****

# Practices for Secure Software Report

Table of Contents

[Practices for Secure Software Report 1](#_Toc196074880)

[Client 4](#_Toc196074881)

[Instructions 4](#_Toc196074882)

[Developer 5](#_Toc196074883)

[1. Algorithm Cipher 5](#_Toc196074884)

[2. Certificate Generation 6](#_Toc196074885)

[3. Deploy Cipher 7](#_Toc196074886)

[4. Secure Communications 7](#_Toc196074887)

[5. Secondary Testing 8](#_Toc196074888)

[6. Functional Testing 9](#_Toc196074889)

[7. Summary 10](#_Toc196074890)

[8. Industry Standard Best Practices 10](#_Toc196074891)

**Document Revision History**

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **April 13, 2025** | **Carmen Mitchum** | **Review requirements and necessary information** |
| **1.1** | **April 14, 2025** | **Carmen Mitchum** | **Wrote and reviewed Section 1: Algorithm Cipher** |
| **1.2** | **April 15, 2025** | **Carmen Mitchum** | **Configured and ran Certificate data for Section 2: Algorithm Cipher** |
| **1.3** | **April 16, 2025** | **Carmen Mitchum** | **Rewrote the hash code to implement Section 3 of the deploy cipher.** |
| **1.4** | **April 19, 2025** | **Carmen Mitchum** | **Supplied proof that the deployed cipher from section 3 meets Section 4’s HTTPS requirement** |
| **1.5** | **April 19, 2025** | **Carmen Mitchum** | **Applied Secondary Testing with cipher deployment in Section 5.** |
| **1.6** | **April 20, 2025** | **Carmen Mitchum** | **Section 6 provides proof that a suppression list of false positives was implemented.** |
| **1.7** | **April 20, 2025** | **Carmen Mitchum** | **Wrote and reviewed the summary in Section 7** |
| **1.8** | **April 20, 2025** | **Carmen Mitchum** | **Provided a description best practices throughout the implementation of this project, within Section 8.** |
| **2.0** | **April 20, 2025** | **Carmen Mitchum** | **Reviewed and edited the entire edition.** |

## 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

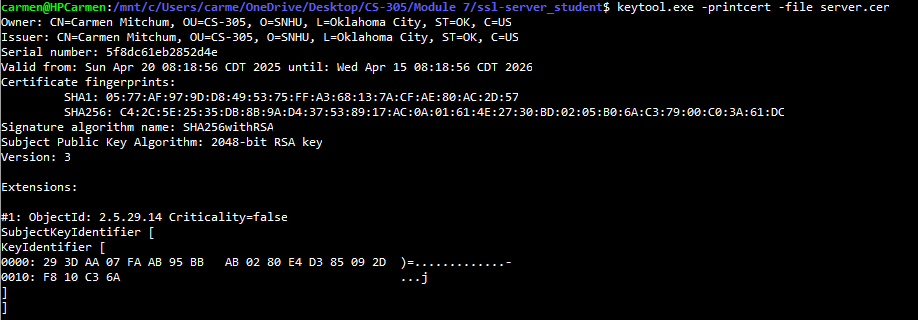
Carmen Mitchum

## Algorithm Cipher

Implementing the Advanced Encryption Standard (AES) as the primary encryption algorithm for Global Rain is an ideal choice to meet the company’s security requirements while delivering efficient and secure products to its customers. AES supports key sizes of 128, 192, and 256 bits, each offering a different level of encryption strength, and operates on 128-bit data blocks. AES-256 is the most secure option, though it may require more memory and slightly impact performance. However, its layered encryption approach provides robust protection against unauthorized access.

Given that Global Rain works with both governmental and non-governmental clients, AES is especially well-suited, as it is an encryption standard authorized for use across both sectors. This enables the product to meet strict security rules while still working well for different types of clients.

## Certificate Generation



A screenshot of a certificate

AI-generated content may be incorrect.

## Deploy Cipher

A close up of a number

AI-generated content may be incorrect.

## Secure Communications

A screenshot of a computer

AI-generated content may be incorrect.

## Secondary Testing

A screenshot of a computer screen

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

## Functional Testing

A screenshot of a computer

AI-generated content may be incorrect.

## Summary

This product plan outlines the key security features implemented to enhance the overall quality of the application. This revised edition includes evidence of encryption, signature verification, and vulnerability assessment. It details the creation of an encryption hash for outbound data, the use of a certificate signature for secure decryption, and a dependency-check report to identify potential vulnerabilities in third-party components. For Global Rain, this report demonstrates the comprehensive application of advanced security protocols to help strengthen and safeguard the company’s products.

## Industry Standard Best Practices

The role of a software developer is often accompanied by the assumption that technical expertise extends to securing applications and protecting sensitive data. While this expectation seems reasonable, the ability to design and deploy functional software doesn’t always equate to a comprehensive understanding of cybersecurity. In today’s technology-driven landscape, developers are increasingly expected to go beyond functionality and ensure their applications are built with strong security foundations.

As the development process becomes more complex, so do the threats targeting modern applications. Issues like data interception, unauthorized access, and manipulation remain common, highlighting the importance of using established best practices to safeguard sensitive information. A well-rounded developer must now consider security as a core component of the development lifecycle.

This report demonstrates the integration of several essential security strategies. It includes examples of how encryption helps protect data, how digital certificates are used to validate authenticity and ownership, and how dependency-check tools can identify potential vulnerabilities in a software project. These implementations support the creation of secure, reliable applications that align with industry standards and build user trust.