****

# 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** | **6/23/2024** | **Quinlin MacKenzie** |  |

## 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

Quinlin MacKenzie

## Algorithm Cipher

For Artemis Financial, selecting an encryption algorithm cipher involves careful consideration of security, regulatory compliance, and operational efficiency, especially for securing long-term archive files and financial data. Among the Java Security Standard Algorithm Names recommended by Oracle, the Advanced Encryption Standard (AES) emerges as the most suitable choice due to its robust security features, efficiency, and widespread adoption across government and industry sectors.

**Overview of AES:** AES is a symmetric encryption algorithm designed to securely encrypt and decrypt data. It supports key sizes of 128, 192, and 256 bits, which are recommended to resist brute force attacks effectively. AES is known for its computational efficiency in both software and hardware implementations, ensuring minimal impact on system performance when encrypting large volumes of data.

**Hash Functions and Bit Levels:** AES can be complemented with hash functions like SHA-256 to enhance authentication processes. This combination ensures data integrity alongside encryption, further securing sensitive information stored by Artemis Financial.

**Use of Random Numbers, Symmetric vs. Non-symmetric Keys:** AES operates with symmetric keys, where the same key is used for both encryption and decryption. This simplicity in key management facilitates efficient data processing and encryption. Random numbers play a crucial role in AES for generating initialization vectors (IVs), enhancing the security of encrypted data by introducing randomness into the encryption process.

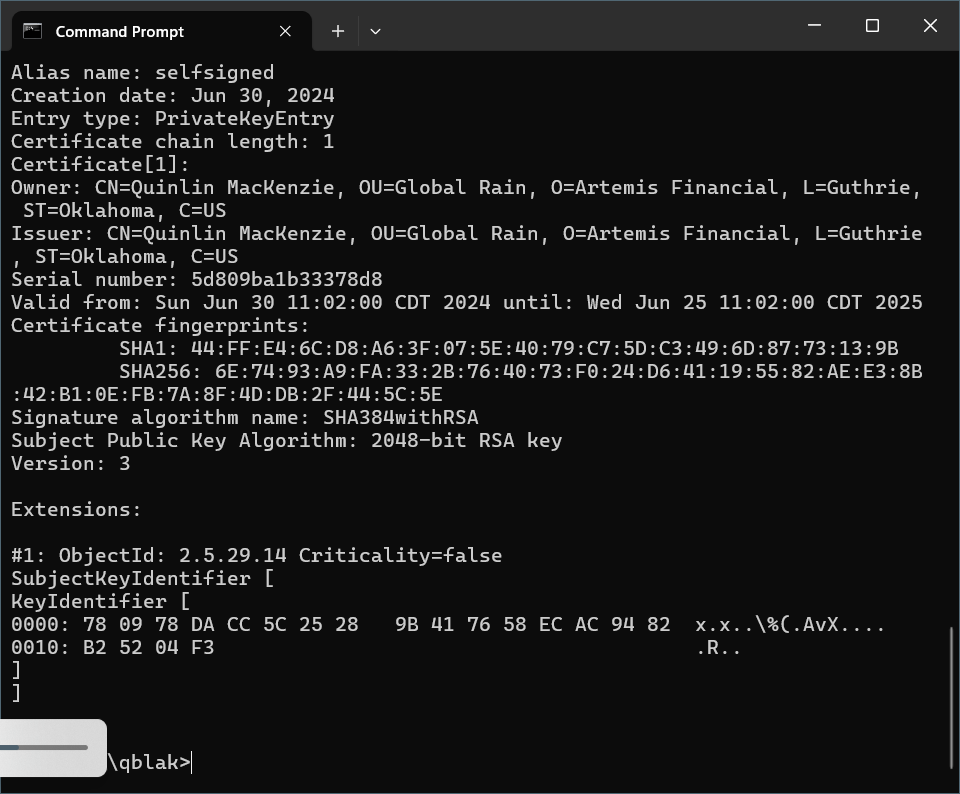
**History and Current State of Encryption Algorithms:** AES was adopted by the U.S. National Institute of Standards and Technology (NIST) in 2001 after a rigorous selection process that included evaluation against various criteria for security and performance. Since then, AES has become the de facto standard for encryption, trusted globally for its reliability and resistance to cryptographic attacks.

**Regulatory Compliance:** AES compliance extends to various regulatory frameworks such as GDPR, HIPAA, and PCI-DSS, ensuring that Artemis Financial meets stringent data protection and privacy requirements. By adhering to these standards, Artemis Financial can mitigate legal risks associated with data breaches and ensure data sovereignty by maintaining control over encryption keys and data storage locations.

In conclusion, AES stands out as an optimal encryption algorithm cipher for Artemis Financial's needs, providing a balance of strong security, regulatory compliance, and operational efficiency essential for safeguarding sensitive financial and archival data over the long term.

## Certificate Generation

Insert a screenshot below of the CER file.



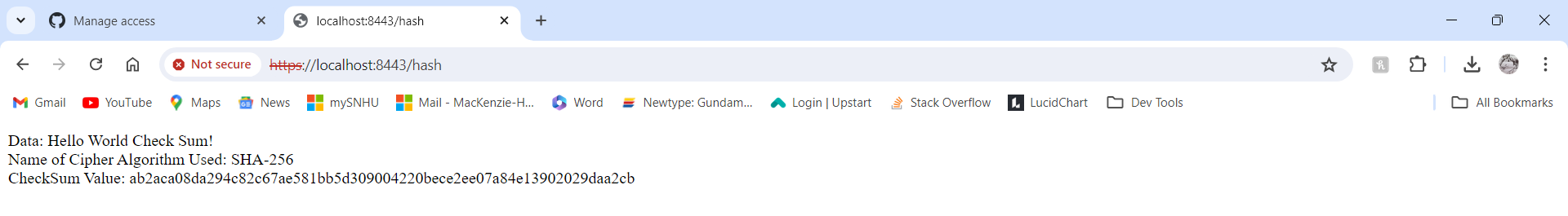
## Deploy Cipher

Insert a screenshot below of the checksum verification.

[Insert screenshots here.]

## Secure Communications

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



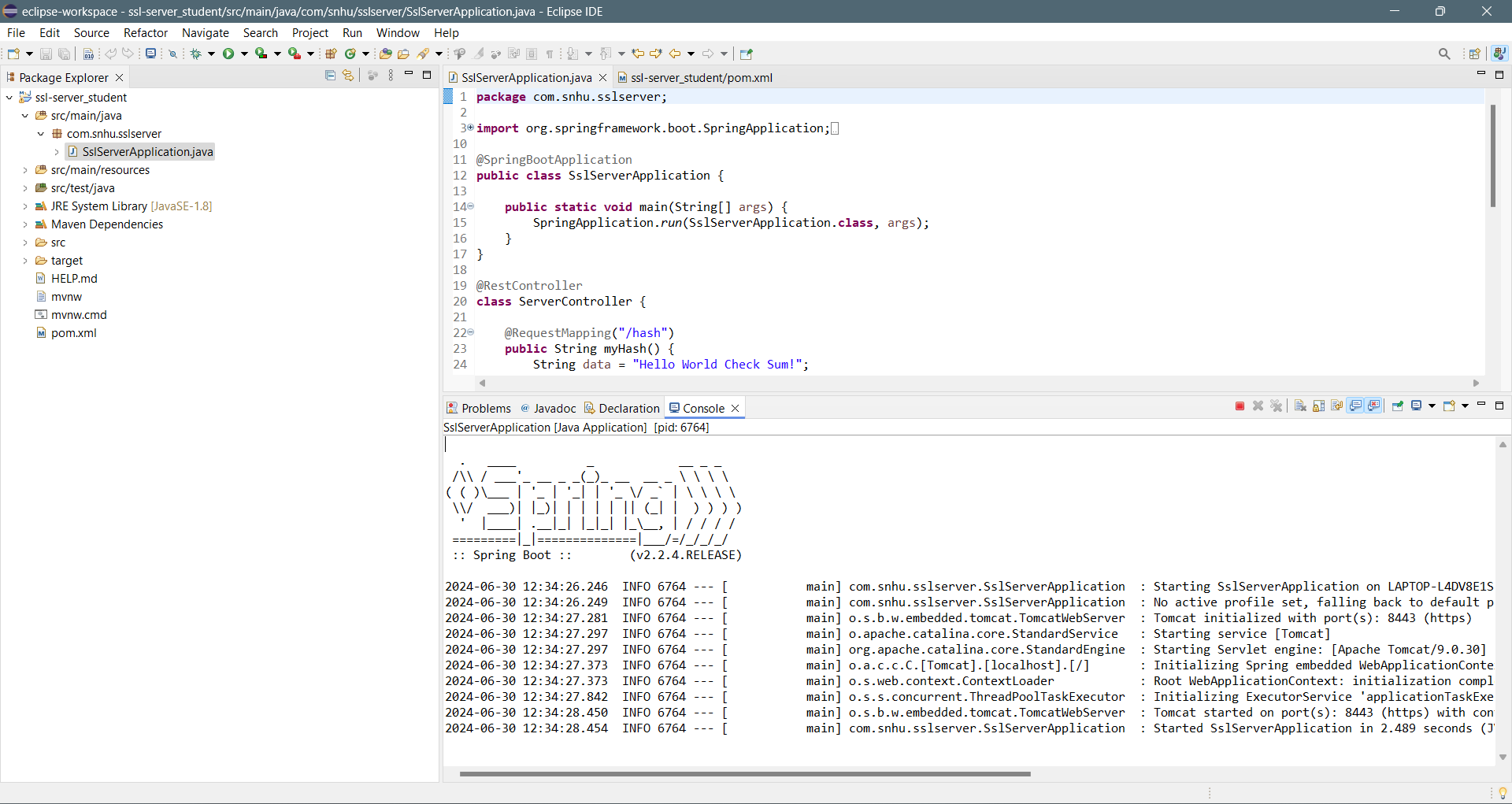
## Secondary Testing

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

[Insert screenshots here.]

## Functional Testing

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



## Summary

The SSL server application was refactored to enhance security and comply with testing protocols. This included configuring HTTPS using an SSL keystore (keystore.jks) to encrypt data in transit, ensuring confidentiality and integrity. Additionally, a SHA-256 cryptographic hash function was integrated to compute checksums, verifying data integrity and guarding against tampering during transmission or storage.

Layers of security were added by implementing HTTPS for encrypted communication and integrating SHA-256 for data integrity checks. These measures bolster the application's defenses against interception and data manipulation risks.

## Industry Standard Best Practices

Industry-standard best practices guided the implementation, emphasizing secure coding techniques and robust cryptographic algorithms. Regular security assessments, including static code analysis and vulnerability scans, ensured early detection and mitigation of potential threats.

Applying secure coding practices like HTTPS implementation and SHA-256 hashing strengthens the application's resilience against cyber threats. It safeguards sensitive data, mitigates risks of breaches, and fosters trust with stakeholders by demonstrating commitment to security and compliance with industry standards. This approach contributes to business continuity and protects the company's reputation, minimizing the impact of security incidents and regulatory penalties.