

SWEEP

Provisional Runtime and Configuration Assessment

State Street Galaxy Onchain Liquidity Sweep Fund
Public-evidence review of an unauthenticated candidate Solana deployment

REPORT	B3-SWEEP-2026-001
ISSUED	1 October 2026
BASELINE	Candidate identity and supply rechecked at finalized context slot 451,412,449; detailed runtime/configuration observations at slots 451,392,301-451,393,190
AUTHOR	bench3.ai

Provisional opinion. State Street, SSGA and Galaxy have not publicly authenticated the reviewed mint as the production representation of a specified SWEEP legal vehicle or share class. Exact mainnet source and reproducible builds were not available; this is neither a complete source audit nor a full authenticated product audit.

Contents

1 Executive Summary 3

2 Scope and Assessment Basis 4

3 System and Threat Model 5

4 Technical Assessment 6

5 Recorded Validation and Coverage 7

6 Findings and Control Observations 8

7 RWA Linkage and Public Verifiability 9

8 Limitations and Conclusion 10

A Candidate Deployment and Authority Inventory 11

B Evidence and Source Index 11

Assessment of a publisher-correlated but issuer-unconfirmed candidate mint, hook, controller and authority graph. Scope, methods and exclusions are defined in Section 2.

1 Executive Summary

bench3.ai assessed the recorded runtime, configuration and representative execution evidence for a Solana Token-2022 mint whose metadata identifies State Street Galaxy Onchain Liquidity Sweep Fund with symbol SWEEP. The mint, transfer hook, MMF controller, ProgramData accounts, authority PDA and ExtraAccountMetaList form a coherent live graph, and Galaxy's public portal IDL strongly correlates the application family. No issuer-approved artifact was found that maps this exact graph to a specified onshore, offshore, master, feeder or share class. The deployment remains a candidate and the opinion is provisional. [E01-E06; S01-S04]

Recorded work covered Token-2022 extensions, current supply and token accounts, upgradeable-loader state, ProgramData payload identities, EAML configuration, PDA derivation, role/user accounts and representative subscription, redemption and transfer-hook traces. The exact deployed hook/controller source, mainnet IDLs and reproducible-build correspondence were unavailable, so observed guard behavior cannot be generalized to every executable branch. [E01-E04]

Provisional assessment conclusion

No reportable vulnerability was confirmed in the assessed candidate runtime and configuration. Two control observations and four material limitations are reported. The evidence supports a bounded configuration/runtime assessment, not an exhaustive mainnet source audit or an authenticated opinion on the SWEEP legal product.

Classification	Recorded result
Confirmed vulnerabilities	Critical 0 High 0 Medium 0 Low 0
Control observations	2; upgrade authority and protocol authority-PDA trust dependencies
Unconfirmed candidates	0; unresolved branch completeness is reported as a scope limitation
Deployment identity	Very-high-confidence publisher-correlated candidate; legal mapping unconfirmed

Material qualification

The authority PDA controlling mint, freeze, metadata and hook configuration is deterministically derived under the MMF controller, and recorded production traces place PDA signatures inside role-, attestation- or payment-bound controller workflows. This is strong negative evidence against a simple ordinary-caller path. It is not proof that every dispatcher branch reaching invoke_signed is correctly authorized because exact deployed source, the mainnet IDL and a complete control-flow reconstruction were unavailable. [E03-E04]

2 Scope and Assessment Basis

2.1 Candidate deployment baseline

Parameter	Assessment record
Network	Solana mainnet-beta
Candidate Token-2022 mint	AgBSDfS7CNRUnBeREHHdF9S57fai5b3EXH1hgvZkRPhB
Transfer-hook program	3SajY54CXjD1efuLnH42tNWzu8ZVHZCLQ17mXjRmHq9Z
MMF controller	CnuNzfvSq5fTZ8gWfjH8TyQaEFmZypg69VbQrNgZGhxY
Principal identity and supply recheck	Finalized context slot 451,412,449
Detailed runtime/configuration observations	Finalized context slots 451,392,301-451,393,190; EAML observed at slot 451,392,448
Identity status	Very-high-confidence technical candidate; issuer and legal-vehicle mapping not established

At the principal identity and supply recheck at finalized context slot 451,412,449, the candidate mint had eight decimals, raw supply 15,635,537,103,049,540, and seven enumerated token accounts whose balances summed exactly to supply. The mint account SHA-256 was 5d9191f21c94b6e20d4182bf3e2611d643fb6c0cf00aba6783416a6f6e2d41ef. Detailed mint-extension, program, ProgramData, role and user observations were recorded earlier at finalized context slots 451,392,301-451,393,190, with the EAML specifically observed at slot 451,392,448. A fixed-state balance reconciliation establishes on-chain arithmetic at its stated snapshot; it does not establish legal shares, NAV or assets under custody. [E01-E04]

2.2 Assessment type and methods

Method	Applied scope
Read-only account decoding	Token-2022 mint and extensions, token-account census, program/ProgramData state, EAML, role accounts and user accounts at finalized slots.
Runtime identity review	ProgramData deployment slots, common upgrade authority, exact ELF payload hashes and embedded instruction/error strings.
Deterministic derivation	Recomputation of mint_v1, mmf_authority, system/program-state and hook-authority PDAs.
Historical trace review	Representative successful FiatSubscribe, StablecoinSubscribe, redemption, Token-2022 transfer-hook and burn workflows.
Public identity and RWA review	Issuer, manager, portal and regulatory materials available through 30 September 2026.

Method boundary: all production interactions supporting this assessment were read-only. Candidate identity and supply were rechecked at finalized context slot 451,412,449; detailed runtime, loader, role and user evidence came from finalized context slots 451,392,301-451,393,190; and the EAML observation was at slot 451,392,448. Historical transaction evidence is bound to the separately identified finalized records. No state-changing production transaction or private-system test forms part of the evidence basis. [E01-E04]

2.3 Included and excluded boundaries

Included: the candidate mint; current Token-2022 extensions; hook and controller loader state; ProgramData identities; EAML; authority and state PDAs; current role/user-account enumeration; and representative public execution traces. Excluded: issuer authentication of the graph; exact mainnet source, IDLs and reproducible builds; exhaustive branch-level semantics; signer custody; private portal configuration; offering documents; legal register; NAV feed history; portfolio, custody and settlement records; and financial, reserve or legal assurance.

The publication date is 1 October 2026. It is not a chain observation date. The technical conclusions are bound to the finalized slots, ProgramData payload hashes and transaction records cited in the evidence; the public RWA evidence cutoff is 30 September 2026.

3 System and Threat Model

The candidate deployment uses Token-2022 with metadata stored on the mint and a transfer-hook extension. The mint and freeze authorities, metadata update authority and hook-configuration authority are the same off-curve mmf_authority PDA. The MMF controller is the only program that can sign for that PDA. The transfer hook resolves controller-owned state, role and source/destination user accounts through a seven-entry ExtraAccountMetaList. [E03-E04]

Security principal	Recorded authority or dependency
Common program upgrade authority	On-curve address 3Haaa6MJjH6F5swCjRR72Mi6qsGeNGR79zvQYXmvGDi8 controls both hook and controller ProgramData.
MMF controller	Owns the role/user state and can sign for the authority PDA inside installed program logic.
Authority PDA	Controls Token-2022 mint, freeze, metadata and transfer-hook configuration for the candidate mint.
Role-bound users	Seven active role-account classes and 15 user accounts were recorded; representative privileged paths use role, signer, attestation or asset-transfer context.
Fund and service providers	Private feeder/master/share-class mapping, register, NAV, custody and settlement remain external to public runtime state.

Assessed security properties

The review considered technical mint-to-hook binding, transfer-hook state inputs, controller/PDA authority, representative privileged CPI routes, role configuration, supply reconciliation and upgrade authority. The ordinary-attacker boundary requires an unauthorized public path to make the controller sign for mint, burn, freeze, thaw, SetAuthority, metadata or hook-configuration actions, or to bypass the transfer hook's intended account constraints.

No such path was established in the recorded evidence. Exact deployed source and complete branch reconstruction are absent, so this negative conclusion remains bounded to observed configuration, runtime artifacts and representative traces. [E03-E04]

4 Technical Assessment

4.1 Token-2022 mint and supply state

At finalized context slot 451,392,301, the 439-byte candidate mint was owned by the Token-2022 program. Its base fields named authority PDA EnAjiqVor92SjieJvRFW7aXgVWJAb1WdhjwqaGCpnAk4 as both mint and freeze authority. The MetadataPointer pointed to the mint itself; TokenMetadata recorded the fund name and SWEEP symbol; TransferHook pointed to 3SajY54CXjD1efuLnH42tNWzu8ZVHZCLQ17mXjRmHq9Z. The detailed account census in the 451,392,301-451,393,190 observation window found seven initialized token accounts and none recorded as frozen. Candidate identity, supply and the seven-account reconciliation were rechecked at finalized context slot 451,412,449. [E01-E04]

The technical mint-to-hook relationship is established. The same data does not authenticate the mint as the authoritative representation of a particular SWEEP feeder, master fund or share class. On-chain metadata is corroboration, not issuer attestation. [E01-E04]

4.2 Transfer hook and ExtraAccountMetaList

At finalized context slot 451,392,301, the transfer-hook program resolved to ProgramData DmU5BTBvVj9nFW18u84WPNc9RfRF4DSSvsQxrT3QCKy, deployment/upgrade slot 440,081,553. Its 334,064-byte payload SHA-256 is 31927ccf5beaac5cf269169a6b48cc4a91ed4a105133960c2316e7177fb1b5d9. The hook-owned 261-byte EAML was separately observed at finalized context slot 451,392,448; it has SHA-256 e889b1b10e42a2f21b6871548cebaca0e68c8c27c0ecbfc53b48ed646faff98a and supplies seven entries tying transfers to hook authority, controller, controller state, role and source/destination user records. [E03-E04]

Embedded hook strings expose TransferHook admission, source/destination whitelist, same-role, same-jurisdiction and account-association checks. Two recorded successful redemption transfers show Token-2022 TransferChecked invoking the exact hook with EAML-resolved controller accounts. These observations materialize the runtime/configuration surface but do not replace exact deployed source or a complete decompilation. [E03]

4.3 Controller and PDA authority

The MMF controller resolves to ProgramData ATA5HPY9UZfPJmWJDwyPjP28ACZwbB89Yr6f18D2zSc6X, deployment/upgrade slot 440,081,414. Its 2,691,856-byte payload SHA-256 is c7d1fe01110bc800d4ea3faf873d0aa61ffac3fb55bdac0776e2236992cb182. Deterministic recomputation derives the authority PDA from [mmf_authority] with bump 255 and the candidate mint from [mint_v1] with bump 254 under this controller. [E03-E04]

Seven active role accounts and 15 user accounts were enumerated during the detailed finalized-state observation window at slots 451,392,301-451,393,190. Representative FiatSubscribe evidence recorded an active OPERATIONS signer, Ed25519 attestation and subsequent Token-2022 MintTo with the authority PDA as signer. StablecoinSubscribe traces included investor/payment signers and asset-transfer context before minting. Redemption traces exercised transfer-hook and subsequent burn workflows. This supports, but does not exhaustively prove, role- and transaction-bound use of PDA authority. [E03-E04]

4.4 Publisher correlation and build boundary

Galaxy's public portal IDL identifies mmf_solana v0.1.0 and includes PDA seeds and instruction discriminators that match the candidate application's observed structure and production transactions. The IDL's embedded address refers to a different devnet program whose executable hash differs from the candidate mainnet controller. The authenticated portal API containing actual mainnet properties was not publicly accessible. The IDL therefore supports application-family correlation but not exact mainnet source/build correspondence. [E01-E02; S04]

Neither standard on-chain Anchor IDL account was present at the recorded finalized slot, and no publisher source revision, compiler/dependency lockfiles or reproducible build matching the two mainnet payload hashes was obtained. This prevents an unconditional statement that every privileged dispatcher branch is correctly authorized. [E03-E04]

5 Recorded Validation and Coverage

Validation relevant to the opinion is summarized below.

Recorded check	Result and evidentiary meaning
Mint and extension decode	Established the Token-2022 mint, metadata, transfer-hook binding and common authority PDA in the detailed finalized-state window beginning at slot 451,392,301; identity and supply were rechecked at slot 451,412,449.
Token-account census	Seven initialized accounts summed exactly to raw supply; the identity/supply recheck was finalized at slot 451,412,449 and establishes fixed-state on-chain conservation only.
Loader and payload identity	Recovered hook/controller ProgramData, deployment slots, common upgrade authority and exact payload SHA-256 values.
EAML decode	At finalized context slot 451,392,448, recovered seven transfer-hook account requirements tying execution to controller-owned state and user/role records.
PDA recomputation	Confirmed that only the controller program can sign for the authority PDA under Solana's PDA model.
Representative transaction traces	Observed successful subscription, redemption, hook and burn routes with signer, role, attestation or payment context; not exhaustive branch coverage.
Publisher-correlation review	Official portal IDL seeds and discriminators correlate with the application family, but the IDL is not a mainnet build attestation.

No local validator, bank snapshot or exhaustive instruction harness was executed. Absence of an unauthorized path in representative traces is not a proof about unobserved binary branches. [E03-E04]

6 Findings and Control Observations

No implementation vulnerability was confirmed. The observations below concern authorized control and upgrade concentration. They are not included in vulnerability severity totals, and neither implies an ordinary caller can exercise the authority. No issuer response or remediation verification was available.

ID	Title	Classification / status
B3-SWEEP-001	A common authority can upgrade both candidate application programs	Privileged-control observation; applicable at snapshot
B3-SWEEP-002	A controller-derived PDA holds the token lifecycle authorities	Privileged-control observation; applicable at snapshot

001 | A common authority can upgrade both candidate application programs

Attribute	Record
Affected components	Transfer-hook ProgramData and MMF controller ProgramData
Classification	Privileged-control observation. No implementation-vulnerability severity assigned.
Evidence	E01-E04; Appendix A

Description. Hook and controller ProgramData both identify on-curve address 3Haaa6MJjH6F5swCjRR72Mi6qsGeNGR79zvQYXmvGD8 as upgrade authority. Authorized use can replace either executable payload, including the policy checks and authority-signing logic on which the candidate token depends.

Impact and preconditions. Compromise or misuse of this authority could alter transfer restrictions, role enforcement and token lifecycle controls across both programs. The condition requires control of the authorized upgrade principal; no ordinary-caller path to the authority was established. Signer custody, approval thresholds and incident controls were not assessed.

Recommendation. The program operator should use verifiable multi-party upgrade approval, publish signed release manifests identifying ProgramData payload hashes and source/build inputs, and monitor loader-state and authority changes. Emergency upgrade procedures should be narrowly defined and followed by public release reconciliation.

Status. Applicable to the candidate snapshot; compensating custody and governance controls were not assessed.

O02 | A controller-derived PDA holds the token lifecycle authorities

Attribute	Record
Affected components	MMF controller; authority PDA; candidate Token-2022 mint
Classification	Privileged-control observation. No implementation-vulnerability severity assigned.
Evidence	E03-E04; Appendix A

Description. The controller can sign for the mmf_authority PDA, which holds mint, freeze, metadata-update and transfer-hook-configuration authority. Recorded role state and representative traces show these signatures inside structured workflows, but exact source was unavailable for exhaustive verification of every privileged instruction.

Impact and preconditions. An authorized or compromised controller path can change supply, freeze state, metadata or the hook configuration. No ordinary caller was shown to induce such an action without required role, signer, attestation or payment context. Residual uncertainty concerns unreviewed binary branches rather than a confirmed bypass.

Recommendation. The program operator should provide exact controller and hook source, IDLs, compiler/dependency lockfiles and reproducible builds matching the recorded payload hashes. Every public instruction capable of MintTo, Burn, FreezeAccount, ThawAccount, SetAuthority, metadata update or hook configuration should be covered by role, signer, mint, amount, recipient and replay-binding tests in a non-production environment.

Status. Applicable to the candidate snapshot; unauthorized branch-level reachability was not substantiated and exhaustive source review was not possible.

7 RWA Linkage and Public Verifiability

Official materials establish that State Street and Galaxy launched SWEEP on Solana and describe a private liquidity-fund structure investing in U.S. Treasury securities, fully collateralized repurchase agreements and cash. They identify State Street, Galaxy, Anchorage, NAV Consulting and Chainlink roles. The public materials do not publish the candidate mint/program graph or state whether the mint represents an onshore feeder, offshore feeder, master fund, a specific share class or another record. [E01; E05; S01-S03]

Layer	Publicly supported statement	Unresolved boundary
Legal product	Public launch and regulatory materials establish the fund family and legal entities.	The candidate mint is not mapped to a precise vehicle, feeder/master structure or share class.
Pricing	Public materials describe NAV-based fund economics and planned Chainlink NAVLink use.	A production NAV feed address, history and dealing cutoff were not established for this mint.
Fund assets	The stated strategy and named custody/administration providers are public.	Portfolio, liabilities, custody balances and contemporaneous signed NAV were not assessed.
On-chain units	Candidate supply and seven token accounts reconciled at fixed state.	Supply cannot be equated with legal shares or assets without issuer mapping and register reconciliation.

Public evidence does not establish the legal-product-to-mint mapping or provide aligned NAV and register records. Those gaps prevent a complete token-to-fund reconciliation; they do not establish that the fund is unbacked. [E05]

8 Limitations and Conclusion

ID	Limitation	Effect on conclusions
B3-SWEEP-L01	Issuer-approved mint-to-vehicle/share-class mapping is unavailable.	The report cannot authenticate the candidate graph as the production representation of a specified SWEEP legal interest.
B3-SWEEP-L02	Exact deployed hook/controller source, mainnet IDLs and reproducible builds are unavailable.	The report cannot claim complete source coverage or exact source-to-mainnet-binary provenance.
B3-SWEEP-L03	A complete public-entry-to-invoke_signed control-flow review was not possible.	Representative guarded traces support the opinion, but unobserved authorization defects cannot be categorically excluded.
B3-SWEEP-L04	Private offering, register, NAV, custody and settlement records were outside scope.	No legal ownership, valuation, reserve, solvency or completed-payment assurance is provided.

Conclusion

Subject to the provisional identity and executable-coverage boundaries above, no reportable vulnerability was confirmed in the candidate mint, transfer-hook configuration, controller/PDA relationship, recorded role state or representative subscription/redemption routes. Common upgrade control and the protocol authority PDA remain material trust dependencies.

This opinion applies only to the listed candidate accounts, ProgramData payload hashes and observation slots. It must not be presented as an authenticated SWEEP product audit or a complete source audit. Any program upgrade, authority change, EAML change, role change or authenticated deployment manifest requires an applicability review.

A Candidate Deployment and Authority Inventory

The inventory combines the candidate identity/supply recheck at finalized context slot 451,412,449 with detailed runtime/configuration observations from slots 451,392,301-451,393,190 and the EAML observation at slot 451,392,448. Product identity remains provisional because no issuer-controlled artifact maps this graph to a precise SWEEP legal vehicle or share class. [E01-E04]

Component	Address / identifier	Recorded identity
Candidate mint	AgBSDfS7CNRUnBeREHHdF9S57fai5b3EXH1hgvZkRPhB	Token-2022; 8 decimals; candidate
Transfer hook	3SajY54CXjD1efuLnH42tNWzu8ZVHZCLQ17mXjRmHq9Z	Upgradeable program
Hook ProgramData	DmU5BTBvVj9nFW18u84WPnc9RfRFf4DSSvsQxrT3QCKy	Payload SHA-256 31927ccf...b1b5d9
MMF controller	CnuNzfvSq5fTZ8gWfjH8TyQaEFmZypg69VbQrNgZGhxY	Upgradeable program
Controller ProgramData	ATA5HPY9UZfPjMwJDwyPjP28ACZwB89Yr6f18D2zSc6X	Payload SHA-256 c7d1fe01...cb182
ExtraAccountMetaList	5m28uwYVWYfT9xWzZRZryFyxpWjDg4AQX4bNfgzWWK U	Seven entries; hook-owned
Authority PDA	EnAjiqVor92SjieJvRFW7aXgVWJAb1WdhjqwaGCpnAk4	Mint/freeze/metadata/hook authority
Common upgrade authority	3Haaa6MJjH6F5swCjRR72Mi6qsGeNGR79zvQYXmvGDi8	On-curve control surface for both programs

Hook deployment/upgrade slot: 440,081,553. Controller deployment/upgrade slot: 440,081,414. These are deployment metadata, not the report's observation slots. Detailed loader/runtime observations were recorded at finalized context slots 451,392,301-451,393,190, the EAML at 451,392,448, and candidate identity/supply were rechecked at 451,412,449. The abbreviated hashes in the table are printed in full in Section 4 and the scope object. [E01-E04]

B Evidence and Source Index

Assessment workpapers are retained separately and are not attached. The scope manifest identifies each record by SHA-256 and includes deployment and source references. Checksums identify records; they do not attest to their contents.

ID	Assessment record
E01	SWEEP public deployment-identity evidence review
E02	SWEEP public deployment-identity evidence record
E03	SWEEP runtime, authority and transaction evidence record
E04	SWEEP technical assessment outcome
E05	Tokenized Treasury RWA anchor and public-verifiability assessment
E06	SWEEP deployment registry snapshot
E07	Tokenized Treasury final assurance and delivery opinion

Primary public sources

S01 | State Street and Galaxy SWEEP launch announcement

Official product, strategy, Solana launch and service-provider evidence retained through 29 September 2026; no mint or program manifest is published.

S02 | Galaxy State Street SWEEP product page

Official product and portal relationship evidence retained through 29 September 2026; no mainnet deployment manifest is published.

S03 | SEC Form D index for State Street Galaxy Onchain Liquidity Sweep Onshore Fund, LLC

Regulatory evidence for the onshore legal vehicle; it does not map the candidate mint to a share class.

S04 | Galaxy public MMF Solana IDL

Publisher-hosted application-family evidence recorded on 29 September 2026. The embedded address refers to a different devnet binary and is not an exact mainnet build attestation.

S05 | Candidate SWEEP mint explorer record

Explorer view of the candidate mint; corroborative technical evidence, not issuer authentication.

S06 | Candidate transfer-hook program explorer record

Explorer view referenced by the archived runtime assessment.

S07 | Candidate MMF controller explorer record

Explorer view referenced by the archived runtime assessment.

Scope attachment

sweep-scope-manifest-en.json

SHA-256: 4c65a14f08c37fc63905709af181c941b215018c597a155678604a6ceb1f9619