****

# 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** | **12/6/2023** | **Zackery Spears** |  |

## 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

Zackery Spears

## Algorithm Cipher

After reviewing Artemis Financial needs and looking at the list of Java Security Standard Algorithm Names, the best encryption algorithm cipher would be Advanced Encryption Standard (AES). AES was founded in the 21st century by the U.S. government to ensure the encryption of electronic data, as stated on the website GeeksForGeeks(2023). The AES algorithm cipher can encrypt files for Artemis Financial transactions and secure the storage of passwords for users' accounts. Companies may want to avoid ASE because it can be challenging to add to your software. Also, if misconfigured, it can create opportunities for cryptanalysis by attempting "to crack a cipher by studying how it operates using different keys. The related-key attack proved to be a threat only to AES systems" (Bernstein & Cobb, 2021).

AES creates a secure, unreadable value so hackers cannot steal the data. Bit levels are the length of characters that can be stored in a key. For AES, the key size can be 128, 192, and 256 bits of characters. Artemis Financial can benefit from using AES key size since the size of 256-bit is impossible to hack. Symmetric cryptography is used for encryption rather than signing. It uses one secret key for both encrypting and decrypting data. Using these symmetric keys, companies must ensure that the key stays safe to keep everything secure. In comparison, asymmetric cryptography uses two separate keys for encrypting and decrypting data. One is private, and the other one is a public key. (Manico & Detlefsen, 2015). Random numbers are used for keys to ensure hackers cannot crack the code easily.

The history of encryption dates back to the era Before Christ(BC). Most notable is Caesar's cipher, which dates back to 60 B.C. "Julius Caesar invents a cypher that shifts characters by three places in the alphabet: A becomes D, B becomes E, etc."(A brief history of encryption (and cryptography) 2023). This was a simple but impressive encoding method for its time. Computer-based encryption has been around since the early 1970s. During this period, the U.S. government adopted the Data Encryption Standard to secure the data. This was the primary source of securing data until 1997 when it was cracked. In the 2000s, the U.S. government adopted AES as its primary way of securing data, which we still use today (A brief history of encryption (and cryptography) 2023).

## Certificate Generation

## A screenshot of a certificate 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.

Browser issues I was told but it is using https

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 program

Description automatically generated

A white background with text

Description automatically generated

## Functional Testing

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

A screen shot of a computer program

Description automatically generated

## Summary

To begin with, I created a self-signed certificate to allow the project to use HTTPS. To enable the HTTPS, I had to add the SSL keystore to the server. This allows for a more secure web browser for Artemis Financial. To refactor the code, I added a secure RestController to the SSLServerApplication.java file as the Securecontroller for the hash RESTful endpoint. This ServerController class addresses the secure coding concern in the Vulnerability Assessment Diagram and fulfills the requirements. The hash cipher I chose to use for this project is SHA-256. The last stage of development was to make sure the vulnerabilities were patched. I updated the Spring Framework from 2.2.4.RELEASE to 3.0 .0 and Maven Dependency Check version from 5.3.0 to 9.04 in the pom.xml file to ensure the software is updated to the latest version.

## Industry Standard Best Practices

The way to mitigate against known security vulnerabilities and maintain the software application is to ensure that the company applies the industry's best standards. As I explained in the summary, I made the changes to ensure the code is up to those standards by using the most secure cipher hash, SHA-256, which creates an impossible key size that is impossible to hack user input validation. As well as making sure the application uses the most updated software version.

For the company Artemis Financial going forward, they must ensure their software stays secure by maintaining the application properly. They must use error handling, input validation, updated software, the principle of least privilege, and secure data storage transmission. Error handling prevents the leakage of sensitive information. Validating input prevents attacks like SQL injection and command injection. Updating your software prevents the risk of the code from being exploited by any vulnerabilities found in the out-of-date version. The principle of least privilege ensures that the users are given the minimum necessary permission to complete their tasks. This allows no one to access unnecessary parts of the system, preventing information leaks. Secure data storage transmission ensures that the company uses industry-standard encryption algorithms and HTTPS communications protocols.

Applying industry standard best practices for securing code should be crucial, since it shows the consumer who will be actively trusting their banking information with Artemis Financial that they will do everything to protect their information. This will build the company's reputation and give them more users and partners willing to invest in them.

Sources:

GeeksforGeeks. (2023, May 22). Advanced encryption standard (AES). GeeksforGeeks. <https://www.geeksforgeeks.org/advanced-encryption-standard-aes/>

Manico, J., & Detlefsen, A. (2015). Iron-clad java: Building secure web applications. McGraw-Hill Education.

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

Manico, J., & Detlefsen, A. (2015). Iron-clad java: Building secure web applications. McGraw-Hill Education.