****

# 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 5](#_Toc102040759)

[3. Deploy Cipher 5](#_Toc102040760)

[4. Secure Communications 5](#_Toc102040761)

[5. Secondary Testing 6](#_Toc102040762)

[6. Functional Testing 7](#_Toc102040763)

[7. Summary 8](#_Toc102040764)

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

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **August 25, 2024** | **Jonathan C. Sanchez** | **Project Two** |

## 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

Jonathan C. Sanchez

## Algorithm Cipher

The Advanced Encryption Standard (AES) is secure, efficient, and widely accepted. Therefore, AES is my recommendation for Artemis Financial for their local and international security needs. The encryption cipher supports three levels of encryption: 128 (bits), 192 (bits), and 256 (bits). Having three different levels of encryption allows for varying levels of security that can be tailored to fit the customer’s needs. AES is a robust symmetric encryption algorithm that ensures the confidentiality and integrity of its users’ data.

The justification for AES speaks for itself through its resilience against attacks, and recognition on a global level. AES was first endorsed by the National Institute of Standards and Technology (NIST) in 2001 and has become a global standard for encrypting unclassified information since. The usage and implementation of AES will put Artemis in compliance with the Gramm-Leach-Bliley Act (GBLA) for protecting financial institutions and meeting the requirements of the Federal Information Processing Standards 197 (FIPS 197). Staying in compliance is key to the longevity of an organization.

AES is a block cipher that generates random keys to encrypt fixed-sized blocks of 128 bits. The randomness achieved ensures that if the same plaintext is encrypted multiple times, it will not generate the same ciphertexts.

* An initial 128-bit key is expanded into several round keys to ensure uniqueness (Key Expansion).
* The expanded key is then combined with plaintext blocks to start the encryption process (Add Key).
* Each byte of plaintext is then substituted with a corresponding value from a fixed S-box (Sub Bytes).
* The rows of the current state are shifted left based on the index (Row Shift).
* The columns are then mixed by multiplying each value with a fixed matrix value (Mix Columns).
* Each byte of the current state is then combined with a corresponding round key byte (Add Round Key).

The number of times the above process is looped depends on the desired key size. AES-128 requires 10 rounds, AES-192 requires 12 rounds and AES-256 requires 14 rounds.

Hash functions are not natively supported by AES. AES generates variable key lengths to encrypt data. Hash functions such as SHA-256 are generally used to produce fixed-sized hash values to use during authentication. While AES does not support this functionality “out of the box” the functionality can be built in to use both AES and SHA.

Although AES is robust and secure it does not guarantee 100% security. To achieve higher levels of safety, Artemis must implement multiple levels of security in their systems and processes. Some of the most common best practices to implement are multi-factor authentication, input validation, network security, access controls, and user training. Adding these additional measures with help improve the safety and security of the system.

## Certificate Generation

Insert a screenshot below of the CER file.

A screenshot of a computer

Description automatically generated

## Deploy Cipher

Insert a screenshot below of the checksum verification.

**Code:**

**A screen shot of a computer

Description automatically generated**

**Cipher:**

**A number on a white background

Description automatically generated**

## Secure Communications

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

Although the cert has been created and updated, my connection is still not secure. However, the page loads properly on my machine.

A screenshot of a computer

Description automatically generated

## Secondary Testing

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

**Terminal:**

Code Execution: Error(s)

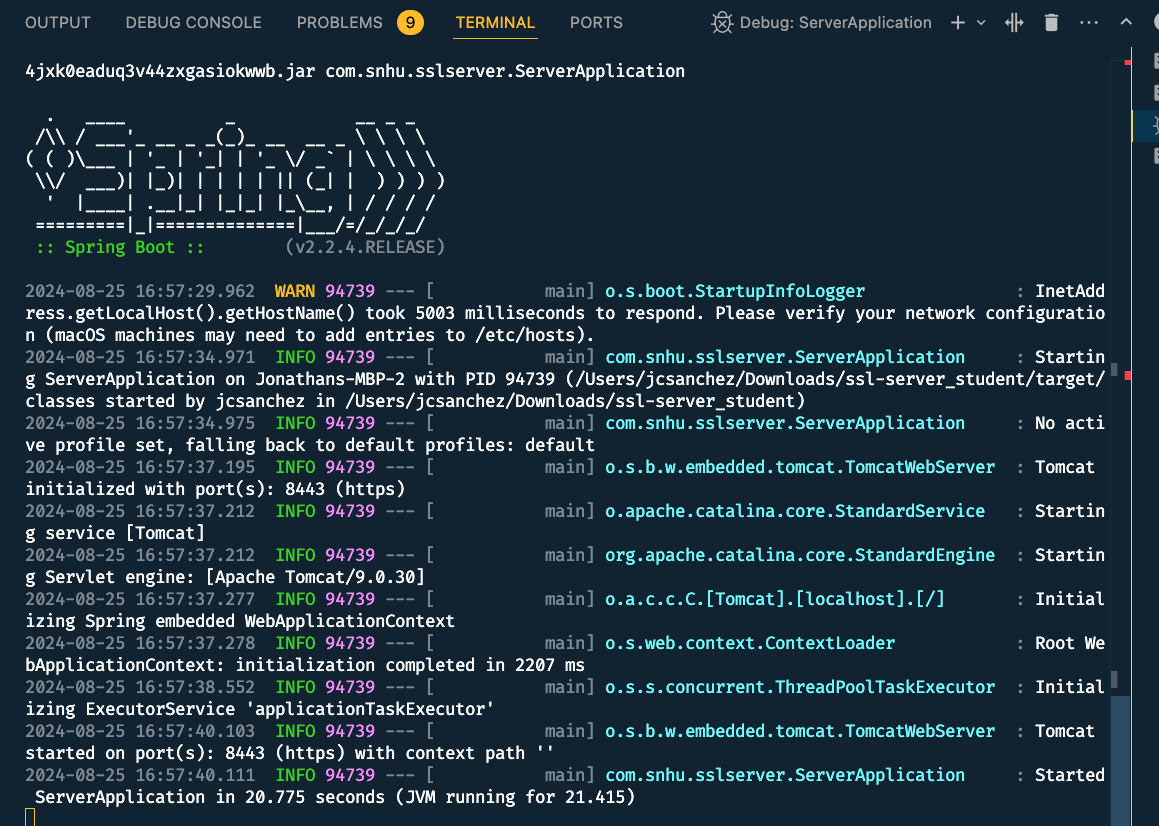
A blue screen with white lines

Description automatically generated

A computer screen shot of a program

Description automatically generated

Code Execution: No Error(s)



**Dependency-Check: (Not updated), see updated version in functional testing:**

**A screenshot of a computer

Description automatically generated**

## Functional Testing

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

Code:

**A screen shot of a computer

Description automatically generated**

A screenshot of a computer

Description automatically generatedA computer screen shot of a program

Description automatically generated

**Updated Dependency Check:**

**A screenshot of a computer

Description automatically generated**

## Summary

In Project Two, the Advanced Encryption Standard was chosen for as the best algorithm cipher for Artemis Financial. AES has proven high levels of security, efficiency, and global recognition. The Secure Hash Algorithm (SHA), is the preferred choice to produce hash value encryption. SHA was developed by the National Security Agency and like AES, is recognized by NIST. If Artemis chooses to use AES to encrypt stored and shared data, and SHA for authentication, the two together will provide higher levels of security and ensure safety. As well as keep them in compliance with local and global regulations. The approach taken in this project ensures that the best encryption options are provided to the customer, additional security measures are presented and, implementation is properly tested.

## Industry Standard Best Practices

The implementation of any process should adhere to industry standards and best practices. In addition to encryption, Artemis Financial should also consider least privilege protocols, input validation, network security, access controls, and user training. As well as perform regular updates and monitor regulations for any new additions or amendments. This approach reduces the amount of security risk Artemis takes on and safeguards sensitive information.