HACKEN

SMART CONTRACT CODE REVIEW AND SECURITY ANALYSIS REPORT

Customer: Crepe Inc
Date: 10 May, 2023

Hacken OÜ
Parda 4, Kesklinn, Tallinn,
10151 Harju Maakond, Eesti,
Kesklinna, Estonia
support@hacken.io

Document

Name	Smart Contract Code Review and Security Analysis Report for Crepe Inc
Approved By	Paul Fomichov | Lead Solidity SC Auditor at Hacken OU
Type	ERC20 token; MetaTX
Platform	EVM
Language	Solidity
Methodology	Link
Website	https://crepe.fund/
Changelog	03.05.2023 - Initial Review 10.05.2023 - Second Review

Hacken OÜ
Parda 4, Kesklinn, Tallinn,
10151 Harju Maakond, Eesti,
Kesklinna, Estonia
support@hacken.io

Table of contents

Hacken OÜ
Parda 4, Kesklinn, Tallinn,
10151 Harju Maakond, Eesti,
Kesklinna, Estonia
support@hacken.io

Introduction

Hacken OÜ (Consultant) was contracted by Crepe Inc (Customer) to conduct a Smart Contract Code Review and Security Analysis. This report presents the findings of the security assessment of the Customer's smart contracts.

System Overview

The provided repository consists of a single contract that:

- Inherits ERC20, ownable, and burnable.
- Mints 1B tokens on deployment.
- Acts as an EIP2721 recipient contract as a part of a Meta-transactions system.

The files in the scope:

- **CREFinal.sol** - Acts as EIP2771 Recipient contract: it accepts meta transactions from the trustedForwarder. ERC20, ownable, and burnable. Pre-mints 1B tokens to the deployer address.

Privileged roles

- Owner: Deploys the contract and receives 1B minted tokens. Can transfer the token ownership to a new address.
- Trusted Forwarder: A contract trusted by the Recipient to correctly verify signatures and nonces before forwarding the request from Transaction Signers.

Hacken OÜ
Parda 4, Kesklinn, Tallinn,
10151 Harju Maakond, Eesti,
Kesklinna, Estonia
support@hacken.io

Executive Summary

The score measurement details can be found in the corresponding section of the scoring methodology.

Documentation quality

The total Documentation Quality score is **3** out of **10**.

- Poor system description.
- No NatSpec.
- Technical description is not provided.

Code quality

The total Code Quality score is **6** out of **10**.

- The development environment is not configured.
- Solidity Style Guide violation.
- Redundant Code.
- Inefficient Gas Model.

Security score

As a result of the audit, the code contains **1** low severity issue. The security score is **10** out of **10**.

All found issues are displayed in the “Findings” section.

Summary

According to the assessment, the Customer's smart contract has the following score: **8.5**.The system users should acknowledge all the risks summed up in the risks section of the report.

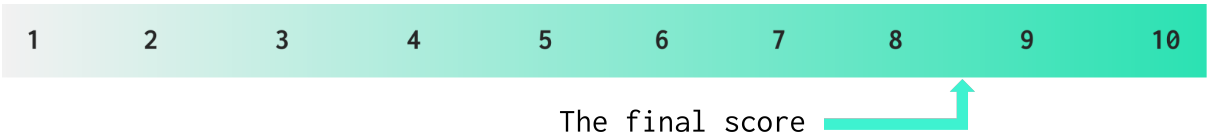

Table. The distribution of issues during the audit

Review date	Low	Medium	High	Critical
03 May 2023	1	0	2	0
10 May 2023	1	0	0	0

Hacken OÜ
Parda 4, Kesklinn, Tallinn,
10151 Harju Maakond, Eesti,
Kesklinna, Estonia
support@hacken.io

Risks

- Untrusted parties can act as Gas Relayers.
- A malicious forwarder may forge the value of _msgSender(), extracting address data appended from an untrusted contract, and effectively send transactions from any address.
- If a forwarder is upgradeable, then one must also trust that the contract will not perform a malicious upgrade.
- As exposed in H02, the system relies on the external infrastructure from Biconomy, which is out of the scope of this audit.

Hacken OÜ
Parda 4, Kesklinn, Tallinn,
10151 Harju Maakond, Eesti,
Kesklinna, Estonia
support@hacken.io

Checked Items

We have audited the Customers' smart contracts for commonly known and specific vulnerabilities. Here are some items considered:

Item	Description	Status	Related Issues
Default Visibility	Functions and state variables visibility should be set explicitly. Visibility levels should be specified consciously.	Passed	
Integer Overflow and Underflow	If unchecked math is used, all math operations should be safe from overflows and underflows.	Not Relevant	
Outdated Compiler Version	It is recommended to use a recent version of the Solidity compiler.	Passed	
Floating Pragma	Contracts should be deployed with the same compiler version and flags that they have been tested thoroughly.	Failed	L01
Unchecked Call Return Value	The return value of a message call should be checked.	Not Relevant	
Access Control & Authorization	Ownership takeover should not be possible. All crucial functions should be protected. Users could not affect data that belongs to other users.	Passed	H01, H02
SELFDESTRUCT Instruction	The contract should not be self-destructible while it has funds belonging to users.	Not Relevant	
Check-Effect-Interaction	Check-Effect-Interaction pattern should be followed if the code performs ANY external call.	Passed	
Assert Violation	Properly functioning code should never reach a failing assert statement.	Passed	
Deprecated Solidity Functions	Deprecated built-in functions should never be used.	Passed	
Delegatecall to Untrusted Callee	Delegatecalls should only be allowed to trusted addresses.	Not Relevant	
DoS (Denial of Service)	Execution of the code should never be blocked by a specific contract state unless required.	Passed	

Hacken OÜ
Parda 4, Kesklinn, Tallinn,
10151 Harju Maakond, Eesti,
Kesklinna, Estonia
support@hacken.io

Race Conditions	Race Conditions and Transactions Order Dependency should not be possible.	Passed	
Authorization through tx.origin	tx.origin should not be used for authorization.	Not Relevant	
Block values as a proxy for time	Block numbers should not be used for time calculations.	Not Relevant	
Signature Unique Id	Signed messages should always have a unique id. A transaction hash should not be used as a unique id. Chain identifiers should always be used. All parameters from the signature should be used in signer recovery. EIP-712 should be followed during a signer verification.	Not Relevant	
Shadowing State Variable	State variables should not be shadowed.	Passed	
Weak Sources of Randomness	Random values should never be generated from Chain Attributes or be predictable.	Not Relevant	
Incorrect Inheritance Order	When inheriting multiple contracts, especially if they have identical functions, a developer should carefully specify inheritance in the correct order.	Passed	
Calls Only to Trusted Addresses	All external calls should be performed only to trusted addresses.	Not Relevant	
Presence of Unused Variables	The code should not contain unused variables if this is not justified by design.	Failed	I04
EIP Standards Violation	EIP standards should not be violated.	Passed	
Assets Integrity	Funds are protected and cannot be withdrawn without proper permissions or be locked on the contract.	Not Relevant	
User Balances Manipulation	Contract owners or any other third party should not be able to access funds belonging to users.	Not Relevant	
Data Consistency	Smart contract data should be consistent all over the data flow.	Not Relevant	

Flashloan Attack	When working with exchange rates, they should be received from a trusted source and not be vulnerable to short-term rate changes that can be achieved by using flash loans. Oracles should be used.	Not Relevant	
Token Supply Manipulation	Tokens can be minted only according to rules specified in a whitepaper or any other documentation provided by the Customer.	Passed	
Gas Limit and Loops	Transaction execution costs should not depend dramatically on the amount of data stored on the contract. There should not be any cases when execution fails due to the block Gas limit.	Not Relevant	
Style Guide Violation	Style guides and best practices should be followed.	Failed	I01, I02
Requirements Compliance	The code should be compliant with the requirements provided by the Customer.	Passed	
Environment Consistency	The project should contain a configured development environment with a comprehensive description of how to compile, build and deploy the code.	Failed	
Secure Oracles Usage	The code should have the ability to pause specific data feeds that it relies on. This should be done to protect a contract from compromised oracles.	Not Relevant	
Tests Coverage	The code should be covered with unit tests. Test coverage should be sufficient, with both negative and positive cases covered. Usage of contracts by multiple users should be tested.	Failed	
Stable Imports	The code should not reference draft contracts, which may be changed in the future.	Not Relevant	

Hacken OÜ
Parda 4, Kesklinn, Tallinn,
10151 Harju Maakond, Eesti,
Kesklinna, Estonia
support@hacken.io

Findings

■■■■ Critical

No critical severity issues were found.

■■■ High

H01. Coarse-Grained Access Control

Impact	High
Likelihood	Mid

The current implementation of the project has a coarse-grained authorization model that may not be sufficient to protect contracts with multiple layers of functionality. A single point of failure.

There might only be a single owner role controlling everything (including transfers of ownership), which increases the risk to the system in case of a key leak.

As a consequence, the totality of funds from the owner can be lost, in addition to the contract ownership.

Path: ./Contract/CREFinal.sol : transferTokenOwnershipAndSupply()

Recommendation:

Implement a multiple signature scheme for the admin role.

Found in: 1036f0a

Status: Mitigated (with Customer notice: The CREPE DAO owns the CREPE Token contract with a Gnosis Multisig wallet. The CREPE DAO owns all the CREPE Tokens to make sure it is distributed as written in the Whitepaper.)

H02. Unverifiable Logic

Impact	High
Likelihood	Mid

EIP2771 Recipient contracts have implicit security considerations that must be explained to protocol so that they are aware of them.

The risks this project integration is exposed to are:

- Untrusted parties can act as Gas Relayers.
- A malicious forwarder may forge the value of _msgSender(), extracting address data appended from an untrusted contract, and effectively send transactions from any address.

- If a forwarder is upgradeable, then one must also trust that the contract will not perform a malicious upgrade.

Path: ./Contract/CREFinal.sol

Recommendation:

It is necessary to publicly acknowledge (e.g. in Documentation) the high risks that an EIP2771 Recipient Contract is exposed to when integrated into a system.

By implementing this recommendation: explicitly explaining how Trusted Forwarders may have malicious intentions since they are not part of the scope, that they can also be upgradeable and uncontrollable, and Gas Relayers can also be out of control; this issue can be mitigated.

Found in: 1036f0a

Status: Mitigated (with Customer notice: We use Biconomy GSN network. Therefore, the transferForwarder is a node provided by Biconomy network.)

Medium

No medium severity issues were found.

Low

L01. Floating Pragma

Contracts should be deployed with the same compiler version and flags that they have been tested with thoroughly. Locking the pragma helps to ensure that contracts do not accidentally get deployed using, for example, an outdated compiler version that might introduce bugs that affect the contract system negatively.

Paths: ./Contract/CREFinal.sol

Recommendation: Consider locking the Solidity pragma version. Find more in SWC-103.

Found in: 1036f0a

Status: Reported

Informational

I01. Style Guide: Order of Functions

The provided projects should follow the official guidelines. Functions should be grouped according to their *visibility* and ordered:

1. Constructor

2. Receive function (if exists)
3. Fallback function (if exists)
4. External
5. Public
6. Internal
7. Private

Path: ./Contract/CREFinal.sol

Recommendation: Consider following the official Solidity guidelines.

Found in: 1036f0a

Status: Reported

I02. Style Guide: NatSpec

It is recommended that Solidity contracts are fully annotated using NatSpec for all public interfaces (everything in the ABI).

Path: ./Contract/CREFinal.sol

Recommendation: Consider following the official Solidity guidelines.

Found in: 1036f0a

Status: Reported

I03. Gas Optimization: Variables Can Be Immutable

The state variable _trustedForwarder is never updated after deployment; thus, it can be set to immutable.

Use immutable and constant keywords on state variables to limit changes to their state and save Gas.

Path: ./Contract/CREFinal.sol

Recommendation: Set _trustedForwarder as immutable.

Found in: 1036f0a

Status: Reported

I04. Redundant Import

The contract ERC2771Context.sol is imported but never used.

Path: ./Contract/CREFinal.sol

Recommendation: Contract should not have code that is not used.

Found in: 1036f0a

Status: Reported

Hacken OÜ
Parda 4, Kesklinn, Tallinn,
10151 Harju Maakond, Eesti,
Kesklinna, Estonia
support@hacken.io

Disclaimers

Hacken Disclaimer

The smart contracts given for audit have been analyzed based on best industry practices at the time of the writing of this report, with cybersecurity vulnerabilities and issues in smart contract source code, the details of which are disclosed in this report (Source Code); the Source Code compilation, deployment, and functionality (performing the intended functions).

The report contains no statements or warranties on the identification of all vulnerabilities and security of the code. The report covers the code submitted and reviewed, so it may not be relevant after any modifications. Do not consider this report as a final and sufficient assessment regarding the utility and safety of the code, bug-free status, or any other contract statements.

While we have done our best in conducting the analysis and producing this report, it is important to note that you should not rely on this report only — we recommend proceeding with several independent audits and a public bug bounty program to ensure the security of smart contracts.

English is the original language of the report. The Consultant is not responsible for the correctness of the translated versions.

Technical Disclaimer

Smart contracts are deployed and executed on a blockchain platform. The platform, its programming language, and other software related to the smart contract can have vulnerabilities that can lead to hacks. Thus, the Consultant cannot guarantee the explicit security of the audited smart contracts.

Hacken OÜ
Parda 4, Kesklinn, Tallinn,
10151 Harju Maakond, Eesti,
Kesklinna, Estonia
support@hacken.io

Appendix 1. Severity Definitions

When auditing smart contracts Hacken is using a risk-based approach that considers the potential impact of any vulnerabilities and the likelihood of them being exploited. The matrix of impact and likelihood is a commonly used tool in risk management to help assess and prioritize risks.

The impact of a vulnerability refers to the potential harm that could result if it were to be exploited. For smart contracts, this could include the loss of funds or assets, unauthorized access or control, or reputational damage.

The likelihood of a vulnerability being exploited is determined by considering the likelihood of an attack occurring, the level of skill or resources required to exploit the vulnerability, and the presence of any mitigating controls that could reduce the likelihood of exploitation.

Risk Level	High Impact	Medium Impact	Low Impact
High Likelihood	**Critical**	**High**	**Medium**
Medium Likelihood	**High**	**Medium**	**Low**
Low Likelihood	**Medium**	**Low**	**Low**

Risk Levels

Critical: Critical vulnerabilities are usually straightforward to exploit and can lead to the loss of user funds or contract state manipulation.

High: High vulnerabilities are usually harder to exploit, requiring specific conditions, or have a more limited scope, but can still lead to the loss of user funds or contract state manipulation.

Medium: Medium vulnerabilities are usually limited to state manipulations and, in most cases, cannot lead to asset loss. Contradictions and requirements violations. Major deviations from best practices are also in this category.

Low: Major deviations from best practices or major Gas inefficiency. These issues won't have a significant impact on code execution, don’t affect security score but can affect code quality score.

Hacken OÜ
Parda 4, Kesklinn, Tallinn,
10151 Harju Maakond, Eesti,
Kesklinna, Estonia
support@hacken.io

Impact Levels

High Impact: Risks that have a high impact are associated with financial losses, reputational damage, or major alterations to contract state. High impact issues typically involve invalid calculations, denial of service, token supply manipulation, and data consistency, but are not limited to those categories.

Medium Impact: Risks that have a medium impact could result in financial losses, reputational damage, or minor contract state manipulation. These risks can also be associated with undocumented behavior or violations of requirements.

Low Impact: Risks that have a low impact cannot lead to financial losses or state manipulation. These risks are typically related to unscalable functionality, contradictions, inconsistent data, or major violations of best practices.

Likelihood Levels

High Likelihood: Risks that have a high likelihood are those that are expected to occur frequently or are very likely to occur. These risks could be the result of known vulnerabilities or weaknesses in the contract, or could be the result of external factors such as attacks or exploits targeting similar contracts.

Medium Likelihood: Risks that have a medium likelihood are those that are possible but not as likely to occur as those in the high likelihood category. These risks could be the result of less severe vulnerabilities or weaknesses in the contract, or could be the result of less targeted attacks or exploits.

Low Likelihood: Risks that have a low likelihood are those that are unlikely to occur, but still possible. These risks could be the result of very specific or complex vulnerabilities or weaknesses in the contract, or could be the result of highly targeted attacks or exploits.

Informational

Informational issues are mostly connected to violations of best practices, typos in code, violations of code style, and dead or redundant code.

Informational issues are not affecting the score, but addressing them will be beneficial for the project.

Hacken OÜ
Parda 4, Kesklinn, Tallinn,
10151 Harju Maakond, Eesti,
Kesklinna, Estonia
support@hacken.io

Appendix 2. Scope

The scope of the project includes the following smart contracts from the provided repository:

Initial review scope

Repository	https://github.com/Crepeinc/CrepeTokenContracts
Commit	1036f0a4f077b2a724d7bd61a8a25d55467a1b8c
Whitepaper	Link
Requirements	Link
Technical Requirements	Not provided
Contracts	File: ./CrepeFinal/Contract/CREFinal.sol SHA3: f246d97604a16d6c73553dbb2289633dfb67d72e088839403fc3ea15977b33bc

Second review scope

Repository	https://github.com/Crepeinc/CrepeTokenContracts
Commit	6f41bfb34938268eb7f17dc13beaab29eb67b65f
Whitepaper	Link
Requirements	Link
Technical Requirements	Not provided
Contracts Addresses	-
Contracts	File: ./CrepeFinal/Contract/CREFinal.sol SHA3: 1b6c3eb0f0e0fd1ee73d73e880332b179415076ef5ecf54a4a3a92cb72f49a60