META365

Security Assessment

18 July 2024

TRUSCOVA

TRUSTED CODE VALIDATION

Prepared for: META365

Prepared by: Dr. Muhammad Hassan

WE SECURE YOUR SMART CONTRACTS

About Truscova

Founded in last quarter of 2022 and headquartered in Bremen, Germany, Truscova aims to secure Web 3.0 by providing security assessment, audit, advisory and training services using formal verification and other leading technologies. Truscova founders include eminent scientists with more than 35 books, several patents, and more than 20,000 google scholar citations in the areas of verification, testing, security, and machine learning.

We focus on smart contracts testing and code review projects in Ethereum ecosystem, supporting client organizations in technology, defense, and finance industries, as well as government entities. We specialize in applying formal verification, dynamic analysis, fuzz testing, metamorphic testing, advanced coverage metrics, and static analysis to secure Web 3.0 projects.

We maintain an exhaustive list of publications at https://github.com/Truscova, with links to papers, presentations, public audit reports, and blog articles.

To explore our latest news and developments, please follow @truscova on Twitter or LinkedIn. You can also explore our repository at https://github.com/Truscova or blog articles at https://truscova.com/blog.php. To engage us directly, visit our “Contact” page at https://www.truscova.com/.

Truscova GmbH
Wilhelm-Liebknecht-Str. 4
28329 Bremen, Germany

Geschäftsführung
Dr. Muhammad Hassan

Tel. +49 (162) 919 6783
E-Mail: hassan@truscova.com
https://www.truscova.com

SOLARIS
IBAN DE81 1101 0101 5569 4416 33
BIC SOBKDEB2XXX

Handelsregister: HRB 38524
Registergericht: Amtsgericht Bremen
Umsatzsteuer-ID: DE360065309

Notices and Remarks

Copyright and Distribution

Test Coverage Disclaimer

All activities undertaken by Truscova in this project were performed in accordance with terms of the project agreement.

Truscova uses a combination of automated testing techniques and manual inspection to conduct security assessments and identify security flaws of the target system. Each method carries its own limitations.

Security assessments are time bound (hence not exhaustive) and are reliant on information provided by the client. As a result, the findings documented in this report should not be considered a comprehensive list of security issues, flaws, or defects in the target system or codebase.

Truscova GmbH
Wilhelm-Liebknecht-Str. 4
28329 Bremen, Germany

Geschäftsführung
Dr. Muhammad Hassan

Tel. +49 (162) 919 6783
E-Mail: hassan@truscova.com
https://www.truscova.com

SOLARIS
IBAN DE81 1101 0101 5569 4416 33
BIC SOBKDEB2XXX

Handelsregister: HRB 38524
Registergericht: Amtsgericht Bremen
Umsatzsteuer-ID: DE360065309

Contents

Truscova GmbH
Wilhelm-Liebknecht-Str. 4
28329 Bremen, Germany

Geschäftsführung
Dr. Muhammad Hassan

Tel. +49 (162) 919 6783
E-Mail: hassan@truscova.com
https://www.truscova.com

SOLARIS
IBAN DE81 1101 0101 5569 4416 33
BIC SOBKDEB2XXX

Handelsregister: HRB 38524
Registergericht: Amtsgericht Bremen
Umsatzsteuer-ID: DE360065309

Executive Summary

Engagement Overview and Scope

META365 engaged Truscova GmbH from 09th July 2024 till 23th July 2024 to review and audit the code base provided via online deployed contract available at following address:

0x43717C5b595714d3C1D6FcC55b7F0b5cf5CAE017

The scope of audit is limited to the following:

- UCC token

One security expert at Truscova audited the above code base using static analysis, fuzzing, proprietary Truscova Tools, and manual inspection. A summary of findings is discussed in the next subsection.

Summary of Findings

The uncovered vulnerabilities in codebase during the course of the audit are summarized in the following table:

Vulnerability Classification

Classification	*Count*
Informational	2
Medium	1
High	1

Vulnerability Categorization

Category	*Count*
Dead code	1
Library	1
Solidity Version	1
Centralization	1

Truscova GmbH
Wilhelm-Liebknecht-Str. 4
28329 Bremen, Germany

Geschäftsführung
Dr. Muhammad Hassan

Tel. +49 (162) 919 6783
E-Mail: hassan@truscova.com
https://www.truscova.com

SOLARIS
IBAN DE81 1101 0101 5569 4416 33
BIC SOBKDEB2XXX

Handelsregister: HRB 38524
Registergericht: Amtsgericht Bremen
Umsatzsteuer-ID: DE360065309

Project Summary

Contact Information

Following officials from Truscova participated in this project.

Dr. Muhammad Naiman Jalil, naiman@truscova.com	Project Coordination
Dr. Muhammad Hassan, hassan@truscova.com	Security Assessment Expert

Project Timeline

The significant project events and milestones are as follows:

Date	Event
08th July, 2024	First Contact
09th July, 2024	Contract Agreement
13th July, 2024	Assessment Start
16th July, 2024	Assessment Complete
16th July, 2024	Initial Audit Report Submitted
17th July, 2024	Corrected Audit Report Submitted
18th July, 2024	Final Audit Report Submitted

Truscova GmbH
Wilhelm-Liebknecht-Str. 4
28329 Bremen, Germany

Geschäftsführung
Dr. Muhammad Hassan

Tel. +49 (162) 919 6783
E-Mail: hassan@truscova.com
https://www.truscova.com

SOLARIS
IBAN DE81 1101 0101 5569 4416 33
BIC SOBKDEB2XXX

Handelsregister: HRB 38524
Registergericht: Amtsgericht Bremen
Umsatzsteuer-ID: DE360065309

Project Goals

The engagement was scoped to assess the security of META365 token UCC contracts. Specifically, we focused to answer the following non-exhaustive list of questions:

- Are there appropriate access controls in place?
- Are user-provided parameters sufficiently validated?
- Are the arithmetic calculations and state changes performed during token purchases, correct?
- Could an attacker steal funds from the system?
- Could an attacker take over the contract's ownership?
- How does the minting of tokens work?
- Are there any centralization risks?

Truscova GmbH
Wilhelm-Liebknecht-Str. 4
28329 Bremen, Germany

Geschäftsführung
Dr. Muhammad Hassan

Tel. +49 (162) 919 6783
E-Mail: hassan@truscova.com
https://www.truscova.com

SOLARIS
IBAN DE81 1101 0101 5569 4416 33
BIC SOBKDEB2XXX

Handelsregister: HRB 38524
Registergericht: Amtsgericht Bremen
Umsatzsteuer-ID: DE360065309

Project Targets

The engagement involved a review and testing of the following targets:

META365 UCC Token

1. Contract 0x43717C5b595714d3C1D6FcC55b7F0b5cf5CAE017

Codebase Type: Solidity

Platform: BNB Smart Chain

Truscova GmbH
Wilhelm-Liebknecht-Str. 4
28329 Bremen, Germany

Geschäftsführung
Dr. Muhammad Hassan

Tel. +49 (162) 919 6783
E-Mail: hassan@truscova.com
https://www.truscova.com

SOLARIS
IBAN DE81 1101 0101 5569 4416 33
BIC SOBKDEB2XXX

Handelsregister: HRB 38524
Registergericht: Amtsgericht Bremen
Umsatzsteuer-ID: DE360065309

Project Coverage

This section provides an overview of the analysis coverage of the review, as determined by our high-level engagement goals. Our approaches and their results include the following:

UCC Token

The UCC contract is a BEP20 token. The contract is designed with the following functionalities:

Token Details:

- Name: META365
- Symbol: UCC
- Max Supply: 1000000000 * 10**18 UCC tokens

Dependencies:

- Inherits functionalities from OpenZeppelin's ERC20, Ownable, and ERC20Burnable contracts.

Constructor:

- Initializes the token with a specified symbol and name.
- Inherits from the ERC20 and Ownable contracts.
- The constructor mints the total maximum supply (1,000,000,000 tokens) to the contract deployer's address (msg.sender).

Inherited Contracts:

- ERC20
- Ownable
- ERC20Burnable

Functions and Features

- _mint: Called within the constructor to mint the initial supply to the deployer.
- Ownership Transfer: Managed by the Ownable contract, enabling the owner to transfer control to another address.
- Token Burning: Enabled by the ERC20Burnable contract, allowing holders to burn their tokens, thus reducing the total supply in circulation.

We conducted a review of the contract and investigated the following:

- We reviewed if an attacker could bypass the access control on burning functions.
- We checked the arithmetic operations.
- We checked if the contract's functionality for transferring ownership works as intended, allowing secure updates to the ownership role.
- We checked if token transfer works as expected.

Truscova GmbH
Wilhelm-Liebknecht-Str. 4
28329 Bremen, Germany

Geschäftsführung
Dr. Muhammad Hassan

Tel. +49 (162) 919 6783
E-Mail: hassan@truscova.com
https://www.truscova.com

SOLARIS
IBAN DE81 1101 0101 5569 4416 33
BIC SOBKDEB2XXX

Handelsregister: HRB 38524
Registergericht: Amtsgericht Bremen
Umsatzsteuer-ID: DE360065309

Automated Testing

In this evaluation, Echidna, a smart contract fuzzer, was utilized to swiftly examine various system states and verify security properties through malicious, coverage-guided test case generation. Automated testing techniques were employed to supplement manual security reviews rather than replace them. However, each technique has limitations, such as Echidna's inability to randomly generate an edge case that violates a property. To maximize the effectiveness of security testing, a consistent process is followed. In the case of Echidna, 100,000 test cases are generated per property.

The focus of our automated testing and verification efforts was on the essential properties and elements of the UCC Token. Our aim was to ensure that the critical system properties are maintained to ensure correct protocol behavior.

Basic properties for standard functions

Property	Result
Total supply should be constant for non-mintable and non-burnable tokens.	-
No user balance should be greater than the token's total supply.	Passed
The sum of users balances should not be greater than the token's total supply.	Passed
Token balance for address zero should be zero.	Passed
transfers to zero address should not be allowed.	Passed
transferFroms to zero address should not be allowed.	Passed
Self transfers should not break accounting.	Passed
Self transferFroms should not break accounting.	Passed
transfers for more than account balance should not be allowed.	Passed
transferFroms for more than account balance should not be allowed.	Passed
transfers for zero amount should not break accounting.	Passed
transferFroms for zero amount should not break accounting.	Passed
Valid transfers should update accounting correctly.	Passed
Valid transferFroms should update accounting correctly.	Passed
Allowances should be set correctly when approve is called.	Passed
Allowances should be updated correctly when approve is called twice.	Passed
After transferFrom, allowances should be updated correctly.	Passed

Tests for burnable tokens

Property	Result
User balance and total supply should be updated correctly when burn is called.	Passed
User balance and total supply should be updated correctly when burnFrom is called.	Passed
Allowances should be updated correctly when burnFrom is called.	Passed

Truscova GmbH
Wilhelm-Liebknecht-Str. 4
28329 Bremen, Germany

Geschäftsführung
Dr. Muhammad Hassan

Tel. +49 (162) 919 6783
E-Mail: hassan@truscova.com
https://www.truscova.com

SOLARIS
IBAN DE81 1101 0101 5569 4416 33
BIC SOBKDEB2XXX

Handelsregister: HRB 38524
Registergericht: Amtsgericht Bremen
Umsatzsteuer-ID: DE360065309

Summary of Findings

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

ID	Title	Type	Severity
1	Variable MAX_SUPPLY is never used	Dead code	Informational
2	Use SafeERC20 instead of ERC20	Library	Medium
3	Using an older version of Solidity	Solidity version	Informational
4	Centralization Risk	Centralization	High

Truscova GmbH
Wilhelm-Liebknecht-Str. 4
28329 Bremen, Germany

Geschäftsführung
Dr. Muhammad Hassan

Tel. +49 (162) 919 6783
E-Mail: hassan@truscova.com
https://www.truscova.com

SOLARIS
IBAN DE81 1101 0101 5569 4416 33
BIC SOBKDEB2XXX

Handelsregister: HRB 38524
Registergericht: Amtsgericht Bremen
Umsatzsteuer-ID: DE360065309

Detailed Findings

1. Variable MAX_SUPPLY is never used

Severity: Informational	Difficulty: -
Type: Dead code	Finding ID: TCV-UCC-1
Target: UCC	

Description

The MAX_SUPPLY constant is defined but not used in the contract.

```
uint256 public constant MAX_SUPPLY = 1000000000 * 10**18;

    constructor(
        string memory name,
        string memory symbol
    ) ERC20(name, symbol)
    {
        _mint(msg.sender, 1000000000 * 10**18);
    }
```

Figure 1 – MAX_SUPPLY never used

Recommendation

We recommend using MAX_SUPPLY instead of “1000000000 * 10**18” in the contract to make it less error-prone.

Truscova GmbH
Wilhelm-Liebknecht-Str. 4
28329 Bremen, Germany

Geschäftsführung
Dr. Muhammad Hassan

Tel. +49 (162) 919 6783
E-Mail: hassan@truscova.com
https://www.truscova.com

SOLARIS
IBAN DE81 1101 0101 5569 4416 33
BIC SOBKDEB2XXX

Handelsregister: HRB 38524
Registergericht: Amtsgericht Bremen
Umsatzsteuer-ID: DE360065309

2. Use SafeERC20 instead of ERC20

Severity: Medium	Difficulty: Easy
Type: Library	Finding ID: TCV-UCC-2
Target: UCC	

Description

To enhance security, it is recommended to use OpenZeppelin's SafeERC20 library instead of the standard ERC20. The SafeERC20 library addresses the issues associated with non-standard ERC20 tokens. Unlike standard ERC20 tokens, which return a boolean value for *transfer* and *transferFrom* operations and revert transactions upon failure, SafeERC20 ensures robust handling of these operations.

```
contract UCC is ERC20, Ownable, ERC20Burnable {
    uint256 public constant MAX_SUPPLY = 1000000000 * 10**18;
```

Figure 2 – Use SafeERC20 instead of ERC20

Recommendation

We recommend using SafeERC20 library by OpenZeppelin.

You can do the following:

- import "@openzeppelin/contracts/token/ERC20/utils/SafeERC20.sol";

Truscova GmbH
Wilhelm-Liebknecht-Str. 4
28329 Bremen, Germany

Geschäftsführung
Dr. Muhammad Hassan

Tel. +49 (162) 919 6783
E-Mail: hassan@truscova.com
https://www.truscova.com

SOLARIS
IBAN DE81 1101 0101 5569 4416 33
BIC SOBKDEB2XXX

Handelsregister: HRB 38524
Registergericht: Amtsgericht Bremen
Umsatzsteuer-ID: DE360065309

3. Using an older version of Solidity

Severity: Informational	Difficulty: -
Type: Solidity version	Finding ID: TCV-UCC-3
Target: UCC	

Description

An older version of Solidity is under use.

```
// SPDX-License-Identifier: Apache-2.0
pragma solidity 0.8.10;

import "@openzeppelin/contracts/token/ERC20/ERC20.sol";
import "@openzeppelin/contracts/access/Ownable.sol";
import "@openzeppelin/contracts/token/ERC20/extensions/ERC20Burnable.sol";
```

Figure 3 – Use of older version of Solidity

As mentioned in the Solidity's official guide:

> *When deploying contracts, you should use the latest released version of Solidity. Apart from exceptional cases, only the latest version receives security fixes. Furthermore, breaking changes, as well as new features, are introduced regularly. We currently use a 0.y.z version number to indicate this fast pace of change.*

Recommendation

Please use the latest version of Solidity, i.e., Solidity 0.8.26.

Truscova GmbH
Wilhelm-Liebknecht-Str. 4
28329 Bremen, Germany

Geschäftsführung
Dr. Muhammad Hassan

Tel. +49 (162) 919 6783
E-Mail: hassan@truscova.com
https://www.truscova.com

SOLARIS
IBAN DE81 1101 0101 5569 4416 33
BIC SOBKDEB2XXX

Handelsregister: HRB 38524
Registergericht: Amtsgericht Bremen
Umsatzsteuer-ID: DE360065309

4. Centralization Risk

Severity: High	Difficulty: Easy
Type: Centralization	Finding ID: TCV-UCC-4
Target: UCC	

Description

The constructor mints the entire supply to the *msg.sender*, also the owner. It centralizes the initial distribution, which might not be desirable for all use cases.

```
constructor(
        string memory name,
        string memory symbol
    ) ERC20(name, symbol)
    {
        _mint(msg.sender, 1000000000 * 10**18);
    }
```

Figure 3 – Use of older version of Solidity

Recommendation

Consider a more decentralized or gradual distribution mechanism.

Truscova GmbH
Wilhelm-Liebknecht-Str. 4
28329 Bremen, Germany

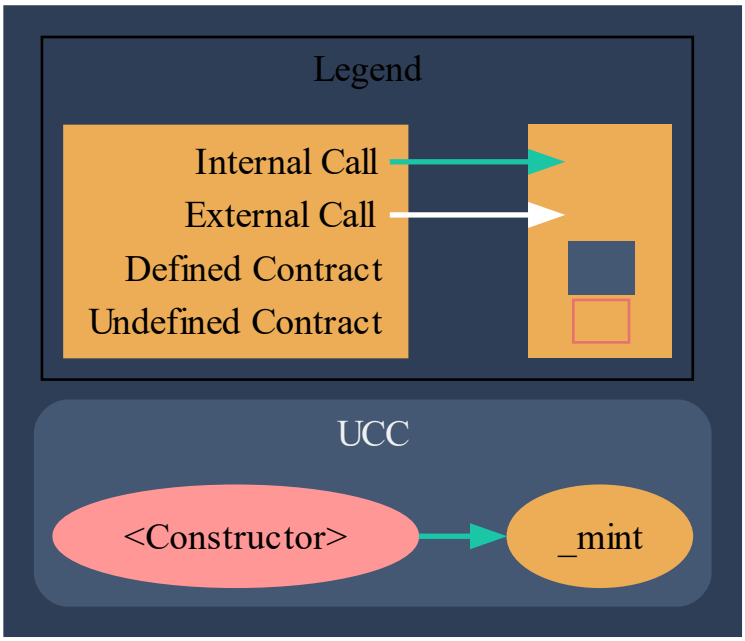
Geschäftsführung
Dr. Muhammad Hassan

Tel. +49 (162) 919 6783
E-Mail: hassan@truscova.com
https://www.truscova.com

SOLARIS
IBAN DE81 1101 0101 5569 4416 33
BIC SOBKDEB2XXX

Handelsregister: HRB 38524
Registergericht: Amtsgericht Bremen
Umsatzsteuer-ID: DE360065309

Call Graph for UCC Token



Truscova GmbH
Wilhelm-Liebknecht-Str. 4
28329 Bremen, Germany

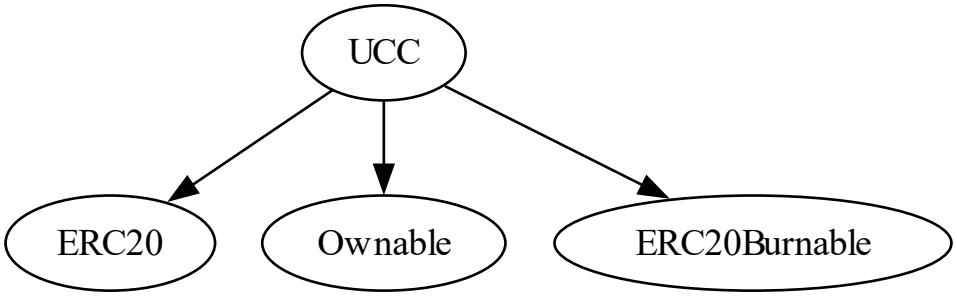
Geschäftsführung
Dr. Muhammad Hassan

Tel. +49 (162) 919 6783
E-Mail: hassan@truscova.com
https://www.truscova.com

SOLARIS
IBAN DE81 1101 0101 5569 4416 33
BIC SOBKDEB2XXX

Handelsregister: HRB 38524
Registergericht: Amtsgericht Bremen
Umsatzsteuer-ID: DE360065309

Inheritance Graph for UCC Token



Truscova GmbH
Wilhelm-Liebknecht-Str. 4
28329 Bremen, Germany

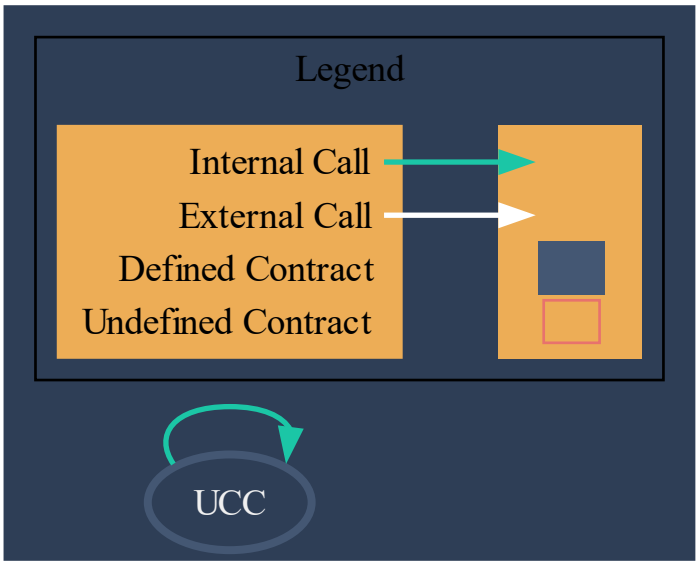
Geschäftsführung
Dr. Muhammad Hassan

Tel. +49 (162) 919 6783
E-Mail: hassan@truscova.com
https://www.truscova.com

SOLARIS
IBAN DE81 1101 0101 5569 4416 33
BIC SOBKDEB2XXX

Handelsregister: HRB 38524
Registergericht: Amtsgericht Bremen
Umsatzsteuer-ID: DE360065309

Interaction Graph for UCC Token



Truscova GmbH
Wilhelm-Liebknecht-Str. 4
28329 Bremen, Germany

Geschäftsführung
Dr. Muhammad Hassan

Tel. +49 (162) 919 6783
E-Mail: hassan@truscova.com
https://www.truscova.com

SOLARIS
IBAN DE81 1101 0101 5569 4416 33
BIC SOBKDEB2XXX

Handelsregister: HRB 38524
Registergericht: Amtsgericht Bremen
Umsatzsteuer-ID: DE360065309

Summary of Recommendations

The META365's UCC Token is a BEP20 token and it satisfies the necessary properties of BEP20 tokens. These include constant total supply, correct user balances, the ability to set allowances, the prevention of transfers to the zero address, and the ability to burn tokens. The fulfillment of these properties ensures the token's security and functionality. Truscova recommends that META365 team address the following for future iterations:

- Develop a detailed incident response plan to ensure that any issues that arise can be addressed promptly and without confusion.
- Create good documentation which will be helpful for the next phases of the project.
- Create a security architecture of the project as it progresses through various development stages.

Truscova GmbH
Wilhelm-Liebknecht-Str. 4
28329 Bremen, Germany

Geschäftsführung
Dr. Muhammad Hassan

Tel. +49 (162) 919 6783
E-Mail: hassan@truscova.com
https://www.truscova.com

SOLARIS
IBAN DE81 1101 0101 5569 4416 33
BIC SOBKDEB2XXX

Handelsregister: HRB 38524
Registergericht: Amtsgericht Bremen
Umsatzsteuer-ID: DE360065309