Tim Jayson

CS-305 Module 5 assignment 2

**Certificate Authorities**:

* 1. Why would you want to use a CA for security?

A Certificate Authority (CA) is a trusted third-party organization that issues a digital certificate. The CA uses its own private key to digitally sign a website’s certificate. When a web browser connects to that website over HTTPS, it is able to verify that the certificate was signed by a recognized CA and that the website’s public key belongs to the owner of the domain. This verification helps to prevent man-in-the-middle attacks. The following are some of the advantages of using a CA for security:

* Verification of Authenticity: A CA helps to confirm that the server/website owns the domain name.
* Trust: Web browsers trust certificates issued by recognized CAs automatically.
* Revocation of certificate: A CA can revoke compromised certificates which can help to protect users from connecting to compromised websites.
* Ease of use: In a real world environment, it is impractical for all users to self-verify all certificates.
  1. What are the advantages of using a CA?

There are a variety of advantages to using a Certificate Authority (CA):

* CAs offer enhanced security: A CA signed certificate are harder to forge or fake making them more secure for the end user.
* Cas are widely trusted by web browsers: A website with a signed CA typically does not issue warnings to the end users, alternatively if a website does not have a CA the browser will warn the user before continuing onto the page.
* Centralized management: using a Certificate Authority makes it easier to renew, revoke, and maintain certificates.
* Regulatory compliance: There are many industries that require the use of CA-signed certificates.

**Certificate Generation**

A screenshot of a computer program

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

Sources:

Awati, R., & Loshin, P. (2025, March 7). *What is a Certificate Authority (CA)?: Definition from TechTarget*. Search Security. https://www.techtarget.com/searchsecurity/definition/certificate-authority

Gitlan, D. (n.d.). *What is a certificate authority and why it matters - SSL dragon*. SSL Dragon. https://www.ssldragon.com/blog/certificate-authority/

*What is a Ca? certificate authorities explained*. DigiCert. (n.d.). https://www.digicert.com/blog/what-is-a-certificate-authority