|  |  |
| --- | --- |
|  | CIS-1290 Principles of Information Security |

Topic 8 Assignment 2

|  |  |
| --- | --- |
| To: | Mike MacDonald |
| From: | Christopher Sigouin |
| Date: | April 10, 2015 |
| Subject: | Digitally sign a document using certificates |
|  |  |

This assignment was to digitally sign a word document using a digital certificate from Verisign. Once the document was signed an explanation was to be provided on the benefits of signed documents. Below I outline these benefits and all steps taken to produce the digitally signed document

I began with the process of acquiring the certificate from Verisign within a Windows 7 virtual machine environment using Mozilla Firefox 37.0.1. Upon registration at the site I received two emails. One contained a hyperlink back to VeriSign authorizing the installation of the digital certificate and the second provided a password to be used in conjunction with the linked page. Once entered, it allowed me to generate and install the certificate and private key. After the site indicated a successful private key creation along with an installed certificate, I received the following message in a popup box:

*This certificate can’t be verified and will not be imported. The certificate issuer might be unknown or untrusted, the certificate might have expired or been revoked, or the certificate might not have been approved.*

I am uncertain why the error occurred, but allowed me to view the certificate within the certificates section under options in Mozilla Firefox. Within the management console of Windows 7, I searched for the certificate and it was not listed. Due to this, I proceeded to export the certificate from Mozilla Firefox by double clicking on it and choosing export with the desktop as the destination. I proceeded to install it and choose to save it under “Personal “. Once completed I opened a prior assignment in Microsoft Word and chose the option to “Protect Document “. It provided me with a message box stating to acquire a digital ID and offered to redirect me to Microsoft. I attempted the same procedure with Internet Explorer and ran into further issues: When attempting to click on the ‘generate key and certificate’ button from the site, IE wanted to know what to do with a file called SelfService.Action.

With assistance I found that I was not exporting the private key and certificate from Mozilla Firefox. When clicking on export I was only saving the certificate. Choosing backup allowed me to acquire both, allowing me to install it and view in the management console. Microsoft Word then allowed me to digitally sign the document using the key.

I could determine various pieces of information from the signature such as the signer's information (including date/time of signing) and address information, small amount of information regarding the system that signed the document and details regarding the certificate itself such as the type of certificate, the date range that the certificate is valid through and the certificate authority that issued it.

The benefits of digitally signing documents is to ensure trust that the document is from the intended organization or individual that is expected. Also it ensures that the integrity of the document remains unchanged and prevents the signer of the document from denying that they signed it (non-repudiation).

Some of the benefits and/or drawbacks of using a self-signed certificate vs. a trusted authority’s certificate are listed below:

|  |  |
| --- | --- |
| **Benefits**   * A self-signed certificate may be considered less in value to an attacker vs. one that is signed by an enterprise level CA ( more valuable target ) * Easier to customize * Can be created for free. Financial cost less of an issue | **Drawbacks**   * Self-signed certificates cannot be revoked, possibly allowing attackers to spoof identity. * Speed of transferring public keys may be an issue between parties. With a trusted authority, the interaction is between the certificate holder and the CA root server * Can drive away potential customer trust if used with an e-commerce solution due to warnings shown by a browser |