



CFG NINJA AUDITS

Security Assessment

Zksyncpad Token

May 3, 2023

Audit Status: Pass

Audit Edition: Advance



POWERED BY
BLADE POOL

Table of Contents

1 Assessment Summary

2 Technical Findings Summary

3 Project Overview

3.1 Main Contract Assessed

4 Smart Contract Risk Checks

5 Contract Ownership

7 KYC Check

8 Smart Contract Vulnerability Checks

8.1 Smart Contract Vulnerability Details

8.2 Smart Contract Inheritance Details

8.3 Smart Contract Privileged Functions

9 Assessment Results and Notes(Important)

10 Social Media Check(Informational)

11 Technical Findings Details

12 Disclaimer



Assessment Summary

This report has been prepared for Zksyncpad Token on the Zksync network. CFGNINJA 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:

- 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.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders
- Thorough line-by-line manual review of the entire codebase by industry experts.



Project Overview

Token Summary

Parameter	Result
Address	0xbD7039f1Ca560F30C9111396346f30A5798596ca
Name	Zksyncpad
Token Tracker	Zksyncpad (ZKSP)
Decimals	18
Supply	138450000
Platform	Zksync
compiler	v0.8.17+commit.8df45f5f/Zsolcv1.3.7
Contract Name	ZKSP
Optimization	Yes with 200 runs
LicenseType	MIT
Language	ZkSolidity
Codebase	https://explorer.zksync.io/ address/0xbD7039f1Ca560F30C9111396346f30A5798596ca
Payment Tx	



Main Contract Assessed Contract Name

Name	Contract	Live
Zksyncpad	0xbD7039f1Ca560F30C9111396346f30A5798596ca	No

TestNet Contract was Not Assessed

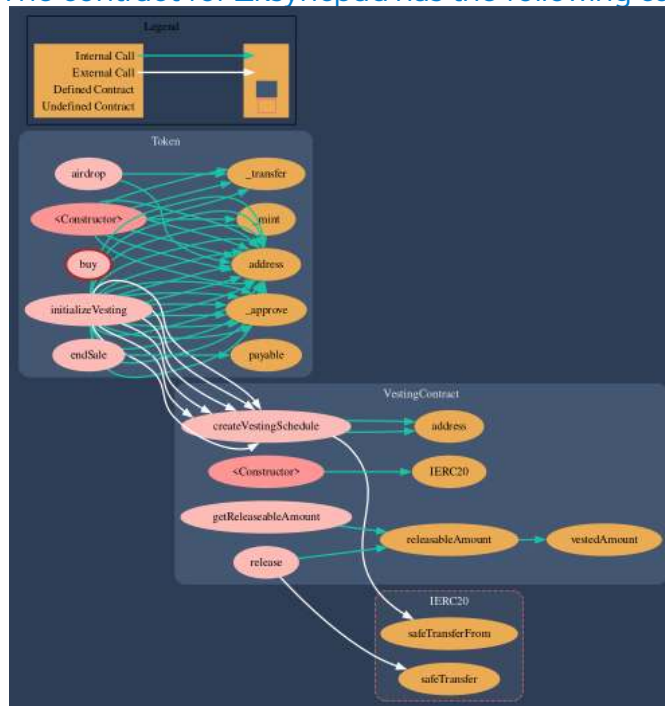
Solidity Code Provided

SolID	File Sha-1	FileName
Token	d5d1fbed23c76765fd3696cdb0a0875c76e5cc2a	Token.sol



Call Graph

The contract for Zksyncpad has the following call graph structure.



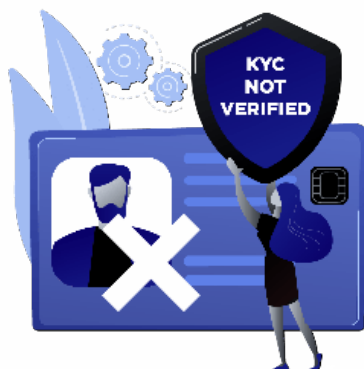
KYC Information

The Project Owners of Zksyncpad is not KYC.

KYC Information Notes:

Auditor Notes:

Project Owner Notes:



Smart Contract Vulnerability Checks

The Smart Contract Weakness Classification Registry (SWC Registry) is an implementation of the weakness classification scheme proposed in EIP-1470. It is loosely aligned to the terminologies and structure used in the Common Weakness Enumeration (CWE) while overlaying a wide range of weakness variants that are specific to smart contracts.

ID	Severity	Name	File	location
SWC-100	Pass	Function Default Visibility	Token.sol	L: 0 C: 0
SWC-101	Pass	Integer Overflow and Underflow.	Token.sol	L: 0 C: 0
SWC-102	Pass	Outdated Compiler Version file.	Token.sol	L: 0 C: 0
SWC-103	Pass	A floating pragma is set.	Token.sol	L: 2 C: 0
SWC-104	Pass	Unchecked Call Return Value.	Token.sol	L: 0 C: 0
SWC-105	Pass	Unprotected Ether Withdrawal.	Token.sol	L: 0 C: 0
SWC-106	Pass	Unprotected SELFDESTRUCT Instruction	Token.sol	L: 0 C: 0
SWC-107	Pass	Read of persistent state following external call.	Token.sol	L: 0 C: 0
SWC-108	Pass	State variable visibility is not set..	Token.sol	L: 0 C: 0
SWC-109	Pass	Uninitialized Storage Pointer.	Token.sol	L: 0 C: 0
SWC-110	Pass	Assert Violation.	Token.sol	L: 0 C: 0



ID	Severity	Name	File	location
SWC-111	Pass	Use of Deprecated Solidity Functions.	Token.sol	L: 0 C: 0
SWC-112	Pass	Delegate Call to Untrusted Callee.	Token.sol	L: 0 C: 0
SWC-113	Pass	Multiple calls are executed in the same transaction.	Token.sol	L: 0 C: 0
SWC-114	Pass	Transaction Order Dependence.	Token.sol	L: 0 C: 0
SWC-115	Pass	Authorization through tx.origin.	Token.sol	L: 0 C: 0
SWC-116	Pass	A control flow decision is made based on The block.timestamp environment variable.	Token.sol	L: 0 C: 0
SWC-117	Pass	Signature Malleability.	Token.sol	L: 0 C: 0
SWC-118	Pass	Incorrect Constructor Name.	Token.sol	L: 0 C: 0
SWC-119	Pass	Shadowing State Variables.	Token.sol	L: 0 C: 0
SWC-120	Pass	Potential use of block.number as source of randommness.	Token.sol	L: 0 C: 0
SWC-121	Pass	Missing Protection against Signature Replay Attacks.	Token.sol	L: 0 C: 0
SWC-122	Pass	Lack of Proper Signature Verification.	Token.sol	L: 0 C: 0
SWC-123	Pass	Requirement Violation.	Token.sol	L: 0 C: 0
SWC-124	Pass	Write to Arbitrary Storage Location.	Token.sol	L: 0 C: 0
SWC-125	Pass	Incorrect Inheritance Order.	Token.sol	L: 0 C: 0



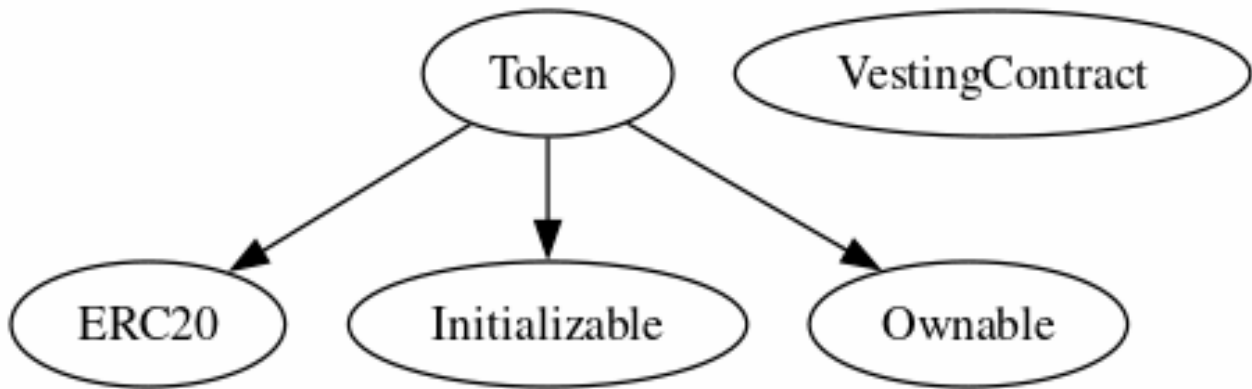
ID	Severity	Name	File	location
SWC-126	Pass	Insufficient Gas Griefing.	Token.sol	L: 0 C: 0
SWC-127	Pass	Arbitrary Jump with Function Type Variable.	Token.sol	L: 0 C: 0
SWC-128	Pass	DoS With Block Gas Limit.	Token.sol	L: 0 C: 0
SWC-129	Pass	Typographical Error.	Token.sol	L: 0 C: 0
SWC-130	Pass	Right-To-Left-Override control character (U+202E).	Token.sol	L: 0 C: 0
SWC-131	Pass	Presence of unused variables.	Token.sol	L: 0 C: 0
SWC-132	Pass	Unexpected Ether balance.	Token.sol	L: 0 C: 0
SWC-133	Pass	Hash Collisions with Multiple Variable Length Arguments.	Token.sol	L: 0 C: 0
SWC-134	Pass	Message call with hardcoded gas amount.	Token.sol	L: 0 C: 0
SWC-135	Pass	Code With No Effects (Irrelevant/Dead Code).	Token.sol	L: 0 C: 0
SWC-136	Pass	Unencrypted Private Data On-Chain.	Token.sol	L: 0 C: 0

We scan the contract for additional security issues using MYTHX and industry-standard security scanning tools.



Inheritance

The contract for Zksyncpad has the following inheritance structure.



Privileged Functions (onlyOwner)

Please Note if the contract is Renounced none of this functions can be executed.

Function Name	Parameters	Visibility
airdrop	address[] calldata	External
endSale	_buyers	External



Smart Contract Advance Checks

ID	Severity	Name	Result	Status
ZKSP-01	Minor	Potential Sandwich Attacks.	Pass	Not-Found
ZKSP-02	Minor	Function Visibility Optimization	Pass	Not-Found
ZKSP-03	Minor	Lack of Input Validation.	Pass	Not-Found
ZKSP-04	Major	Centralized Risk In addLiquidity.	Pass	Not-Found
ZKSP-05	Major	Missing Event Emission.	Pass	Not-Found
ZKSP-06	Minor	Conformance with Solidity Naming Conventions.	Pass	Not-Found
ZKSP-07	Minor	State Variables could be Declared Constant.	Pass	Not-Found
ZKSP-08	Major	Dead Code Elimination.	Pass	Not-Found
ZKSP-09	Major	Third Party Dependencies.	Pass	Not-Found
ZKSP-10	Major	Initial Token Distribution.	Pass	Not-Found
ZKSP-11	Critical	distributeTokensBetween Holders is a multisender of tokens from contract.	Pass	Not-Found
ZKSP-12	Major	Centralization Risks In The X Role	Pass	Not-Found
ZKSP-13	Informational	Extra Gas Cost For User..	Pass	Not-Found
ZKSP-14	Medium	Unnecessary Use Of SafeMath	Pass	Not-Found








ID	Severity	Name	Result	Status
ZKSP-15	Medium	Symbol Length Limitation due to Solidity Naming Standards.	Pass	Not-Found
ZKSP-16	Medium	Invalid collection of Taxes during Transfer.	Pass	Not-Found








Technical Findings Summary

Classification of Risk

Severity	Description
 Critical	Risks are those that impact the safe functioning of a platform and must be addressed before launch. Users should not invest in any project with outstanding critical risks.
 Major	Risks can include centralization issues and logical errors. Under specific circumstances, these major risks can lead to loss of funds and/or control of the project.
 Medium	Risks may not pose a direct risk to users' funds, but they can affect the overall functioning of a platform
 Minor	Risks can be any of the above but on a smaller scale. They generally do not compromise the overall integrity of the Project, but they may be less efficient than other solutions.
 Informational	Errors are often recommended to improve the code's style or certain operations to fall within industry best practices. They usually do not affect the overall functioning of the code.

Findings

Severity	Found	Pending	Resolved
 Critical	0	0	0
 Major	0	0	0
 Medium	0	0	0
 Minor	0	0	0
 Informational	0	0	0
Total	0	0	0



Social Media Checks

Social Media	URL	Result
Twitter	https://twitter.com/zkSyncpads	Pass
Other	https://discord.com/invite/xBDFchjjMy	Pass
Website	https://zksynclaunchpad.com	Pass
Telegram	https://t.me/zkSyncpadOfficial	Pass

We recommend to have 3 or more social media sources including a completed working websites.

Social Media Information Notes:

Auditor Notes: undefined

Project Owner Notes:



Audit Result

Final Audit Score

Review	Score
Security Score	99
Auditor Score	95

The Following Score System Has been Added to this page to help understand the value of the audit, the maximum score is 100, however to attain that value the project must pass and provide all the data needed for the assessment. Our Passing Score has been changed to 80 Points, if a project does not attain 80% is an automatic failure. Read our notes and final assessment below.

Audit Passed



Assessment Results

Important Notes:

- No issues or vulnerabilities were found.
- The following is a token contract, combined with a vesting based on a defined schedule and ICO contract.

Auditor Score =95
Audit Passed



Appendix

Finding Categories

Centralization / Privilege

Centralization / Privilege findings refer to either feature logic or implementation of components that act against the nature of decentralization, such as explicit ownership or specialized access roles in combination with a mechanism to relocate funds.

Gas Optimization

Gas Optimization findings do not affect the functionality of the code but generate different, more optimal EVM opcodes resulting in a reduction on the total gas cost of a transaction.

Logical Issue

Logical Issue findings detail a fault in the logic of the linked code, such as an incorrect notion on how block.timestamp works.

Control Flow

Control Flow findings concern the access control imposed on functions, such as owner-only functions being invoke-able by anyone under certain circumstances.

Volatile Code

Volatile Code findings refer to segments of code that behave unexpectedly on certain edge cases that may result in a vulnerability.

Coding Style

Coding Style findings usually do not affect the generated byte-code but rather comment on how to make the codebase more legible and, as a result, easily maintainable.

Inconsistency

Inconsistency findings refer to functions that should seemingly behave similarly yet contain different code, such as a constructor assignment imposing different requirements on the input variables than a setter function.

Coding Best Practices

ERC 20 Coding Standards are a set of rules that each developer should follow to ensure the code meets a set of criteria and is readable by all the developers.



Disclaimer

CFGNINJA has conducted an independent security assessment to verify the integrity of and highlight any vulnerabilities or errors, intentional or unintentional, that may be present in the reviewed code for the scope of this assessment. This report does not constitute agreement, acceptance, or advocacy for the Project, and users relying on this 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 the Project in question may pursue, and 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 entirely 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. Information is provided 'as is, and CFGNINJA is under no covenant to audited completeness, accuracy, or solidity of the contracts. In no event will CFGNINJA 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 or actions with regards to the information provided in this audit report.

The assessment services provided by CFGNINJA are subject to dependencies and are under continuing development. You agree that your access 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 with high levels of technical risk and uncertainty. The assessment reports could include false positives, negatives, and unpredictable results. The services may access, and depend upon, multiple layers of third parties.

