

# KISHIELD

Security Audit

**millennium Token**

August 29, 2022



Audit Passed



# Table of Contents

## **1 Audit Summary**

## **2 Project Overview**

### 2.1 Token Summary

### 2.2 Main Contract Assessed

## **3 Smart Contract Vulnerability Checks**

## **4 Contract Ownership**

### 4.1 Privileged Functions

## **5 Important Notes To The Users**

## **6 Findings Summary**

### 6.1 Classification of Issues

### 6.1 Findings Table

01 Public function that could be declared external

02 Public function that could be declared external

03 Public function that could be declared external

## **7 Statistics**

### 7.1 Liquidity

### 7.2 Token Holders

### 7.3 Liquidity Holders

## **8 Liquidity Ownership**

## **9 Disclaimer**



# Audit Summary

This report has been prepared for millennium Token on the Ethereum network. KISHIELD provides both client-centered and user-centered examination of the smart contracts and their current status when applicable. This report represents the security assessment made to find issues and vulnerabilities on the source code along with the current liquidity and token holder statistics of the protocol.

A comprehensive examination has been performed, utilizing Cross Referencing, Static Analysis, In-House Security Tools, and line-by-line Manual Review.

The auditing process pays special attention to the following considerations:

- Ensuring contract logic meets the specifications and intentions of the client without exposing the user's funds to risk.
- Testing the smart contracts against both common and uncommon attack vectors.
- Inspecting liquidity and holders statistics to inform the current status to both users and client when applicable.
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Verifying contract functions that allow trusted and/or untrusted actors to mint, lock, pause, and transfer assets.
- Thorough line-by-line manual review of the entire codebase by industry experts.

# Project Overview

## Token Summary

Parameter	Result
Address	Not Deployed Yet
Name	millennium
Token Tracker	millennium (MILL)
Decimals	Not Deployed Yet
Supply	Not Deployed Yet
Platform	Ethereum
compiler	v0.7.5
Optimization	Yes with 2 runs
LicenseType	BUSL-1.1
Language	Solidity
Codebase	MIL_erc20.sol
Url	<a href="https://dev-app.millennium.cash/">https://dev-app.millennium.cash/</a>

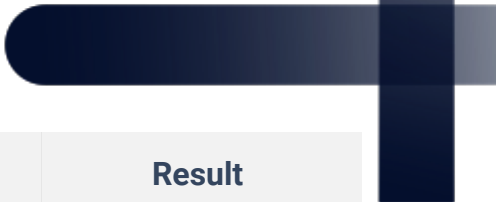
## Main Contract Assessed

Name	Contract	Live
MillenniumToken (Ownable, ERC20)	Not Deployed Yet	No

\*Token audit will be updated when the token is deployed to mainnet.

# Smart Contract Vulnerability Checks

Vulnerability	Automatic Scan	Manual Scan	Result
Unencrypted Private Data On-Chain	Complete	Complete	✓ Low / No Risk
Code With No Effects	Complete	Complete	✓ Low / No Risk
Message call with hardcoded gas amount	Complete	Complete	✓ Low / No Risk
Hash Collisions With Multiple Variable Length Arguments	Complete	Complete	✓ Low / No Risk
Unexpected Ether balance	Complete	Complete	✓ Low / No Risk
Presence of unused variables	Complete	Complete	✓ Low / No Risk
Right-To-Left-Override control character (U+202E)	Complete	Complete	✓ Low / No Risk
Typographical Error	Complete	Complete	✓ Low / No Risk
DoS With Block Gas Limit	Complete	Complete	✓ Low / No Risk
Arbitrary Jump with Function Type Variable	Complete	Complete	✓ Low / No Risk
Insufficient Gas Griefing	Complete	Complete	✓ Low / No Risk
Incorrect Inheritance Order	Complete	Complete	✓ Low / No Risk
Write to Arbitrary Storage Location	Complete	Complete	✓ Low / No Risk
Requirement Violation	Complete	Complete	✓ Low / No Risk
Missing Protection against Signature Replay Attacks	Complete	Complete	✓ Low / No Risk
Weak Sources of Randomness from Chain Attributes	Complete	Complete	✓ Low / No Risk



Vulnerability	Automatic Scan	Manual Scan	Result
Authorization through tx.origin	Complete	Complete	✓ Low / No Risk
Delegatecall to Untrusted Callee	Complete	Complete	✓ Low / No Risk
Use of Deprecated Solidity Functions	Complete	Complete	✓ Low / No Risk
Assert Violation	Complete	Complete	✓ Low / No Risk
Reentrancy	Complete	Complete	✓ Low / No Risk
Unprotected SELFDESTRUCT Instruction	Complete	Complete	✓ Low / No Risk
Unprotected Ether Withdrawal	Complete	Complete	✓ Low / No Risk
Unchecked Call Return Value	Complete	Complete	✓ Low / No Risk
Outdated Compiler Version	Complete	Complete	✓ Low / No Risk
Integer Overflow and Underflow	Complete	Complete	✓ Low / No Risk
Function Default Visibility	Complete	Complete	✓ Low / No Risk

## Contract Ownership

The owner wallet has the power to call the functions displayed on the privileged functions chart below, if the owner wallet is compromised this privileges could be exploited.

There is no requirement for the owners to renounce ownership of the contract because the owner privileges over the contract have no effect on the transfer functions and functionality of an ERC-20 token.

## Important Notes To The Users:

- There is no tax on the purchase, sale, or transfer of tokens.
- Wallets cannot be blacklisted by the owner.
- The owner is unable to halt token transfers or trading.
- There are no transaction minimums or maximums.
- Anyone can use the `mintIfNeeded` method to mint new tokens on a predetermined `EMISSION_SCHEDULE` that cannot be modified.
- Newly minted tokens go to a Central wallet, which contributes to the entire Millennium ecosystem.
- Once the owner renounces ownership of the contract, none of the following are applicable.
- The owner has the option to take a group of addresses' balances out of the computation for circulating supply.
- No high-risk Exploits/Vulnerabilities were found in token source code.
- The Millenium team provided a testing suite for the token minting schedule, which KISHIELD examined and verified.

EMISSION SCHEDULE	Amount (Millions)
GENESIS_SUPPLY	35
MONTH_6_SUPPLY	95
YEAR_1_SUPPLY	140
YEAR_2_SUPPLY	180
YEAR_3_SUPPLY	220
YEAR_4_SUPPLY	250



## Audit Passed

# Technical Findings Summary

## Classification of Issues

\*All Issues Found are Informational

Severity	Description
● High	Exploits, vulnerabilities or errors that will certainly or probabilistically lead towards loss of funds, control, or impairment of the contract and its functions. Issues under this classification are recommended to be fixed with utmost urgency
● Medium	Bugs or issues with that may be subject to exploit, though their impact is somewhat limited. Issues under this classification are recommended to be fixed as soon as possible.
● Low	Effects are minimal in isolation and do not pose a significant danger to the project or its users. Issues under this classification are recommended to be fixed nonetheless.
● Info	Consistency, syntax or style best practices. Generally pose a negligible level of risk, if any.

## Findings

Severity	Found
● High	0
● Medium	0
● Low	0
● Info	3
Total	3



# Findings

## Public function that could be declared external

ID	Severity	Contract	Function
01	● Informational	MillenniumToken	Functions: burn, setExcludedCirculationAddresses, circulatingSupply

### Description

Gas Optimization. Public function that could be declared external

### Recommendation

Public functions that are never called by the contract should be declared external to save gas.

## Public function that could be declared external

ID	Severity	Contract	Function
02	● Informational	Ownable	Functions: owner, renounceManagement, pushManagement, pullManagement

### Description

Gas Optimization. Public function that could be declared external

### Recommendation

Public functions that are never called by the contract should be declared external to save gas.

## Public function that could be declared external

ID	Severity	Contract	Function
03	<span style="color: purple;">●</span> Informational	ERC20	Functions: name, symbol, decimals, totalSupply, transfer, allowance, approve, transferFrom, increaseAllowance, decreaseAllowance

### Description

Gas Optimization. Public function that could be declared external

### Recommendation

Public functions that are never called by the contract should be declared external to save gas.

## Privileged Functions (onlyOwner & Others)

Function Name	Parameters	Visibility
renounceManagement	none	public
pushManagement	address newOwner_	public
setExcludedCirculationAddresses	memory _addresses	public

# Statistics

## Liquidity Info

Parameter	Result
Pair Address	Not Deployed Yet
MILL Reserves	0.00 MILL
ETH Reserves	0.00 ETH
Liquidity Value	\$0 USD

## Token (MILL) Holders Info

Parameter	Result
MILL Percentage Burnt	0.00%
MILL Amount Burnt	0 MILL
Top 10 Percentage Own	100.00%
Top 10 Amount Owned	0 MILL
Top 10 Aprox Value	\$NaN USD

## LP (MILL/ETH) Holders Info

Parameter	Result
MILL/ETH % Burnt	0.00%
MILL/ETH Amount Burnt	0 MILL/ETH
Top 10 Percentage Owned	0.00%
Top 10 Amount Owned	0 MILL/ETH
Locked Tokens Percentage	0.00%
Locked Tokens Amount	0 MILL/ETH

\* All the data displayed above was taken on-chain at block Not Deployed Yet

\* The tokens on industry-standard burn wallets are not included on the top 10 wallets calculations

## Liquidity Ownership

The token does not have liquidity at the moment of the audit, block Not Deployed Yet

# KISHIELD



## Disclaimer

KISHIELD has conducted an independent audit to verify the integrity of and highlight any vulnerabilities or errors, intentional or unintentional, that may be present in the codes that were provided for the scope of this audit. This audit report does not constitute agreement, acceptance or advocacy for the Project that was audited, and users relying on this audit report should not consider this as having any merit for financial advice in any shape, form or nature. The contracts audited do not account for any economic developments that may be pursued by the Project in question, and that the veracity of the findings thus presented in this report relate solely to the proficiency, competence, aptitude and discretion of our independent auditors, who make no guarantees nor assurance that the contracts are completely free of exploits, bugs, vulnerabilities or deprecation of technologies.

All information provided in this report does not constitute financial or investment advice, nor should it be used to signal that any persons reading this report should invest their funds without sufficient individual due diligence regardless of the findings presented in this report. Information is provided 'as is', and KISHIELD is under no covenant to the completeness, accuracy or solidity of the contracts audited. In no event will KISHIELD or its partners, employees, agents or parties related to the provision of this audit report be liable to any parties for, or lack thereof, decisions and/or actions with regards to the information provided in this audit report.

The assessment services provided by KISHIELD is subject to dependencies and under continuing development. You agree that your access and/or use, including but not limited to any services, reports, and materials, will be at your sole risk on an as-is, where-is, and as-available basis. Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. The assessment reports could include false positives, false negatives, and other unpredictable results. The services may access, and depend upon, multiple layers of third-parties.