Strato - Native Token Bridging & Timelock (PR#6913, PR#6932)

1 Executive Summary
2 Scope
3 Key Findings
3.1 Native bridge lifecycle and custody
3.2 `AdminRegistry` timelock correctness
3.3 Role separation and operational posture
3.4 Monitoring, events, and operational clarity
4 Remediation and Outcome
5 Residual Risk Profile
Appendix 1 - Files in Scope
Appendix 2 - Disclosure
A.2.1 Purpose of Reports
A.2.2 Links to Other Web Sites from This Web Site
A.2.3 Timeliness of Content

Engagement Summary

Date	May 2026
Auditors	George Kobakhidze, Martin Ortner

This document is a standalone summary of the security engagement conducted by Consensys Diligence for STRATO. It is separate from the full security review report and is intended as an external-facing overview of the engagement.

Please contact the STRATO team for a copy of the full report.

1 Executive Summary

Consensys Diligence conducted a two-week review of selected STRATO pull requests introducing native token bridging functionality and timelock-based governance changes. The review covered PR-6913, which introduced the native bridge contracts spanning STRATO and an external EVM environment, and PR-6932, which added timelocked action queuing and configurable instant-execution paths to the governance contract, `AdminRegistry`. The `MercataBridge` contract was also reviewed as part of the PR-6932 review.

The review produced findings that focused on correctness of the bridge deposit and withdrawal lifecycle, custody accounting, governance execution paths, initialization behavior, and the operational assumptions around privileged roles and off-chain bridge operators.

The initial review identified implementation and operational risks across the native bridge lifecycle and the `AdminRegistry` timelock changes. In total, the review produced 30 findings (1 Critical, 10 Major, 6 Medium, 8 Minor, 5 Informational) that are laid out in detail in the full report. STRATO subsequently provided a remediation pass, addressing key and prioritized findings, which has also been reviewed. The STRATO team also provided a set of acknowledged design assumptions and operational responsibilities documented for STRATO operators.

We would like to note that this was a time-boxed review focused on selected changesets within a large and evolving codebase. The engagement identified a number of findings across the reviewed areas, underscoring the complexity and security sensitivity of cross-chain bridge and governance systems. As with any targeted assessment, areas outside the defined scope and changes introduced after the reviewed commits were not evaluated. We therefore recommend continued security review, testing, and operational monitoring as development progresses.

2 Scope

The engagement was conducted from May 4, 2026 to May 15, 2026, with a total effort of 2x10 person-days.

This review focused on select code changes with the following PR's:

PR #6913 - 4 new contracts to support native token bridging (last commit `8fb1aa7fcbc61b10ad58cfa56bd0f7f62f759c6c`):

- `mercata/contracts/concrete/Bridge/StratoNativeBridge.sol`
- `mercata/contracts/concrete/Bridge/StratoNativeCustodyVault.sol`
- `mercata/ethereum/contracts/bridge/StratoNativeRepresentationBridge.sol`
- `mercata/ethereum/contracts/bridge/StratoNativeRepresentationToken.sol`

PR #6932 - Timelock functionality related contracts (last commit `013caa9b2254d6808297bb74278c98316fc76f33`):

- `mercata/contracts/concrete/Bridge/MercataBridge.sol` (full file)
- `mercata/contracts/concrete/Admin/AdminRegistry.sol` (changes only as per the PR)

3 Key Findings

3.1 Native bridge lifecycle and custody

Findings centered on tightening the multi-step deposit and withdrawal state machine - ensuring intermediate states cannot be bypassed by transaction ordering (operator or block producer), that abort and recovery paths are correctly gated against external-chain settlement, and that custody accounting is robust against any future token implementation that may introduce transfer callbacks.

3.2 `AdminRegistry` timelock correctness

Findings addressed the integrity of the new timelock execution path, the initialization surface of the registry implementation, the structure of self-governance and whitelist semantics, and the consistency of event emission for state-changing administrative actions.

3.3 Role separation and operational posture

Findings focused on whether the distribution of privileges matched the operational risk profile of a cross-chain bridge. The review identified places where distinct roles were collapsed onto a single address, increasing the blast radius of access compromise or operator error, and recommended clearer separation of duties between frequently-used operational roles and broader administrative roles.

3.4 Monitoring, events, and operational clarity

Findings focused on improving visibility into bridge state for off-chain systems, operators, and integrators - covering event coverage, lifecycle metadata recording, consistency between comments and enforced behavior, and documentation of design assumptions relevant to relayers and monitoring processes.

4 Remediation and Outcome

Consensys Diligence reviewed the remediation pass and responses from the STRATO team and recorded the resulting status for each finding.

Code changes made during remediation included:

- reentrancy protections in the native custody vault
- simplifications to the withdrawal lifecycle
- restrictions on the post-confirmation abort window
- representation token management improvements
- hardening of `AdminRegistry` initialization
- reordering of queued state invalidation ahead of external calls in governance execution
- improved event coverage in several areas

Role separation on the external representation bridge was addressed through deployment runbook procedures rather than code changes.

Some findings were acknowledged as intentional design choices documented emergency-admin interventions as the remediation path for them.

5 Residual Risk Profile

The risk profile of the reviewed contracts includes assumptions characteristic of cross-chain bridges: trusted operator behavior, privileged role management, external-chain finality, and reliance on off-chain monitoring and reconciliation for correctness guarantees that cannot be fully enforced on-chain. Operational complexity remains the primary challenge.

Appendix 1 - Files in Scope

This review covered the following files.

Files from PR-6913:

File	SHA-1 hash
./mercata/contracts/concrete/Bridge/StratoNativeBridge.sol	ea87300f1e354ad27a0b2bc2cad4c4a8a1c5a2b0
./mercata/contracts/concrete/Bridge/StratoNativeCustodyVault.sol	d0aab9211bbbd34cc91a24dede917ccd1d30dd2e
./mercata/ethereum/contracts/bridge/StratoNativeRepresentationToken.sol	e81d81cbe576e79d45645560c18b292b2eb266d6
./mercata/ethereum/contracts/bridge/StratoNativeRepresentationBridge.sol	d89f59bb62eb75d67903817ad9b2f57f3d0b4a08

Files from PR-6932

File	SHA-1 hash
./mercata/contracts/concrete/Bridge/MercataBridge.sol	fdcb566a4091656f94923d952130930b510435e6
./mercata/contracts/concrete/Admin/AdminRegistry.sol	3a1125a4977b91683878aa16d8e9528bd96a3df0

Appendix 2 - Disclosure

Consensys Diligence (“CD”) typically receives compensation from one or more clients (the “Clients”) for performing the analysis contained in these reports (the “Reports”). The Reports may be distributed through other means, including via Consensys publications and other distributions.

The Reports are not an endorsement or indictment of any particular project or team, and the Reports do not guarantee the security of any particular project. This Report does not consider, and should not be interpreted as considering or having any bearing on, the potential economics of a token, token sale or any other product, service or other asset. Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. No Report provides any warranty or representation to any third party in any respect, including regarding the bug-free nature of code, the business model or proprietors of any such business model, and the legal compliance of any such business. No third party should rely on the Reports in any way, including for the purpose of making any decisions to buy or sell any token, product, service or other asset. Specifically, for the avoidance of doubt, this Report does not constitute investment advice, is not intended to be relied upon as

investment advice, is not an endorsement of this project or team, and it is not a guarantee as to the absolute security of the project. CD owes no duty to any third party by virtue of publishing these Reports.

A.2.1 Purpose of Reports

The Reports and the analysis described therein are created solely for Clients and published with their consent. The scope of our review is limited to a review of code and only the code we note as being within the scope of our review within this report. Any Solidity code itself presents unique and unquantifiable risks as the Solidity language itself remains under development and is subject to unknown risks and flaws. The review does not extend to the compiler layer, or any other areas beyond specified code that could present security risks. Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. In some instances, we may perform penetration testing or infrastructure assessments depending on the scope of the particular engagement.

CD makes the Reports available to parties other than the Clients (i.e., “third parties”) on its website. CD hopes that by making these analyses publicly available, it can help the blockchain ecosystem develop technical best practices in this rapidly evolving area of innovation.

A.2.2 Links to Other Web Sites from This Web Site

You may, through hypertext or other computer links, gain access to web sites operated by persons other than Consensys and CD. Such hyperlinks are provided for your reference and convenience only, and are the exclusive responsibility of such web sites’ owners. You agree that Consensys and CD are not responsible for the content or operation of such Web sites, and that Consensys and CD shall have no liability to you or any other person or entity for the use of third party Web sites. Except as described below, a hyperlink from this web Site to another web site does not imply or mean that Consensys and CD endorses the content on that Web site or the operator or operations of that site. You are solely responsible for determining the extent to which you may use any content at any other web sites to which you link from the Reports. Consensys and CD assumes no responsibility for the use of third-party software on the Web Site and shall have no liability whatsoever to any person or entity for the accuracy or completeness of any outcome generated by such software.

A.2.3 Timeliness of Content

The content contained in the Reports is current as of the date appearing on the Report and is subject to change without notice unless indicated otherwise, by Consensys and CD.

2026 All rights reserved