****

# 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** | **8/14/2023** | **Louis Constante** |  |

## 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

Louis Constante

## Algorithm Cipher

**Recommendation**

The recommended encryption algorithm cipher is 256-bit AES, or advanced encryption standard. This is a strong option that can store Artemis Financials archived data with a high level of security. While the stronger versions of this encryption algorithm cipher will require more computational resources, the increased security provided by the 256-bit version will provide the company and its clients an appropriate amount of security considering the highly sensitive nature of the archived data.

The cipher's hash functions are tools used to ensure data integrity. They serve to generate digital signatures and create password hashes that make it very hard to crack the cipher without the encryption key. The bit level of 256 will cause the algorithm to generate long keys that provide a high level of security at the cost of computational resources. For encrypting operations to be unpredictable, random integers are essential. They are employed to improve security and produce encryption keys. While asymmetric keys provide an additional layer of protection with paired encryption and decryption keys, symmetric keys allow for faster communication. AES is a symmetric encryption algorithm, meaning that it will use the same key for encryption and decryption. This will result in faster secure communications than asymmetric encryption can provide. From simple ciphers to contemporary algorithms, encryption has a long history. Due to flaws, DES was eventually supplanted by AES as a significant symmetric encryption technique (Roback & Dworkin, 1999). Data security in the digital age is ensured through encryption, which is currently evolving to combat new threats like those presented by quantum computing.

## Certificate Generation

Below is a screenshot of the cer file printed in command prompt.

A computer screen with text on it

Description automatically generated

## Deploy Cipher

Insert a screenshot below of the checksum verification.

A screenshot of a computer

Description automatically generated

## Secure Communications

A screenshot of a computer

Description automatically generated

(A screenshot verifying that the self-signed certificate is recognized and applied. The warning that the connection is not secure will be resolved once a third party CA cert is applied.)

## 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 computer program

Description automatically generated

## Functional Testing

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

A screenshot of a computer

Description automatically generated

## Summary

To ensure the security of Artemis Financials’ Restful API, we've implemented several preventative measures. Our implementation of a secure RestController incorporates SSL and CA certificate validation protocols, creating a robust security layer that encrypts and protects all interactions between the server and clients. This guarantees that sensitive data remains confidential and safe from any potential eavesdropping or tampering. By adopting the SHA-256 encryption algorithm, we've further elevated the security standards of our API. Known for its exceptional resistance to attacks, SHA-256 promotes data integrity, drastically reducing the risk of unauthorized access or data manipulation. This ensures that even in the face of evolving cyber threats, our API maintains a robust defense mechanism. Incorporating secure coding practices has been the top priority in our approach. Through access controls, error handling, and sophisticated cryptographic techniques, we've established a line of defense against potential vulnerabilities. These practices solidify the API's resilience, granting users the assurance of a safe and trustworthy financial platform. We have upgraded the OWASP dependency check to its latest iteration, version 8.3.1. This enables us to detect and address the most current vulnerabilities within our dependencies, reinforcing the API's overall level of security. Our approach ensures that Artemis Financials’ Restful API has a protective layer of security measures, providing clients with a trusted platform for their financial operations.

## Industry Standard Best Practices

* Utilize strong 256-bit AES encryption for data security.
* Generate long and secure encryption keys.
* Implement hash functions for data integrity and digital signatures.
* Employ SSL and CA certificate validation for secure server-client communication.
* Adopt SHA-256 for enhanced security and data integrity.
* Incorporate access controls, error handling, and cryptographic techniques.
* Regularly update dependency check to address vulnerabilities.
* Keep plugins and configurations updated for ongoing security against evolving threats.

**References**

Roback, E., & Dworkin, M. (1999). Conference report: First advanced encryption standard (AES) candidate conference, Ventura, CA, August 20-22, 1998. *Journal of Research of the National Institute of Standards and Technology*, *104*(1), 97. https://doi.org/10.6028/jres.104.007