16-124-836
Marcel Matti ZAUDER

5.5 Question 5

5.5.A What is a Public-Key Certificate? How is this being used (having the overall X.509 scheme in mind) and what advantages does it bring against other techniques? (keep it less than 200-250 words)

A Public-Key Certificate is used as an electronic document to ensure the validity of a public key. It contains some information about the key itself, about the identity of the key's owner and a digital signature in order to verify the content's within the certificate. One of the main advantages using this certificate is to enable secure authentication and also ensuring the integrity. The Public-Key Certificate is issued by a trusted thir-party, a so called certificate authority, in order to verify the identities of parties partaking in an exchange of information using the internet.

5.5.B Explain briefly what a Certificate Authority and a Public-Key Infrastructure is.

A certificate authority issues public-key certificates in order to validate a person's identity. These PKCs form a part of the Public-Key infrastructure, a system that uses encryption technology to secure messages and data. The four main components of this PKI are:

1. Public Key Encryption
2. Trusted Third Parties (CA for example)
3. Registration Authority
4. Certificate Database or Store