****

# Practices for Secure Software Report

Table of Contents

[Practices for Secure Software Report 1](#_Toc128312051)

[Document Revision History 3](#_Toc128312052)

[Client 3](#_Toc128312053)

[Developer 4](#_Toc128312054)

[1. Algorithm Cipher 4](#_Toc128312055)

[2. Certificate Generation 4](#_Toc128312056)

[3. Deploy Cipher 4](#_Toc128312057)

[4. Secure Communications 5](#_Toc128312058)

[5. Secondary Testing 6](#_Toc128312059)

[6. Functional Testing 6](#_Toc128312060)

[7. Summary 7](#_Toc128312061)

[8. Industry Standard Best Practices 7](#_Toc128312062)

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **2/26/2023** | **Ray Cooke** | **Final** |

## Client



## Developer

Ray Cooke

## Algorithm Cipher

I recommend SHA-256 as an algorithm Cipher for this project. This cipher is an extremely robust algorithm that has been vigorously tested. SHA-256 is among the most widely used algorithm ciphers that are available to use and has been approved by the United States government. 256-bit encryption keys enable a tremendously low chance of being guessed and/or mixed up with another key. These features would empower Artemis Financial to modernize their security practices.

Using random numbers makes an encryption key harder to guess. This results in better security due to attackers having to decipher an enormous number of characters. AES uses symmetric keys, meaning that the same key will lock and unlock data. Non-symmetric keys require two unique keys for locking and unlocking data. While encryption predates Christianity, the use of computer has exponentially assisted us to create increasingly difficult methods for protecting information.

## Certificate Generation

Insert a screenshot below of the CER file.

Table

Description automatically generated

## Deploy Cipher

Text

Description automatically generated

## Secure Communications

Graphical user interface, text, application

Description automatically generated

## Secondary Testing

Graphical user interface, text, application

Description automatically generated

## Functional Testing

Text

Description automatically generated

## Summary

By modifying the application properties file, I have inserted my password key and defined that the server is supposed to deal exclusively in HTTPS. This will close security gaps in the transportation of data and enforce encryption between the server and its users. Employing a hash function with SHA-256 as an algorithm cipher closed security gaps and made the API much harder to exploit.

## Industry Standard Best Practices

It is considered a best practice to keep up to date with dependencies used within a Maven project. The OWASP dependency check is a great method for staying on top of this. Dependencies can be updated in a command line with Maven configured. There Maven commands that automatically update dependencies in a project and update the POM.xml file. Keeping all dependencies up to date and ensuring proper configurations will provide Artemis Financial and their clients more security in how their money is protected, this is an essential step for financial institutions.

References

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