

Centrally Managing Trust, Security & Compliance in Educational Institutions

Public Key Infrastructure (PKI) CASE STUDY: Education

SSL Certificate Management

Too many SSL Certificates, Not Enough Time

Large, thriving enterprises have more sensitive information on their computers than ever before. Customers and regulations require that the information be simultaneously accessible and secure.

To control information, enterprises use SSL certificates to encrypt data. For small organizations, users or user groups can administer their own certificates. Larger organizations, however, find that with more system endpoints and normal employee turnover, within a few years, administration becomes chaotic.

A University with a continuously expanding number of web-enabled applications, servers and internet/networking arrangements was acquiring hundreds of SSL certificates each year. Multiple IT project leaders were independently sourcing digital certificates for each project or user as the requirement arose. Further, many of these certificates were used to support applications processing financial, personal and business confidential information. Without a simple way to coordinate and manage this critical and dynamic security environment, the University shouldered a costly administrative, digital certificate overhead. Just as important, security management and compliance controls were difficult, if not impossible, to assure. The distributed and ad-hoc approach to digital certificate management was inadvertently negating important security benefits.

Sound familiar?

Comodo has repeatedly found this situation across dozens of leading universities. By helping them to consolidate their SSL certificate administration, Comodo has drastically reduced these costs. Through an easy-to-use and secure web-based interface, Comodo Certificate Manager, these universities achieved significant cost savings with volume discounts that range between 30% and 70% off of retail rates. Comodo Enterprise Certificate Manager also enabled the universities to improve their web application and IT security practices through the advanced certificate lifecycle management, organization and

reporting utilities empowered by this management tool. Each university is now able to self-administer and instantly produce SSL certificates. This ability significantly shortens deployment times, reduces project costs and impresses impatient project leaders faced with critical deadlines.

Besides delivering substantial cost savings to the university, and to program leaders that were now able to afford to fund other critical needs, Comodo Enterprise PKI Manager reduced the administrative burden through its stream-lined SSL certificate and security management process. The rewards to the universities were clear and immediate.

De-Centralized SSL Certificate Management Is a Costly Process

The on-going requirement to deploy and manage SSL certificates creates the need for a solution that must carefully consider internal and external costs, as well as the critical information security and identity protection that's required.

Managing digital certificate requirements on a one-by-one basis may be appropriate for a very small organization having a limited number of SSL security deployments. Managing numerous certificates across multiple departments and geographies, however, is a much more complex and costly challenge. This becomes magnified when decentralized certificate acquisitions eliminate the benefit of volume discounts. Even with modest requirements, volume discounts can be substantial. Further, when certificates are centrally managed the internal administrative costs, security risks and issuance delays are greatly reduced so that all program participants realize significant benefits.

Fortunately, Comodo's Enterprise Public Key Infrastructure (EPKI) Certificate Manager is a web-based solution that enables substantial cost-savings, administrative simplicity, IT security controls, and immediate certificate issuance capabilities that make this an easy and effective decision.

Reducing Internal Management Processes & Costs - A Lifecycle Event

The initial price of the SSL Certificate is not the only cost to consider, especially in organizations with multiple server types, locations and server administrators. Just as important, if not more important, is the elimination of unnecessary and complex tasks that accompany the administration of certificates across an entire organization in a manner that preserves security deployment standards.

A de-centralized approach magnifies management costs by duplicating tasks and resources needed to purchase, acquire and deploy SSL certificates. This activity, including the necessary Certification Authority (CA) validation activities associated with high-trust certificates, can also create delays or obstacles that tend to increase IT security risks. Further, administrative costs must be considered over the term of a certificate's validity period, called the certificate lifecycle, and not just those incurred during acquisition and deployment.

The life cycle of an SSL certificate requires six stages:

- **Order** – application to purchase an SSL certificate. Includes submission of the organization's eligibility and administrative data
- **Approve** – Certificate Authority (CA) verifies the organization's eligibility, and grants approval for the certificate order request
- **Reject** – Administrative (CA) rejects a certificate order request if not organizationally validated or trusted
- **Issue** – CA issues the certificate, enabling requestor to install it on a designated server or device so as to enable server identity verification and SSL communication services
- **Revoke** – Administrative revocation of a certificate due to expiration of requirement or validity period
- **Renew** – Redefines certificate validation (expiration) date. Ensures that each certificate is properly renewed with the CA in a timely manner

As you might guess, attempting to individually manage a multitude of certificates becomes tedious, time consuming, error-prone and often overwhelming - especially in large, distributed organizations. As a result, the total cost of an SSL Certificate acquired in a de-centralized manner becomes much higher than the initial purchase price. Errors in the certificate life cycle can present security risks to un-managed, complex services.

Fully Managed Certification Authority Operations

Comodo operates the backend Certification Authority used to issue the SSL and Corporate Secure Email Certificates, including high availability secure redundant server systems, high speed FIPS 140-1 Level 4 signing devices, backup and customer support. All Certificates issued through the EPKI Manager are fully supported by Comodo's industry leading customer support department.

For additional information on Comodo – Creating Trust Online™ : <http://www.comodo.com/corporate/ops.html>.

Comodo EPKI - Certificate Manager

Instant security for your web operations, internal and external networks and email.

Comodo Certificate Manager is a core component of Comodo's Identity, Trust and Security portfolio that provides a flexible and scalable system for digital certificate issuance and lifecycle management. Establishing the trust carried by certificates and managing the use of certificate keys is critical to the proper deployment and security of web-enabled applications and other network transactions. By automating and centralizing the management of cryptographic keys and digital certificates, Certificate Manager is designed to allow organizations to more easily deploy and scale the security of their applications and e-business services.

Comodo's EPKI Certificate Manager enables instant security for your web operations, internal and external networks and email, giving you full access to a Certificate Authority platform for all digital certificate requirements.

- Easy to use web-based console
- High quality, fully trusted SSL Certificates
- Secure Email Certificates are issued quickly to employees and partners
- Easy creation, management and assignment of specific user issuance and reporting permissions
- Savings on standard Certificate buy prices
- No extra software / hardware required
- Full reporting
- Full/ Certificate lifecycle management

With Comodo's hosted solution and CA infrastructure that's WebTrust Certified by KPMG there's no need for you to invest in expensive hardware, software or Certificate Authority expertise. Certificates can be immediately issued through the web console, enabling web servers, users and other networked applications to be secured in minutes rather than days. Additionally, Certificate Manager can automate the enrollment process for issuing and digitally signing end-user (client authentication / email) certificates.

Secure Email

The need for secure, confidential and integral email is a growing concern for almost every organization. Comodo Corporate Secure Email Certificates address this critical problem and provide the ability to secure and digitally sign email and attachments using any popular mail client. The EPKI Manager provides convenient and secure access to your own web-based console to administer your Corporate Secure Email Certificates.

Comodo Certificate Manager is also designed to manage the lifecycle of secure email certificates for use with S/MIME-compatible messaging applications, enabling end users to encrypt and digitally sign important communications including attachments so that only intended recipients can access the message.

Comodo is among a select few Certificate Authorities certified to support Microsoft® Exchange Server 2007 and Office Communications Server 2007 with its Unified Communications certificates supporting the multiple application services embedded within these Microsoft® products. These offerings fully ensure the identity, authenticity, confidentiality and integrity of information being exchanged across a unified communications environment.

Secure your intranets, extranets & websites

SSL Certificates are the industry-standard technology used to secure communications between browsers and web servers, whether via the Internet or internally through intranet or extranets. Some organizations require multiple SSL Certificates to secure multiple servers, spanning intranets, extranets, web server operations and load balancing. To meet the needs of your organization, the EPKI Manager allows you to procure all of Comodo's Internet Trust, Identity and SSL Certificates on demand, as well as to provision Comodo's Network Scanning service to perform comprehensive evaluations and reports on the effectiveness of your IP perimeter defense system(s).

Assure customers and partners of your identity

Assuring customers of your identity is an essential factor for successful online business. Certificates issued through the EPKI Manager help assure customers of your online and email identity, leading to a higher confidence in who you are. Through the user-friendly interface you can issue digital certificates to web servers, internal servers, employees and partners, certificates that in turn represent the identities and credentials of their owner. The EPKI Manager helps you achieve trust and confidence within an environment where trust and confidence is essential yet currently unavailable.

Comodo Multifactor Authentication

Secure end-user account access and applications to prevent personal information losses, phishing attacks and brute-force password threats.

Comodo offers a Multi-Factor Authentication (MFA) solution to augment PKI-based security practices. MFA provides a flexible, cost-effective and simplified means to deploy a more secure and trusted user authentication service. Comodo's solution both supplements and significantly secures simple, password-enabled applications and account access processes. It works by always maintaining a "something you know with something you have" authentication rule...WITHOUT costly physical "tokens". Unlike other services that require the use of expensive physical tokens, Comodo provides users with a client digital certificate that is automatically installed on their machine, or machines.

If the user endeavors to access the desired network through a machine other than their own, the network will not detect the necessary certificate. Comodo's solution maintains the multi-factor authentication scheme by creating single-use passwords delivered via SMS messaging, voice message, pre-stored e-mail address and/or personal security questions. This flexibility provides maximum policy compliance, simplicity. The ease of this solution satisfies both end users and administrators.

PCI Compliance Reporting Solution

Comodo has built a customizable PCI compliance reporting solution to centrally manage an enterprise compliance effort. Improve your transparency internally, and report back to your merchant bank easier with a central reporting console. Comodo has built this system to appeal to both the compliance manager and the responsibility unit endpoints.

All endpoints go through the PCI Compliance Wizard, an annual PCI self-assessment questionnaire, and are provided with a customized remediation plan for meeting PCI compliance standards. The responsibility units follow the plan and check off remediation items or change their answers to receive a new remediation plan to continually manage their compliance. Comodo provides many security solutions to meet PCI requirements that are identified through the compliance wizard. All responsibility units are reported back to the compliance manager via the centralized reporting console. From here, the compliance manager can identify areas of weakness and overall compliance to take corrective action. Multiple views allow the compliance manager to drill down to the amount of detail needed to make informed decisions.

Endpoint Security Manager

In addition to the wide array of products Comodo offers, it is best known for its award-winning firewall and a host of other innovative desktop security products. These products are now available to be centrally-managed and administered, protecting your workforce with the significant cost savings associated with having the ability to deploy products such as Comodo Internet Security, Comodo Disk Encryption, Comodo DiskShield, and much more. This ability to centrally manage policies not only saves countless hours on behalf of the system administrator, it saves money.

As networks and the regulations governing them grow more complex, large enterprises are devoting more time and money to securing their data. Comodo's Enterprise Web Solutions can help organizations like yours simplify their SSL and endpoint security needs, freeing them up to concentrate on what they do best.

About Comodo

Comodo is a leading global provider of Identity and Trust Assurance services on the Internet. Comodo offers a comprehensive array of PKI Digital Certificates, eCommerce Acceleration and Infrastructure Security solutions including Enterprise Endpoint Security software, User Access Authentication (Two-Factor / Multi-Factor), Network Vulnerability Scanning and PCI compliance services.

Continual innovation, a core competence in PKI, and a commitment to reversing the growth of Internet-crime distinguish the Comodo companies as vital players in the Internet's ongoing development. Comodo secures and authenticates online transactions and communications for over 200,000 business customers and 3,000,000 users of our desktop security products.

Located in Jersey City, NJ with offices in the UK, Ukraine, China, Romania and India, the company offers businesses and consumers the intelligent security, authentication and assurance services necessary to ensure trust in online transactions.

As a leading Certification Authority, and in combination with the Digital Trust Lab (DTL), Comodo offers enterprises reliable, third generation solutions that improve customer relationships, enhance customer trust and create efficiencies across digital ecommerce operations.

Comodo Group, Inc.

525 Washington Blvd.
Jersey City, NJ 07310
United States

Tel: +1.888.256.2608
Tel: +1.703.637.9361
Fax: +1.201.963.9003

Email: EnterpriseSolutions@Comodo.com

Comodo CA Limited

3rd Floor, 26 Office Village, Exchange Quay
Trafford Road, Salford, Manchester M5 3EQ
United Kingdom

Tel: +44 (0) 161 874 7070
Fax: +44 (0) 161 877 1767

For additional information on Comodo - visit <http://www.enterprise.comodo.com/>