****

# 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** | **4/13/2023** | **Matt Smith** | **Filled out document** |

## 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

Matt Smith

## Algorithm Cipher

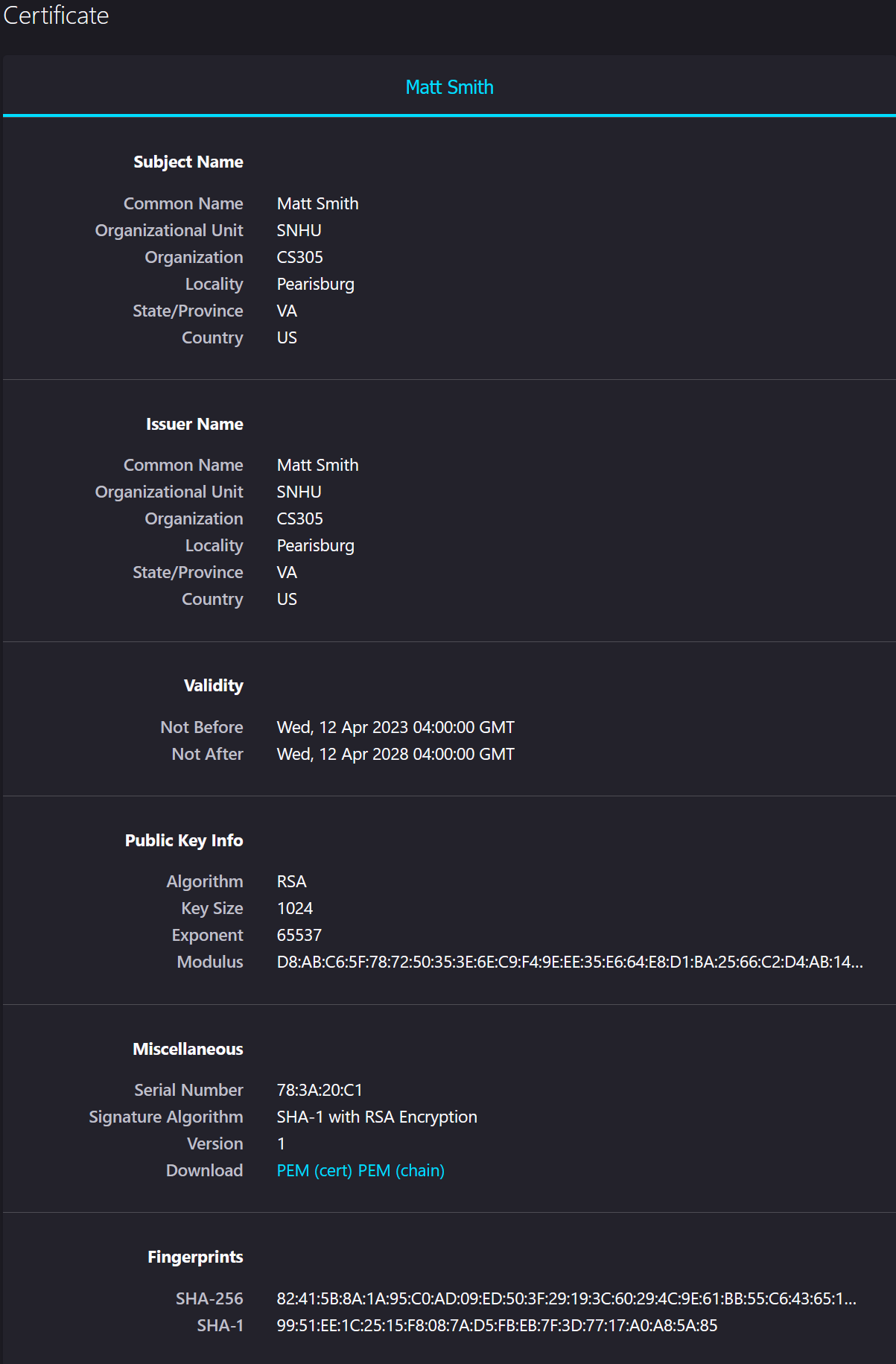
Considering Artemis Financial wants to encrypt their archive files, I would recommend using the American Encryption Standard (AES). AES is one of the most secure encryption algorithms available today. It’s been adopted as a standard by the United States government and is used in many applications worldwide. AES uses symmetric key encryption which means that it uses the same key for encryption and decryption. This makes it fast and efficient compared to other encryption algorithms.

AES uses a hash function to convert plaintext data into an encrypted form, using a specific number of bits. The higher the bit level, the stronger the encryption. The cipher’s purpose is to ensure confidentiality by making the data unreadable to unauthorized users.

AES uses a symmetric key so that means the same key is used for both encryption and decryption. Random numbers are used to generate the encryption key which needs to be kept secret. Non-symmetric keys are used in public-key cryptography where the encryption and decryption keys are different.

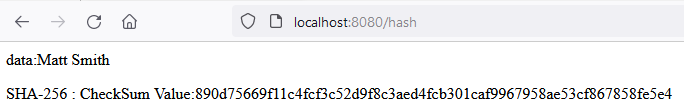
Encryption algorithms have been around since ancient times when secret messages were encoded using simple substitution ciphers. Modern encryption algorithms have evolved a lot over the years, becoming more sophisticated and secure. They also had evolved to keep up with new threats and vulnerabilities. Today, researchers are always looking for ways to improve the security of these algorithms.

## Certificate Generation

Insert a screenshot below of the CER file.

## Deploy Cipher

Insert a screenshot below of the checksum verification.



## Secure Communications

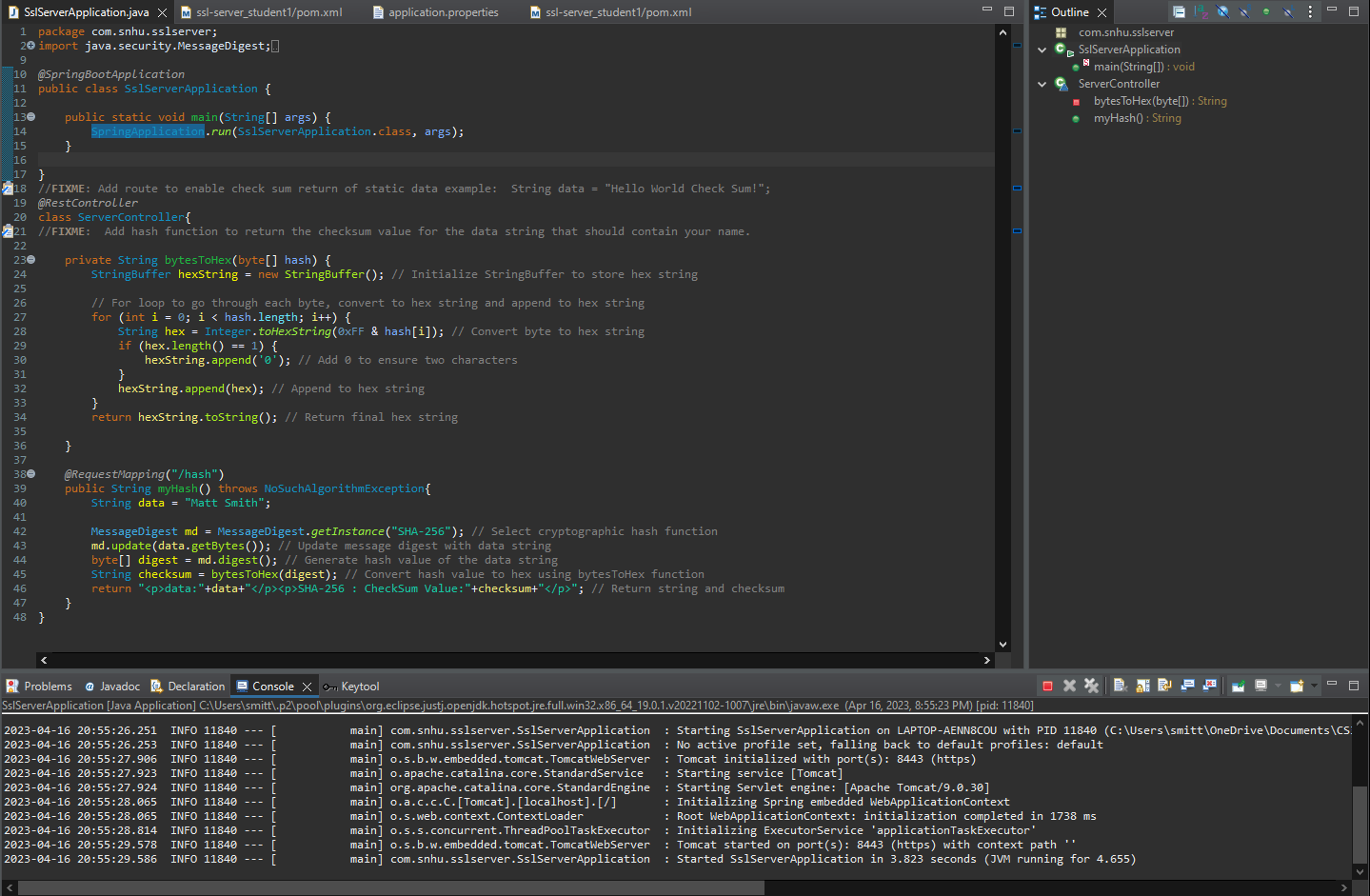
Insert a screenshot below of the web browser that shows a secure webpage.

Graphical user interface, text, application, email

Description automatically generated

## Secondary Testing

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



**Dependency-check before adding code:**Text

Description automatically generated

**Dependency-check after adding code:**

**Text

Description automatically generated**

## Functional Testing

I couldn’t identify any syntactical vulnerabilities with the code.   
  
When it comes to logical vulnerabilities, the bytesToHex function could be improved by checking the input for null values. Another possible logical vulnerability is that the myHash method has a fixed value for the data variable which could be improved by allowing a user to input their own data to be hashed.

For security vulnerabilities, the myHash method doesn’t have any protection against potential attacks like a hash collision. The myHash method is also returning the input data with the checksum value in the same string, which means it’s leaking sensitive information. The code also doesn’t have any authentication or authorization mechanisms to protect against unauthorized access to the myHash method endpoint.

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

A screenshot of a computer

Description automatically generated with medium confidence

## Summary

After referring to the Vulnerability Assessment Process Flow Diagram, the areas of security that I addressed were Cryptography, Input Validation, and Encapsulation.

For cryptography, I used the SHA256 hash function to generate a hash value of the data string. This helps with the integrity and authenticity of the data being transmitted and received.

For input validation, the getBytes method is used to convert the data string to a byte array before hashing. This helps make sure that if there are any special characters that could cause issues are properly encoded and validated.

For encapsulation, the SslServerApplication class handles initializing and running the Spring Boot application. The ServerController class handles the incoming HTTPS requests and generates the checksum.

## Industry Standard Best Practices

I applied industry best practices by using a secure hash algorithm and input validation. I used a SHA256 hash function which is a secure algorithm for generating hash values. This helps prevent unauthorized modification of data. For input validation, the code validates the data before generating the hash value. This helps protect against injection attacks and other vulnerabilities.

By applying industry best practices for secure coding, a company can prevent security breaches that can lead to data loss, financial losses, and damage to the company’s reputation. A company can also build more secure and trustworthy applications that customers can use with confidence. The most valuable part of a company applying industry standard best practices is that it can help them avoid costly fines and legal action.