Certificate Authorities (CA) Explanation

A Certificate Authority (CA) acts as a reliable go-between to assist ensure the security of websites. Your web browser verifies that a secure website—like the one run by your bank—is legitimate and safe to use by contacting the CA. It is the CA's responsibility to verify that the website is authentic and not a fraud.

Why would you need a CA for security?   
You can make sure that you're on the legit website and not a fraudulent one that is attempting to steal some of your information by using a CA. Also it can help guarantee the privacy and security of any information you are sending or using, including stuff like your username and password.

What are the advantages of using a CA?

* Trust: Web browsers trust certificates signed by CAs, so you can trust the site too.
* Encryption: CAs help create secure websites (with HTTPS) that keep your data private.
* Authentication: CAs check that the website really belongs to the person or company it claims to.

For this assignment, instead of using a paid CA, I will create my own certificate using a tool called Java Keytool. This makes me the CA for testing or development, which is common when you’re building or testing software.

A screen shot of a computer

AI-generated content may be incorrect.A black screen with white text

AI-generated content may be incorrect.A screenshot of a computer

AI-generated content may be incorrect.