**Abstract**

Code signing allows consumers to better trust developers by allowing developers to ensure their product is protected from unwanted tampering by a third-party. Through various methods including SSL encryption,

1. **Code Signing Introduction**

Security and protection are very important to consumers as it allows people to feel safer when using their computer. Consumers can ensure their applications are safe typically when developers undergo the process of code signing. Code signing allows developers to digitally sign their applications as to ensure that the code written is valid and not harmful. This process is very important as it is the base form of protection against unwanted tampering of code. Certification authorities (also known as CAs) sign each person’s program with a public key linked with their identity to create their certificate. The process of obtaining a certificate is not complex but is very integral for the developer’s software to be determined as safe for the public. The certification authorities help combat against malicious developers which are becoming more of a threat.

1. **Authentication and Integrity**

The two keywords to proper code signing, *Authentication* allows the consumer to verify the author of the application and *Integrity* which allows the verification that the application’s code has not been modified since signed. Authentication not only lets the user know where the application is from and who developed it, but rather the knowledge that the application is reputable enough to not question the validity. Integrity ensures all participants are willing to understand that their application is proper, and any malicious code is directed to the signed applicants.

1. **Code Signing Process**

The retrieval process for a certificate is miniscule however the underlying steps are 100% unique to each party and require unique info from the first party.

* 1. **Generating Certificate Signing Request (CSR)**

Using a proper operating system such as most Linux-distributions:

1. openssl req -new -key domain.com.key -out /path/to/www\_server\_com.csr will generate the requires *certificate signing request* (CSR) file needed to send to a proper CA. domain.com needs to be altered to where the user’s website address is located.
2. Following will prompt several instructions to input:
   1. Common Name: domain.com
   2. Organization Name: Example Inc.
   3. Organization Unit: Marketing
   4. City/locality: Silicon Valley
   5. State/province: California
   6. Country/Region: US
3. When instructed, do not input challenge password.
   1. **Obtaining certificate with CSR**

The CSR generated allows the user to obtain a certificate from a trusted CA. There are many examples of CAs across the internet including but not limited to, DigiCert, Let’s Encrypt, Google Trusted Services, etc. Options including Let’s Encrypt are nonprofit solutions that do not require payment and are trusted the same as other CAs.

**SSL Encryption**

SSL (Secure Sockets Layer) encryption allows companies to receive authorization that their website is safe for the public and contain no malicious content. Creating an authorized environment involves a similar process as one obtains a certificate from CAs. SSL encryption is dedicated to making websites safe and viewable for everyone. Using a

<https://casecurity.org/wp-content/uploads/2013/10/CASC-Code-Signing.pdf>

<https://www.digicert.com/ssl/>

<https://www.sslshopper.com/what-is-code-signing.html>

<https://www.ssl.com/how-to/manually-generate-a-certificate-signing-request-csr-using-openssl/>