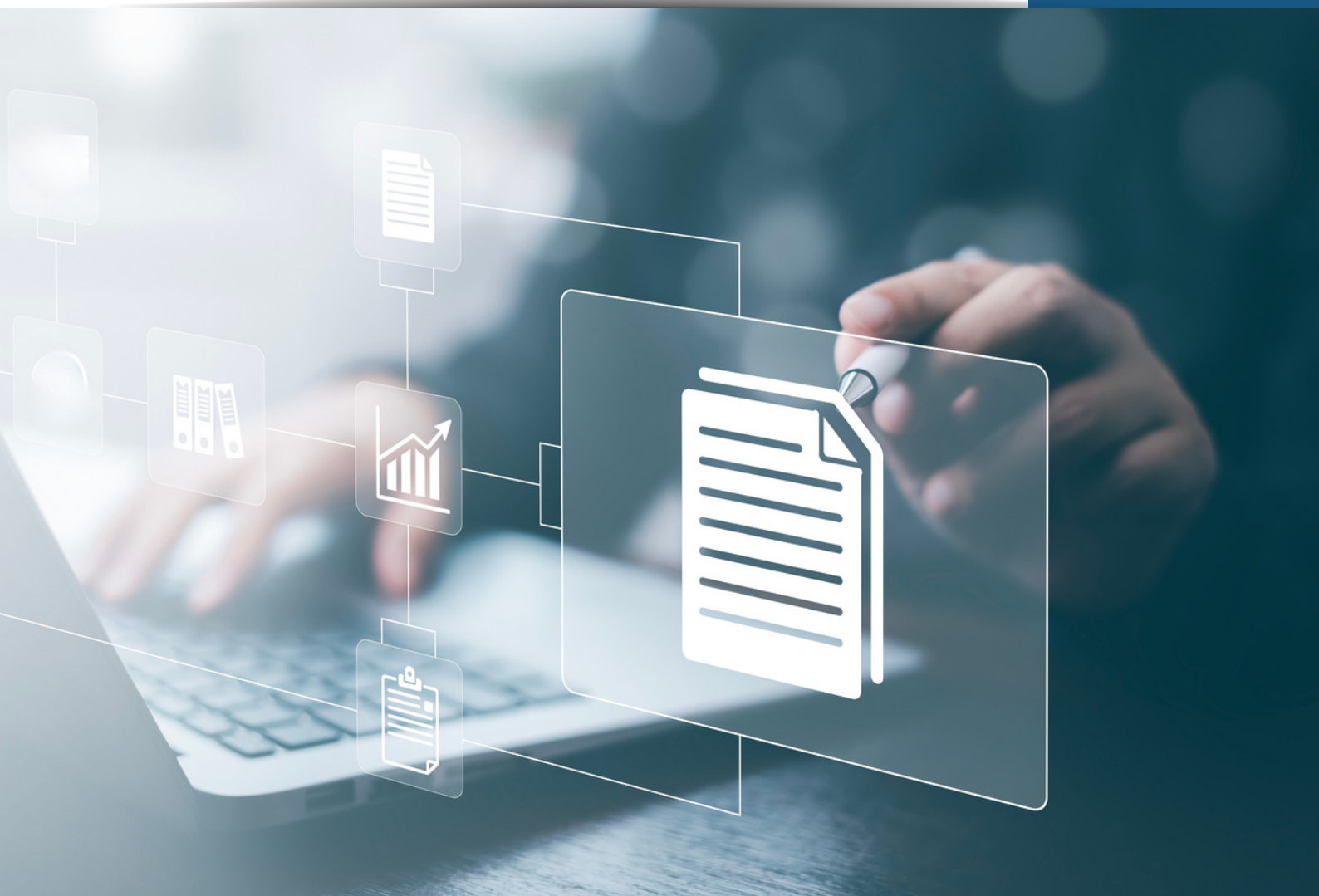




Certificate Lifecycle Management System



www.comsigntrust.com

Managing the digital certificates of the organization is a challenging mission:



Inactivity of services
and systems



Inability to manage
existing certificates
and their status



Utilizing manual
processes that result
in issues

**CertM performs an automatic scanning process
that updates the validity of all certificates
through a central PKI management system.**

The central management system addresses challenges such as:

- Using digital processes instead of error-prone manual processes.
- Digital certificates
- Detecting and viewing existing certificates and their status
- Maintenance optimization and efficiency
- Centralized system for managing PKI infrastructures
- Automation throughout certificate lifecycles
- Automatic certificate renewal
- Certificate expiration alerts
- Integration with international CA providers and organizational CA

Functionality

Monitoring and Alerts

- Reports and statistics
 - Filtering and screening to generate reports based on required criteria
 - Certificate expiration alerts and warnings, to facilitate timely action
 - Logs collected by monitoring systems through SNMP/SYSLOG
-

Interfaces

- System is On-Prem
 - Integrates with several CAs, organizational CA services (supports MSCA/EJBCA), external CA services (DigiCert), third-party systems, HSM components (given CSP), AD, data security and monitoring systems, external DB
-

Central Management

- Easy-to-use and Intuitive Control Screen (WEB) for management
 - Issues various digital certificates such as SSL, Authentication, etc.
 - Digital certificate creation, configuration, signing, and issuance
 - Display of all network certificates, with advanced filtering options
 - Automatic certificate renewal close to the expiration date (configurable)
 - Alerts to system manager regarding expiring certificates
 - Revocation/suspension of digital certificates
 - Certificate display/download
 - Full resilience
-

CA and Network Scanning

- Network scanning and status display of all existing digital certificates (including IIS, Apache, F5, Imperva etc.)
- Verification of certificates installed on system-linked CAs
- Automatic search for certificates installed on the organizational network
- Direct scanning via an Enrollment Agent
- Certificates catalogued by the components in which they are embedded: protocols, IP addresses, ports, URLs, and more

Functionality

Automation

- Automatic digital certificate renewal
- Certificate expiration alerts
- Automated action configuration via API

Display

- All the organization's digital certificates centralized on a single screen
- Comprehensive display of all existing digital certificates on the network and CAs
- Current status of every digital certificate throughout its lifecycle

Management and Monitoring

- Digital certificate lifecycle management
- Search/filter/sort based on required criteria
- Revocation/suspension of digital certificates
- Manual/automated management

Reporting

- Digital certificate filtering by CA
- Filtering based on protocols/ports/devices and more
- Reports and statistics
- Alerts and warnings

CA and Network Scanning

- Network and CA scanning to detect all network digital certificates (SSL/TLS, SSH, Mobile, Kubernetes, WiFi & VPN)
- Direct scanning via an Enrolment Agent
- Integrating with Private/Public CAs
- API for interfacing with Third-Party systems
- Integrating with AD

Cert M System Advantages

Reduced costs and operating times



CONTACT US



www.comsigntrust.com



*8770



info@comsigntrust.com



[Comsigntrust](#)