CERTIK
FOUNDATION

SaltSwap

CertiK Security Services Proposal

February 26, 2021

Proposal for SaltSwap

Proposal for SaltSwap

Scope of Services

Application name : SaltSwap

Date : 02/26/2021

Objective: Smart Contract Auditing

Version : Link provided

- A comprehensive **Security Audit** to assess the code security of the SaltSwap project and provide a full-version Security Audit report.
- Dedicated security engineers as resources for Q&A and improvement suggestions regarding raising the security standard of Customer's project.

Estimated Cost

	Security Audit
Fee Base	$13,000 per week for 2 security auditors
Time Frame	4 Business Days *Delivered report within 1.5 weeks
Cost	**$8,000**

	Skynet
Fee Base	$7,200
Time Frame	Duration of audit
Cost	**Complimentary**

Methodologies

This methodology covers all phases, from the initial planning to the post-review phase. All tasks are divided into several subtasks.

1. Planning
   - 1.1 Preparation
   - 1.2 Test Design
   - 1.3 Environment Setup
2. Execution
   - 2.1 Managed Mode
   - 2.2 Defined Mode
   - 2.3 Optimized Mode
3. Assessment
   - 3.1 Technical Report
   - 3.2 Impact Analysis
   - 3.3 Findings Prioritization
4. Reporting
   - 4.1 Report
   - 4.2 Finalization
   - 4.3 Post-Review

Planning

The first phase of the review covers the information collection needed in order to plan properly. This includes the compilation of the basic information about the code and all the key papers about the technology stacks used or implemented.

1. Preparation : information gathering, defining scope.
2. Test Design : establish and design test scenarios and key points to review.
3. Environment Setup : installation of tools.

Execution

The execution phase covers the test scenarios for the code review that were selected on the Test Design. It is divided into three phases, each phase will provide data using automated and manual tools.

1. Managed Mode :

   This mode covers the execution of automated tools for the analysis of the code.

   Source code analysis tools and strict custom linters applied to isolate key areas of interest and provide insights about the state of the code.

   Custom tooling for gathering information about common areas of interest. Analysis of best coding practices via automated tools is also conducted on this step.

2. Defined Mode :

   In this phase we are going to examine the results of the managed mode and the automated tools for issues.

   We are going to start with the examination of the automated phase findings and manually review each finding. Specifically, we will first assimilate the findings of the automated tools and manually review each one to filter out false positives as well as assess and replicate any major vulnerabilities that may arise from them.

   Afterwards, an overall manual pass will be done on the codebase of the smart contracts and their inter-relationships based on the definitions provided in the documentation of the smart contracts as well as any supplementary documentational material provided to us by SaltSwap .

   As the project at hand considers a complex protocol implementation, the interdependencies between the contracts as well as the proper cross-contract inherited interactions and implementations will be closely examined in correlation with the specifications of the project.

   Lastly, a line-by-line audit will finally be conducted that will examine the source code in depth to ensure the highest level of scrutiny is applied on the codebase and to identify more obscure vulnerabilities as well as any inefficiencies that can be optimized to save gas cost when transacting with the contracts.

If any major vulnerabilities are found, supplementary test cases that replicate the vulnerabilities will be provided.

3. **Optimized Mode** :

   This mode of the execution phase focuses on those key areas of the software that are found most at risk. Additional testing may occur if needed in this phase.

Assessment

This phase covers the evaluation of the findings identified in the previous phase. Findings are validated and are given a corresponding risk score.

Once the scores are added to each finding, a prioritization process is carried out to sort those findings.

1. **Technical Report** : Review of the results, validation of findings, removing false-positives.
2. **Impact Analysis** : Determination of risk score depending on the issues of nature.
3. **Findings Prioritisation** : Sorting of findings

Disclaimer

This report is subject to the terms and conditions (including without limitation, description of services, confidentiality, disclaimer and limitation of liability) set forth in the Services Agreement, or the scope of services, and terms and conditions provided to the Company in connection with the Agreement. This report provided in connection with the Services set forth in the Agreement shall be used by the Company only to the extent permitted under the terms and conditions set forth in the Agreement. This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes without CertiK's prior written consent.

This report is not, nor should be considered, an "endorsement" or "disapproval" of any particular project or team. This report is not, nor should be considered, an indication of the economics or value of any "product" or "asset" created by any team or project that contracts CertiK to perform a security assessment. This report does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors, business, business model or legal compliance.

This report should not be used in any way to make decisions around investment or involvement with any particular project. This report in no way provides investment advice, nor should be leveraged as investment advice of any sort. This report represents an extensive assessing process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology.

Blockchain technology and cryptographic assets present a high level of ongoing risk. CertiK's position is that each company and individual are responsible for their own due diligence and continuous security. CertiK's goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies, and in no way claims any guarantee of security or functionality of the technology we agree to analyze.

About CertiK

Founded in 2017 by leading academics in the field of Computer Science from both Yale and Columbia University, CertiK is a leading blockchain security company that serves to verify the security and correctness of smart contracts and blockchain-based protocols. Through the utilization of our world-class technical expertise, alongside our proprietary, innovative tech, we're able to support the success of our clients with best-in-class security, all whilst realizing our overarching vision; provable trust for all throughout all facets of blockchain.