****

# Practices for Secure Software Report

Table of Contents

[Document Revision History 3](#_Toc102040754)

[Client 3](#_Toc102040755)

[Instructions 3](#_Toc102040756)

[Developer 4](#_Toc102040757)

[1. Algorithm Cipher 4](#_Toc102040758)

[2. Certificate Generation 4](#_Toc102040759)

[3. Deploy Cipher 4](#_Toc102040760)

[4. Secure Communications 4](#_Toc102040761)

[5. Secondary Testing 4](#_Toc102040762)

[6. Functional Testing 4](#_Toc102040763)

[7. Summary 4](#_Toc102040764)

[8. Industry Standard Best Practices 4](#_Toc102040765)

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **12/17/2023** | **Jonah Soun** |  |

## Client



## Instructions

Submit this completed practices for secure software report. Replace the bracketed text with the relevant information. You must document your process for writing secure communications and refactoring code that complies with software security testing protocols.

* Respond to the steps outlined below and include your findings.
* Respond using your own words. You may also choose to include images or supporting materials. If you include them, make certain to insert them in all the relevant locations in the document.
* Refer to the Project Two Guidelines and Rubric for more detailed instructions about each section of the template.

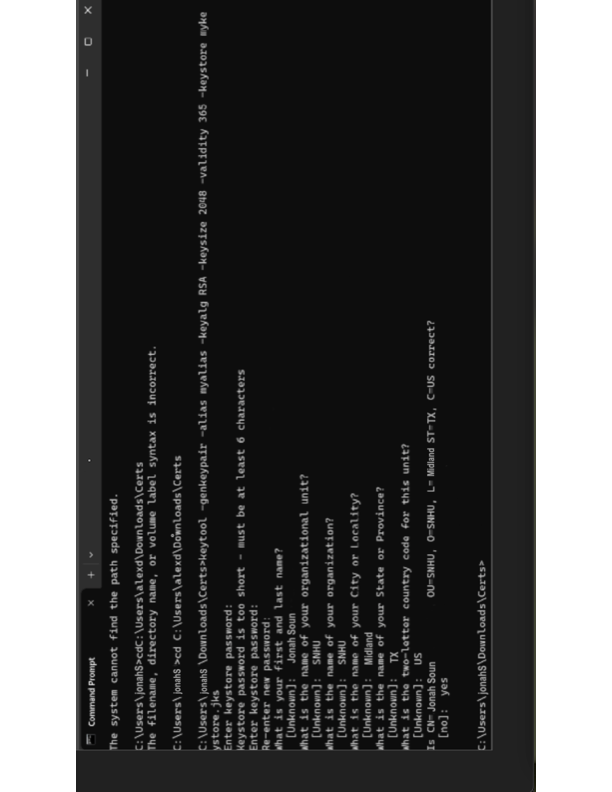
## Developer

Jonah Soun

## Algorithm Cipher

The algorithm cipher that I would recommend for the security vulnerabilities is Blowfish block cipher. The Blowfish was designed by Bruce Schneier as an alternative for different existing encryption. The cipher is unpatented and license-free that is available for all uses. The hash function increases the workload and duration to reduce threats. The bit length for the Blowfish cipher is 32 to 448 bits. The use of random numbers has constants with the hexadecimal digits. The use of symmetric uses the same key for encryption and decryption. The blowfish cipher is now considered outdated and more prone for cryptographic attacks.

## Certificate Generation

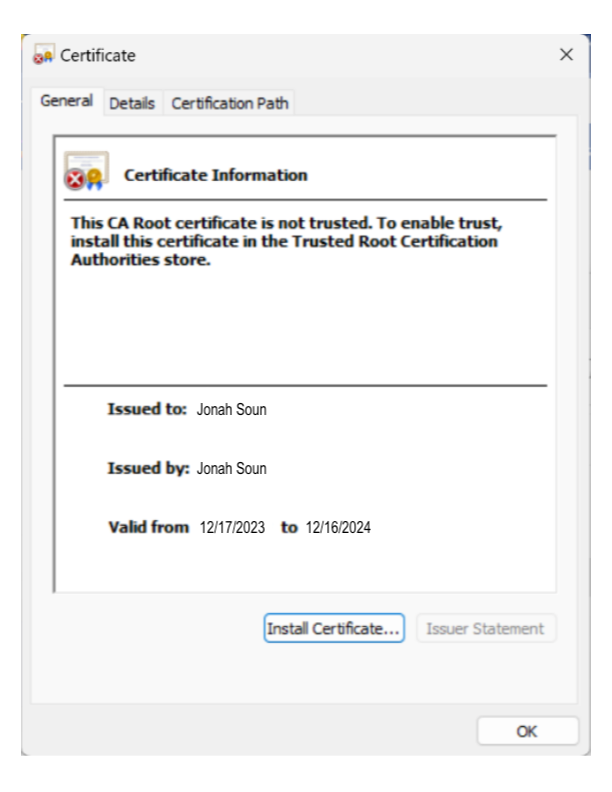


## Deploy Cipher

Insert a screenshot below of the checksum verification.

[Insert screenshots here.]

## Secure Communications



## Secondary Testing

Insert screenshots below of the refactored code executed without errors and the dependency-check report.

[Insert screenshots here.]

## Functional Testing

Insert a screenshot below of the refactored code executed without errors.

[Insert screenshots here.]

## Summary

In a project there are several different things that could go wrong. Therefore, there needs to be test to make sure that all the security requirements are met. The requirements are important because the client is usually the ones that outline the code. For example, generating the certificate to deploying the cipher all helps meet the client’s security requirements.

## Industry Standard Best Practices

In a lifetime of a software there are always updates pushed out in order to resolve any issues that may arise after the release of the app. Which is why there are several different tests that could be generated in order to prevent security hackers in order to protect everyone’s private information.