****

# 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** | **6/23/2025** | **Phillip Kimbrel** |  |

## 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

Phillip Kimbrel

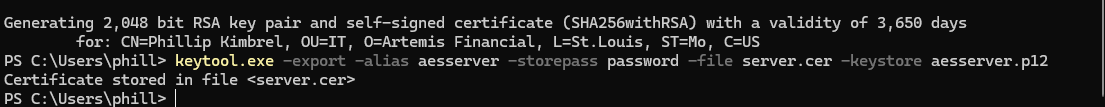
## Algorithm Cipher

For Artemis financial I have decided to use the AES-128 encryption while using SHA 256 for hashing.

The way AES works is that each block cipher in 128 bits and are put into a 4x4 grid array each point having 16 bits and the key size can be one of three different sizes for 128, 192, or 256 bits. The keys length determines the number of rounds of encryption the input will go through. Each round goes through 4 steps: Sub bytes where each byte gets substituted with another; shift rows where the rows of bits are shifted a certain number of times; then mix columns in which this step uses multiplication by multiplying each column with a matrix changing each byte in the column; and then the final step is adding a round key. The way SHA-256 works by hashing the data which converts everything to a set of fixed length string of letters and numbers via a hash function with each function generating a 32-Character hash that is unique to each hash. The AES encryption is a symmetric encryption algorithm as it requires a private key to decrypt the data and keeps data more secure. Unlike asymmetric which has a public key making it weaker as it uses a public key meaning any can decrypt the data and get at it.

## Certificate Generation

Insert a screenshot below of the CER file.



A screenshot of a computer

AI-generated content may be incorrect.

## Deploy Cipher

Insert a screenshot below of the checksum verification.

A screenshot of a computer screen

AI-generated content may be incorrect.

## Secure Communications

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

A screenshot of a computer

AI-generated content may be incorrect.

## Secondary Testing

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

A screenshot of a computer

AI-generated content may be incorrect.

## Functional Testing

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

A screen shot of a computer

AI-generated content may be incorrect.

## Summary

With the new refactored code, we added encryption and encapsulated all the code into one class and add an API element using RESTful API. The encryption added was a combination of AES-128 and SHA-256. This is done to make sure that the data is protected and that it shows that the codes will be different depending on the time activated from the server. Even with one of them decoded they would have to figure out how to get through the second form of encryption. The RESTful API is brought in via printing out the checksum by getting the input data, encrypted data, and the SHA-256 and printing it out on a web page

## Industry Standard Best Practices

The main practice followed here was data protection as was done by combining two cryptographic algorithms making the data stored in the file more protected than it was before with no encryption. Applying industry standards best practices makes sure that not only data gets protected but that they know what sessions are happening; how to handle errors; who has what kind of control in the system; and multi-factor authentication. Following these practices will help the company’s overall well-being by making sure that the money of the customers is being protected as well as protecting the privacy and private information of the customers and clients of Artemis Financial.

**References**

GeeksforGeeks. (2024, July 16). *Advanced Encryption Standard (AES)*. GeeksforGeeks. https://www.geeksforgeeks.org/advanced-encryption-standard-aes/

Codecademy. (2023, April 28). *What Is Hashing, and How Does It Work?* Codecademy Blog. https://www.codecademy.com/resources/blog/what-is-hashing/

GeeksforGeeks. (2024, June 13). *How Does a Secure Hash Algorithm work in Cryptography?* GeeksforGeeks. <https://www.geeksforgeeks.org/computer-networks/how-does-a-secure-hash-algorithm-work-in-cryptography/>

GeeksforGeeks. (2020, January 29). *Difference Between Symmetric and Asymmetric Key Encryption*. GeeksforGeeks. <https://www.geeksforgeeks.org/computer-networks/difference-between-symmetric-and-asymmetric-key-encryption/>

*What are Application Security Frameworks?* (2025, February 19). Wiz.io; Wiz.io. https://www.wiz.io/academy/application-security-frameworks