****

# 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** | **12/11/2022** | **Richard Pangelinan** |  |

## 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

Richard Pangelinan

## Algorithm Cipher

Security uses ciphers and keys which can be symmetrical or asymmetrical. The use of the keys is dependent on the legacy of the code you are keeping as symmetrical keys were reserved for use prior to the introduction of asymmetrical keys. The two aim to achieve the same thing, make interactions between servers and clients secure, but the two have different techniques in achieving the same.

The use of symmetrical keys is not as secure as asymmetrical keys and the reason for this is that of how the keys are distributed. Symmetrical keys use one key for encrypting and decrypting the cipher that is used. While you can achieve security as long as the key is protected once the key falls into the wrong hands it becomes a security concern for exploiting both read and write operations.

Asymmetrical keys are more secure because they require two keys; one to encrypt the data and the other to decrypt the data. Once stored into a client the keys are able to shake hands and decide to exchange the data between that client and the server. This allows for a better security infrastructure as it allows for processing to be encapsulated into different security abstractions.

For these reasons I believe that the most reasonable choice for creating an interface for archiving files would be to use asymmetrical keys to develop the security practices in this application. With archiving, comes more files that meet the eligibility of becoming archived with time, so this application must be able to encrypt the data in one server side method and decrypt in the client side.

The best cipher to use for archiving would be RSA as it is has a strong standard set up by its implementation. The use of RSA is widely accepted and the implementation in applications is straightforward.

## Certificate Generation

Text

Description automatically generated

## Deploy Cipher

Graphical user interface, application, Word

Description automatically generated

## Secure Communications

Graphical user interface, application, Word

Description automatically generated

## Secondary Testing

A screenshot of a computer

Description automatically generated with medium confidence

Graphical user interface, text, application

Description automatically generated

## Functional Testing

A screenshot of a computer

Description automatically generated with medium confidence

## Summary

During this project I learned how to configure java projects with Maven. It was hard learning the ins and outs of setting up the projects but I was able to deploy code that I was proud of. The use of security in applications is very important and learning the procedures for deploying secure apps was a good experience.

## Industry Standard Best Practices

In this project I used the best practices of the industry to develop checksum generators and improve my static testing through open source software.