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

Proposal №. 23032021-SCA\01
for providing limited access engagement
(Solidity Code Review)
Dated 23.03.2021

Hacken OÜ, a company with a principal address at Kai tn 1-5M, Tallinn city, Harju county, 10111, Estonia ("**Company**"), and

Trustswap a company (**"Client"**). Collectively referred to herein as the "Parties" and individually as a "Party".

"Hacken" (referred to as the Consultant) specializing in cybersecurity consulting services offers Trustswap (the Client) Solidity Code Review services of limited number of a pre-production contract:

(1) https://testnet.bscscan.com/address/0x997fb70a90f918f87a18e533c8e7b38710d5448d#code

(2) https://github.com/trustswap/swap-contracts/tree/feature/swap-18-partial-unstake
39435fd

swap-contracts-feature-swap-18-partial-unstake/contracts/SmartSwap.sol	out of scope
swap-contracts-feature-swap-18-partial-unstake/contracts/SwapSmartLock.sol	out of scope
swap-contracts-feature-swap-18-partial-unstake/contracts/SwapStakingContract.sol	in scope
swap-contracts-feature-swap-18-partial-unstake/contracts/SwapToken.sol	out of scope
swap-contracts-feature-swap-18-partial-unstake/contracts/PriceEstimator.sol	out of scope
swap-contracts-feature-swap-18-partial-unstake/contracts/Migrations.sol	out of scope
swap-contracts-feature-swap-18-partial-unstake/contracts/IPriceEstimator.sol	out of scope
swap-contracts-feature-swap-18-partial-unstake/contracts/IERC20Extended.sol	out of scope

The following sections provide a summary of the project objectives, technical solution, scope, deliverables, budget and estimated time of engagement. In this proposal, we have provided a Consultant background, differentiators, competencies and professional security services.

1 GOALS AND OBJECTIVES OF AUDIT

Code Review is performed by the professional team of consultants in accordance with internal methodology. Hacken team analyses smart contract's functionality and performs all necessary checks against known vulnerabilities.

Objectives of the assessment are: check whether the smart contract is vulnerable to known attacks; verify that it doesn't have any logic or access control issues; verify that it is compliant to Solidity Code Style Guide.

The goal of the audit is to find and fix security issues to protect the application from hacker attacks. Vulnerabilities analyzed during the smart contract audit include:

Table 1 Vulnerabilities Categories

Category	Check Item
Code review	▪ Reentrancy ▪ Ownership Takeover

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

	▪ Timestamp Dependence ▪ Gas Limit and Loops(Solidity) ▪ DoS with (Unexpected) Throw ▪ DoS with Block Gas Limit(Solidity) ▪ Transaction-Ordering Dependence ▪ Style guide violation ▪ Costly Loop ▪ ERC20 API violation(Solidity) ▪ Unchecked external call ▪ Unchecked math ▪ Unsafe type inference ▪ Implicit visibility level ▪ Deployment Consistency ▪ Repository Consistency ▪ Data Consistency
Functional review	▪ Business Logics Review ▪ Functionality Checks ▪ Access Control & Authorization ▪ Escrow manipulation ▪ Token Supply manipulation ▪ User Balances manipulation ▪ Data Consistency manipulation ▪ Kill-Switch Mechanism ▪ Operation Trails & Event Generation

Stages of Code Review[1]

The Services are conducted in several stages:

Table 2 Work Specification

Stage	Info
1. Preparation	Hacken team deploys smart contract locally and manually analyze the business model of smart contracts, their logic flows, and expected behavior. Auditors are clarifying and obtaining the missing information for reference specifications of contracts
2. Contracts analysis	Auditors scan smart contracts with automated tools (solc, Mythrill and Remix IDE) and review discovered issues manually Hacken team manually checks smart contracts against known attacks: reentrancy, reordering, overflows, etc. Auditors analyze smart contracts in accordance with Solidity Code Style Guide Auditors checking functionality of the smart contract vs the technical design if it provided.

[1] Notice. This engagement is not UAT testing, these two activities overlap but are not interchangeable. User Acceptance Testing (UAT) is one of the last stages of the software development life cycle and sometimes known as End User Testing. UAT should be conducted by the client team in a prod or pre-prod environment and cover by test all-planned integrations.

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

3. Documentation of findings	Auditors write a detailed report that contains: ▪ General project info ▪ Executive summary ▪ As-is overview ▪ Audit overview (contains all issues and steps on how to fix them) ▪ Conclusion and Disclaimers ▪ Appendixes with evidence
4. Final	After remediation check Hacken team publish on company site.

2 BUDGET, SCHEDULE & PAYMENT TERMS

We propose to implement security assessment using Bundled Fixed Price approach:
Table 3 Price

#	Stage	Duration workdays	Cost	Price
1.1	Solidity Code Review (1)	2-3		3500 USD
1.2	Solidity Code Review (2)	3		4000 USD
1.2	One-time free remediation check. (second and next remediation checks is extra $500 each)			
	TOTAL:			7500 USD
	Retainer required to commence engagement (100% of total)			7500 USD

3 LIMITATIONS

This project limited by the scope of this document

During this project, the Consultant will follow the following limitations:

- The operational impact to the networks will be maintained to the minimum but coordinated with the client
- No active backdoor or Trojans will be installed
- No client data will be copied, modified or destroyed.

4 CLIENT RESPONSIBILITIES

The Client is responsible for presenting and agrees of correct materials, test data-set, that developed application should be working with the and all needed graphical resources such as logos, slogan and preferable design elements, etc.

Client acknowledges that the completion of various parts of the deliverables under this Proposal may depend on and require the Client's commitment to provide certain resources. Client agrees to provide such resources and to timely complete and fulfill its required actions for Consultant to be able to fully comply with its obligations under this Proposal. Client's failure to provide such resources and to timely fulfill such obligations shall not constitute a basis for the retention of payments and/or allegations of breach of contract by Consultant.

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

The client will provide representatives from the IT department for communication and answering project-related questions during project execution, available 4 hours per day from Monday to Friday, 8-12 am Central Time. Failure to allocate needed people from the client may lead to project end date adjustment and later delivery.

5 OWNERSHIP

Consultant acknowledges Client's ownership to intellectual property rights and to all proprietary software products used about the fulfillment of this contract including related documentation, reports and software as well as all related materials and all confidential Client's information.

The software program developed hereunder, its source code, and any other material developed hereunder which constitutes part of its design and which may be necessary for its future development shall constitute a work made for hire under the copyright laws and shall be owned by Client.

6 LIMITATION OF LIABILITY

Under no circumstances shall Consultant have any liability for any claim arising from or relating to this Proposal more than the amount paid to Consultant by Client under it. The amount paid does not pertain to those deliverables that have been accepted and approved by Client. Neither party hereto shall have any liability for consequential, incidental, special, or indirect damages (including, without limitation, loss of profit and business opportunities) regardless of whether the party has been advised, or is aware, of the possibility of such damages.

7 INDEPENDENT CONTRACTOR

Consultant's relationship with Client is that of an independent contractor, and nothing in this Proposal should be construed to create a partnership, agency, joint venture or employment relationship.

8 FORCE MAJEURE

No liability shall result from the non-performance of any obligation under this Proposal caused by circumstances beyond the control of the non-performing party including, without limitation, natural catastrophes, extreme weather conditions, fire, war, strikes, hostilities, acts of terrorism, civil unrest, governmental interference, and embargoes (collectively, "Force Majeure") for that period commencing from the time at which notice of the existence of the Force Majeure is given by the non-performing party and terminating when the Force Majeure has ended or would have ended had the non-performing party taken those steps which it could reasonably have been expected to take to overcome the Force Majeure provided it could be overcome. The Force Majeure shall automatically extend the period for performing the obligation under this Proposal of the non-performing party. If a Force Majeure continues for more than 3 (three) months, either party may terminate this Proposal relating to software development not yet delivered.

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

INVOICE 23032021-SCA\01

Date and Place: 23 March 2021, Estonia, Tallin
Contractor: Hacken OÜ, located at Kai tn 1-5M, Tallinn city, Harju county, 10111, Estonia
Customer: Trastswap
Subject matter: Solidity Smart Contract audit (code review)
Currency: USDT
Price of the services: 7500 USD
Terms of payments and acceptance: Advance payment – 100% of the invoice total amount. The services were rendered at the location of the Customer.
Payment address details: 0x301f10637445f9171156a6a7b1a30d2a67aafc45 /**USDT ERC20**

№	Description	Quantity	Price, USDT	Amount, USDT
1	Solidity Smart Contract audit (code review)	1	7500	7500
			Total:	7500

This Invoice is an offer to enter into an agreement. The payment, according to this document, shall be deemed as an acceptance of the offer to enter into the agreement on the terms and conditions set here. The payment must be made not later than 25 March 2021.

Please note, that the payment is considered to be the evidence of the performed work and delivered services according to the scope.

The payment shall be the confirmation that Parties have no claims to each other and have no intention to submit any claims in future. The agreement shall not include penalty and fine clauses.

The Parties shall not be liable for non-performance or improper performance of the obligations under the agreement during the term of insuperable force circumstances.

All the legal relations between Parties shall be regulated by the law of England and Wales. Any disputes or controversy arising from the Agreement or related to it shall be settled through negotiations between the Parties.

Should the Parties fail to settle a dispute through negotiations, it shall be referred to and finally resolved by arbitration under the Rules of Arbitration (Vienna Rules) of the Vienna International Arbitral Centre (VIAC) of the Austrian Federal Economic Chamber by three arbitrators appointed in accordance with the said Rules.