# SOLIDIFIED

Audit Report for Wiva Digital - July 4, 2021

## Summary

Audit Report prepared by Solidified covering the WIVA ERC-20 token smart contracts.

## Process and Delivery

Two (2) independent Solidified experts performed an unbiased and isolated audit of the code. The debrief on 2 July 2021.

## Audited Files

The source code has been supplied in the form of a GitHub repository:

https://github.com/wivtech/wiva-smc

Final Commit number: `d330d23edf3b1a517676e24522738da019cce0f7`

The scope of the audit was limited to the following files:

```
contracts
├── Migrations.sol
└── WIVA.sol
```

## Intended Behavior

The smart contracts implement an ERC-20 token with a capped maximum supply of 200,000,000, snapshot capability, and mint (owner-controlled) and burn operations.

## Code Complexity and Test Coverage

Smart contract audits are an important step to improve the security of smart contracts and can find many issues. However, auditing complex codebases has its limits and a remaining risk is present (see disclaimer).

Users of a smart contract system should exercise caution. In order to help with the evaluation of the remaining risk, we provide a measure of the following key indicators: **code complexity**, **code readability**, **level of documentation**, and **test coverage**.

**Note, that high complexity or lower test coverage does equate to a higher risk. Certain bugs are more easily detected in unit testing than a security audit and vice versa. It is, therefore, more likely that undetected issues remain if the test coverage is low or non-existent.**

| Criteria | Status | Comment |
|---|---|---|
| Code complexity | Low | - |
| Code readability and clarity | High | - |
| Level of Documentation | High | - |
| Test Coverage | High | - |

Audit Report for Wiva Digital - July 4, 2021

## Issues Found

Solidified found that the WIVA token contract contains no issues.

## Disclaimer

Solidified audit is not a security warranty, investment advice, or an endorsement of Wiva Digital or its products. This audit does not provide a security or correctness guarantee of the audited smart contract. Securing smart contracts is a multistep process, therefore running a bug bounty program as a complement to this audit is strongly recommended.

The individual audit reports are anonymized and combined during a debrief process, in order to provide an unbiased delivery and protect the auditors of Solidified platform from legal and financial liability.

*Solidified Technologies Inc.*