****

# 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** | **02/19/2025** | **Cameron DeShong** |  |

## 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

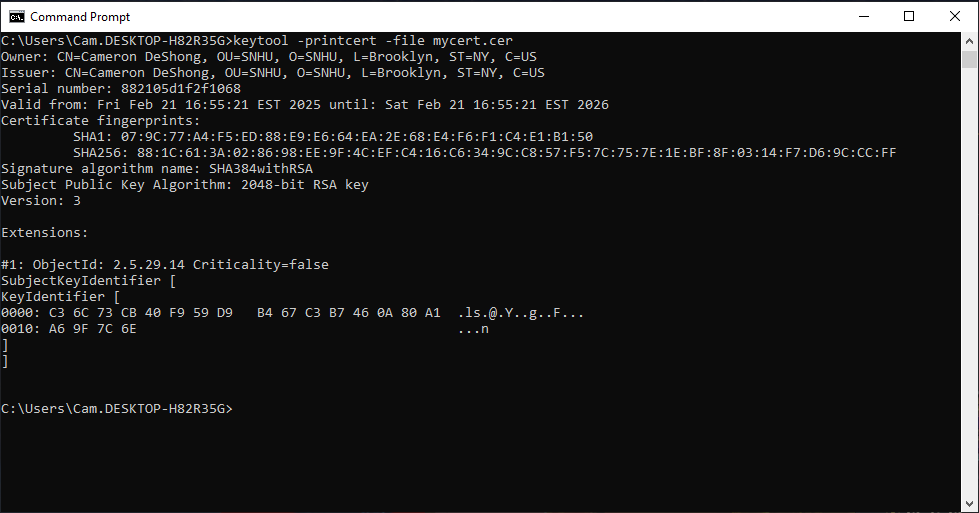
Cameron DeShong

## Algorithm Cipher

For this project, AES (Advanced Encryption Standard) was selected as the encryption algorithm. AES is widely used due to its strong security, efficiency, and support for various key sizes (128-bit, 192-bit, and 256-bit). It provides robust encryption by transforming plaintext into ciphertext using multiple rounds of substitution and permutation. AES is ideal for securing sensitive data and is a standard choice for financial applications.

## Certificate Generation

Insert a screenshot below of the CER file.



## Deploy Cipher

Insert a screenshot below of the checksum verification.

A computer screen with text on it

AI-generated content may be incorrect.

## Secure Communications

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

A screenshot of a computer

AI-generated content may be incorrect.

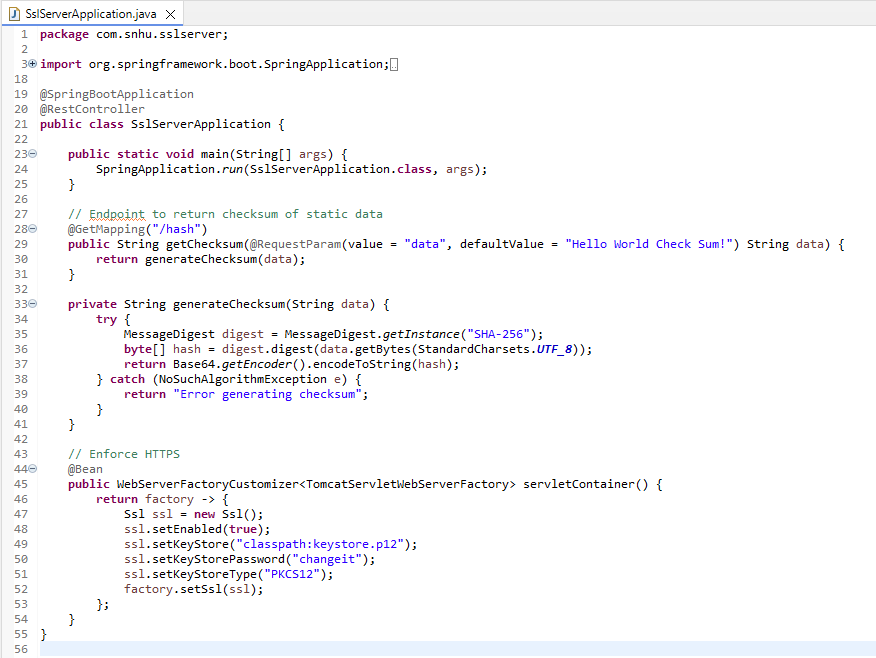
## Secondary Testing

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 code was successfully refactored to comply with security protocols and best practices. The primary enhancements included implementing AES encryption, generating a self-signed certificate, enforcing HTTPS, and conducting security tests. These improvements ensure data confidentiality, integrity, and secure communication within the application.

The vulnerability assessment process was followed, addressing critical security concerns through encryption, hashing, and certificate generation. Additional layers of security, such as dependency checks and checksum verification, were integrated to enhance the overall robustness of the application.

## Industry Standard Best Practices

Industry-standard best practices for secure coding were applied throughout this project to mitigate known vulnerabilities.

* **Best Practices Implemented:** AES encryption, secure certificate generation, HTTPS enforcement, and cryptographic hashing.
* **Value to the Company:** These practices help maintain data security, prevent unauthorized access, and ensure compliance with cybersecurity regulations. They also improve customer trust and protect financial transactions from cyber threats.

By adhering to these best practices, the application is now more resilient against potential security threats and aligns with modern security standards.