****

# Practices for Secure Software Report

# Table of Contents

# Document Revision History . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 3

# Client Information . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 3

# Developer Information . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 3

# Algorithm Cipher . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 4

# Certificate Generation . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 5

# Deploy Cipher / Secure Communications . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 6

# Secondary Testing . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 7

# Dependency Check . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 8

# Functional Testing . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 9

# Summary and Industry Standards . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 10 - 11

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **4/14/2023** | **Stanley Niles** | **Initial Document Creation** |

## Client



## 

## Developer

Stanley A. Niles

## Algorithm Cipher

## Regarding the nature of the data that Artemis Financial works with, it is recommended to use an AES-256 algorithm to properly protect their sensitive client data. The Advanced Encryption Standard, AES, is a symmetric key block cipher that operates on 128 blocks of data. It supports multiple key sizes of 128, 192 and 256. AES is a widely used and adopted global standard that offers a high level of security with exceptional performance.

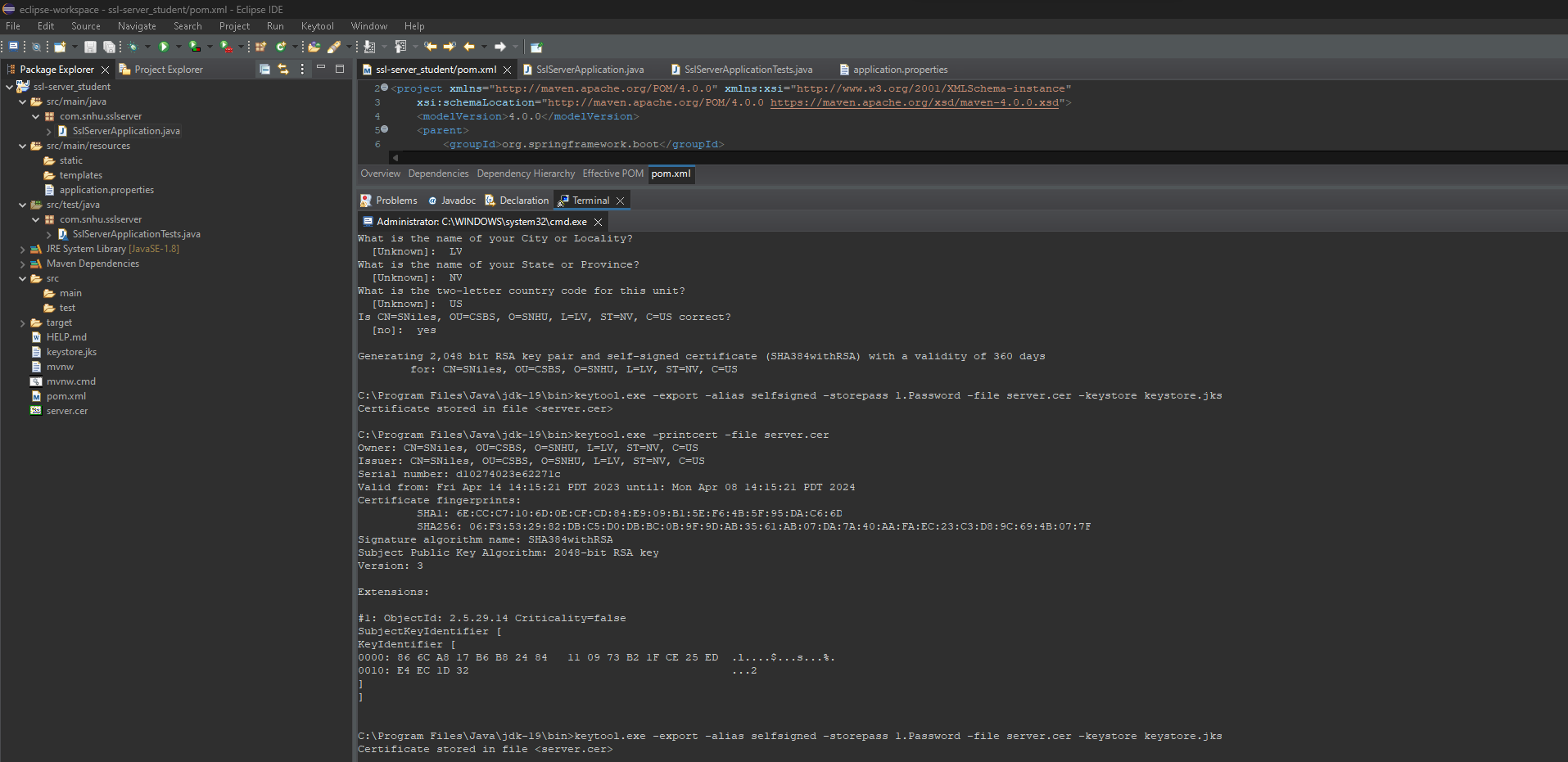
## AES-256 is not a hash function, however, it can and is suggested that Artemis Financial utilizes the AES-256 algorithm in combination with a Security Hash Algorithm – 256. SHA-256 is a cryptographic function that receives an input and returns a fixed sized string of bytes. Together these methods would ensure the security and authenticity of the stored data.

AES is a symmetric-key encryption algorithm; therefore, the same key is used for both encryption and decryption. This does pose a potential risk associated with using AES as it therefore requires appropriate secure key management and the secure sharing of these keys between communicating parties. Appropriate and randomized key choices are also appropriate to prevent easily found patterns and enhance security.

AES is widely considered as the go-to encryption algorithm for numerous applications. It was established as the standard by the National Institute of Standards and Technology (NIST) in 2001 and is currently used as the standard encryption of the US government. It has been subjected to rigorous evaluation and testing procedures by the security community and remains one of the top algorithms to protect sensitive data.

## 

## Certificate Generation



## Deploy Cipher / Secure CommunicationA screenshot of a computer Description automatically generated with medium confidence

## Secondary Testing

## Text Description automatically generated

## Dependency Check

## 

## Functional Testing

Text

Description automatically generated

## Summary

In this project, regarding the Vulnerability Assessment Process Flow Diagram, the code was refactored to address the areas of Input Validation, Cryptography, Code Quality and Encapsulation specifically by the following methods:

Input Validation: A unique data string was used and processed for generating a hash value. Thereby limiting any vulnerabilities from invalid input.

Cryptography: An SHA-256 hashing algorithm was implemented to secure the data using a unique data string.

Code Quality: The refactored code follows secure coding practices which include items such as exception handling, code organization and code readability.

Along with the above items, layers of security were added to the software application by the hashing algorithm, updating the APIs to remove known vulnerabilities and the implementation of the HTTPS communication protocols.

## Industry Standard Best Practices

For this project I implemented Industry Standard Best Practices by following secure coding principles and implemented new levels of security that not only maintained but improved upon the already existing security. Applying industry standard best practices is vital to a company’s well-being and reputation in the business world. Not only will this ensure trust in their customers, but also limits potential legal liabilities. By continuing to follow these best practices, the company can continue to mitigate security risks to maintain data integrity and security and limit potential vulnerabilities stemming from data breaches or other threats to its software infrastructure.