****

# 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** | **2/20/2024** | **Christopher King** |  |

## 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

Christopher King

## Algorithm Cipher

It is my recommendation that the most appropriate algorithm cypher for Artemis Financial’s needs is Advanced Encryption Standard (AES). The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information (Announcing the advanced encryption standard (AES) 2001). The AES algorithm utilizes cryptic keys of 128, 192, and 256 bit and is used to encrypt and decrypt data blocks of 128 bits. AES is one of the algorithm cyphers that the National Security Agency has approved for US government use.

AES adheres to security protection best practices by providing a high level of protection against security attacks. When using appropriate key lengths, AES ensures confidentiality through strong encryption which in turn makes it resistant to brute force attacks. Risks associated with AES tend to revolve around human error. Risks can be cause by not implementing the AES algorithm properly resulting in vulnerabilities and/or non-working encryption. Another risk involves the keys. The keys are important for encrypting and decrypting the data. Poorly managed keys or compromised key storage can result in unauthorized access. It is important to regularly update keys, and utilizing secure key storage to mitigate risks. Another risk is employee knowledge. There should be regular employee training to ensure that the employees have a strong knowledge of security best practices. With more and more regulations and laws being enacted, it is important to stay updated on any changes made to these regulations and laws. The current government regulations in place will be met with the AES algorithm as it aligns with the specifications and security requirements outlined by National Institute of Standards and Technology (NIST). The AES algorithm will be used for encrypting Artemis Financial’s long -term archives. It will be integrated into the archives system processes allowing for the encryption and decryption of data with ease. The best cipher for Artemis Financial’s needs is AES. AES is the best choice because it has proven security, flexibility to support key sizes of 128, 192, and 256 which allows for some customization based on the current security needs, and it provides fast encryption and decryption. One reason someone might not choose the most secure cipher could be the industry or region may have specific regulatory requirements that dictate the use of a particular encryption algorithm. Another reason could be that the system in question is a legacy system and may not support the latest and most secure algorithms.

AES utilizes cipher’s has functions, such as SHA-256, for integrity verification. This ensure that even if someone gains access to the encrypted data and makes changes, the system will be alerted to potential tampering due to the hash value changing. Bit levels and key sizes in AES correlates with the level of security the algorithm will create. AES utilizes 128, 192, and 256 bits, the greater the bits the higher level of security. Longer keys generally provide stronger security against brute force attacks. Random numbers play a critical role in key generation. The security of the encryption system heavily relies on the unpredictability of the encryption keys. Utilizing a high-quality random number generator helps ensure that the resulting keys are robust and not susceptible to patters that attackers could exploit. AES utilizes symmetric keys which means that the same key is used for both encryption and decryption processes. Utilizing symmetric keys helps reduce computational complexity which allows large amounts of data to be encrypted and decrypted efficiently. AES was established as the encryption standard in 2001 by the National Institute of Standards and Technology. AES was selected to be the successor to the aging Data Encryption Standard. AES was selected based on it’s security, efficiency, and suitability for various applications. Over time AES has become the standard for symmetric encryption globally.

## Certificate Generation

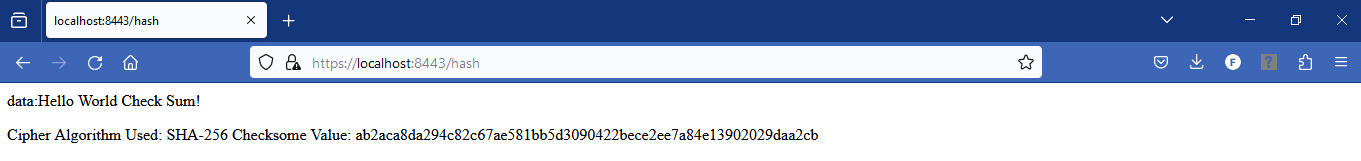
Insert a screenshot below of the CER file.

A computer screen with white text

Description automatically generated

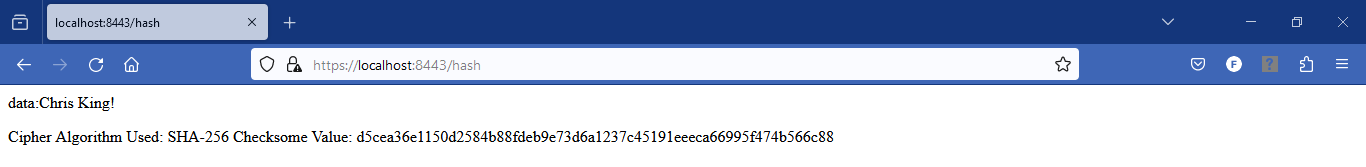
## Deploy Cipher

Insert a screenshot below of the checksum verification.



## Secure Communications

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



## Secondary Testing

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

A screenshot of a computer program

Description automatically generated

A screenshot of a computer

Description automatically generated

## Functional Testing

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

A screenshot of a computer program

Description automatically generated

A screenshot of a computer

Description automatically generated

## Summary

In refactoring the code for Artemis Financial’s software, several security measures were implemented. Throughout the process we conducted a comprehensive code review to identify and rectify potential vulnerabilities. I chose to utilize SHA-256 hashing cipher as it is the best option that has little chances of collisions and is secure. As part of my updates, I generated self-signed certificates using Java Keytool and exported certificates to CER files for verification. The code was refactored to switch from HTTP to HTTPS. With all the updates/changes made we are able to provide increased security by including input validation, strong authentication, and encryption for sensitive financial data.

## Industry Standard Best Practices

While refactoring the code, I followed some key industry standard best practices. I ensured that compliance with OWASP guidelines were followed for secure coding and mitigation of common vulnerabilities. Followed established secure coding standards to ensure code integrity is maintained and aligned with industry standards to reduce susceptibility to exploitation. Application of industry standard best practices enhances the software’s resilience against emerging threats. Enhanced security directly contributes to the overall well-being of the company by safeguarding sensitive data, maintaining customer trust, and avoiding financial and reputational costs associated with security breaches.