****

# Practices for Secure Software Report

Table of Contents

[Practices for Secure Software Report 1](#_Toc148887555)

[Document Revision History 3](#_Toc148887556)

[Client 3](#_Toc148887557)

[Developer 4](#_Toc148887558)

[1. Algorithm Cipher 4](#_Toc148887559)

[2. Certificate Generation 4](#_Toc148887560)

[3. Deploy Cipher 5](#_Toc148887561)

[4. Secure Communications 5](#_Toc148887562)

[5. Secondary Testing 6](#_Toc148887563)

[Below you will find Screenshots of both the final working code and the Dependency report: 6](#_Toc148887564)

[6. Functional Testing 7](#_Toc148887565)

[7. Summary 8](#_Toc148887566)

[8. Industry Standard Best Practices 8](#_Toc148887567)

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.1** | **10/19/2023** | **Jason Robbins** |  |

## Client



## Developer

Jason Robbins

## Algorithm Cipher

As per our original recommendation in a previous report, we believe that for our client, Artemis Financial, that for increased security for their communications between them, their clients and other financial institutions that employ an encryption algorithm cipher for their transactions. As per the recommendation in the previous report, we recommend that our client use an AES (Advanced Encryption Standard) Cipher, specifically we recommended the AES-256 cipher as it complies with government regulations regarded keeping customers information confidential while preventing suspicious behavior on the side of either of the transactional financial institutions.

AES-256 is a symmetric encryption algorithm, meaning that the same key that is used to encrypt the message is also the key that is used to decrypt the message. The “256” of the AES-256 is that it uses a 256-character bit length when generating encryption keys, this means that a hacker would need to attempt 2^256 combinations with powerful computers to try and access your data.

When paired with SHA-256 hash function to monitor whether your data had been tampered with, we believe that this will provide an excellent level of security for our clients’ institution. Compared to the old DES which was for a time the gold standard, AES replaced it in the early 2000’s with the rise of faster computers that could process much more brute force attempts than older generations. Now, with Quantum computing on the horizon, AES remains the gold standard and is used by the government for protecting their information now and in the future.

## Certificate Generation

Below is the screenshot of the generated Server Certificate:

A computer screen with text and numbers

Description automatically generated

## Deploy Cipher

Below is a screenshot of the Checksum Verification:

A screenshot of a computer

Description automatically generated

## Secure Communications

Modifications made to applications config file but appears to have not affected the security unsure of how to proceed

A screenshot of a computer

Description automatically generated

## Secondary Testing

## Below you will find Screenshots of both the final working code and the Dependency report:



A screenshot of a computer

Description automatically generated

## Functional Testing

## Below you will find a screenshot of the final working code for the SSLServer application. I believe that I could have refined this further by including more classes that would have dealt with converting the HTTP to HTTPS but I could not properly configure the classes without error. In the future I will look for more solutions to help with make the software more secure.

A screen shot of a computer program

Description automatically generated

## Summary

When refactoring the code, I used an updated Servercontroller class so that handles hash calculation. I had this hash coupled with the SHA-256 hash algorithm so that there would be a way to verify that there was not code manipulation from transmission to reception. I also find that any information going into the main class for the program would have to include Input Validation. On further iterations of the code, it is needed that there is an update to the java version in the pom.xml file. There should be an update to both the spring framework and any additional dependencies that are needed from the dependency report.

## Industry Standard Best Practices

While working with financial information of the clients and to not invoke the ire of the Department of Treasury, Industry standard best practices dictate that you should use encryption and hash algorithms to both ensure that if the code is tampered with that you dissuade attackers and ensure clients data security and to track that your client’s data has not been tampered with. This will be met with our recommendations of using an AES-256 encryption algorithm and an SHA]-256 hashing algorithm, these are both systems that are being used by leading financial institutions and government departments.

As for our further recommendations, dependency checks should be carried out at least once a month on the program to ensure that there are not any newfound vulnerabilities within installed dependencies for the springboot system. This is considered best practice as it will lessen the likelihood of attacks on Artemis’ systems by ensuring up to date data protection.