



Security Assessment

Final Report

Silo Token V2

May 2025

Prepared for
Silo Team

Table of contents

Project Summary	3
Project Scope	3
Project Overview	3
Protocol Overview	3
Findings Summary	4
Severity Matrix	4
Informational Issues	5
I-01. Token name and Token symbol are reversed	5
I-02. Token can't pause core functionality	5
I-03. Consider adding some mitigation techniques to allow for a more cross-chain robustness	5
I-04. Add a documentation that Silo Token can't be used with some pools	5
Disclaimer	7
About Certora	7

Project Summary

Project Scope

Project Name	Repository (link)	Latest Commit Hash	Initial Commit Hash	Platform
xSilo: Silo Token V2	Repo	69b0a5c	bd8348b	EVM

Project Overview

This document describes the specification and verification of **silo contracts v2** using the Certora Prover and manual code review findings. The work was undertaken from **May 4th to May 6th 2025**

The following contract list is included in our scope:

```
x-silo/contracts/token/SiloGovernanceTokenV2.sol
```

Protocol Overview

SiloGovernanceTokenV2 Is a simple burnable capped Token deployed for compatibility with Cross-Link CCIP.

Findings Summary

The table below summarizes the findings of the review, including type and severity details.

Severity	Discovered	Confirmed	Fixed
Critical	-	-	-
High	-	-	-
Medium	0	0	0
Low	0	0	0
Informational	4	4	1
Total	4	4	1

Severity Matrix

Impact	High	Medium	High	Critical
	Medium	Low	Medium	High
	Low	Low	Low	Medium
		Low	Medium	High
		Likelihood		

Informational Issues

I-01. Token name and Token symbol are reversed.

Description: The order in the constructor of ERC20 is name then symbol.

```
ftrace
19 | constructor(address _initialOwner↑, ERC20Burnable _silov1↑)
20 |     ERC20("SILO", "Silo Governance Token")
```

Recommendation: Should reverse the order of the token symbol and token name.

Customer's response: Fixed.

I-02. Token can't pause core functionality

Description: Currently the owner can't pause, burn and transfer actions. This might limit possible mitigations for cross chain attacks.

Recommendation: Consider adding pausing functionality to the _update call.

Customer's response: Acknowledged would not fix.

I-03. Consider adding some mitigation techniques to allow for a more cross-chain robustness

Description: Some cross-chain tokens implement some mitigation patterns to lower the impact of an attack. Some of those patterns are:

1. Rate limiting.
2. Time locking.
3. Pausing.

Depending on the used pool, you might want to implement a version of those patterns.

Customer's response: Acknowledged would not fix at this moment.

I-04. Add a documentation that Silo Token can't be used with some pools

Description: The current minting pattern means that burn-mint pools should never be registered with SiloToken, this should be documented.

Customer's response: Acknowledged, the Token would only be used in Mint-Lock and Unlock-Lock pools.



Disclaimer

Even though we hope this information is helpful, we provide no warranty of any kind, explicit or implied. The contents of this report should not be construed as a complete guarantee that the contract is secure in all dimensions. In no event shall Certora or any of its employees be liable for any claim, damages, or other liability, whether in an action of contract, tort, or otherwise, arising from, out of, or in connection with the results reported here.

About Certora

Certora is a Web3 security company that provides industry-leading formal verification tools and smart contract audits. Certora's flagship security product, Certora Prover, is a unique SaaS product that automatically locates even the most rare & hard-to-find bugs on your smart contracts or mathematically proves their absence. The Certora Prover plugs into your standard deployment pipeline. It is helpful for smart contract developers and security researchers during auditing and bug bounties.

Certora also provides services such as auditing, formal verification projects, and incident response.