**Southern New Hampshire University**

Joshua Wozny

[joshua.wozny@snhu.edu](mailto:joshua.wozny@snhu.edu)

June 4, 2023

**CS-305: Journal: Certificate Authorities**

Certificate authorities (CAs) play an essential role in creating trust and security in online communications. CAs are responsible for issuing digital certificates to verify the identify the identity of individuals, organizations, or devices. These certificates are used to authenticate entities involved in secure online transactions and communications (6 Protecting Sensitive Data - Iron-Clad Java [Book], n.d.).

CA issued certificates act as a trusted third party that verifies the identity of the certificate holder. Various methods are used by the CA to ensure that the entity requesting the certificate is legitimate. Users rely on the legitimacy of the CA to rely on the accuracy and reliability of the information contained in the certificate. CAs are organized in a hierarchical structure, where higher-level CAs vouch for the authenticity and reliability of lower-level CAs. This hierarchy allows for a chain of trust, where certificates issued by lower-level CAs are validated and trusted based on the reputation and credibility of the higher-level CAs. This simplifies the task of verification as long as the trust authority remains unbroken (Poettering, B., & Stebila, D., 2017).\

CAs play a vital role in the following:

* Identity Verification: CAs play an important role in verifying the identity of individuals, organizations, or devices requesting digital certificates. Through domain validation or organizational validation, certificate holder's identities can be verified and trusted.
* Establishing Trust: CAs operate within a hierarchical structure, known as the "certificate chain of trust." This chain of trust allows users to validate the authenticity of a certificate by tracing it back to a trusted root CA, establishing trust in the certificate and the associated entity.
* Encryption and Secure Communications: Digital certificates issued by CAs facilitate secure communication by employing encryption techniques, such as TSL
* Code Signing and Software Integrity: CAs also issue code signing certificates, which are used by software developers to digitally sign their applications or code. This ensures the integrity and authenticity of the software, assuring users that it has not been tampered with or modified by unauthorized parties.

In summary, utilizing certificate authorities providing references enhances the trustworthiness and reliability of digital certificates. The references help establish a chain of trust within the certificate hierarchy and provide additional information about the entity behind the certificate. By leveraging these references, users can make informed decisions about the security and authenticity of online communications and transactions.

**REFERENCES**

6 Protecting Sensitive Data - Iron-Clad Java [Book]. (n.d.). Learning. <https://learning.oreilly.com/library/view/iron-clad-java/9780071835886/ch06.html>.

Poettering, B., & Stebila, D. (2017). Double-authentication-preventing signatures. *International Journal of Information Security*, *16*(1), 1–22. <https://doi-org.ezproxy.snhu.edu/10.1007/s10207-015-0307-8>