****

# 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** | **[Date]** | **[Your Name]** |  |

## 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

Collin Zielinski

## Algorithm Cipher

The recommended algorithm cipher to implement is AES\_256\_SHA384. AES is a symmetric encryption algorithm named Advanced Encryption Standard that is an established standard by the NIST(National Institute of Standards and Technology). It is widely accepted globally and is well known for finding a good balance between security and performance. SHA-384 is part of the SHA-2(Secure Hash Algorithm 2) family, it’s a cryptographic hash function with a 384-bit hash value. AES-256 uses a key length of 256 bits. It provides a higher level of security than the lesser numbers 128 and 192 and is widely used to protect sensitive data. SHA-384 produces a 384-bit hash value. If a hash does not accomplish defeating those attacks, it is useless. It is very resistant to collision attacks and preimage attacks which target hash functions, making it good for data authenticity and integrity.

Random numbers in a cryptographic process are needed for generating keys, initialization vectors, and nonces. Random generation ensures unpredictability and helps with security. AES-256 is symmetric, and a symmetric key is used for both encryption and decryption. It’s fast and needs a secure method for key exchange. Non-symmetric keys use a pair of keys, a public key encryption and a private for decryption. SSL/TLS often start with non-symmetric, and then switch to symmetric for a data transfer to combine security and convenience. Another useful method is using perfect forward secrecy, and ensures that if a key is compromised communications from the past are not compromised.

Modern encryption origins date back to the 1970’s when DES (Data Encryption Standard) began. It was eventually overtaken by the AES due to found vulnerabilities in DES. Over time, many have come and gone with vulnerabilities found and more secure algorithms taking their place. Currently, TLS 1.3, the latest version, has streamlined and strengthened the encryption process by removing many older, less secure algorithms and focusing on a set of better ciphers. This shows how the industry has been improving.

## Certificate Generation

Insert a screenshot below of the CER file.

A close-up of a computer screen

Description automatically generatedA white background with numbers and time

Description automatically generated

## Deploy Cipher

Insert a screenshot below of the checksum verification.

A screenshot of a computer

Description automatically generated

## Secure Communications

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

A screenshot of a computer

Description automatically generated

## Secondary Testing

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

A screenshot of a computer code

Description automatically generatedA screenshot of a computer

Description automatically generatedA white background with blue lines

Description automatically generated

## Functional Testing

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

A screenshot of a computer code

Description automatically generatedA close-up of text

Description automatically generated

## Summary

The code was refactored to address security issues and to ensure it conforms to industry best coding practices. Firstly, Spring boot was used, which is reliable and modular. Making sure that inputs are validated and sanitized is important. Using SHA-256 as a hashing algorithm, all future data used will be protected using this algorithm and will help keep it secure. Spring also maintains the client/server model, which helps with keeping it safe. Code errors were looked at and refactored to make sure there were no errors, and the objective was handled correctly. The code was refactored to be efficient, and the dead code was removed. The data that is holding sensitive data is also encapsulated. Specifically for this code, input sanitization, cryptography, exception handling, and code structure such as using controllers.

## Industry Standard Best Practices

Industry standard practices that we used include following secure coding guidelines, such as the ones in the VAPF, and regularly reviewing and checking on dependency reports and acting on them along with making sure there are no errors contributed to the success of the code.

Applying industry best practices are a must. Code is complex, and the business of code makes it more complex. Using the best up to date methods and practices allows it to be done efficiently within cost and time. From a technical standpoint, standards make sure every developer is on the same page and that their mission has a start and end goal that is reasonable with a path on how to get there. This allows the company to be successful by allowing its employees to function as one while also meeting clients needs so that a profit is possible.