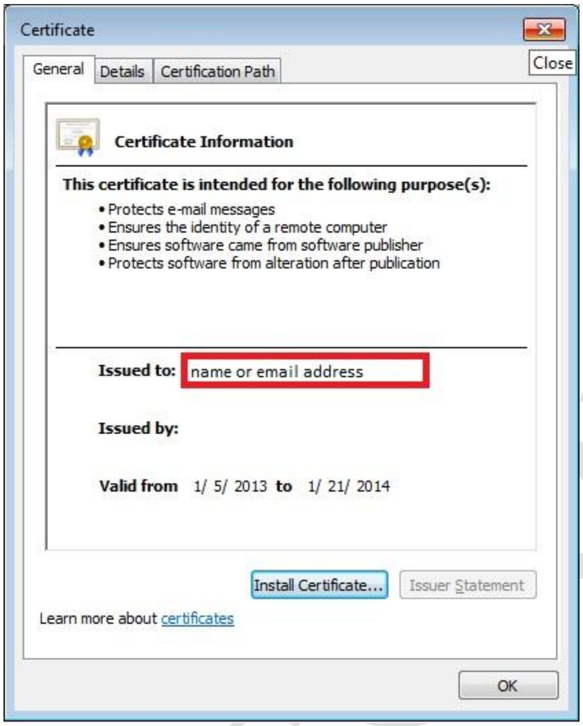
Digital Certificates



This certificate is intended for the following purpose(s):

- Protects e-mail messages
- Ensures the identity of a remote computer
- Ensures software came from software publisher
- Protects software from alteration after publication

Issued to: name or email address

Issued by:

Valid from 1/ 5/ 2013 to 1/ 21/ 2014

Learn more about certificates

Digital certificate is issued by a trusted third party who proves sender's identity to the receiver and receiver's identity to the sender.

A digital certificate is a certificate issued by a Certificate Authority (CA) to verify the identity of the certificate holder. The CA issues an encrypted digital certificate containing the applicant's public key and a variety of other identification information. Digital certificate is used to attach public key with a particular individual or an entity.

Digital certificate contains:-

- **Serial Number**: Used to uniquely identify the certificate.
- **Subject**: The person or entity identified.
- **Signature Algorithm**: The algorithm used to create the signature.
- **Signature**: The actual signature to verify that it came from the issuer.
- **Issuer**: The entity that verified the information and issued the certificate.

- **Valid-From**: The date the certificate is first valid from.
- **Valid-To**: The expiration date.
- **Key-Usage**: Purpose of the public key (For example: encipherment, signature, certificate signing...).
- **Public Key**: The public key.
- **Thumbprint Algorithm**: The algorithm used to hash the public key certificate.
- **Thumbprint**: The hash itself, used as an abbreviated form of the public key certificate.

Certification Authorities

You can obtain a client certificate from a mutually trusted, commercial organization called a certification authority. Before issuing a certificate, the authority requires you to provide identification information, such as a name, address, and organization name. The extent of this information can vary with the identification assurance requirements of the certificate. If you need a certificate to provide absolute assurance about your identity, then the certification authority will require substantial information from you; gathering this information may require a personal interview with the authority and the endorsement of a notary.

Note: Ultimately, the success of certificate authentication depends on whether the party receiving a certificate trusts the authority who issued the certificate, and that the authority properly verified the certificate owner's identity. But beyond this trust, certificates do not provide conclusive proof about the identity, trustworthiness, or intentions, of the user or server.