****

# Practices for Secure Software Report

Table of Contents

[Practices for Secure Software Report 1](#_Toc128329062)

[Document Revision History 3](#_Toc128329063)

[Client 3](#_Toc128329064)

[Developer 4](#_Toc128329065)

[1. Algorithm Cipher 4](#_Toc128329066)

[2. Certificate Generation 4](#_Toc128329067)

[4](#_Toc128329068)

[3. Deploy Cipher 5](#_Toc128329069)

[4. Secure Communications 5](#_Toc128329070)

[5. Secondary Testing 5](#_Toc128329071)

[6](#_Toc128329072)

[6. Functional Testing 6](#_Toc128329073)

[7. Summary 6](#_Toc128329074)

[8. Industry Standard Best Practices 6](#_Toc128329075)

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **2-25-23** | **Chris McLernon** |  |

## Client



## Developer

Chris McLernon

## Algorithm Cipher

Encryption algorithms use mathematical processes to convert plaintext into ciphertext to safeguard sensitive data and restrict access to authorized parties. These algorithms have a long history that dates to ancient ciphers and has since evolved to modern-day algorithms such as AES, RSA, and SHA-256. As technology advances, encryption algorithms continue to become more complex and sophisticated to counteract cyberattacks and protect data privacy and security.

Hash functions, like SHA-256, generate a fixed-size output known as a digest from an input message, serving as a digital fingerprint to ensure message authenticity and integrity. Random numbers are an essential component of cryptographic algorithms, generating keys and other parameters to make it challenging for attackers to break the encryption. Symmetric encryption algorithms, like AES, use one key for both encryption and decryption, while asymmetric encryption algorithms, like RSA, use two keys for encryption and decryption.

Encryption algorithms are widely used in secure communications, e-commerce, and online banking to protect sensitive data from unauthorized access. However, vulnerabilities can arise from weak algorithms or compromised keys, making it crucial for encryption algorithms to continue evolving to address new security threats and computing advances. Ultimately, the effectiveness of encryption algorithms depends on their ability to adapt to the changing threat landscape and protect data privacy and security in a rapidly changing digital world.

## Certificate Generation

## A computer screen capture Description automatically generated with medium confidence

## 

## Deploy Cipher

Graphical user interface, text, application, email

Description automatically generated

## Secure Communications

Graphical user interface, application

Description automatically generated

## Secondary Testing

## Graphical user interface, text, application Description automatically generated

## Functional Testing

## Summary

Adding a checksum hash involves calculating a unique value from a file's content and using it to verify the integrity of the file. In the context of a server running on HTTPS, the checksum hash can be used to ensure that the data being transmitted has not been modified during transmission.

To enable HTTPS on a Spring Boot server, a keystore file in PKCS12 format containing a self-signed certificate can be used. The keystore file can be generated using the Java keytool utility, and the self-signed certificate can be signed using the SHA-256 hash algorithm. Once the keystore file is generated, it can be configured in the Spring Boot application's properties file to enable HTTPS. By using a checksum hash and a self-signed certificate with SHA-256, the server can ensure the integrity and security of the data being transmitted over HTTPS. Furthermore, I included a /hash GET endpoint to allow for the retrieval of the checksum hash code.

## Industry Standard Best Practices

I applied industry standard best practices for secure coding in developing the software app to prevent known security vulnerabilities. Applying industry standard best practices for secure coding is crucial for the company's overall well-being. It protects sensitive data, prevents costly data breaches, ensures compliance with industry regulations and standards, and builds trust with customers and stakeholders.