****

# 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** | **2/22/2025** | **Brandon Dolan** |  |

## 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

Brandon Dolan

## Algorithm Cipher

The goal of Artemis Financial is to provide its customers with financial plans and increase the security of their web application. They need high security due to the types of financial services they provide and customer data that can easily be exposed. I would recommend using AES or Advanced Encryption Standard. AES permits key lengths of 128, 192 or 256 bit. Even 128 bit keys are infeasible to break via brute force with current computing (Code, L. 2025). AES is the standard bearer when it comes to encryption and is used for securing such things as internet traffic, stored data, and financial systems. SHA-256 is often the recommended cipher to use due to it having the highest number of bits.

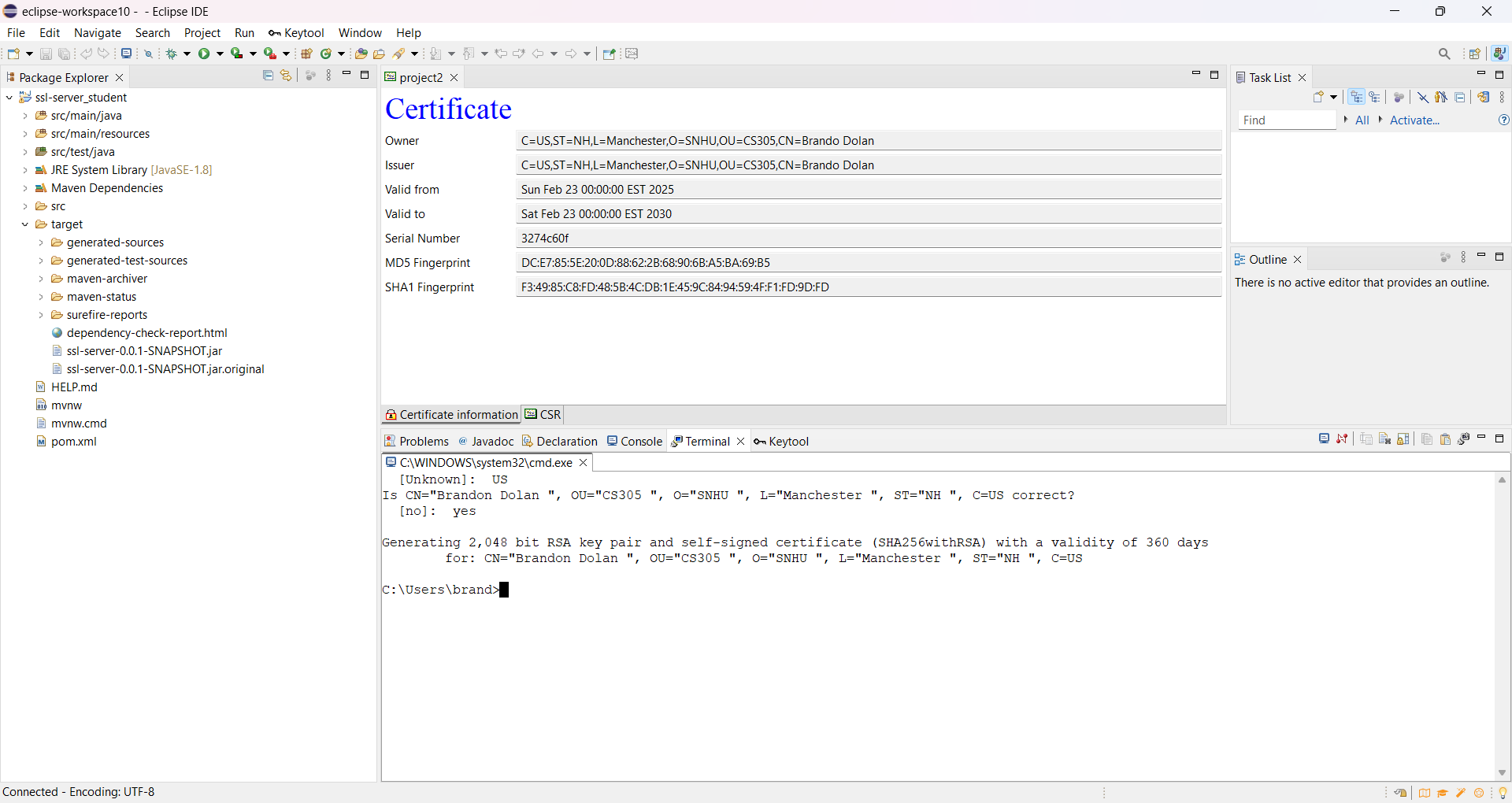
Hash functions are used to provide extra security. They can be used to store values such as passwords. The output, typically a number, is called the hash code or hash value. The main purpose of a hash function is to efficiently map data of arbitrary size to fixed-size values, which are often used as indexes in hash tables. (GeeksforGeeks, 2024). These functions are used to transform a given data set into a bit string of fixed size that is known as a hash value.

Random numbers are used to generate keys and provide extra security. Symmetric encryption uses a single key that is sent by the original user. It provides quicker access and less resource intensive to perform the function. Asymmetric encryption provides more security and uses two separate keys, one public and one private (Crane, C 2021) to encrypt and decrypt data.

Encryption algorithms date back all the way to 600 bc. The Spartans used would send messages out as puzzles during battle for translation. The current standard of encryption known as AES was not founded until the year 2000 to replace DES which had then lasted around 30 years.

## Certificate Generation

Insert a screenshot below the CER file.



A screenshot of a computer

AI-generated content may be incorrect.

## Deploy Cipher

Insert a screenshot below of the checksum verification.

A screenshot of a computer

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.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

## Functional Testing

A screenshot of a computer

AI-generated content may be incorrect.

## Summary

The first part of this project involved creating a certificate to make sure your website goes through a secure protocol. This was used with a 256-bit cypher and filtered through trusted source. Next, I was able to generate a checksum value using the key store. This would eventually use the hash function to confirm that the data had integrity and there were no duplicate keys assigned.

We were then able to take the HTTPS of the port server and use the hash function to eventually retrieve our checksum verification string and check to see if the certificate that was generated through the key store was valid. This would help increase their security protocol and make sure there were no collisions found. Lastly, I was able to run the dependency check to see what vulnerabilities were published and that needed to eventually be addressed by patching and updating the system. This helps Artemis Financial clients have a sound state of mind that their sensitive data is secure.

## Industry Standard Best Practices

The best practice to secure a server is to use SHA-256 especially for the purpose of this project. This also includes HTTPS protocol which allows for a secure connection, identifying which vulnerabilities need to be suppressed to provide extra security, and using a hash function to prevent attackers from exploiting user data. Certificate generation will help provide users with a guarantee that their data is secured through a trustful authority. Updating a package from time to time also goes a long way for protection when it is still supported.

References

Code, L. (2025, January 6). *Encryption Algorithms Explained with Examples*. TheLinuxCode. <https://thelinuxcode.com/encryption-algorithms-explained-with-examples/>

GeeksforGeeks. (2024, May 20). *Hash Functions and Types of Hash functions*. GeeksforGeeks. <https://www.geeksforgeeks.org/hash-functions-and-list-types-of-hash-functions/>

Crane, C. (2021, January 5). *Symmetric vs Asymmetric Encryption: A Guide for Non-Techies*. HackerNoon. <https://hackernoon.com/symmetric-vs-asymmetric-encryption-a-guide-for-non-techies-p03c316t>

*A brief history of encryption (and cryptography)*. (2023, February 1). Thales Group. https://www.thalesgroup.com/en/markets/digital-identity-and-security/magazine/brief-history-encryption