Certificate Management

Certificate management is the act of monitoring, facilitating, and executing digital x.509 certificates (SSL certificates). It plays a critical role in keeping communications between a client and server operating, encrypted, and secure.

Certificate lifecycle management catches faulty, misconfigured, and expired certificates, then performs the following processes

Creating,Purchasing,Storing,Disseminating,Deploying,Renewing,Suspending,Revoking,Replacing

A good certificate lifecycle management system is capable of performing these actions for an entire certificate infrastructure, automatically and in real-time, to prevent downtime and outages.

Problem Statement

A Certificate management system has to be created to track life cycle of a certificate on server

New certificate has to be generated and issued to new users and

Old certificated has to be expired on timely basis and notification has to be sent to users/clients

Expectation

The created system should be able to generated certificates of X.509 standard version 3

The system should monitor certificates on server and notify user of certificates that are about to expire

Certificates canbe validated by a CA or can also be validated locally for use in internal network

Solution

User Stories

1.Build a module to generate a certificate file .The generated certificate should of standard X.509 v3

2.Build a module to monitor different certificate dates and issue notification for certificate to be expired to administrator

3.Build a module to renew certificate that are about to expire

4.Build a module to accept a request from a client regarding issuing of a new certificate

5.For validating certificate locally a module can be created to generate a local CA. The local CA will require a private key for .The same should be generated through module

6.The public key and private key should be generated along with certificate

7.The system should be able to generate four types of certificates

- Self-signed certificates
- Signed certificates
- Certificate authority (CA) certificates
- Unsigned certificates (rarely used)

8. When you create a self-signed or signed certificate (including CA certificates) you can specify a *subject*. The subject of a certificate is the set of attributes of an X.500

Distinguished Name that is encoded in the certificate. The subject enables the recipient of a certificate to see information about the owner of the certificate. The subject describes the certificate owner, but is not necessarily unique.

COMMON NAME (CN) CN=Patel Agrawal

ORGANIZATION (O) O=IBM Corporation

ORGANIZATIONAL UNIT (OU) OU=IBM Software Group

COUNTRY (C) C=IN

LOCALITY (L) L=Bangalore

STATE or PROVINCE (ST) ST=Kanataka

E-MAIL ADDRESS (emailAddress)
emailAddress=agrawal@abc.ibm.com