****

# 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** | **10/15/2025** | **Corey Agnew** |  |

## 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

Corey Agnew

## Algorithm Cipher

I am going to write this portion regarding the instruction “Recommend an appropriate encryption algorithm cipher to deploy” but I wanted to address the fact that a cipher suite would be more appropriate here, as the keystore uses RSA, the checksum uses SHA-256, and HTTPS uses AES.

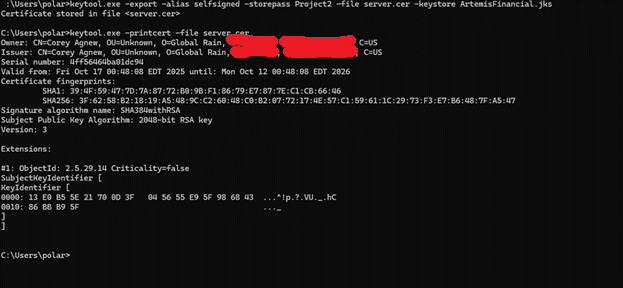
Reviewing Artemis Financials’ security concerns has led me to recommend the Advanced Encryption Standard (AES) as the preferred encryption algorithm. AES is an industry-standard cipher for the protection of sensitive communications between our business and clients. It uses a shared secret to both encrypt and decrypt data, allowing for confidentiality and integrity. AES can also be used to secure the sensitive data that we are holding, in addition to the communication. In this case, AES should be combined with Galois/Counter Mode (GCM) to create AES-GCM to ensure that no two blocks of encryption are the same.

The purpose of AES’s bit levels is to change the level of security. AES supports key lengths of 128, 192, or 256 bits. The larger the number of bits in the key, essentially, the longer the key and the harder it is to brute force it. Hashing is a process that irreversibly transforms data for integrity verification. AES does not support this function, as it provides reversible encryption.

Hashing algorithms such as SHA are frequently used in conjunction with AES. The use of random numbers within AES revolves around a cryptographically secure random number generator that generates the key for the cipher. There are algorithms, such as Cryptographically secure pseudorandom number generators, used with AES to provide random numbers. If a person were to create the key, then the subsequent key, and so on, a pattern may emerge, making the keys easier to guess. AES is a symmetric algorithm, meaning it does not use a key pair; instead, it employs the same key for both encryption and decryption. Asymmetric ciphers such as RSA use a key pair that allows the user with the public key to encrypt a message and only the person with the private key to decrypt the message.

In days past, hiding messages was still a common practice. We have progressed from simple ciphers, which change individual characters in the same repeated pattern, in the Roman age. In the 1500s, a basic cipher was developed using a set keyword for encryption and decryption. In the early 1900s, technology began to take hold of ciphers, leading to the development of machines that used a rotating disc to substitute letters. Building upon this is the famous Enigma cipher, used by the Germans during World War II and considered uncrackable at the time. As years pass, we reach the dawn of the computerized revolution, where encryption is built into software and utilizes complex mathematical formulas. (*A brief history of encryption (and cryptography), 2023).* AES, created in 2001, is now the modern standard for symmetric encryption, while RSA is the asymmetric standard.

## Certificate Generation



A screenshot of a computer code

Description automatically generated

## Deploy Cipher

A screenshot of a computer

Description automatically generated

## Secure Communications A screenshot of a computer Description automatically generated

## Secondary Testing

A close-up of a computer screen

Description automatically generated

A screenshot of a computer

Description automatically generated

## Functional Testing

A screenshot of a computer program

Description automatically generated

## Summary

In accordance with the Vulnerability Assessment Process Flow chart, we built on several security concepts to ensure software security. The program was reviewed to ensure high code quality and to identify any errors or vulnerabilities. This includes implementing the OWASP dependency checker to perform a static check on the code to scan our dependencies for vulnerabilities. Additionally, manual code review was done. Cryptography was also an important part of the refactoring of our code. We switched our process from HTTP to HTTPS, significantly increasing security against potential spies trying to intercept the information passed between us and our clients. I also created a checksum that can then be used to ensure data integrity between us and the user. The API we developed is currently secure, as it only returns static data that we provided. As the endpoint does not currently take user input, it is also secure against overflow attacks. While the current functionality is secure, future improvements could include adding a rate limit to the API to prevent DoS threats.

## Industry Standard Best Practices

In our transformation of the code base into that of a more security-focused one, we used several industry best practices. The first thing we did was encapsulate our data into different files and classes to allow for a more readable code base and to restrict unauthorized access to the other methods. During the implementation of the OWASP dependency check, I updated the version to increase the likelihood that all vulnerabilities within our dependencies would be found. We also used high code quality using comments and clean code. This helps us in the present by enabling us to follow the code easily, which hopefully allows most, if not all, vulnerabilities to be found. This also allows future security scans to work on the code fast and efficiently.

Applying and maintaining industry-standard best practices for secure coding should be a major concern for a company's well-being. There are countless examples of companies suffering security breaches with dire consequences. The most extreme is that some companies have either forced restructuring or a complete shutdown. This year alone, Oracle has suffered massive breaches that expose it to a loss of brand trust, which is very hard to regain, as well as potential lawsuits that could cost millions of dollars. Oracle was the example I used, but a quick Google search shows that breaches, ranging from weak passwords to years-old vulnerabilities not being patched, are all too common.

*A brief history of encryption (and cryptography)*. Thalesgroup.com. (2023, February 1). https://www.thalesgroup.com/en/markets/digital-identity-and-security/magazine/brief-history-encryption

TRIAD, C. (2025, August 21). *The biggest supply chain hack of 2025: 6M records exfiltrated from Oracle Cloud affecting over 140k tenants: CloudSEK*. RSS. https://www.cloudsek.com/blog/the-biggest-supply-chain-hack-of-2025-6m-records-for-sale-exfiltrated-from-oracle-cloud-affecting-over-140k-tenants

*What is Advanced Encryption Standard (AES)?*. Portnox. (n.d.). https://www.portnox.com/cybersecurity-101/what-is-advanced-encryption-standard-aes/

Whittaker, Z. (2025, October 9). *“dozens” of organizations had data stolen in Oracle-linked hacks*. TechCrunch. https://techcrunch.com/2025/10/09/dozens-of-organizations-had-data-stolen-in-oracle-linked-hacks/