COMODO

WHITE PAPER

Comodo Certificate Manager
Advanced certificate issuance and lifecycle management

Why SSL Certificates?

SSL certificates play a vital role in nearly all online transactions, ensuring a secure, trusted connection between a given browser and a given website. Ensuring the safe transmission of data, login information, and other key Internet-facilitated functionality, SSL certificates provide the foundation for online trust, and provide the foundation for online banking, shopping and bill-paying that have become so ingrained into 21st century life.

The foundation for SSL-based security is encryption, an extremely reliable process when properly configured, but which can suffer from dangerous vulnerabilities if not effectively implemented or managed correctly. In fact, business security is too often compromised by a lack of automated certificate management tools. Attempts to manually track and monitor multiple certificates from various vendors will almost always result in error and mismanagement, leading to missed renewals and expired certificates, which, in turn, generally lead to insecure connections, lack of trust, and a tarnished brand, among other problems.

Comodo Certificate Manager is a robust, centralized certificate management solution designed to provide enterprise clients with a secure, reliable and consistent structure for the entire certificate lifespan, featuring streamlined but powerful tracking, management and compliance functionality for all of their SSL/PKI needs.

Effective enterprise certificate management protects against data breaches, failed audits and costly unplanned downtime. Just one expired certificate can lead to major outages, potentially costing tens of thousands of dollars to remediate, and damaging brand integrity.

Why Comodo?

Comodo Certificate Manager, developed in partnership with several Fortune 500 companies, consistently and securely manages large volumes of digital certificates of all types and signature algorithms (SSL, ECC, RSA); CCM is the solution to these common – and potentially extremely costly – enterprise challenges.

Created by the world leader in SSL Certificates, Comodo Certificate Manager is an industry-leading, fully integrated automated enterprise solution designed to simplify digital certificate issuance and lifecycle management. Through its advanced capabilities, CCM provides businesses the ability to self-administer, instantly provision, and control all SSL certificates throughout their organization. Comodo leads the SSL certificate industry as an originator of the Certificate Authority/Browser (CA/B) Forum, a consortium of CAs and Internet browser providers that develop guidelines to govern the issuance and management of CAs. Comodo has been a pioneer in certificate management since the founding of the CA/B Forum in 2005 and issues more certificates than anyone else on earth, having surpassed Symantec (Verisign) in February, 2015, and has widened its lead over their nearest competitor by over 10% since then, currently holding over 40% of market share.

Comodo Streamlines Auto Discovery

CCM's Auto Discovery feature simplifies the formerly arduous and error-prone manual discovery process. Rather than logging into various vendor portals to monitor each certificate's lifecycle, and manually collecting detailed information on SSL certificates purchased at different times from different CAs, Comodo Certificate Manager automates the process. After conducting a comprehensive scan of external (as well as internal) networks to discover every certificate regardless of the issuer, CCM automatically imports all relevant information, bringing the entire certificate inventory under central control and offering a comprehensive view of all certificates. CCM's Auto Discovery feature provides vital details about each certificate, including:

- The location of each SSL certificate (on both internal and external networks)
- The name of the CA that issued each SSL certificate
- The date each SSL certificate is set to expire
- Whether any certificates have weak keys (as of January 2014, keys must be 2048 bit or higher)
- Scheduling scans to run on a recurring basis.
- Providing the Signature Algorithm used to sign the certificate
- Identifying what ciphers are supported on the targets

"Since installing the Comodo Certificate Manager solution, it has become a major part of our IT management infrastructure, allowing us to update, add and delete thousands of digital certificates with a streamlined dashboard and email alert system."

~ Craig Hurter, IT Security Manager, University of Colorado at Boulder

Internal Certificate Authorities

When we boil down all the use cases it really comes down to two possible scenarios: certificates issued by an Internal Certificate Authority such as Microsoft Certificate Services and those issued by publicly trusted CAs, such as Comodo. With the ever-increasing need to issue more certificates due to mobile devices, email, and IoT, more companies are choosing internally signed certificates authorities such as Microsoft Certificate Services for internal applications. While this reduces the need to purchase publicly trusted certificates, all of these certificates still need to be managed. CCM's Active Directory controller works as a proxy between the Comodo CA and Microsoft Active Directory. This direct integration ensures automated discovery and management of certificates issued by Microsoft Certificated Services. CCM will scan a Microsoft Active Directory environment to discover every certificate regardless of type. CCM then classify them based upon their Extended Key Usage (EKU) and imports them into a temporary staging area where administrators can more easily manage them.

WebTrust Certification

CCM is a proven, well-regarded and thoroughly trusted global solution for enterprise certificate management. Comodo's CA infrastructure is WebTrust certified by Ernst & Young. CCM creates an efficient, productive and secure business environment that allows organizations to issue SSL certificates for use within internal and external networks, websites, and email systems.

Quick, Easy and Cost-Effective
CCM offers scaled discounts on Comodo's already low SSL certificate pricing, enabling quick, easy and cost-effective fulfillment of multiple certificate requirements for distributed systems, email and devices.

Fast, Customer-Focused Rollout
CCM's Software-as-a-Service (SaaS) architecture enables PKI management within hours. CCM significantly reduces administrative obstacles and time delays. SSL certificates can be issued immediately through a secure web console, thus enabling network servers, users, applications, objects and devices to be secured quickly. CCM also automates the enrollment process for requesting and issuing SSL, client authentication, code signing and S/MIME certificates.

Multiple Administrative Tiers
CCM provides 3 layers of delegated administration. This enables very granular user management, enabling a master administrator to assign specific permissions to various personnel across the org chart. Business sectors can be delegated in such a way that the certificate asset management of a particular department, network, domain or subdomain can be assigned in whatever way is most beneficial to the organization, even to a specific person.

Maximize Certificate Management with Minimal Resource Expenditure
Comodo safeguards businesses against the interruptions associated with manual CA management. CCM discovers all certificates in the trust chain (root, intermediate and end-entity) and provides details of each individual certificate including its issuing authority and expiration date. In addition, the "Important Messages" panel displays any certificate or server vulnerabilities.

Automatic Installation and Renewal
CCM provides administrators the ability to manage and schedule automatic renewal and installation of certificates. Administrators install an agent where the certificate is installed. This agent monitors the certificate and at renewal time, generates a private key and certificate signing request. This request is submitted to CCM. Once the domain is validated, the certificate is issued and the agent downloads and installs it automatically. This set-and-forget functionality applies to all certificate types, including multi domain and wildcard certificates*.

Device Certificates
While the majority of companies now support BYOD in the workplace, few have been able to effectively manage the phenomenon, especially the need for so many new certificates, new security measures and necessary network improvements. Additional concerns are time to implementation and the costs of monitoring many devices. With the introduction of Comodo Mobile Certificates (CMCs), enterprises can now authenticate users requiring access to internal networks from smartphones and tablets. CMCs offer the fastest, most secure method for securing BYOD connectivity without the cost and complexity of installing agent software on employee mobile devices. CCM also provides an API to access and use CCM as a Simple Certificate Enrollment Protocol (SCEP) server. *

Features

Certificate Lifecycle Administration
Extensive portfolio of SSL, Code-Signing, S/MIME and client authentication certificates allowing for the rapid enrollment, approval, issuance, revocation and renewal of all certificates.

Automatic Scheduled Renewal and Installation*
Provides scheduled revalidation and installation of critical certificates; this set-and-forget functionality ensures that users never receive an expired certificate error and applies to all certificate types.

Internal and External Discovery Scanning - Administrators can track and see all the details of each certificate purchased from different vendors.

Secure, Multi-Tiered Administrative Web Interface - Flexible organizational alignment of administrative domains that easily adjusts to your business model.

Configurable Email Notifications - Allows the administrator to be notified about requests, approvals, expirations or revocations and enables certificate owners and administrators to receive expiration notices in advance.

Same-Day Expirations - Administrators control the term and expiration of all issued certificates.

Dashboard - Provides one common, intuitive dashboard to view.

Reporting - Produce detailed reports, certificate and administrative status, and activity logs.

Client Key Management Services - Escrow and recovery of private keys enable a protected (policy-driven) restoration of user encrypted data.

Automatic Deployment with Microsoft Active Directory or CSV File Upload - Rapid client certificate distribution and management achieving tight integration with a variety of directory-based employee/device management systems.

Automatic CSR Generation and Private Key Management - Escrow and recovery of private keys for SSL certificates in a secure and redundant way simplifying key management and protecting certificate assets from human error and data loss.

Device Certificates* - With the introduction of Comodo Mobile Certificates (CMCs), enterprises can now authenticate users who require access to internal networks from smartphones and tablets.

API Access* – Allows organizations with other device management and reporting solutions to access elements of CCM.

Self-Enrollment Web Interface – Provides a secure self-service workflow for SSL or client certificates, enabling easy certificate enrollment and distribution.

Customized Web Interfaces - Can be customized with your corporate logo and images to help maintain your brand identity.

Reliable OCSP - Comodo real-time Online Certificate Status Protocol (OCSP) is distributed worldwide to maintain high availability.

Code Signing on Demand – Rapid code-signing service lets enterprises give their development teams a centrally managed platform to sign their code. This allows them to manage which users can sign code, what code has been signed, and which code-signing certificate was used to sign it, as well as the status of those code-signing certificates. This can be done on premises or via the cloud.

Two-Factor Authentication and/or IP Address Validation - Highly secure administrative account access protection.

Private CA – CCM's 'Private CA' feature allows companies to seamlessly and expertly issue and manage privately trusted certificates without any of the usual associated setup and management costs, on premises or in the cloud.

Assured Compliance – Comodo will automatically keep Private CAs in compliance with any changes to certificate regulations.

Web Service API's- API's are available for the enrollment, renewal and revocation of SSL and Client Certificates.

Quick Implementation and Setup – Featuring fast and efficient auto enrollment and auto installation.

About Comodo

The Comodo organization is a global innovator of cybersecurity solutions, protecting critical information across the digital landscape. Building on its unique position as the world's largest certificate authority, Comodo authenticates, validates and secures networks and infrastructures from individuals, to mid-sized companies, to the world's largest enterprises. Comodo provides complete end-to-end security solutions across the boundary, internal network and endpoint with innovative technologies solving the most advanced malware threats, both known and unknown. With global headquarters in New Jersey and branch offices in Silicon Valley, Comodo has 12 international offices across Europe and Asia.

*Features available in CCM 6.5 release