Session 06 – Viewing Digital Certificates Wei Cui

Q: Why does Google create a secure HTTP connection regardless https:// is type?

A: Because Google relies on the big data to improve all its service, e.g. when we search for something in google.com, the ranking of a website in the search result based on how many people has clicked on it in the same search. The users contribute to its giant database to make its search results more accurate. To prevent the data being intercepted by its adversaries, google must encrypt it through a secure HTTP connection.

Q: Why is the site not concerned about distributing the public key? How does embedded key in a digital certificate protect it from impersonators?

A: The public key is for others to encrypt and send the messages to the site. It must be distributed. The digital certificate allows the public key embedded to be verified by the certificate authority.

Q: Why is the expiration date of the root certificate is longer than that of the website certificate?

Because website certificates are derived from root certificates. The company receives the web certificates from the CA and use the root certificate as part of the validation process.

Q: Why are so many root certificate authorities?

The Web is worldwide. The CA business is fragmented and dominated by the regional providers. This is because the use of digital certificates are linked to local laws, regulations, and accreditation schemes for CA.

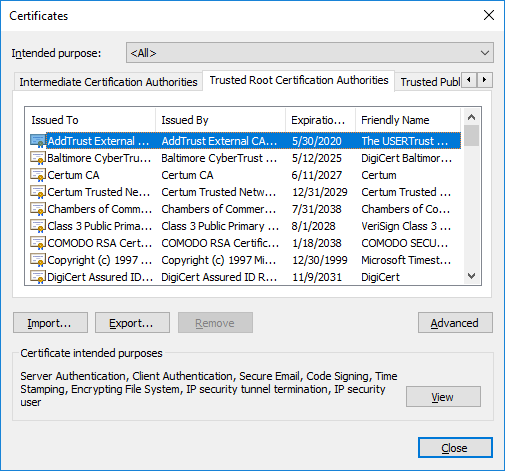


Fig. 1. Screenshot of Trusted Root Certification Authorities (Step 13)