Assure DeFi®

THE VERIFICATION **GOLD STANDARD**

Security Assessment

USDE

Date: 16/05/2025

Audit Status: PASS

[WARNING]

Audit Edition: Solana

ASSURE DEFI®

THE VERIFICATION **GOLD STANDARD**

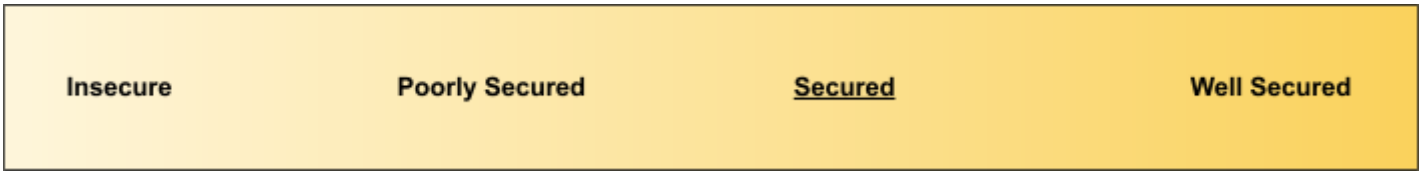
Risk Analysis

Vulnerability summary

Classification	Description
High	High-level vulnerabilities can result in the loss of assets or manipulation of data.
Medium	Medium-level vulnerabilities can be challenging to exploit, but they still have a considerable impact on smart contract execution, such as allowing public access to critical functions.
Low	Low-level vulnerabilities are primarily associated with outdated or unused code snippets that generally do not significantly impact execution, sometimes they can be ignored.
Informational	Informational vulnerabilities, code style violations, and informational statements do not affect smart contract execution and can typically be disregarded.

Executive Summary

According to the Assure assessment, the Customer's smart contract is **Secured.**



Scope

Target Code And Revision

For this audit, we performed research, investigation, and review of the USDE verifying the functional and superficial part of the contract since it is generated in SPL token creator and we do not have access to the base code.

Target Code And Revision

Project	Assure
Language	Rust
Codebase	Deployed address: 8dt9fQhoRKuWCSAsYweG2UMF3rbcG9xzNCTWXXSmdmEi *Creation:* *Token program*
Audit Methodology	Static, Manual

AUDIT OVERVIEW

Findings

Title	Description	Result
A1. Token Distribution and Liquidity Monitoring	A significant portion of the token's total supply is concentrated in a few private wallets, which presents a risk of market manipulation or sudden price volatility due to large, unexpected sell-offs. Additionally, there is involvement in liquidity pools that are relatively obscure or not widely recognized.	Moderate Risk
Owner and Wallet Security	No scams linked to the owner's wallet.	No Issues
Token functions	The token's Name, Symbol, Description, and URI can be modified. The token can be minted additionally. Project can freeze user accounts to prevent users from making transactions.	Moderate Risk
Ownership and Token Distribution	A substantial portion of the token's total supply is concentrated in a few private wallets, which creates a risk of market manipulation or abrupt price fluctuations resulting from large, unforeseen sell-offs.	Moderate Risk

Metadata and Technical Security	No concerning metadata found. Metadata could be changed [The token's Name, Symbol, Description, and URI can be modified]. No custom fees applied.	Low Risk
Market Activity and Transparency	Recent user activity confirmed. Liquidity pools not widely recognized. Active interaction in the last 30 days.	Moderate Risk

Assessment Results

Score Results

Review	Score
Global Score	**85/100**
Assure KYC	Not completed
Audit Score	85/100

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 84 Points for a higher standard, if a project does not attain 85% is an automatic failure. Read our notes and final assessment below. The Global Score is a combination of the evaluations obtained between having or not having KYC and the type of contract audited together with its manual audit.

Audit PASS [WARNING]

This audit report presents an in-depth analysis of the sol contract functions, emphasizing its immutability, renounced ownership, and financial controls.

The project has successfully passed the security audit but there are several warnings that could potentially impact the project's future:

- Centralized Token Distribution: A large portion of the token’s supply is held in a few private wallets, which could lead to market manipulation or sudden price volatility due to unexpected sell-offs.
- Liquidity Pools: The token is involved in liquidity pools that are not widely recognized, which could pose risks to market stability.
- Modifiable Token Parameters: The token’s Name, Symbol, Description, and URI can be changed, as well as the ability to mint more tokens. This flexibility could be a concern for trust and security.
- User Account Freezing: The project has the ability to freeze user accounts, potentially restricting transactions.
- Metadata: No concerning metadata issues, but the ability to modify key token details remains.

While there are no immediate security concerns, these factors should be closely monitored to avoid potential issues that could affect the project’s long-term viability.

Disclaimer

Assure Defi 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 advocating 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 person reading this report should invest their funds without sufficient individual due diligence, regardless of the findings presented. Information is provided ‘as is, and Assure Defi is under no covenant to audit completeness, accuracy, or solidity of the contracts. In no event will Assure Defi 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 Assure Defi 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.