Information Security Animations - Public Key Infrastructure (Script)

Public Key Infrastructure

Public Key Infrastructure (PKI) provides a safe and reliable environment for electronic transactions on the Internet. It is a security framework that uses public key encryption technique to protect the confidentiality, integrity, authenticity and non-repudiation of data.

Certificate Authority and Digital Certificate

The effective operation of public key infrastructure relies heavily on the support of the certificate authority (CA). The major task of a certificate authority is to proof of identity of the parties in an electronic transaction as a credible third party.

Digital certificate is a certification issued in electronic format.

The data stored in it can be used to verify the identity of the certificate holder. Digital certificates usually contain such information as the user’s public key, name, email address, etc.

After the registration authority (RA) verify the identity of an applicant, CA will issue to the applicant a copy of the certificate signed digitally and publish the applicant’s public key on a public directory.

The Certificate Revocation List (CRL) is issued regularly by a certificate authority. It contains all certificates cancelled or suspended before their expiry dates. Certificates in other parties' public keys must be checked against their validity in order to prevent the abuse of invalid certificates.

Public Key Encryption Technique

Public key encryption technique involves providing every user with a pair of keys - a private key kept secretly by the user and a corresponding public key which is known to others. This pair of

asymmetric but matching keys will be used for data encryption to ensure confidentiality. For instance, if the public key is used to encode the data, only the corresponding private key can decode the encryption.

Take email message transmission as an example. A sender can use the intended recipient's public key to encode the content of an email message. When the recipient receives the message, he will need to use the corresponding private key that he keeps to decode the message. By doing so, the confidentiality of the email content will be secured.

Furthermore, to ensure integrity, authenticity and non-repudiation of the email message, the sender will use mathematical algorithms to generate a message digest and encrypt it with his own private key to create a digital signature. He will then send the email together with the digital signature to the recipient.

When the recipient receives the message, in order to verify its validity, he will verify the digital signature using the public key

corresponding to the sender's private key and apply the same mathematical algorithms to generate a message digest. In this way, the recipient can confirm the email message is in fact from the sender and thus verify the authenticity of the message.

Meanwhile, the sender cannot deny his signature on the email message either, thus ensuring the non-repudiation of the email.

To learn more about information security, please visit the InfoSec website at: http://www.infosec.gov.hk