****

# Practices for Secure Software Report

Table of Contents

[Practices for Secure Software Report 1](#_Toc132569828)

[Document Revision History 3](#_Toc132569829)

[Client 3](#_Toc132569830)

[Developer 4](#_Toc132569831)

[1. Algorithm Cipher 4](#_Toc132569832)

[2. Certificate Generation 5](#_Toc132569833)

[3. Deploy Cipher 7](#_Toc132569834)

[4. Secure Communications 8](#_Toc132569835)

[5. Secondary Testing 10](#_Toc132569836)

[6. Functional Testing 11](#_Toc132569837)

[7. Summary 11](#_Toc132569838)

[8. Industry Standard Best Practices 12](#_Toc132569839)

[9. References 13](#_Toc132569840)

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **04/16/2023** | **David Novosad** | **First Release Reviewed** |

## Client



## Developer

David Novosad

## Algorithm Cipher

As in the previous communication with Artemis Financial, I recommend using hash algorithm SHA-256. The name stands for Secure Hash Algorithm 256-bit. This algorithm is not small or large enough to cause slow speeds or a higher chance of collision. The general rule for the latter is the larger the number (256-bits), the lower chance of two unique hash values being the same. It is part of the SHA 2 family which are successors of the SHA 1 family. The SHA 1 was losing security and strength against brute force attacks and therefore the second family was created as it had more options for hash values and is more secure. This also means that SHA 1 has a higher chance of a collision. On the other hand, it was calculated that the chance of collision in SHA 2 is around 4.6\*10-60, which is way lower than any of the hash algorithms compared with this one.

256-bit refers to the length of the encryption key. In our case the hacker requires to figure out a correct combination out of 2256 different combinations which is not possible even by the fastest computers in the world (Technopedia, 2022).

When talking about symmetric and non-symmetric keys, we need to discuss what is the main difference. This is straightforward. Symmetric encryption uses the same key between the sender and receiver or also called encryption and decryption. Non-symmetric encryption is the opposite the encryption uses a public key, but decryption uses a private key (Arnaud, 2023). Random numbers for the cipher are generated by RNG, sometimes also called RBG (Random Bit Generator).

## Certificate Generation

Text

Description automatically generated

Graphical user interface, text, application

Description automatically generated

## Deploy Cipher

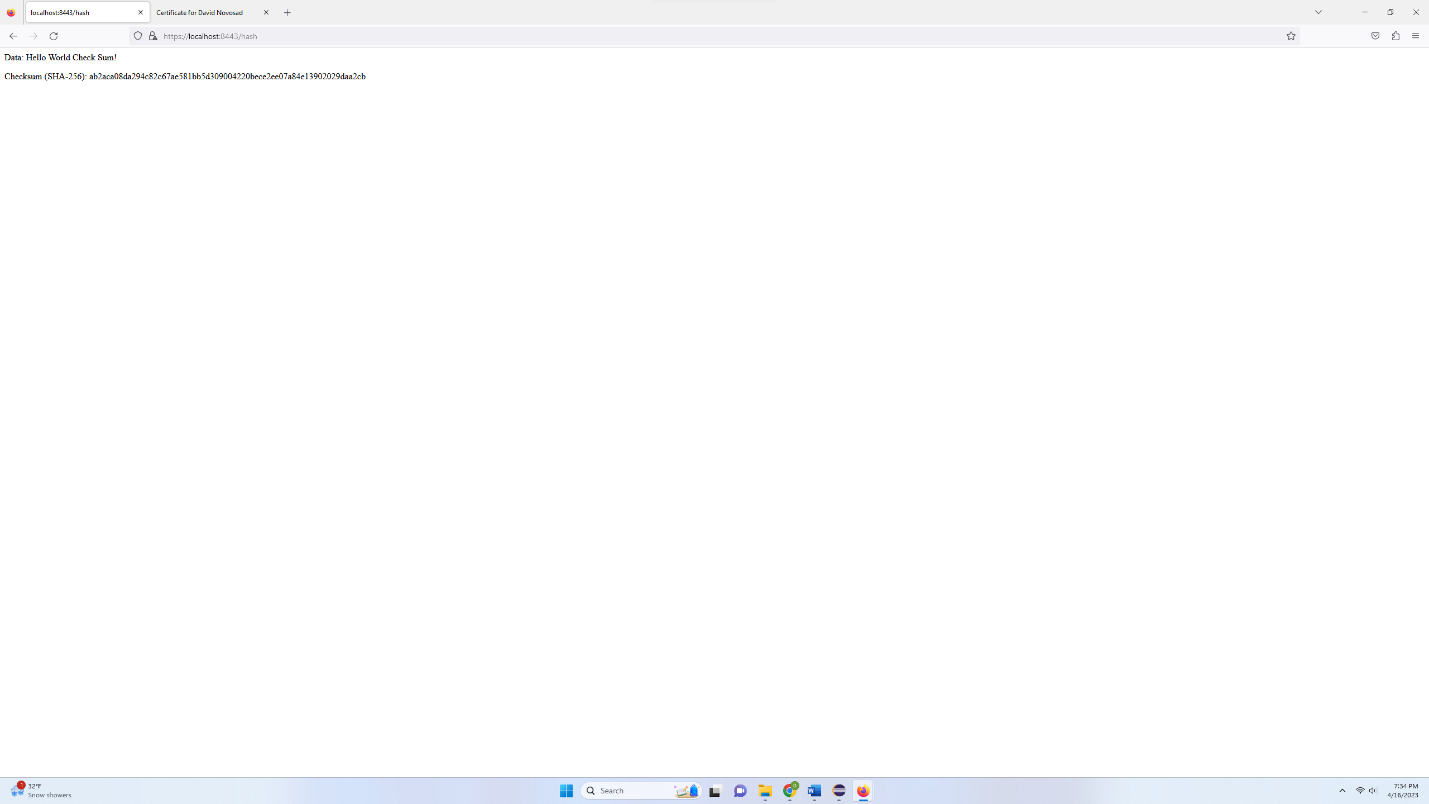
Graphical user interface, application, Word

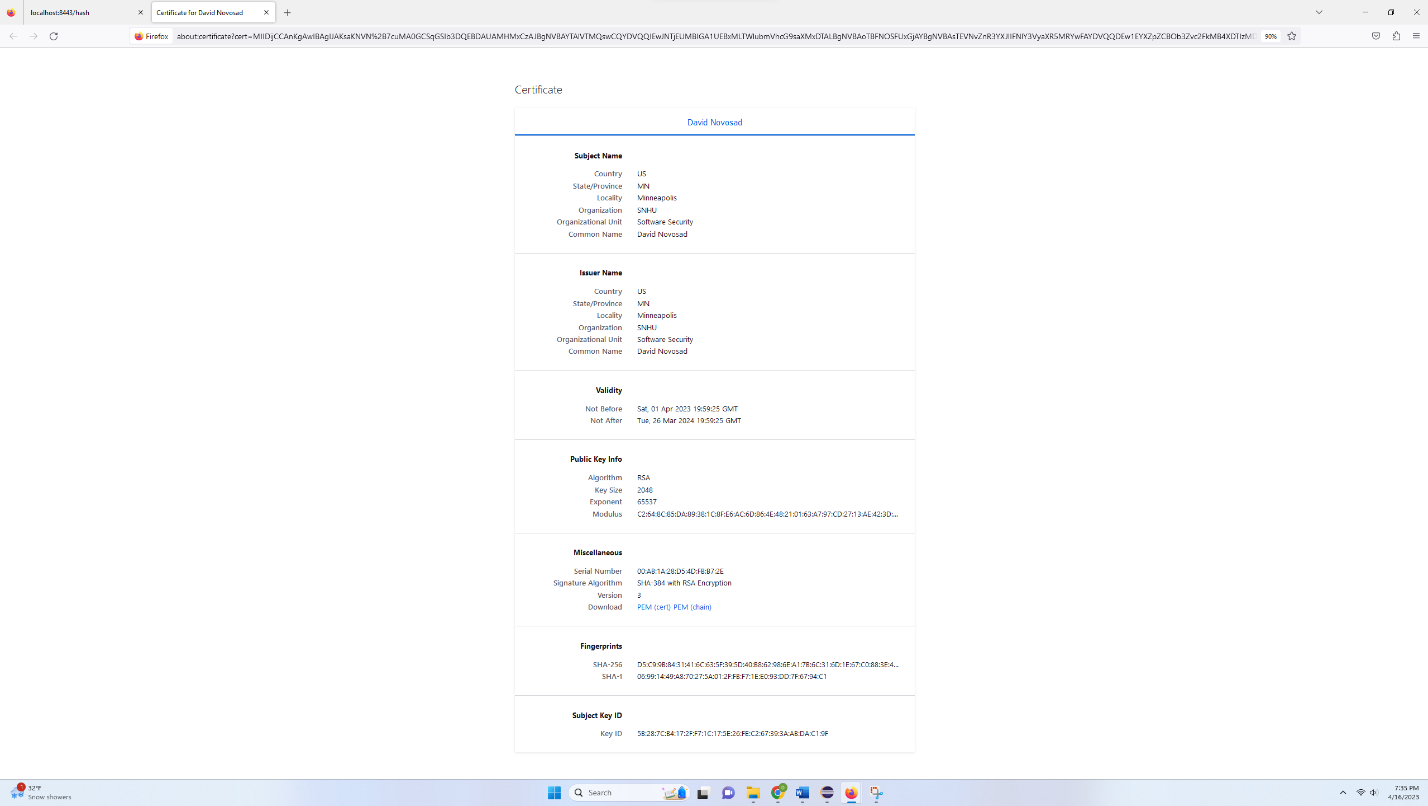
Description automatically generated

## Secure Communications

Graphical user interface, text, application, email

Description automatically generated





## Secondary Testing

Graphical user interface, text, application

Description automatically generated

**Dependency check before new code was added (base code):**

Graphical user interface, text, application

Description automatically generated

**Dependency check after (no new vulnerabilities):**

Graphical user interface

Description automatically generated with medium confidence

## Functional Testing

Graphical user interface, text

Description automatically generated with medium confidence

## Summary

I secured communication with HTTPS protocols by using a self-signed certificate. The certificate uses the RSA algorithm to encrypt the information. The certificate and the code use a checksum and cipher algorithm called SHA-256. This helps with securing the keys when encrypting and decrypting files or website information. This prevents hacker attacks from happening. It returns a string of randomly generated letters and numbers and helps with providing security. The self-signed certificate can be used in this example, but I would recommend switching to a publicly trusted CA certificate to make sure that the connection is always secure, and threats are prevented. On the screenshots we can see that a connection was established through API that shows a simple phrase and a checksum of that phrase. The way this works is when a phrase is sent to the algorithm and a hash is generated and shown. As mentioned at the beginning the algorithm used is SHA-256. As stated, it was selected as the chance of collision in SHA 2 is around 4.6\*10-60. This chance is very small, which gives us a piece of mind about the security of the system. Another way we improved the security is by running the Maven Dependency Check, which looks for issues and vulnerabilities. This combined with manual review of the code and functional tests create a strong base for the system. When all the measures pass, we can confirm that the system is successfully running and is secure. After refactoring the code, a conditional statement was added for the input statement not to be longer than 25 characters. That prevents long malicious codes from being added causing a slippage of information or DoS attacks from happening.

## Industry Standard Best Practices

To confirm the system is on par with security the Maven Dependency Check was used. The newest version (8.2.1) was used with the up-to-date vulnerabilities and issues and those were accounted for when going over the code, refactoring, and executing the code. Also, a certificate was created and added to make sure the API and website are using secure browsing with HTTPS protocols. We all know that in the current era of the internet there are easy ways how sensitive information gets leaked with low effort. Hackers have an easy time accessing websites that are not properly secured. That is why applying industry standard best practices is so important because even a tiny crack in the defense can and most likely will be used by others to access sensitive data. Using dependency check, cipher algorithms, checksum, or certificate are just some of the ways we are protecting the business, users, and the data stored and used on daily basis.

## References

Arnaud. (2023, February 23). Symmetric vs asymmetric encryption: What's the difference? Mailfence Blog. Retrieved April 16, 2023, from https://blog.mailfence.com/symmetric-vs-asymmetric-encryption/#:~:text=The%20main%20difference%20is%20that,private%20key%20to%20decrypt%20information.&amp;text=Both%20symmetric%20and%20asymmetric%20algorithms%20provide%20authentication%20capability.

Manico, J., & Detlefsen, A. (n.d.). Iron-clad Java. O'Reilly Online Learning. Retrieved

March 21, 2023, from https://learning.oreilly.com/library/view/iron-clad-

java/9780071835886/ch06.html#ch06lev1sec1

Novosad, D. (2023). Week 5 Coding Assignment (CS 305 Module Five Coding Assignment Checksum Verification David Novosad)

Rouse, M. (2022, August 11). 256-bit encryption. Techopedia. Retrieved April 16, 2023, from https://www.techopedia.com/definition/29703/256-bit-encryption#:~:text=256%2Dbit%20encryption%20is%20refers,by%20even%20the%20fastest%20computers.