Final Project

He Han

heh32

1. What are the limitations of using self-signed certificates?

Answer:

1. Self-signed certificates aren't trusted by other applications/operating systems, which may lead to authentications errors.
2. Self-signed certificates life time is usually 1 year. Before the year ended, the certificate may need to renew or replace.
3. Self-signed certificates may use low hash and cipher technologies, so the security level that implemented by self-signed certificates may not satisfy the current Security Policy.
4. Self-signed certificates don’t support for advanced Public Key Infrastructure (PKI) functions.
5. Most of the advanced feathers of the server side applications may be required to use a Public Key Infrastructure (PKI), where self-signed certificates cannot be used.
6. What are they useful for?

Answer:

1. Self-signed certificates can be used for limited scenarios, for example, to install a single exchange server in the organization.
2. Self-signed certificates can be used in small group.
3. Self-signed certificates can be used to test servers. If we're creating a website that we need to test over on https connection, we don't need to pay for a signed certificate for that testing site. What we should do is just telling your testers that their browser may pop warning messages.
4. Self-signed certificates can be used to test secure web servers and code signing. For example, when web site access is restricted to a small group.