****

# 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** | **2/15/2023** | **Matthew Ellsworth** |  |

## 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.

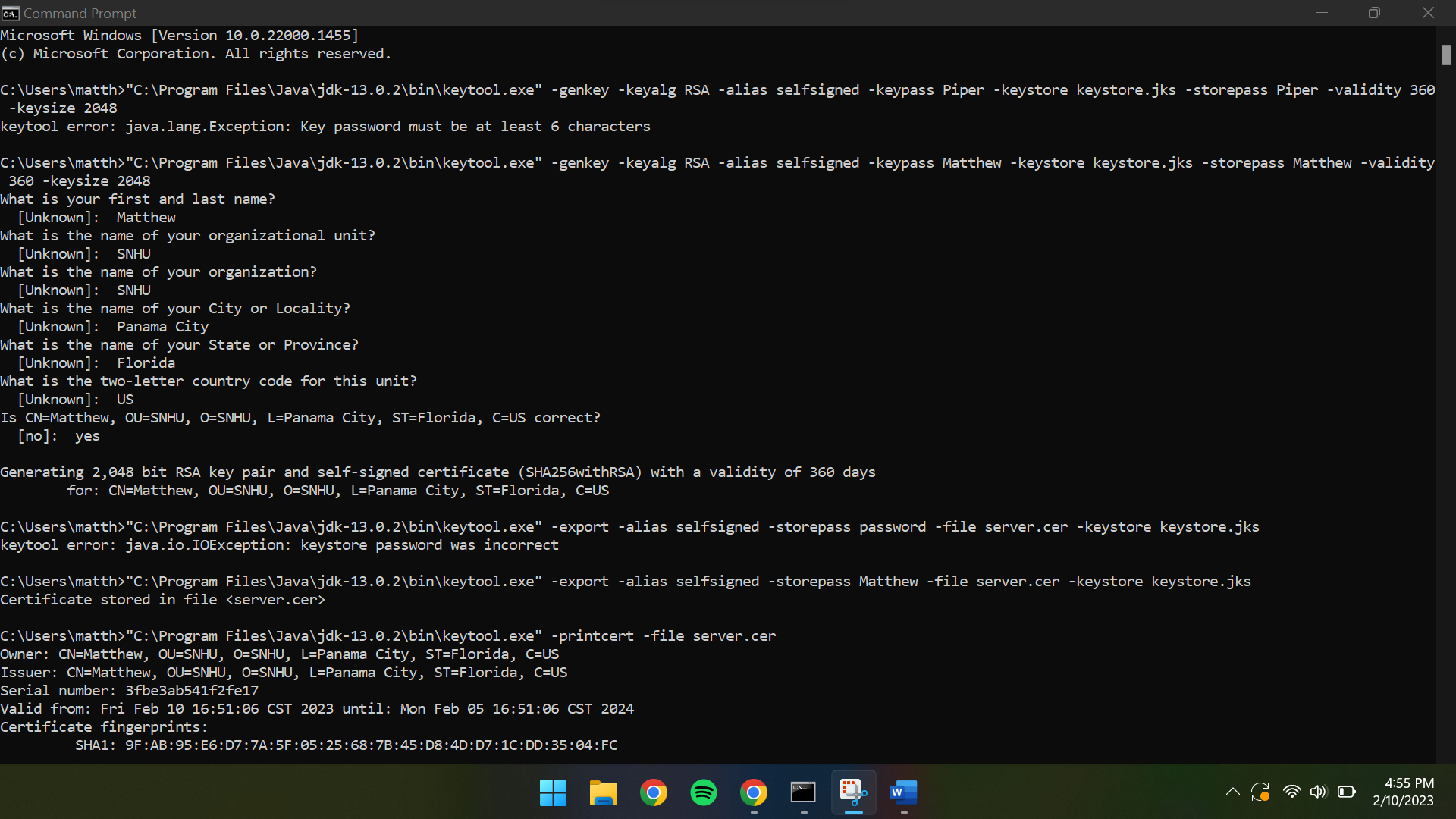
## Developer

Matthew Ellsworth

## Algorithm Cipher

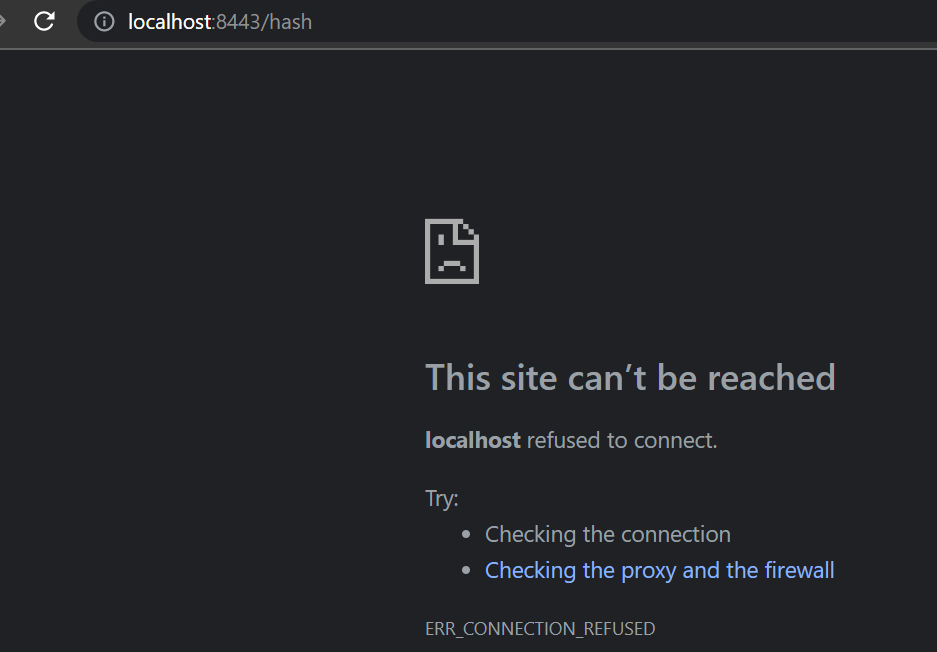
I personally think that the AES or advanced encryption standard algorithm is the best suited for security. This is one that the government and other high level organization use. It is good against brute force attacks and can handle anybody trying to make their way to users information very fast. The focus of hash functions allow for there to be hidden text that people cannot see unless they have the key to read a cypher. Turning text into random numbers are the way that we can transmit data without people being able to see the information in a very easy manner and read it. The symmetry and asymmetry can hide information and make it hard for hackers to read the data if they were able to get their hands on the information. Encryption algorithms are going to keep growing forever and they will forever grow as our knowledge grows and hacker’s knowledge grow.

## Certificate Generation



## Deploy Cipher

## Secure Communications



Firewall is in the way.

## Secondary Testing

A picture containing text

Description automatically generated

## Functional Testing

Graphical user interface, text, application, email

Description automatically generated

## Summary

In conclusion there was a process needed for the algorithm to have a hash and a hidden site that firewalls like to block access to. There were some vulnerabilities found that are able to be handled and managed to make the access harder for people and make it more stable.

## Industry Standard Best Practices

I used the industry practices I learned to install and run the maven download to check for dependencies, added a command site on a prompt to check that the server is brought up and also can suppress an of the dependencies that were found in the pom.xml file. It is important to use standard practice because of many reasons I personally see that using industry practices can be used as a lab for us to be able to check and copy what the person before had done.