****

# 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** | **08/25/2024** | **Christian Wallace** |  |

## 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

Christian Wallace

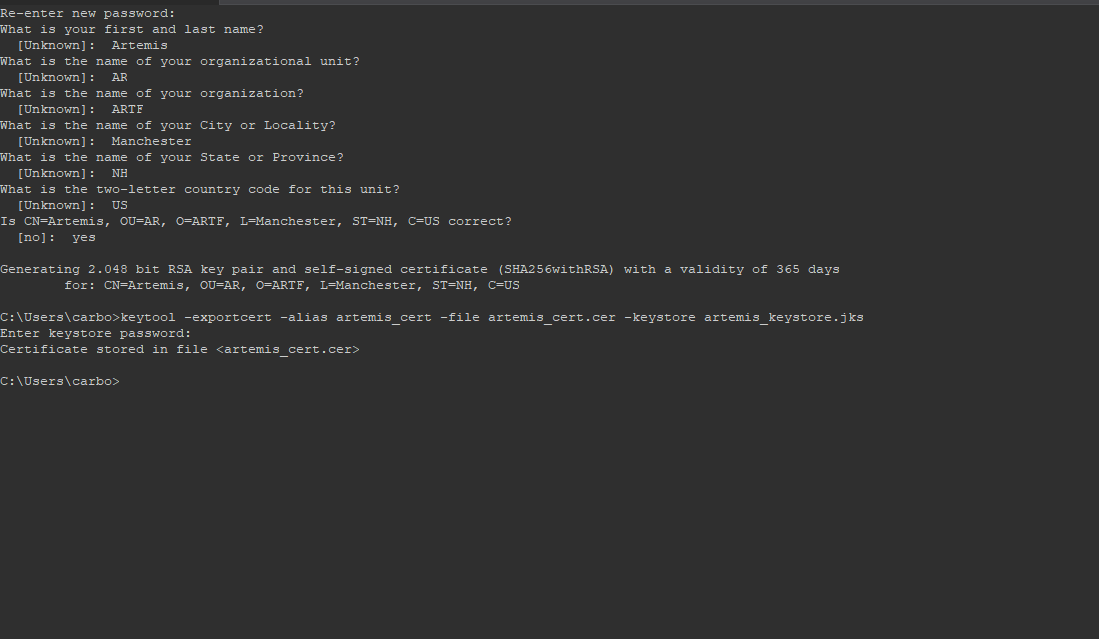
## Algorithm Cipher

**Recommendation**: The recommended encryption algorithm cipher for Artemis Financial is the **Advanced Encryption Standard (AES)**.

* **High-Level Overview**: AES is a symmetric encryption algorithm used globally to secure sensitive data. It operates on blocks of data, typically 128 bits, and can use key sizes of 128, 192, or 256 bits.
* **Hash Functions and Bit Levels**: Although AES itself is not a hash function, it is often used alongside hash algorithms like SHA-256 for checksum verification. The bit levels (e.g., 256-bit) correspond to the encryption key size.
* **Random Numbers**: AES uses initialization vectors (IVs) for encryption, which are random values that ensure different ciphertexts for identical plaintexts.
* **Symmetric vs. Non-Symmetric Keys**: AES uses symmetric keys, meaning the same key is used for both encryption and decryption, necessitating secure key management.
* **History and Current State**: Established by NIST in 2001, AES remains one of the most trusted encryption algorithms, widely adopted for both government and commercial use.

## Certificate Generation

Insert a screenshot below of the CER file.



## Deploy Cipher

Insert a screenshot below of the checksum verification.

A screen shot of a computer program

Description automatically generated

## Secure Communications

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

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.

A screenshot of a computer

Description automatically generated

## Functional Testing

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

A screenshot of a computer program

Description automatically generated

## Summary

The code was refactored to integrate secure communication mechanisms, specifically converting HTTP to HTTPS, implementing AES encryption, and adding checksum verification using SHA-256. During secondary testing, the Dependency-Check tool was used to ensure no new vulnerabilities were introduced. The refactored code executed successfully without errors, and no additional security issues were detected. Functional testing confirmed that the code maintains its integrity and security, complying with industry standards.

## Industry Standard Best Practices

Throughout the refactoring process, industry-standard best practices were applied to maintain and enhance the software’s security. These practices included using AES for encryption, ensuring secure key management, converting communications to HTTPS, and performing thorough vulnerability assessments using tools like Dependency-Check. By adhering to these standards, Artemis Financial can be assured that its client data and financial information are well protected, minimizing the risk of security breaches and maintaining client trust.