
Technical Whitepaper

Kousec Server Certificate Manager

Product Overview

Kousec Software, Inc.

Copyright 2009-2011 Kousec Software, Inc. All rights reserved.
All company names and product names are trademarks of their respective holders.

R7

Table of Contents

INTRODUCTION.....	4
SSL/TLS ENABLED IN EVERY LAYER OF IT SYSTEMS	4
EFFECTIVENESS OF SSL/TLS DEPLOYMENTS	5
PRACTICAL APPROACH TO SECURE SSL/TLS DEPLOYMENT WHILE REDUCING COST.....	6
SUCCESS FACTOR IN DEPLOYING CERTIFICATE MANAGEMENT.....	7
KOUSEC SERVER CERTIFICATE MANAGER.....	7
PRODUCT DEPLOYMENT.....	7
SERVER CERTIFICATE MANAGEMENT CORE COMPONENTS.....	9
<i>Certificate Discovery</i>	9
<i>Certificate Lifecycle Management</i>	10
<i>Monitoring</i>	11
<i>Alerts and Notifications</i>	12
<i>Key Management</i>	12
<i>Built-in Private CA</i>	12
ADMINISTRATION WEB CONSOLE	12
SUPPORT FOR MANAGED SERVER APPLICATIONS AND PLATFORMS	12
INTEGRATION WITH WINDOWS CERTIFICATE SERVICES.....	13
CONCLUSION.....	14

Introduction

Secure network communications with SSL/TLS protocol has become a requirement for IT systems of any size. Unsecure communications and proprietary secure communication technologies are being replaced with SSL/TLS. This trend is growing further as companies and governments are expanding their IT systems into the clouds.

SSL/TLS Enabled in Every Layer of IT Systems

Today, SSL/TLS technology is being deployed in every layer of IT systems. Hardware devices use SSL to protect their management/control communications. Most key components in platforms layer, like operating systems, application platforms, virtualization platforms and middleware, all use SSL as their communication medium to ensure information authenticity and confidentiality.

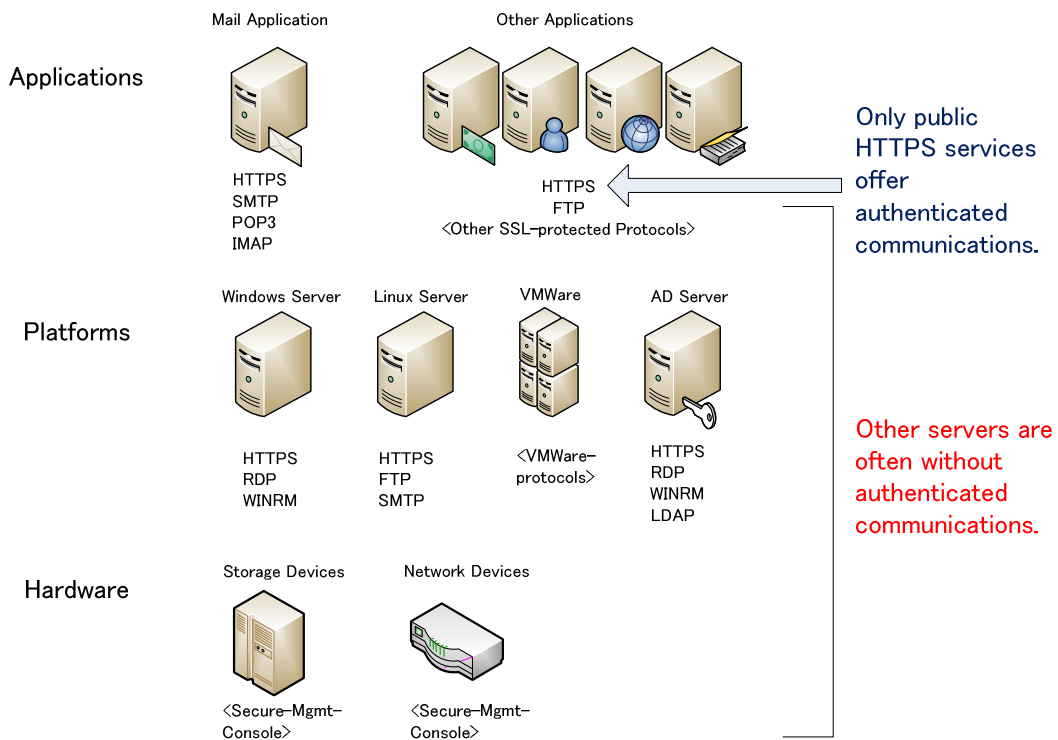


Figure 1. SSL in every layer

Effectiveness of SSL/TLS Deployments

There are two primary security features of SSL/TLS.

- Industry-Proven Encryption Strength
- Authentication of Communication Peers

As the number of SSL-enabled servers grows substantially, however, many SSL deployments fail to attain half of these advantages, or even less. There are several obstacles.

Lack of trusted SSL certificates leads to non-authenticated communication.

SSL-enabled servers are increasing but organizations often obtain trusted SSL certificates only for public HTTPS servers. If a server presents a self-signed or other non-trustworthy certificate to client software (end user or another system), the client cannot be sure that it is communicating with the intended peer. In a typical IT system, the end user or the client computer system then passes user name and password to the server. Without a proper SSL certificate, this is like calling a random number and telling your secret whoever picks up your call.

Example

- Users accessing company email system from a hotel or airport via wireless. Company email servers carry self-signed certificates and users turn off mail server authentication to connect.

Wide use of SSL servers can lead to exposure of private keys.

Compared to encryption keys for disk encryption systems, protection of SSL private keys has been “light”. This is because SSL has to be deployed on many standard servers without HSM (hardware security modules), and frequently relocated and reconfigured to adapt for dynamic business changes. This level of protection poses a serious risk of private keys being leaked outside.

Example

- A hardware upgrade of web servers has been performed without an appropriate secure disk erasure procedure.

Large number of SSL certificates can result in failure of timely renewal.

SSL certificates do expire and with good reasons. Connecting to a backend server having an expired certificate results in persistent connection failure. This in turn can result in a system failure.

Example

- A large ticketing system abruptly started to fail, with only an error diagnosis of “network connection failure”. It turned out to be one of the backend servers with an expired certificate.

Practical Approach to Secure SSL/TLS Deployment while Reducing Cost

To overcome the obstacles mentioned earlier, there must be an appropriate certificate management system in place. A system should include the following capabilities.

Enable certificate administrators to obtain and manage certificates from multiple sources and be able to switch certificate providers as application and/or business requirements change. Using the system, the certificate administrator can start out with certificates from a private CA, replacing install-time self-signed certificates in various applications. Then, as business needs change, he/she can migrate to a commercial CA for a set of public-facing certificates and to the private CA within the company for other certificates. This way, the certificate administrator can put all server certificates under control using the single system.

To mitigate risk of private key leakage, facilitate certificate “rekeying” so that keys can be changed as frequently as necessary.

Private keys should be changed regularly and on any event that poses a leakage risk, regardless of the validity period a certificate has. To realize this, CSR generation and certificate installation in certificate renewals should be automated.

To fully utilize secure and authenticated applications and eliminate system failures due to expired certificates, use a system that continuously monitors corporate network to find unmanaged and expiring certificates.

Without a systematic approach, it is impractical or impossible for certificate administrators and server administrators to track status of all certificates in an organization. Automated, continuous monitoring of managed server certificates and discovery of unmanaged server certificates will be needed to help administrators complete the task.

Simply installing a certificate with multi-year validity period doesn't solve the root

problem because in coming years, the IT system will be reconfigured, relocated, upgraded, or consolidated to accommodate for today's ever-changing business situations.

Success Factor in Deploying Certificate Management

Success factors in deploying certificate management solutions (or any other IT solutions) greatly differ between large organizations and small to mid-sized organizations. Often a large organization, with thousands of servers, employs IT security professionals deploying enterprise PKI systems. On the other hand, many smaller organizations cannot afford a dedicated IT security administrator with full knowledge of PKI.

Those companies do need an appropriate certificate management solution because in many cases their SSL deployment is often left unmanaged due to the complexities of the looks and terminology of PKI.

Choosing a product with ease of use and PKI terminology described in layman's terms is the critical success factor in deploying a certificate management solution.

Kousec Server Certificate Manager

“Server Certificate Management Made Simple”

Kousec Server Certificate Manager is a product that embodies the practical approach to SSL/TLS management. Through its Certificate Discovery and Lifecycle Management features, it helps organizations to realize secure and cost-optimized SSL/TLS infrastructure within an organization.

The product philosophy is centered around ease of use and simplicity. Certificate administrators without much PKI knowledge can deploy it easily and start using it immediately. The product does not try to duplicate the work already done by the existing systems management software in the company.

Product Deployment

Kousec Server Certificate Manager is installed on a computer within the corporate network. It will be the main control center for administrators responsible for

managing server certificates. Certificate administrators can obtain certificate from public CA's, an internal CA (if one exists) or the built-in Private CA and will be able to install certificates and monitor them from the console.

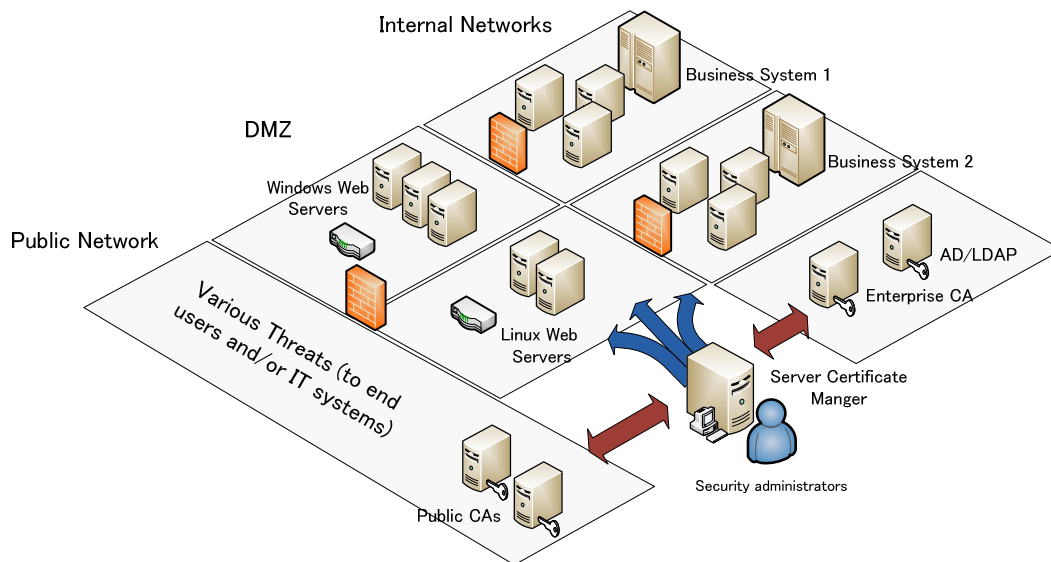


Figure 2. A deployment example

Another deployment scenario is where Server Certificate Manager is installed in a network that is almost disconnected from the networks where managed servers reside. In this case, a website administrator conveys specs for an SSL certificate and the server to the administrator of Server Certificate Manager, who will then provide the certificate in a single-click installer package. This way, a website administrator only needs to run the installer package. The two parties can be separated by business boundaries, for example, certificate reseller and web site owners.

The following figure depicts one example of this scenario.

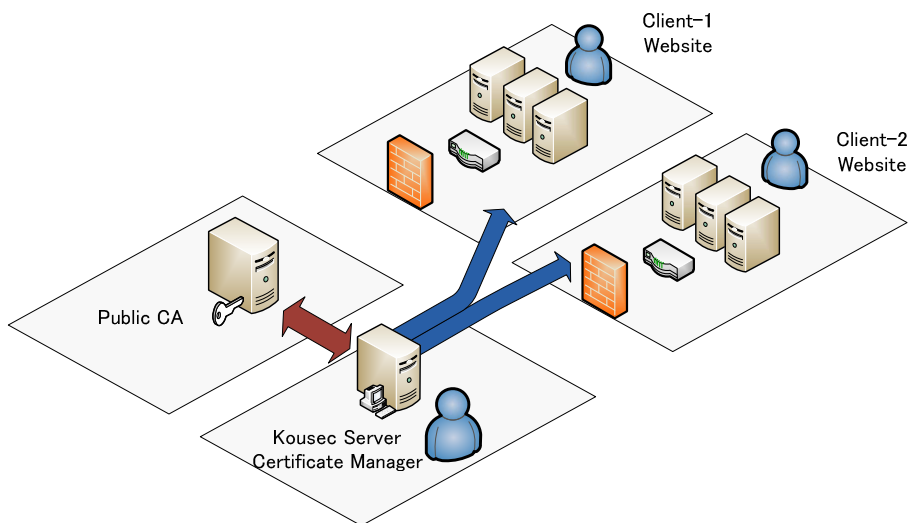


Figure 3. A disconnected deployment

Server Certificate Management Core Components

Core Components in Server Certificate Management provide centralized certificate repository and automated management features as described below.

Certificate Discovery

Certificate Discovery component is used to scan corporate networks to uncover SSL server certificates that are not known to certificate administrators. After finding all certificates, they are validated against trusted certificate policies set in Server Certificate Manager and a report is generated.

Administrators then can decide if the certificate should be brought under the management of Server Certificate Manager and can initiate an import process if so desired.

Certificate Discovery is used as the first step when introducing Server Certificate Manager into the corporate IT system, and should also be used regularly to discover unmanaged certificates that are created at install-time by server applications. The following figure is an example of discovery report.

Discover Certificates - Report

Summary of Server Certificates Found

Out of 14 discovered certificates,
0 are valid certificates,
2 are self-signed certificates,
12 are untrusted certificates,
0 are expired certificates,
0 are revoked certificates.
Analysis Date: 2009/11/18 17:50:09
Trusted Cert Store: CertMgr-Trust-Store
Kousec CertMgr Version: RC-1c

IP Address	Port	Hostname	Port Use	Common Name	Issuer	Validity	Expires	Others
192.168.239.91	21	server1	ftp	www2.example.com	Kousec CertMgr Built-in Private CA	untrusted	2010/10/08	
192.168.239.91	993	server1	imaps	pop.example.com	Kousec CertMgr Built-in Private CA	untrusted	2010/10/08	unsafe-renego
192.168.239.91	587	server1	smtp-submission	smtp.example.com	Kousec CertMgr Built-in Private CA	untrusted	2010/10/08	unsafe-renego
192.168.239.91	995	server1	pop3s	pop.example.com	Kousec CertMgr Built-in Private CA	untrusted	2010/10/08	unsafe-renego
192.168.239.91	636	server1	ldaps	ldap.example.com	Kousec CertMgr Built-in Private CA	untrusted	2010/10/08	
192.168.1.153	3269	WIN2003EN32	msft-gc-ssl	win2003en32.orenosv.com		untrusted untrusted	2010/11/15	
192.168.1.153	636	WIN2003EN32	ldaps	win2003en32.orenosv.com		untrusted untrusted	2010/11/15	
192.168.1.107	902	PC1	vmware-authd	PC1	VMware, Inc.	self-signed	2029/01/11	unsafe-renego
192.168.1.107	8333	PC1	https-vmware	PC1	VMware, Inc.	self-signed	2029/01/11	unsafe-renego
192.168.1.21	3389		ms-wbt-server	win2008jp32base		untrusted untrusted	2010/05/07	

Figure 4. Discovery report

Certificate Lifecycle Management

Once a certificate is imported into Server Certificate Manager, certificate administrators will be able to manage it under Certificate Lifecycle component.

Certificate Enrollment and Renewal: Server Certificate Manager assists certificate administrators in running the process of choosing a certificate product, generating a CSR, placing an order and receiving the certificate. This process, whether for new enrollment or renewal, is called certificate acquisition process in Server Certificate Manager. Certificate Lifecycle Manager forms the foundation for these operations.

With this component, server administrators no longer need to be involved in the request process (to generate a CSR). Also possible is enforcement of certificate policy defined in the company as well as the protected single location of server certificate information and inventory, which is critical to the network and web service

coherency for the company.

Certificate Installation: Once a server certificate is received and stored in Server Certificate Manager, certificate administrators can initiate a certificate deployment process, which will install the certificate on the server, check the operational correctness and register it in certificate monitoring.

Server Certificate Installer selects the best method to install the certificate and the private key as well as any intermediate CA certificates on to the specified server. With this component, certificate installation and operation testing can be fully automated, freeing server administrators from those error-prone operations.

Certificate administrators can choose the level of automation for each server certificate.

- **Fully automated remote installation:** user credentials of the server OS and/or server application need to be registered in Server Certificate Manager.
- **One-click installer:** server administrator receives the certificate installer package and runs it on the server to install the certificate. When a user credential is needed to access the server application, server administrator is prompted to supply the credential. He/she also can control when to install the certificate.
- **Manual installation:** The server administrator receives the certificate package and performs manual installation. This mode is used when the target server application or its configuration needs special treatment by server administrators.

Certificate Retirement: A certificate is retired when superseded by a newer certificate, revoked by the issuing CA, or simply declared as retired when no longer needed. These certificates and their corresponding keys are archived and retained.

Monitoring

Once a server certificate is installed on the server, Server Certificate Manager monitors and validates it at regular intervals. This is to detect such anomalies as certificate that gets overwritten by mistake or non-planned network configuration change.

Alerts and Notifications

Server Certificate Manager raises alerts on important events and notifies concerned parties in the form of email messages and/or SNMP traps. Alerts are raised not only on monitored certificates but also on processes: e.g., certificate enrollment or deployment processes are nearing their deadlines, or renewal process not started when one should have started already.

Key Management

This component generates, stores and protects key pairs used for certificates. It never stores private keys unencrypted on disk and changes encryption password when sending out a private key as part of a certificate install package.

Built-in Private CA

In addition to commercial third-party certification authorities and enterprise CAs within the company, Server Certificate Manager has a built-in private CA capability. This private CA can be readily used during development period. Then as the development winds down, the certificates are migrated to commercial CAs for the production environment. In a company that already deploys Windows Server PKI, this private CA can be part of the PKI CA hierarchy, eliminating the need to deploy another trusted root CA certificate.

Administration Web Console

Administration Web Console is the component that connects certificate administrators with Server Certificate Manager core components. It allows multiple user accounts to be created and user accounts are given two levels of privileges.

Many certificate management screens lead the user with easy-to-follow multi-step flows.

Support for Managed Server Applications and Platforms

Server Certificate Manager supports the following products in the form of automated certificate installer and/or one-click installers. Kousec Software is adding more products to this list based on customer input.

Windows Platform

-
- IIS 6.0, 7.0, 7.5
 - Exchange Server 2003

Linux and Unix platforms

- Apache HTTPD Server
- Mail servers (Postfix, Dovecot)
- FTP servers (vsftpd)

Oracle WebLogic Server 8, 9, 10

Apache Tomcat 4, 5, 6

Sun Java Web Server

VMware ESXi 3.5, 4.0, ESX 4.0, vCenter Server 4.0

Please inquire for current list.

Integration with Windows Certificate Services

Server Certificate Manager can automate requesting certificate issuance to CA's running on Windows Certificate Services (auto-enrollment). This capability allows organizations with already deployed Windows PKI to have the single control over Windows servers and Linux servers.

In addition to Windows CA, Server Certificate Manager also supports Certificate Enrollment Web Service that is introduced in Windows Server 2008 R2.

Conclusion

Kousec Server Certificate Manager enables organizations to be able to attain highly secured systems to meet various privacy regulations and security standards while reducing operations and acquisition costs and well prepare for coming changes in IT systems.

This is made possible with automated certificate discovery, deployment and monitoring as well as optimized selections of SSL certificate providers that suit changing needs.

Many businesses without full-time security administrators will be able to deploy the solution easily. Kousec Software is also prepared to help you to manage SSL certificates in cost effective ways.

For More Information

Kousec Software, Inc.

Tel/Fax: +81-44-833-4666

Email: info@kousec.com

Web: <http://www.kousec.com/>