****

# 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** | **04/18/23** | **Nick Basile** | **Version 1** |

## 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

Nick Basile

## Algorithm Cipher

**Provide a brief, high-level overview of the encryption algorithm cipher.**

**Discuss the hash functions and bit levels of the cipher.**

**Explain the use of random numbers, symmetric vs non-symmetric keys, and so on.**

**Describe the history and current state of encryption algorithms.**

The encryption algorithm cipher would be AES 256-bit for Artemis Financial. AES 256-bit is one of the most well-known and widely used standards in encryption used today. “The AES algorithm was approved by the NSA for handling top secret information soon after, and the rest of the technology world took notice. AES has since become the industry standard for encryption” (N-able, 2023).

AES is a symmetric key cipher; it uses the same key for both encryption and decryption. Asymmetric key systems use a different key for both the sender and receiver of the data. “Asymmetric keys are best for external file transfers, whereas symmetric keys are better suited to internal encryption (N-able, 2023)”.

Historically ciphers were used in the military as a ways to communicate information more securely. Using tables to convert messages with code words and letters, they could send typically more secure communications to front line troops. Since then, modern day technology requires a much more sophisticated system, but the principle remains the same. AES being the standard that is it today, would require an unreasonable amount of time to brute force the key combinations, “it is exponentially greater than the number of atoms in the observable universe (N-able, 2023)”. This is why it is used worldwide in many different systems.

## Certificate Generation

Graphical user interface, application

Description automatically generated  
Graphical user interface, text, application

Description automatically generated

## Deploy Cipher

Insert a screenshot below of the checksum verification.

Graphical user interface, text, application, email

Description automatically generated

## Secure Communications

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

A screenshot of a computer screen

Description automatically generated with medium confidence

## 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 with medium confidence

Graphical user interface, text, application, email

Description automatically generated

## Functional Testing

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

Graphical user interface, text, application, email

Description automatically generated

## Summary

By refactoring the code, the signed certificate and key generation is used for a more secure 256 bit connection. With the addition of using the HTTPS protocol, which is universally used as a more secure method of displaying secure communication, and verifying the secure connection with the checksum, the connection has been brought up to modern day standards. Verifying this, we can see that the users data will not be easily intercepted or retrievable. The final step was running the OWASP Dependency Check to ensure that there were no security vulnerabilities added.

## Industry Standard Best Practices

This change followed the industry standards for secure communication and will help further improve the facilitation of data between Artemis Financial and its customers. The best practices moving forward are to continue to use industry standards to secure information, and to continue to implement them with new changes to the system. Following these standards is key to keeping the system safe and secure, even for new updates and changes. In addition to this, it should be noted that continuously checking for security vulnerabilities is paramount. While there may not be a known vulnerability, tomorrow a new discovery could lead to a large data breach that could jeopardize the safety of customers’ data.

References

N-able. (2023, January 26). *Advanced encryption standard: Understanding AES 256 - N-able*. N. Retrieved April 21, 2023, from https://www.n-able.com/blog/aes-256-encryption-algorithm