PKI Certificate Requirements for SCCM 2012 R2 In this post we will see the PKI certificate requirements for SCCM 2012 R2. This is one of the post which is a part Deploy PKI Certificates for SCCM 2012 R2 Step by Step Guide. Before we proceed let's get to know what PKI is. Public-key cryptography (also called asymmetric-key cryptography) uses a key pair to encrypt and decrypt content. The key pair consists of one public and one private key that are mathematically related. An individual who intends to communicate securely with others can distribute the public key but must keep the private key secret. Content encrypted by using one of the keys can be decrypted by using the other. PKI can be used to secure e-mail, secure web communications, secure web sites, digital signing of software files etc.

When you use Active Directory Certificate Services and certificate templates, the Microsoft PKI solution can ease the management of the certificates. One thing to note here is template-based certificates can be issued only by an enterprise certification authority running on the Enterprise Edition or Datacenter Edition of the server operating system. The HTTPS protocol provides client-to-server communications that are mutually authenticated, signed, and encrypted. Internet clients must use HTTPS, and all clients are more secure if configured to use HTTPS. You must deploy the required certificate to each client and site system that will use HTTPS.

PKI Certificate Requirements for SCCM 2012 R2

The following table lists the types of PKI certificates that are required for Configuration Manager 2012 R2 . I have not listed all the PKI certificates required for SCCM, you can find the complete list of certificates here.

Certificate Requirement	Certificate Description
Web server certificate for site systems that run IIS	This certificate is used to encrypt data and authenticate the server to clients. It must be installed externally from Configuration Manager on site systems servers that run IIS and that are configured in Configuration Manager to use HTTPS.
Client certificate for Windows computers	This certificate is used to authenticate Configuration Manager client computers to site systems that are configured to use HTTPS. It can also be used for management points and state migration points to monitor their operational status when they are configured to use HTTPS. It must be installed externally from Configuration Manager on computers.
Client certificate for distribution points	The certificate is used to authenticate the distribution point to an HTTPS-enabled management point before the distribution point sends status messages. When the Enable PXE support for clients distribution point option is selected, the certificate is sent to computers that PXE boot so that they can connect to a HTTPS-enabled management point during the deployment of the operating system.
Client certificate for Mac computers	This certificate is used to authenticate Configuration Manager Mac computers to management points and distribution points that are configured to support HTTPS. You can request and install this certificate from a Mac computer when you use Configuration Manager enrollment and select the configured certificate template as a mobile device client setting.

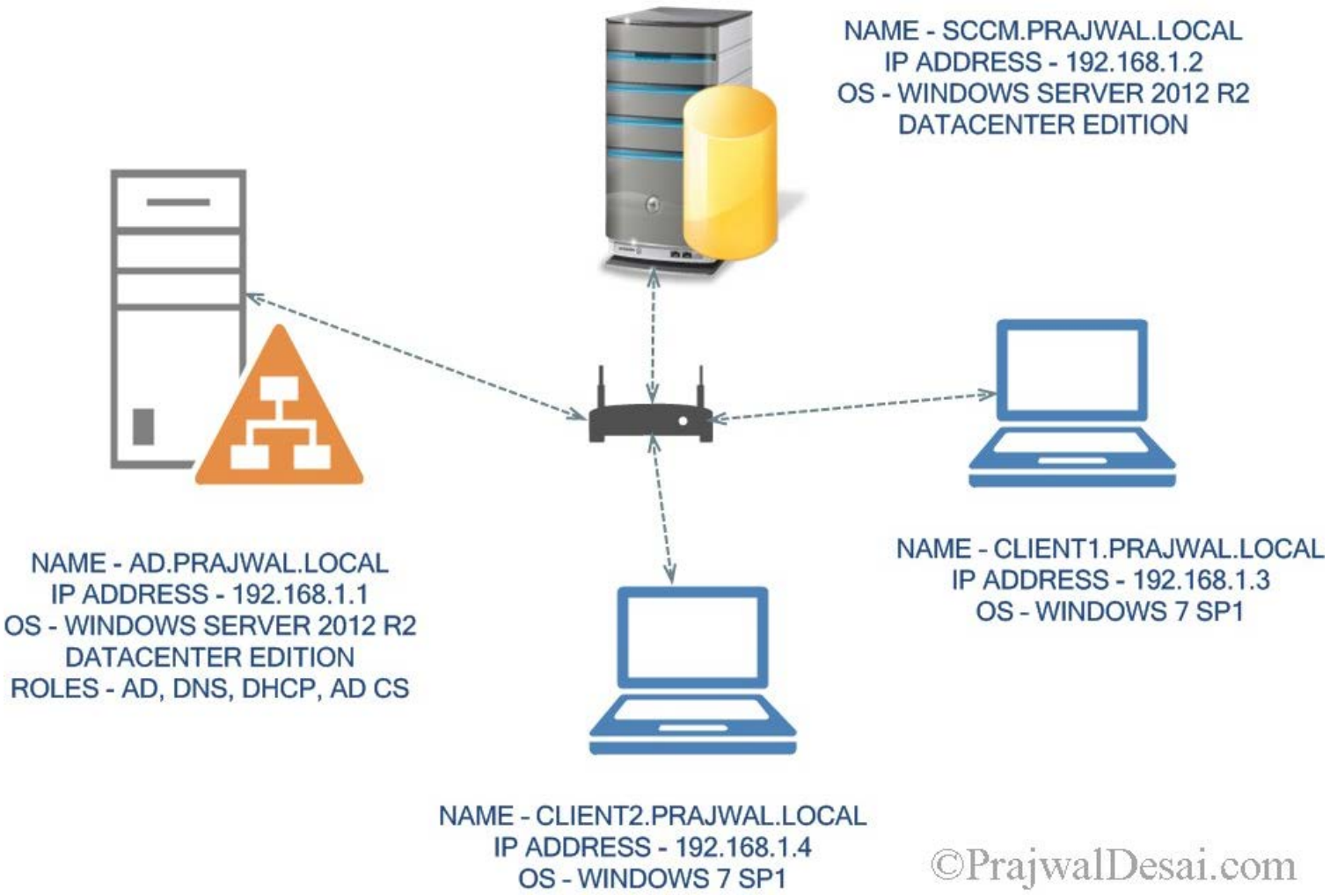
A typical PKI consists of the following elements.

Element	Description
Certification Authority	Acts as the root of trust in a public key infrastructure and provides services that authenticate the identity of individuals, computers, and other entities in a network.
Registration Authority	Is certified by a root CA to issue certificates for specific uses permitted by the root. In a Microsoft PKI, a registration authority (RA) is usually called a subordinate CA.
Certificate Database	Saves certificate requests and issued and revoked certificates and certificate requests on the CA or RA.
Certificate Store	Saves issued certificates and pending or rejected certificate requests on the local computer.
Key Archival Server	Saves encrypted private keys in the certificate database for recovery after loss.

Lab Setup

In my current lab setup, I have got a machine that is running Windows Server 2012 R2 Datacenter edition OS. It is a domain controller (AD.PRAJWAL.LOCAL) that is also configured as DNS, DHCP and AD CS (Active Directory Certificate Services). On the second machine, I have installed Windows Server 2012 R2 Datacenter edition OS. This is machine is running System Center 2012 R2 Configuration Manager and SQL server. You can have few client machines for testing the PKI deployment. The procedures use an enterprise certification authority (CA) and certificate templates. The steps are appropriate for a test network only, as a proof of concept. Because there is no single method of deployment for the required certificates, you must consult your particular PKI deployment documentation for the required procedures and best practices to deploy the required certificates for a production environment.

You can log in with a root domain administrator account or an enterprise domain administrator account and use this account for all procedures in this example deployment.



PKI Certificate Requirements for SCCM 2012 R2 Lab Setup