****

# 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 6](#_Toc102040760)

[4. Secure Communications 6](#_Toc102040761)

[5. Secondary Testing 8](#_Toc102040762)

[6. Functional Testing 9](#_Toc102040763)

[7. Summary 9](#_Toc102040764)

[8. Industry Standard Best Practices 10](#_Toc102040765)

[9. Citations 10](#_Toc102040765)

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **12/07/23** | **Alex Crosswhite** |  |

## 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

Alex Crosswhite

## Algorithm Cipher

There are several cipher algorithm options presented through Oracle. After reading about each of the different cipher standards I have determined that the Advanced Encryption Standard (AES) will be best suited to meet the needs of Artemis Financial. The Advanced Encryption Standard is the recommended option from the National Institute of Standards and Technology (NIST). AES encryption with 256 bits is considered to be the most secure cipher available. It is used in government and military software as well as by businesses in highly regulated industries. Due to the sensitivity of the information Artemis Financial utilizes their software will require a high level of encryption for storing, sending, and receiving data.

The Advanced Encryption Standard includes a robust set of defenses for a variety of security attacks. AES can be implemented using 128, 192, and 256 bits. Each variation is more secure than the last, however even the 128 bit version has yet to be cracked and takes fewer rounds to complete than the stronger 256 bit version. AES has particular strengths against brute force attacks, known-plaintext attacks, and related-key attacks. Despite the current protection this method provides, it is important not to become complacent. No security plan is completely secure and as technology continues to develop, more vulnerabilities will continue to be revealed and accessed. It is important to continue to be vigilant for potential vulnerabilities; a breech can come in many forms and may occur at any time.

An asymmetric cipher uses two different keys, a public key and a private key, to encrypt and decrypt data. An asymmetric cipher is more secure than a symmetrical cipher due the nature of the private key. In a symmetrical cipher the same key must be used to encrypt and decrypt data. AES uses a symmetrical cipher which carries the inherent drawbacks of two parties needing share the key. This is of further concern in larger software that shares data with many sources. Each source must share a separate key with the system in order to provide protection even among other users. Vulnerabilities may occur if a key is obtained by an unauthorized party.

Artemis Financial is subject to the laws and regulations of many countries, including the National Institute of Standards and Technology (NIST). AES is the current recommended algorithm cipher to meet the requirements of NIST. Security laws are a relatively new area of legislation that has grown in interest as technology continues to be more and more integrated in daily life. Additional requirements may continue to develop as new laws are created and Artemis Financial will benefit from an agile approach that maintains compliance of these laws and regulations.

An AES cipher is the best choice for Artemis Financial due to the broad range of protection that it is able to offer. AES’s ability to encrypt and decrypt, through the use of hashing, number randomization, and bit levels, while remaining in compliance with laws and regulations meets the requirements for protecting Artemis Financials users, and the business itself. Each layer of hashing, number randomization, and bit levels that are used increases the security of the system.

For as long as there have been written languages there have been people attempting to disguise or hide communications. It comes as no surprise that when machines began to be used for communication encryption developed alongside them. Early famous examples include Morse code and later the enigma machine used in World War II. War has been a strong motivator for secure communication and cyber security is no exception. There is an ever-growing need for secure data storage and communication as cyber-attacks continue to find vulnerabilities. A secure system today could find that severe breaches exist tomorrow. In this way, additional methods of security must continuously be invented to counter the unrelenting attacks from bad actors searching for vulnerabilities.

## Certificate Generation

## A screenshot of a computer screen Description automatically generated

A screenshot of a certificate

Description automatically generated

## Deploy Cipher

A screenshot of a computer

Description automatically generated

## Secure Communications

## I had quite a bit of trouble with this step. I tried many potential solutions in an effort to create a secure connection. I created and tried several self-signed certificates (both JKS and .p12), however the problem appears to be in the certificates inclusion in the browsers Trusted Root Certification Authorities. I added the certificate to the Trusted Root Certification Authorities and I can see it listed, however it still appears as an insecure connection. I attempted this same process in both the Google Chrome and Microsoft Edge browsers to the same effect.

## A screenshot of a computer Description automatically generated

## A screenshot of a computer Description automatically generated

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

A screenshot of a check box

Description automatically generated

## Functional Testing

A screenshot of a computer

Description automatically generated



## Summary

By refactoring the code, we are able to address several areas of security to meet the standards of security necessary for Artemis Financial. APIs, Cryptography, Client\Server, and Code Quality are the parts of the Vulnerability Assessment Process Flow Diagram that I worked to implement.

First, I reconfigured the code to add AES encryption algorithm using a hash function and bit levels. I ensured that the encryption was in by performing a checksum verification. Once encryption was in place, I created a self-signed certificate using the Java Keytool and exported the certificate. Next, I reconfigured the application.properties file to include the correct settings to implement the self-signed certificate I created. The security of the new https protection was then tested by opening a new browser page with the <https://localhost:8443/hash> address. The page is intended to show a secure connection.

After the code had been refactored, I performed an OWASP Dependency-Check Maven to determine that the refactored code did not introduce any new security vulnerabilities. Once the secondary testing was completed, I performed functional testing by manually reviewing the code for proper functionality and any remaining possible vulnerabilities. I used this step to perform a final check for to ensure the code runs without errors.

## Industry Standard Best Practices

The refactored code for Artemis Financial does not have any direct user input when the program is run, however it does interact with APIs. The use of encryption and a certificate helps to protect the data being transferred by scrambling the data, requiring the proper key to decrypt and access the information. Another best practice that I adhered to was coding with the security in mind. Considering the potential vulnerabilities that each line of code may present and being intentional with the code that is written. Manual and automated tests were run to identify vulnerabilities and ensure that the code could be run with the proper functionality.

Further security could be added by updating the dependencies that are shown to be vulnerable through the OWASP Dependency-Check Maven, however that was not a focus for this project.

**Citations:**

Dworkin, M. , Barker, E. , Nechvatal, J. , Foti, J. , Bassham, L. , Roback, E. and Dray, J. (2001), *Advanced Encryption Standard (AES), Federal Inf. Process. Stds. (NIST FIPS)*, National Institute of Standards and Technology, Gaithersburg, MD, [online], <https://doi.org/10.6028/NIST.FIPS.197>

Brush, K., Rosencrance, L., & Cobb, M. (2021, September). *asymmetric cryptography (public key cryptography)*. TechTarget. <https://www.techtarget.com/searchsecurity/definition/asymmetric-cryptography>

Copeland, B. (2023, November 1). Alan Turing. Encyclopedia Britannica. <https://www.britannica.com/biography/Alan-Turing>

Jeganathan, S. (2019, November 1). *DevSecOps A Systemic Approach for Secure Software Development*. SNHU Shapiro. <https://eds-s-ebscohost-com.ezproxy.snhu.edu/eds/pdfviewer/pdfviewer?vid=1&sid=51202e44-2034-4a8d-bb33-d72f6db0aa8b%40redis>