****

# 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** | **02/23/2023** | **Kendall Ferebee** |  |

## 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

Kendall Ferebee

## Algorithm Cipher

Upon careful evaluation of encryption algorithms provided by Oracle, I propose that the most suitable encryption algorithm for Artemis Financial's needs is the Advanced Encryption Standard (AES). AES offers flexibility in key sizes, ranging from 128 to 256 bits. For a financial institution handling sensitive data, AES-256, with its 256-bit key, provides an additional layer of security essential for long-term protection (Transition to Advanced Encryption Standard (AES) 2023). This choice ensures the security of both consumers and the company's data. While AES is widely acknowledged for its robust security features, potential drawbacks include challenges related to key management, susceptibility to emerging cryptographic attacks, and concerns regarding quantum computing threats. Moreover, AES can be resource-intensive, potentially slowing down lower-end devices.

AES is commonly utilized in payment systems to encrypt sensitive data, such as credit card numbers (Nagaraj, 2023). Implementing the AES algorithm for encrypting long-term archive files at Artemis Financial can significantly enhance data security. This involves integrating authenticated encryption modes, robust key management, and access controls to ensure confidentiality, integrity, and restricted access. Such integration contributes to a comprehensive strategy that safeguards sensitive financial information from unauthorized access and potential security threats.

While AES is widely regarded as the best cipher due to its proven security, NIST standardization, and widespread adoption, there may be situations where a slightly less secure cipher is preferred due to concerns about computational overhead, potential performance impacts, or interoperability issues with legacy systems.

The hash functions integrated into AES play a critical role in ensuring data integrity by generating unique hashes for each piece of information. This ensures the authenticity of sensitive financial data, detecting any tampering or corruption during transmission or storage. Enforcing a one-way encryption process using hashing further enhances data security, making it practically impossible for unauthorized parties to decrypt passwords in the event of a data breach.

AES's flexibility in key sizes, particularly the option for 256-bit keys, enhances the algorithm's resilience against unauthorized decryption attempts, making it well-suited for long-term protection of valuable information. In terms of key management, the use of random numbers strengthens the security of key generation processes, adding an element of unpredictability.

Considering its historical context and ongoing evaluation to address emerging threats, AES stands out as a widely accepted and implemented standard, endorsed by the National Institute of Standards and Technology (NIST). Its reliability and relevance make it a solid choice for Artemis Financial's data security requirements.

One key factor contributing to AES's widespread acceptance is its ongoing evaluation and refinement to address emerging threats. NIST regularly assesses AES and updates its recommendations based on advancements in cryptographic research and changes in computing capabilities. This continuous evaluation ensures that AES remains resilient against evolving security threats, including advancements in cryptanalysis techniques and the potential emergence of quantum computing.

The endorsement of AES by NIST further solidifies its status as a reliable and trusted encryption standard. NIST is a leading authority in the field of cybersecurity and cryptography, and its endorsement carries significant weight in the industry. Organizations worldwide rely on NIST's guidance and recommendations for implementing secure cryptographic solutions, and AES's endorsement by NIST underscores its reliability, relevance, and suitability for securing sensitive data.

## Certificate Generation

Insert a screenshot below of the CER file.

A screenshot of a computer

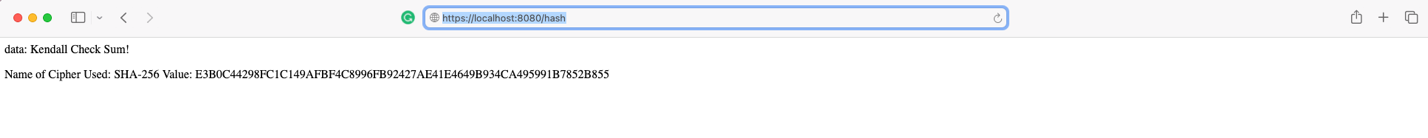
Description automatically generated

A screenshot of a computer

Description automatically generated

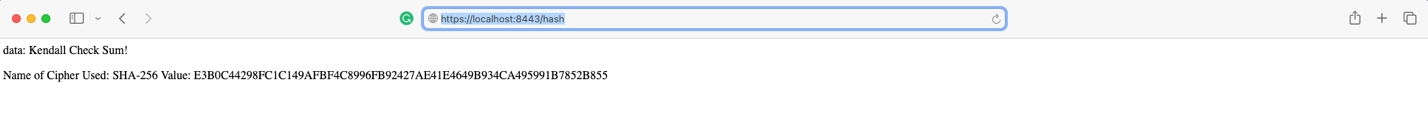
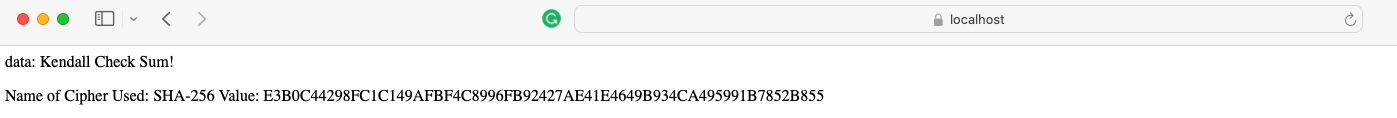
## Deploy Cipher

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 screen shot of a computer

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 screen shot of a computer program

Description automatically generated

A screenshot of a computer

Description automatically generated

## Summary

The refactoring of the sslServiceApplication.java code for Artemis Financial's online application involved a thorough implementation of security measures to align with industry-standard best practices and address vulnerabilities outlined in the Vulnerability Assessment Process Flow Diagram (VAPFD). Firstly, a controller was added to ensure the proper functioning of the program via the designated endpoint (/hash), enhancing control over access points. Additionally, the integration of the SHA-256 hashing algorithm, known for its minimal collisions, fortified cryptographic processes, which is crucial given the sensitive nature of banking data. Transitioning from HTTP to HTTPS protocol significantly bolstered data exchange confidentiality and integrity, a vital step for a financial institution's online platform.

Furthermore, the inclusion of 128-bit AES encryption coupled with self-signed certificates added an extra layer of security, ensuring that only authorized entities could access and decrypt sensitive information. Proactive measures were taken to identify and mitigate vulnerabilities introduced by dependencies through static analysis using tools like OWASP Dependency-Check Maven. This comprehensive approach to dependency management reduces the risk of potential security breaches arising from third-party components.

The refactored code not only prioritizes code quality and adherence to industry best practices but also emphasizes continuous security maintenance. Daily check-ups, including server updates, bug fixes, and dependency checks, are recommended to uphold the application's security over time. By implementing these security measures and adhering to industry standards, the refactored code significantly enhances Artemis Financial's online application's security posture, mitigates known vulnerabilities, and fosters trust with clients. This proactive approach to secure software development not only safeguards sensitive data but also contributes to the company's overall well-being and future success in the ever-evolving landscape of cybersecurity threat.Top of FormBottom of Form

**References**

Cybersecurity and Infrastructure Security Agency (CISA). (2023). *Transition to Advanced Encryption Standard (AES).* Federal Partnership for Interoperable Communications (FPIC).

Nagaraj, K. (2023, March 7). *Advanced encryption standard (AES): A secure and efficient symmetric encryption algorithm*. Medium. https://infosecwriteups.com/advanced-encryption-standard-aes-a-secure-and-efficient-symmetric-encryption-algorithm-319eedb49905

National Institute of Standards and Technology. (2001, November 25). *ADVANCED ENCRYPTION STANDARD (AES).* Federal Information Processing Standards Publications. <https://doi.org/10.6028/NIST.FIPS.197-upd1>

Ortiz, B. (2020, June 16). *Ciphers and Hashes explained*. DEV Community. https://dev.to/somedood/ciphers-and-hashes-explained-3e18