and signing profiles
889. Open deterministic optical verification
890. Macroeconomic stress tests of hybrid offline reserve architectures
891. Empirical stablecoin-specific exposure and recovery datasets
892. Correlation measurement for partitioned custody
893. Human-factors and coercion-resistance trials

Appendix E - Normative Cryptographic Checklist

894. Scheme and threshold fixed per release
895. Field or XOR construction fully specified
896. Entropy source and DRBG documented
897. Independent share domains demonstrated
898. Canonical share encoding and bounds fixed
899. Checksum and cryptographic authentication separated
900. Public-key/address commitment verified
901. Known-answer and malformed-share vectors published
902. Constant-time and zeroization behavior reviewed
903. Rotation, loss, replacement and retirement procedures tested
904. SIT entropy path, compiled configuration and fail-closed health tests independently reviewed
905. Public print-check correlation qualified with synthetic factors, localized defects and a stated confidence bound
906. SIT–signer canonical factor and chain-specific golden vectors matched

907. Direct K-based, privileged and emergency owner-policy bypass attempts rejected

Appendix F - References and Authoritative Sources

[R1] Breton, A. (2026). The Asymmetric Attack Surface of Fiat Substitutes: A Measurement Framework and Owner-Bound Offline Custody Architecture.Full text: https://journals.lincoln.ac.nz/index.php/JFDA/article/view/1418/980

[R2] Becker, G. S. (1968). Crime and Punishment: An Economic Approach. Journal of Political Economy 76(2), 169-217. https://doi.org/10.1086/259394

[R3] Shamir, A. (1979). How to Share a Secret. Communications of the ACM 22(11), 612-613. https://doi.org/10.1145/359168.359176

[R4] Chainalysis (2024). $2.2 Billion Stolen in Crypto in 2024. https://www.chainalysis.com/blog/crypto-hacking-stolen-funds-2025/

[R5] Federal Bureau of Investigation, UCR. Clearances / Offenses Cleared by Arrest or Exceptional Means. https://ucr.fbi.gov/crime-in-the-u.s/2019/crime-in-the-u.s.-2019/topic-pages/clearances

[R6] NIST SP 800-90B. Recommendation for the Entropy Sources Used for Random Bit Generation. https://csrc.nist.gov/pubs/sp/800/90/b/final

[R7] NIST SP 800-57 Part 1 Rev. 5. Recommendation for Key Management. https://csrc.nist.gov/pubs/sp/800/57/pt1/r5/final

[R8] Bitcoin Improvement Proposal 38. Passphrase-protected private key. https://github.com/bitcoin/bips/blob/master/bip-0038.mediawiki

[R9] FATF (2021). Updated Guidance for a Risk-Based Approach to Virtual Assets and VASPs. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html

[R10] FATF (2025). Best Practices in Travel Rule Supervision. https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/Best-Practices-Travel-Rule-Supervision.pdf

[R11] Regulation (EU) 2023/1114 on Markets in Crypto-assets (MiCA). https://eur-lex.europa.eu/eli/reg/2023/1114/oj/eng

[R12] Regulation (EU) 2023/1113 on information accompanying transfers of funds and certain crypto-assets. https://eur-lex.europa.eu/eli/reg/2023/1113/oj/eng

[R13] European Banking Authority (2024). Travel Rule Guidelines. https://www.eba.europa.eu/publications-and-media/press-releases/eba-issues-travel-rule-guidance-tackle-money-laundering-and-terrorist-financing-transfers-funds-and

[R14] BIS Innovation Hub (2023). Project Polaris: Handbook and High-Level Design Guide for Offline CBDC Payments. https://www.bis.org/publ/othp64.htm and https://www.bis.org/publ/othp79.htm

[R15] Reproducibility repository baseline: https://github.com/printdreams/cryptoeconomic-theft-asymmetry, commit f6e87ea7cab8420504cb7f33704ace56cd48f254. A locally validated release candidate exists; cite a replacement public commit only after push and verification.

[R16] International patent publication WO 2025/237814 A1.

[R17] Federal Bureau of Investigation. (2019). Crime in the United States 2019: Table 24, Property Stolen and Recovered, by Type and Value. https://ucr.fbi.gov/crime-in-the-u.s/2019/crime-in-the-u.s.-2019/topic-pages/tables/table-24

[R18] Federal Reserve Board. (2026). Currency in Circulation: Value. https://www.federalreserve.gov/paymentsystems/coin_currcircvalue.htm

[R19] Federal Bureau of Investigation. (2023). Bank Crime Statistics: Federally Insured Financial Institutions, January 1-December 31, 2023. https://www.fbi.gov/file-repository/reports-and-publications/bank-crime-statistics-2023-091724.pdf

[R20] Federal Bureau of Investigation. (2025). 2024 IC3 Annual Report. https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf

[R21] TRM Labs. (2025). Category Deep-Dive: USD 2.2 Billion Was Stolen in Crypto-Related Hacks in 2024. https://www.trmlabs.com/resources/blog/category-deep-dive-2-2-billion-was-stolen-in-crypto-related-hacks-in-2024

[R22] Remote Digital Asset Theft Report (2026). Research report completed 28 October 2026; unpublished research input. Primary incident sources are cited separately below.

[R23] Sygnia. Sygnia's Investigation into the Bybit Hack: What We Know So Far. https://www.sygnia.co/blog/sygnia-investigation-bybit-hack/

[R24] Bitget. Was Bitget Hacked? Security incident timeline, impact and response. https://www.bitget.com/academy/bitget-security-incident-what-happened-timeline-impact-response

[R25] Coinkite (2026). COLDCARD Security Update: Seed Generation, Transaction Integrity, and Data Isolation. https://blog.coinkite.com/coldcard-security-update-5.6.1-1.5.1q/

[R26] LayerZero Labs (2026). KelpDAO Incident Report, 18 May. https://layerzero.network/publications/kelpdao-incident-report.pdf

[R27] Blockstream (2026). Liquid Network Security Incident Assessment, 23 September. https://blog.blockstream.com/liquid-network-security-incident-assessment/

[R28] PrintDreams (2026). System Sequence Specification, version 0.3, document PD-TR-SSS-001; controlled internal technical specification.

[R29] PrintDreams (2026). Secure Issuance Terminal Firmware Technical Specification, version 0.1, document PD-TR-SIT-001; controlled internal technical specification.

[R30] National Institute of Standards and Technology (2024). NIST IR 8547, Transition to Post-Quantum Cryptography Standards, initial public draft. https://csrc.nist.gov/pubs/ir/8547/ipd

[R31] Binance (2026, 30 October). Security Incident Update #2: unauthorized hot-wallet withdrawals, preliminary investigation and response. https://www.binance.com/en/support/announcement/detail/d3306d9dca5243548c813b605e1d1751

[R32] TRM Labs (2026, 29 October). North Korea Steals USD 6.36 Billion From Binance in the Largest Hack in History; on-chain snapshot as of 30 October, 00:30 UTC. https://www.trmlabs.com/resources/blog/north-korea-steals-usd-6-36-billion-from-binance-in-the-largest-hack-in-history

[R33] Chainalysis (2026). Binance Hack: Tracing the $6.4 Billion Theft to North Korea. https://www.chainalysis.com/blog/binance-exploit-latest-findings-and-response/

[R34] Elliptic (2026, updated 1 November). The Largest Theft in History: North Korea likely behind the $6.4 billion Binance hack. https://www.elliptic.co/insights/binance-largest-hack-in-history/

[R35] Federal Bureau of Investigation (2026, 31 October). North Korea Responsible for $6 Billion+ Binance Attack. https://www.fbi.gov/investigate/cyber/alerts/2026/north-korea-responsible-for-6-billion-binance-attack

[R36] Buterin, V., Wilson, S., Dietrichs, A., and lightclient (2024). EIP-7702: Set Code for EOAs. Ethereum Improvement Proposals. https://eips.ethereum.org/EIPS/eip-7702

[R37] Binance (2026, 1 November). Security Incident, Recovery Update #4: Withdrawals Resume in Phases. https://www.binance.com/en-GB/support/announcement/security-incident-recovery-update-4-withdrawals-resume-in-phases-2026-11-01-73911fb819b240f88b88256bdd318eda

[R38] Binance October 2026 Research (2026, 2 November). Incident research and proposed whitepaper integration; unpublished research input. Case-specific factual claims are supported by the primary sources above.