****

# 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** | **Oct/18/2024** | **Jacob Adams** |  |

## Client



## Developer

Jacob Adams

## Algorithm Cipher

I selected the AES (Advanced Encryption Standard) algorithm for its robust security and efficient performance. I opted for the AES-256-bit encryption to ensure a high level of encryption for protecting sensitive data. AES is well-suited for secure data transmission due to its speed and resistance to attacks.

## Certificate Generation

To secure our communications, I generated a certificate using Java Keytool. This certificate is crucial for establishing secure connections and ensuring data integrity

A screenshot of a desktop

Description automatically generated

## Deploy Cipher

I deployed the encryption algorithm within our application, ensuring seamless integration. I verified the deployment through checksum verification to confirm file integrity.

## Secure Communications

I configured the server to use HTTPS, employing the generated certificate to encrypt data in transit. This setup guarantees secure communication between clients and the server.

## Secondary Testing

To ensure everything functions smoothly, I conducted thorough testing. This included running the refactored code and checking for any dependency issues.

## Functional Testing

I conducted thorough functional testing to verify both the performance and security of the application. My goal was to ensure every feature operates smoothly and securely.

* Steps I followed:
* Tested each feature individually to confirm everything works as expected.
* Ran performance tests to check speed and responsiveness.
* Double-checked security measures to make sure data is well- protected.

## Summary

This project successfully integrates strong encryption and secure communication practices, enhancing the application’s reliability and user trust. By implementing AES encryption and HTTPS, I have ensured that sensitive data remains protected throughout its lifecycle.

## Industry Standard Best Practices

I ensured our project aligns with industry standards, such as NIST guidelines. Sticking to these practices is crucial for maintaining high security and performance.

* Steps I took:

1. Reviewed NIST guidelines relevant to encryption and data security
2. Implemented recommended security measures, such as regular updates and monitoring.
3. Conducted compliance checks to ensure adherence to standards.

By following these best practices, I am confident that our applications remain secure and reliable even as security needs evolve.