****

# 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** | **12-10-23** | **Hanna Rawson** |  |

## 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

Hanna Rawson

## Algorithm Cipher

AES combined with SHA-256 as the hash function might be advantageous for Artemis Financial as an algorithm cipher. It has been demonstrated that AES offers strong defense against all kinds of cyberattacks. The fact that this algorithm encryption is used by so many platforms and institutions—including banking systems and political organizations—attests to its effectiveness. AES encrypts and decrypts data using the same (symmetric) key, whereas non-symmetric keys generate a different key for each operation.

The earliest known use of encryption methods dates back to approximately 600 B.C., when the Spartans created the scytale, an encryption tool that allowed troops to transmit messages in secret while engaged in combat using a wooden rod and a leather strap that bore the message's engraving. Going forward in time, a guy by the name of Arthur Scherbius created one of the most well-known encryption tools in 1918. This machine was known as the Enigma, and it used encoded substitution tables that changed every time a new character was input, in addition to rotating disks containing embedded keys.

## Certificate Generation

Insert a screenshot below of the CER file.’

A screenshot of a computer screen

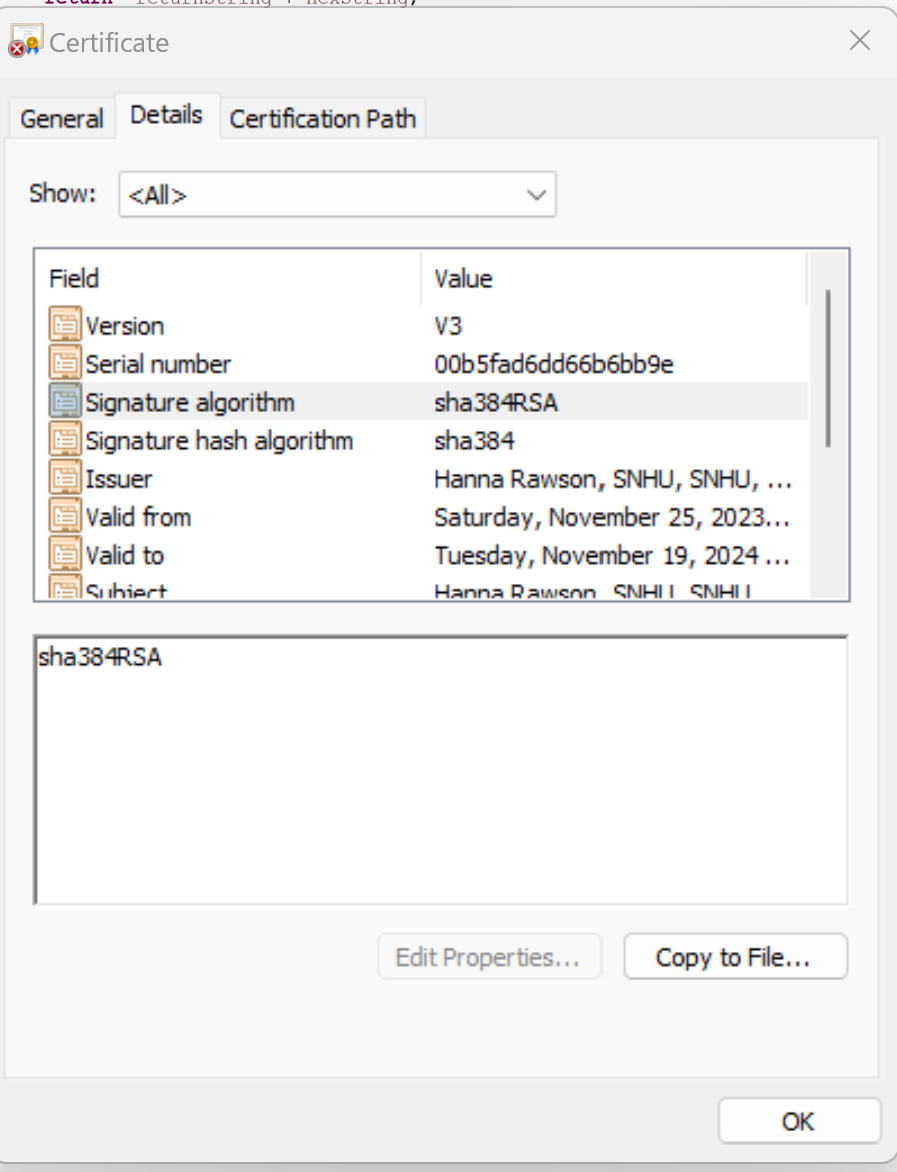
Description automatically generated

A screenshot of a computer screen

Description automatically generated

A computer screen with white text

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 generatedA screenshot of a certificate

Description automatically generated

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

Description automatically generated

A screen shot of a computer code

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

## Functional Testing

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

A screenshot of a computer

Description automatically generated

## Summary

With the code refactoring, I used a hash function to encrypt the data. This strengthened the API's security, particularly because it's a RESTful application. I used a certificate to make sure that data may be shared more securely. Both the client and server's security are enhanced by this. The try and catch clause was used to ensure that the code's integrity would be protected. Keeping the system updated with respect to Tomcat and Spring Boot versions greatly enhanced the application's security and offered protection against any known vulnerabilities. By taking these precautions, Artemis Financial can guarantee that its clients' information is safe on the system.

In the current technical environment, a system's security must be guaranteed. Ensuring the security of your customers' data is the most crucial issue web developers deal with because there are so many possible dangers every day. You can make sure that the system is as secure as possible and that the data is protected from unwanted access by regularly checking the code base, maintaining dependencies, and monitoring the encryption techniques utilized.

## Industry Standard Best Practices

Because security risks are ubiquitous, secure software development best practices are essential. Cyberattacks can impact individuals, organizations, and governments alike in this day and age. Thus, it is imperative to ensure security in software development. According to current theory, safe software development refers to the process of developing software applications that are purposefully planned and carried out with security considerations.

This process should involve integrating different procedures and methodologies to discover and mitigate potential security threats and weaknesses at every level of the software development lifecycle, even if you have access to the best testing toolchains for scanning and analyzing your program. Some steps I’ve taken are secure software coding, code review and testing. Also access control and regular updates and patches would be considered industry standard best practices. For the wellbeing of the overall company, I also think that regular security training is extremely important. It is imperative that developers and other staff members engaged in the software development process undergo periodic security training to guarantee their comprehension of the significance of security and the optimal approaches for safe software development.

Tran, D. (2023, March 31). *Best Practices For Secure Software Development*. Perforce Software. <https://www.perforce.com/blog/sca/best-practices-secure-software-development>

*Top 10 Software Security Best Practices | Synopsys Blog*. (n.d.). Www.synopsys.com. <https://www.synopsys.com/blogs/software-security/top-10-software-security-best-practices.html>

‌