****

# 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** | **10/16/2025** | **Cori-Leigh Diggs** |  |

## 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

Cori-Leigh Diggs

## Algorithm Cipher

After examining Artemis Financials’ needs and their system, the best encryption algorithm cipher for them would be the Advanced Encryption Standard (AES). AES has been referred to as the “gold standard” for encrypting data (Crawford, 2019) because it is an efficient and widely used for securing internet communication. It is used fairly often in everyday cases, through social media or financial transactions, because it is easier to implement compared to similar ciphers. One of the risks to AES is a side channel where hackers can attempt to reverse engineer the cryptography, but they can reduce these attacks by plugging any gaps and using randomization techniques (Awati, 2024).

This cipher would be best to use because it is low-cost, yet it is still very secure and efficient. Using randomization will make it more difficult for any hackers to gain access due to its unpredictability. The early 1970s is when there was some of the first computer-based encryption used when IBM designed a block cipher to protect their clientele data. AES was widely released in 2000s and has been the standard since.

## Certificate Generation

Used as a third-party entity to issue Secure Socket Layer (SSL) certificates that ensure a websites authenticity. It issues a public key to the web browser and an encrypted key is also kept by the user that is using the site and this identifies the user as a certificate holder. This pair allows for a secure communication from user to site and confirms that documents have not been altered by a third party. Certificate Authority is very useful for security measures.

A screen shot of a computer

Description automatically generated

A computer screen shot of a blue screen

Description automatically generated

A computer screen shot of a blue screen

Description automatically generated

## Deploy Cipher

A screenshot of a computer

Description automatically generated

## Secure Communications

Even though I am entering the correct keypass, it is not allowing me to add the certificate.

## Secondary Testing

## Before refactoring code

[Dependency-Check Report\_10-7-2025.html](https://learn.snhu.edu/d2l/le/dropbox/2019659/3747698/DownloadSubmissionFile?fid=223020272&sid=57897318" \t "_blank)

After Refactoring code

[Dependency-Check Report 10\_11\_25.html](https://learn.snhu.edu/d2l/le/dropbox/2019659/3747698/DownloadSubmissionFile?fid=223189603&sid=57959483)

## Functional Testing

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

I am not able to screenshot in eclipse, will attach the document.

## Summary

Once the code is refactored for Artemis Financial, it should have been several featured that would enhance its security and functionality. Most notably, the client/server certificates and RESTful API that were integrated into the project. A REST controller will be added to facilitate the RESTful API, which will operate over the HTTPS- a secure version of the HTTP, which ensures the protection of any transmitted data between the client and the server.

In order to ensure secure communication between the client and the server, a certificate will be generated using the keytool command line program and is integrated into the application through the application.properties file. The certificate will add an extra layer of security by allowing a way to verify and trust the server.

During this refactoring process, there are many features that will be addressed. These features are the API implementation, the cryptography, the client and server security, and the quality of the code. There is also a concentration on the quality of the code, making sure it adheres to the highest standards, and is validated through code review and updated vulnerability reports.

## Industry Standard Best Practices

It is important to conduct regular program testing are essential when trying to ensure an applications security. This can be done by using static testing to identify any potential threats and applying SHA-256 methods to encrypt the data. It is practical to keep up this regular testing to continually uncover any vulnerabilities or weaknesses within the code, and whenever a threat seems to be a false positive it must be suppressed to simplify the process of tracking new and genuine safety threats.

**Reference**

Bernstein, C., Cobb, M., & Awati, R. (2024, February). *What Is the Advanced Encryption Standard (AES)?* SearchSecurity. https://www.techtarget.com/searchsecurity/definition /Advanced-Encryption-Standard

Crawford, D. (2019, February 4). *A Complete Guide to AES Encryption (128-bit & 256-bit) - ProPrivacy.com*. ProPrivacy.com. https://proprivacy.com/guides/aes-encryption