

---

# Managing SSL Certificates for Linux Internet Server

## Test Report of Kousec Server Certificate Manager

### Part 1. Planning for Acquiring and Deploying Certificates

---

Copyright 2009,2010 Kousec Software, Inc. All rights reserved.  
All company names and product names are trademarks of their respective holders.

---

---

## Series Index

[http://www.kousec.com/prod\\_cm.html](http://www.kousec.com/prod_cm.html)

Part 1. Planning for Acquiring and Deploying Certificates

PDF: [http://www.kousec.com/tj/tj\\_review\\_S1\\_en.pdf](http://www.kousec.com/tj/tj_review_S1_en.pdf)

Part 2. Configuring SSL on Server

PDF: [http://www.kousec.com/tj/tj\\_review\\_S2\\_en.pdf](http://www.kousec.com/tj/tj_review_S2_en.pdf)

Part 3. Defining Certificate Specs and Obtaining Certificates

PDF: [http://www.kousec.com/tj/tj\\_review\\_S3\\_en.pdf](http://www.kousec.com/tj/tj_review_S3_en.pdf)

Part 4. Deploying and Monitoring Certificates

PDF: [http://www.kousec.com/tj/tj\\_review\\_S4\\_en.pdf](http://www.kousec.com/tj/tj_review_S4_en.pdf)

Part 5. Best Practices for Security and Operations

PDF: [http://www.kousec.com/tj/tj\\_review\\_S5\\_en.pdf](http://www.kousec.com/tj/tj_review_S5_en.pdf)

---

## Table of Contents

Introduction.....	5
Purpose of Testing.....	5
Test Configuration.....	5
Planning for Acquiring and Deploying Certificates.....	7
SSL Server Certificate for Server or for Service?.....	7
How to Assign Hostnames among Certificates.....	8
Installing one Certificate on Multiple Servers?.....	9
What are EV certificates and Domain certificates?.....	9
Certificates to Obtain.....	10

---

## Introduction

What do you think of an SSL certificate for web site when you are actually handling one? Is it one of chores for a website, are you not sure which server needs an SSL certificate, or do you just get it done and forget it? If you are a company having many web sites for your clients, you may be in a situation where the increasing number of SSL certificates is causing the administrative overhead and increasing the risk of human errors.

On the other hand, the importance and applicability of SSL certificates are ever increasing as privacy regulations are becoming universal and website phishing is becoming common. Businesses need to strike a right balance between efficiency and security in SSL management when building secure internet sites.

Kousec Server Certificate Manager is a SSL certificate management product that meets those needs. In this five-part series of articles, we will use the software to manage SSL certificates on a Linux environment and report findings and recommendations on the software usage and server certificate management.

## Purpose of Testing

The purpose of this testing is to report findings and recommendations on SSL server certificate management using Kousec Server Certificate Manager for a Linux-based internet-facing server environment.

We will use Ubuntu Server Edition 9.04 as the Linux OS, which is becoming popular in Linux server space with commercial support offerings from Canonical, Ltd. Since Ubuntu is based on Debian Linux and differs in many aspects from RHEL/CentOS based distributions, this report might also be helpful for those deploying an Internet server using Ubuntu Server Edition.

## Test Configuration

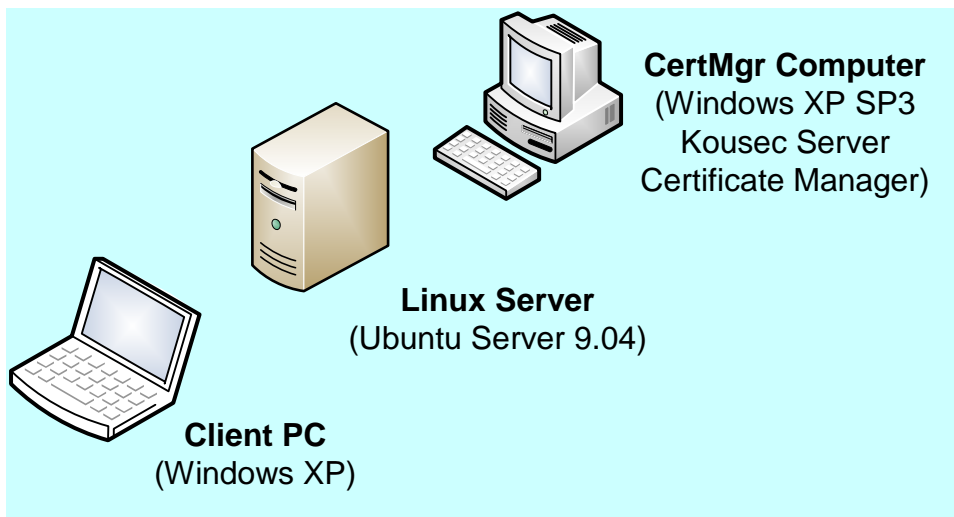
We will install Ubuntu Server 9.04 on an x86 server to build an Internet-facing web/mail server. We will design the server so that we will be able to distribute several services to multiple servers for off-loading in future.

---

**Table 1 Offered Services**

Service	Server Software	Usage Purpose
LDAP	OpenLDAP	Authenticates users from each service
Main web	Apache2	Primary public web site
Sub web	Tomcat6	Partner web site
FTP service	Vsftpd	FTP for partners
SMTP service	Postfix	Sending and relaying emails
POP3 service	Dovecot	Receiving emails from intranet PCs
IMP4 service	Dovecot	Receiving emails from intranet PCs

Kousec Server Certificate Manager will be installed on a PC running Windows XP. The following diagram shows the hardware configuration for this testing.



---

## Planning for Acquiring and Deploying Certificates

In this chapter, we will list services that need SSL server certificates and consider types of SSL certificates that are appropriate for each service.

### SSL Server Certificate for Server or for Service?

Although SSL server certificates are often called “server certificates”, the author feels that in many cases people obtain an SSL certificate for a service, not for a server. In this testing, we will be running many services on one server, but it is typical that as the load rises we divide and distribute work loads on per-service basis. Especially, in a production system the LDAP service should reside behind the inner firewall. Another scenario is to separate servers for web/ftp services and mail services. Therefore, SSL certificates should also be prepared on per-service basis.

There are also cases where preparing server certificates on per server machine basis makes better sense. For example, SSH is used to enable remote management of a server machine. In this case, we would need to obtain a server certificate that identifies and authenticates the managed server, not one that identifies an SSH service that’s not bound to any particular machine. (In our testing, we will be using OpenSSH in Ubuntu that does not support use of server certificates, so we won’t obtain a certificate for SSH)

Therefore it can be said that a per-service certificate is appropriate for server software that offers a service and a per-machine certificate is appropriate for server software that offers a management interface of the running machine.

Based on this discussion, we will list up SSL certificate that are necessary for our testing.

**Table 2 Hostnames that need certificates**

Hostnames authenticated by certificate	Usage	Server to install	Per-server or per-service
ldap.example.com	LDAP	server1	Service
www.example.com	Primary web	server1	Service
www2.example.com	Secondary web	server1	Service
ftp.example.com	FTP Service	server1	Service
smtp.example.com	SMTP Service	server1	Service

pop.example.com	POP3 Service	server1	Service
imap.example.com	IMAP Service	server1	Service

## How to Assign Hostnames among Certificates

In the previous paragraphs, we enumerated services that require server certificates and hostnames for the services. Next we are going to consider what kind of certificate(s) and how many of them we will need.

Depending on the number and types of hostnames that a certificate can cover, SSL certificates can be categorized into three types.

- **Single Domain Certificate:** You can put only one hostname in a certificate.
- **Wildcard Certificate:** One certificate can cover all subdomain hostnames.  
Example: By putting a hostname with "\*" in a certificate, as in "\*.example.com", you can cover all hostnames that end in ".example.com".
- **Multi-domain Certificate:** You can put multiple hostnames, all of which are unrelated in terms of domain names. Sometimes referred to as UC certificates also.  
Example: www.example.com, example.com, another.net, another.org

The simplest way for us is to use a single wildcard certificate to cover all the hostnames used in this testing. However, the reality is not that simple. The reasons are as follows.

- Many CAs do not offer wildcard certificates
- An EV certificate (described later) cannot have a wildcard hostname. This is mandated by the EV specification.
- A typical pricing for a wildcard certificate is much higher than that of a single domain certificate.

Generally, a service that requires high assurance level does not use a wildcard certificate.

A multi-domain certificate is often used in the following scenarios. 1) Exposing an intranet server to the Internet (requiring both internal hostname and external hostname), 2) consolidating multiple SSL-enabled servers, 3) SSL-enabling multiple virtual hosts.

---

## Installing one Certificate on Multiple Servers?

Whether you have a single domain certificate, a wildcard certificate or a multi-domain certificate, many CAs require you to obtain “server licenses” if you want to install a single certificate onto multiple servers. This is a granted right for how many server computers the purchaser can install the certificate on.

Its pricing varies among CAs. When you extend the system to have multiple servers, you may need to pay additional cost to obtain server licenses for a single certificate. Therefore it is not always a good idea to put multiple hostnames in a certificate with the intention of reducing certificate acquisition cost. Be sure to collect information for server licenses when evaluating certificate vendors.

## What are EV certificates and Domain certificates?

Separate from the domain coverage types, there is another categorization for SSL certificate products. It is the method (or strictness) of authenticating the applicant’s organization during certificate issuance process.

An SSL server certificate is used to encrypt network communication and authentication of network peer. Furthermore, because web sites need to give assurance to customers (e.g., credibility of the web site operator), the applying organization must be validated by CA during certificate issuance process. Especially important are EV certificates (Extended Validation certificates), which were introduced several years ago to better combat the increasing phishing scams.

On the other hand, needs for SSL certificates are also rising in personal and non-commercial sites. To fulfill such needs, low-cost domain-validated certificates were introduced.

- **Organization Validation:** Also called business validation by some CAs. Not only the ownership of the domain name, but also applying entities (organizations and persons) are also authenticated and validated.
- **Extended Validation:** Generally referred to as EV certificates. Applying organizations must go through more stringent validation process than that of Organization Validation. Also, types of applying entities are restricted.
- **Domain Validation:** Only the ownership or right to use of the domain name is validated

---

during certificate issuance. It is important to note that only the domain name is set in Distinguish Name section of the certificate.

EV certificates are becoming common for financial companies, health care companies and other renowned services or web sites of renowned companies where phishing scams often target.

On the other hand, the author believes that domain certificates are sufficient for services that are accessed internally, especially accessed by software systems, not humans on web browsers.

Since we are only testing, we will obtain certificates from a private CA. However, for a scenario where we migrate from a test system to the production system, we will do the design that also takes commercial certificates into consideration.

### Certificates to Obtain

Based on the above description, we are obtaining SSL certificates as outlined below.

**Table 3 Certificates to obtain for this testing**

Hostname in Certificate	Install on	Certificate Name	Usage/User	Validation Requirement
ldap.example.com	LDAP	ldap.example.com	Internal Authentication	Domain
www.example.com	Primary web	www.example.com	Public server	Organization (or EV)
www2.example.com	Secondary web	www2.example.com	For employee / partners	Organization
ftp.example.com	FTP service			
smtp.example.com	SMTP service	smtp.example.com	Accepts emails from employees' PCs	Domain

pop.example.com	POP3 service	pop.example.com	Accessible from employees' PCs	Domain
imap.example.com	IMAP service			

Each column of this table is as follows:

**Hostname in Certificate:** Hostname to put in a certificate. When there are more than one hostname for a certificate, we need to obtain a multi-domain certificate. In that case, multiple hostnames will be included in SubjectAltNames field in the certificate.

**Install on:** Service to which install the certificate.

**Certificate Name:** Any friendly name to identify the certificate. If a certificate has multiple hostnames, choose one hostname as primary and make it as the certificate name. We will set this name in Common Name in the certificate's DN. We also use this name as the filename for the certificate and private key files.

**Usage/User:** Entities (person or programs) who actually validate the certificate when connecting the service.

**Validation Requirement:** Validation level that a certificate requires. We choose from EV, Organization Validation, and Domain Validation.

We determined our validation requirements based on the following.

www.example.com, www2.example.com, ftp.example.com:

For services intended for the public or partners, we chose **Organization Validated** certificates because they are accessed by indefinite range of people. Also if the public server will be a well-known web site that accepts information from customers, we will need an **EV** certificate.

ldap.example.com, smtp.example.com, pop.example.com, imap.example.com:

In email client applications and front-end server programs, destination servers that they connect are set by administrators at configuration time. Therefore there is no need to use Organization Validated certificates and we chose **Domain Validated** certificates.

### Domain Validation

One concern with domain validated certificates is its validation process at CAs. The

---

possibility of issuing a certificate to a false applicant may be higher than that of organization validation. It is also true that many CAs that offer domain validated certificates are improving their validation process for both correctness and speed of issuance.

Since our testing is for evaluation of Server Certificate Manager, we won't obtain certificates from commercial CAs but obtain from the private CA that is built in Kousec Server Certificate Manager.

### **Domain name coverage**

We chose to put hostnames `www2.example.com` and `ftp.example.com` into a multi-domain certificate, and put `pop.example.com` and `imap.example.com` into another multi-domain certificate. Because pop and imap services are served by a single server program (Dovecot), it will be much easier to manage if we put them in one certificate. `www2` and `ftp` are served by separate server programs, but for this testing, we made it a multi-domain certificate for a scenario where we consolidate two servers (web server and ftp server) into one server.

This is the end of Planning for Acquiring and Deploying Certificates.  
In the next article, we will install server software on Ubuntu Server and configure SSL for each server program.