****

# 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** | **08/07/2023** | **Dominic Drury** | **Initial Documentation** |

## 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

Dominic Drury

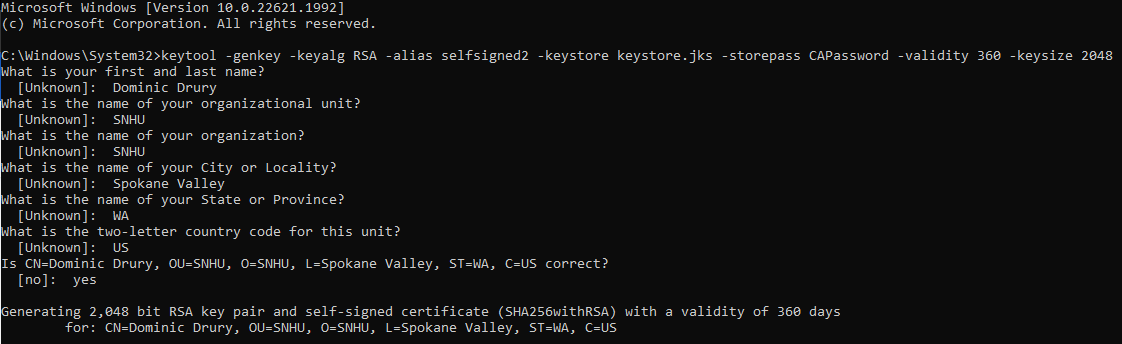
## Algorithm Cipher

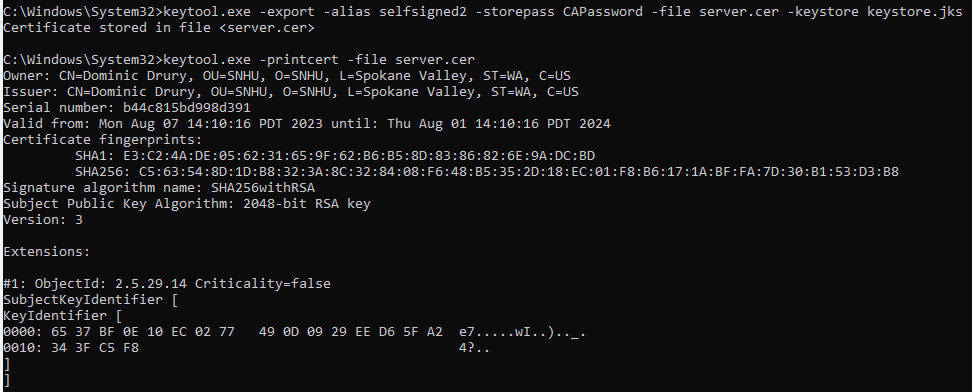
After reviewing Artemis Financials encryption needs regarding encrypting archive files, I suggest the Advanced Encryption Standard 256 bit (Mushtaq, Jamel, Disina, Pindar, Shakir, & Deris, 2017). It is a symmetric algorithm (National Institute of Standards and Technology, 2023) so the data can be encrypted and decrypted easily while remaining secure from unauthorized access. Supporting 256-bit encryption, which has 2256 or over 115 quattuorvigintillion possible combinations for the encryption key, the AES algorithm will protect the data for an extended length of time from attacks that attempt to decrypt the data and other various types of security attacks. AES has the approving authority of the secretary of commerce and its maintenance agency is the Department of Commerce, National Institute of Standards and Technology, and the Information Technology Laboratory (National Institute of Standards and Technology, 2023) so this cipher should meet most of the current government regulations and is in fact allowed by federal departments and agencies for unclassified information.

This cipher was called for by the National Institute of Standards and Technology (NIST) in 1997 because of the increased need for high level security that could operate efficiently (Mushtaq, Jamel, Disina, Pindar, Shakir, & Deris, 2017). Rijndael was selected from the 15 candidates and was developed and employed in 2001 (Mushtaq, Jamel, Disina, Pindar, Shakir, & Deris, 2017). So far as of writing this report the AES-256 has not been cracked. With the sensitivity of the data being stored and the damage any data leak could do both to Artemis Financial and its clientele I would never use anything short of the most secure cipher I could find.

## Certificate Generation

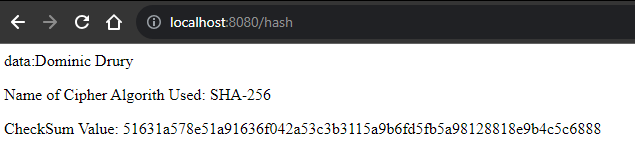
Insert a screenshot below of the CER file.





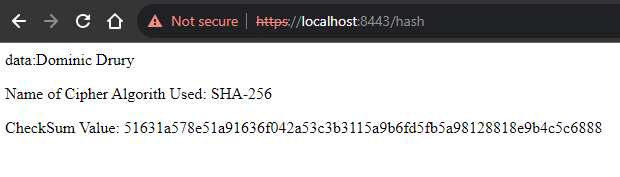
## Deploy Cipher

Insert a screenshot below of the checksum verification.



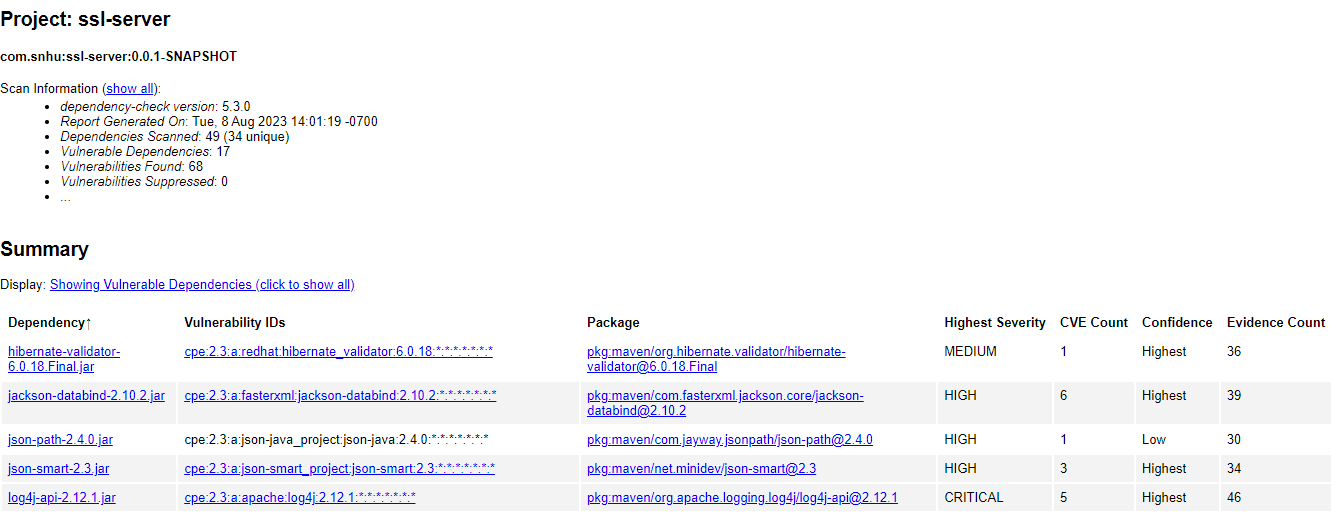
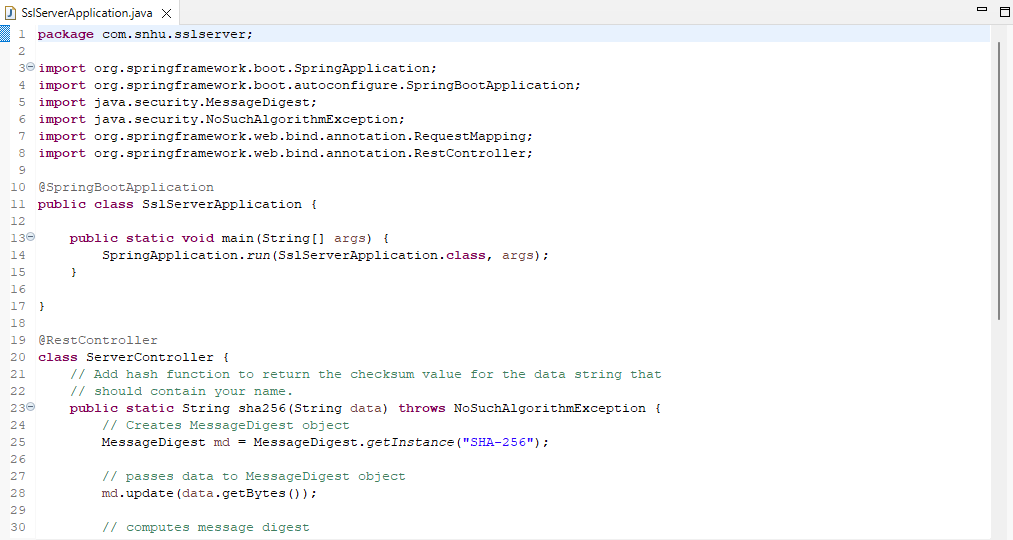
## Secure Communications

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



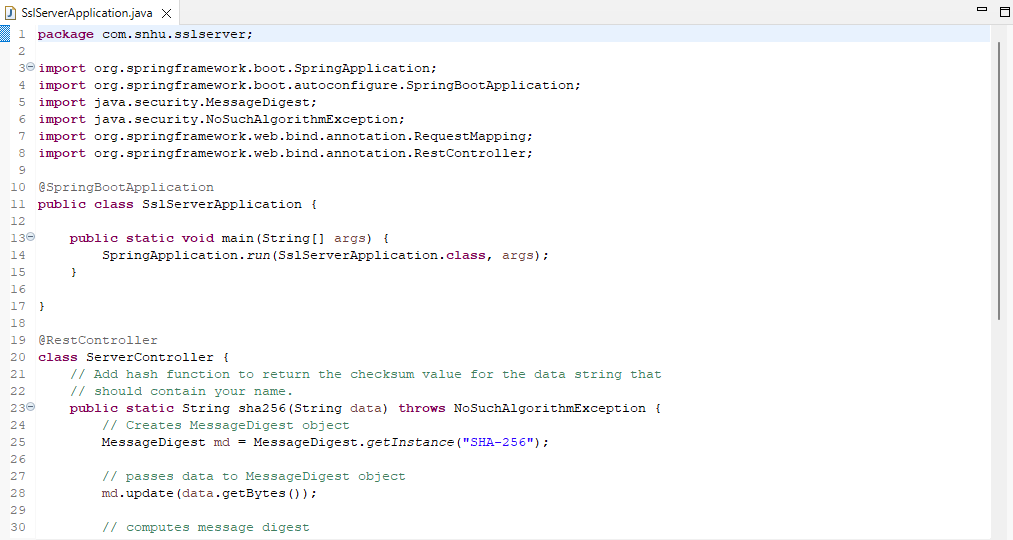
## Secondary Testing

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



## Functional Testing

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





## Summary

Utilizing the Vulnerability Assessment Process Flow Diagram, I refactored the code base to provide Artemis Financial with the proper cryptography necessary for secure communication using a checksum verification with the SHA-256 hash cipher. The size of the cipher along with the minimal size of the AES 256 algorithm (National Institute of Standards and Technology, 2023) provides a high level of security without compromising efficiency. I also converted the HTTP to HTTPS for the added layer of security since the certificate authentication will ensure the data being received has not been tampered with in any way during transport. Finally, I ran a dependency check to verify my added code did not add any new vulnerabilities and did a final manual check of the code for any security concerns.

## Industry Standard Best Practices

In order to maintain best practices for secure coding I made sure to avoid certain known attack methods by doing things like using an appropriately sized cipher to prevent a brute force attack and not passing a string directly through the checksum to avoid an injection attack. I would also recommend the dependency check be ran often to ensure no new vulnerabilities are discovered that need be mitigated, and I would also try to keep all dependencies as up to date as possible to take advantage of patched vulnerabilities. Applying these standards is vital for any business, especially one that handles as sensitive information as a financial institution. These standards help prevent attacks before they happen, keeping client and customer information safe and secure and ensuring continued business.

## References

## Mushtaq, M. F., Jamel, S., Disina, A. H., Pindar, Z. A., Shakir, N. S. A., & Deris, M. M. (2017). A survey on the cryptographic encryption algorithms. International Journal of Advanced Computer Science and Applications, 8(11).

Oracle and/or its affiliates. (n.d.). *Java Security Standard Algorithm Names*. Java security standard algorithm names. <https://docs.oracle.com/javase/9/docs/specs/security/standard-names.html#cipher-algorithm-names>

National Institute of Standards and Technology. (2023, May 9). *Advanced encryption standard (AES)*. CSRC. <https://csrc.nist.gov/pubs/fips/197/final>