****

# 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** | **8/17/2025** | **Alexis Prazak** |  |
| **2.0** | **8/23/2025** | **Alexis Prazak** |  |

## Client



## Developer

Alexis A. Prazak

## Algorithm Cipher

The best hash for Artemis Financial to use is SHA-256. It uses the following amount of bits for key operations:

* Encryption: 96 through 128 bits
* Key Derivation: 128+ bits

This cipher uses random values to prevent attacks, while using symmetric keys for encryption and decryption. These symmetric keys also allow for faster decryption. As computing changes, stricter algorithms are required. Older ciphers, such as MD-5, are at a higher risk of collisions.

## Certificate Generation

A screenshot of a computer

AI-generated content may be incorrect.

**A screenshot of a computer

AI-generated content may be incorrect.**

## Deploy Cipher

Checksum Verification:

A screenshot of a computer

AI-generated content may be incorrect.

## Secondary Testing

Refactored code executed without errors and the dependency-check report:

A screenshot of a computer

AI-generated content may be incorrect.

## Summary

The code for this project has been refactored and complies with security testing protocols.

My first priority when adding security to this code was making sure all dependencies were tested and updated. This was down through the OSWAP dependency check. Then a certificate was created to assist with verifying who is sending data to the user. A trusted certificate can save users from being affected by spoofed sites. Before this code is public the self signed certificate should be replaced by one from a certificate authority.

## Industry Standard Best Practices

It’s common for developers to use libraries like Spring Boot. Using well-tested libraries can help speed up development. Knowing how to incorporate them into a project is essential. Running dependency checks, keeping the libraries up to date, and testing them will keep the application secure. Doing this will require someone to regularly perform these checks. This means the maintenance phase of the software lifecycle will need to

It’s expected that software dealing with sensitive information will use trusted communication verification methods. This includes using trusted certificates and cryptographic libraries. These methods are even required by certain regulations. Not complying with best practices can result in:

* Loss of user trust.
* Legal action from government agencies.
* Attacks on the integrity of the software.

Developers need to keep up with changes in industry standards. As new vulnerabilities are found security needs to be updated.