****

# 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** | **2/16/2023** | **Nick Franklin** | **Filled in all fields** |

## 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

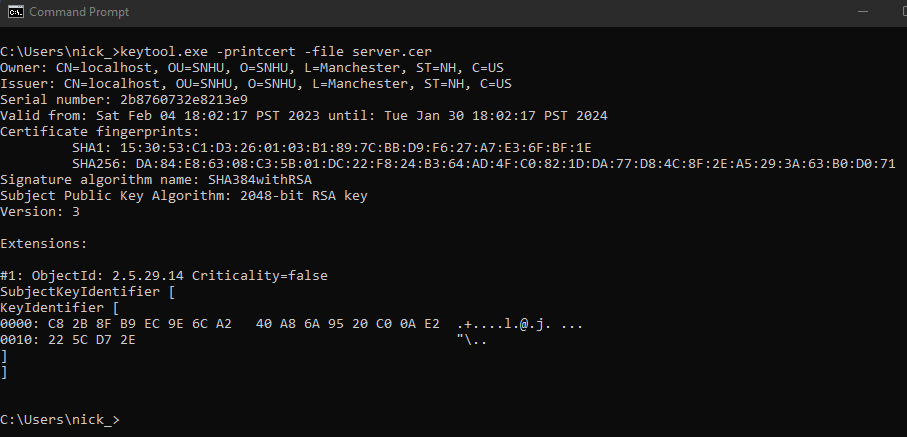
Nicholas Franklin

## Algorithm Cipher

After examining Artemis Financial’s software and security needs, the biggest being data interception, I would recommend the use of the SHA-256 encryption in order to keep their data secure during transit. Basically, the SHA-256 encryption works by first breaking up the data into blocks and padding these blocks and assigning them values. Iterations of these operations happen and result in a hash value and a checksum is generated to validate. The SHA-256 is a symmetrical encryption so the same key is used for both encryption and decryption. The 256 in the name stands for the bit length for the blocks in the encryption. The higher the number of bits, the stronger the encryption but also the longer it takes to decrypt with the key. The encryption makes use of random numbers generated for better encryption and to create a valid checksum that will not allow for deconstruction. Encryption and the tools for hacking encryptions are constantly evolving and many have gone obsolete due to being hacked. The SHA encryption however was designed and is in use by the United States federal government and is virtually non-hackable at the time of writing this and will be for some time which makes it the best encryption for Artemis Financial’s data security.

## Certificate Generation

Insert a screenshot below of the CER file.



## Deploy Cipher

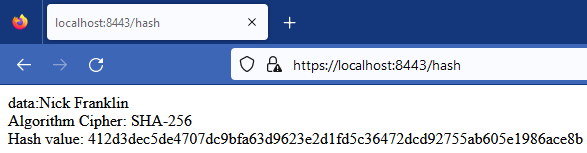
Insert a screenshot below of the checksum verification.

Graphical user interface, text, application

Description automatically generated

## Secure Communications

Insert a screenshot below of the web browser that shows a secure webpage.



## Secondary Testing

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

Text

Description automatically generated



## Functional Testing

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

Text

Description automatically generated

## Summary

I have addressed the Cryptography point in the vulnerability assessment process flow by using the SHA-256 for encryption which is very secure and reliable. By adding a RestController to the program, there is now a secure controller for the Restful server hash which addresses the Code Quality of the vulnerability assessment process flow by following secure coding practices.

## Industry Standard Best Practices

I used industry standard best practices first off by following the vulnerability assessment process flow and making sure that I assessed and addressed any security risks that I came across. Another way I used best practices was by making sure that everything was up to date by checking the pom.xml file. It is very important to use industry standard best practices and keep everything up to date by checking multiple times per month for updates in order to keep the application secure and avoid any data leaks or other risks to the service and company as a whole.