

keyon true-Xtender

Die keyon true-Xtender Suite für Enterprise PKI bietet eine umfassende Lösung für die Ausstellung und Verwaltung von X.509-Zertifikaten.

Die keyon true-Xtender Suite von SITS ist eine umfassende Sammlung von Services und Anwendungen, die Benutzerfreundlichkeit mit zusätzlicher Flexibilität bietet. Funktionen für das manuelle und automatisierte Management von Zertifikaten ermöglichen Krypto-Agilität, um die Anpassungsfähigkeit an sich entwickelnde kryptografische Standards zu gewährleisten.

Unsere Lösung für Ihr Zertifikatsmanagement

Module und Funktionen:

- true-Xtender **Policy Module** erweitert die Funktionen von Microsoft ADCS
- true-Xtender **RA Web Application** ermöglicht die nahtlose Integration des Zertifikatsmanagements
- true-Xtender **RA ACME Service** stellt das ACME-Protokoll bereit
- true-Xtender **RA Enrollment Server** stellt das CMPv2- und das EST-Protokoll bereit
- true-Xtender **RA Web Service Add-on** bietet umfangreiche REST- und/oder SOAP-Schnittstellen
- true-Xtender **RA DCOM Add-on** ermöglicht als DCOM-Schnittstelle die strukturübergreifende Ausstellung und Sperrung von Zertifikaten
- true-Xtender **Third-Party Certificate Manager Add-on** wird zur Überwachung von Third-Party-Zertifikaten verwendet
- true-Xtender **Discovery** ermöglicht eine umfassende Erkennung und Inventarisierung von Zertifikaten
- true-Xtender **PKI Services** bieten zusätzliche unterstützende Funktionen für das Lifecycle-Management von Zertifikaten
- **true-CA** ist eine eigenständige, mandantenfähige Zertifizierungsstelle
- Der **Revocation Provider** stellt sicher, dass CRLs und OCSP-Antworten von einer Zertifizierungsstelle nach einer konfigurierbaren Zeit neu geladen werden
- true-Xtender **AutoEnroll PKI** erweitert die Microsoft-Funktion für die automatische Verteilung von S\MIME Zertifikaten inklusive Archivierung und Wiederherstellung der Schlüssel.



Ihre Vorteile mit SITS:

- **Vertrauen**: Weltweit anerkannte Lösungen, die Vertrauen schaffen und die Digitalisierung fördern.
- **Maßgeschneiderte Beratung**: Individuelle Beratung und Lösungsfindung nach Ihren spezifischen Anforderungen.
- **Umfassender Service:** Von der Beratung bis zur SaaS-Lösung – wir bieten das Komplettpaket.
- **Nahtlose Integration**: Unterstützung bei der Anbindung an Fachanwendungen und der Integration in bestehende Systeme.
- **Erfahrung:** Jahrzehntelange Erfahrung im Bereich der Public Key Infrastruktur garantiert Professionalität und Datenschutz.

WEITERE INFOS

Swiss IT Security AG – SITS
www.sits.com
info@sits.ch

keyon true-Xtender Registration Authority

RA-WA

true-Xtender RA-Webanwendung

Die true-Xtender Registration Authority Webanwendung ermöglicht die nahtlose Integration des Zertifikatsmanagements in die unternehmensinternen Prozesse und bietet neben einer browserbasierten Oberfläche mehrere Enrollment-Protokolle (ACME, CMPv2, EST), sowie eine Webservice-Schnittstelle für automatisierte Prozesse.

Unternehmensspezifische Verwaltungsprozesse können über Metadaten implementiert werden, die zusätzlich in der Datenbank der Registrierungsbehörde (RA) gespeichert werden. Zertifikate können beispielsweise Anwendungen, Einzelpersonen oder Gruppen zugeordnet werden, die im Falle eines Erneuerungsprozesses, einer Sperrung oder anderer Aktivitäten benachrichtigt werden.

In einem umfangreichen Audit-Protokoll werden alle Aktivitäten der Bewerber und der Administratoren gespeichert. Die Berechtigungen für die einzelnen Features werden nach erfolgreicher Authentifizierung auf Basis von Kerberos oder OIDC/OAuth2 durch eine rollenbasierte Zugriffskontrolle gesteuert.

Die RA speichert alle Daten in einer Microsoft SQL-Datenbank. Auswertungen und Berichte können mit Microsoft SQL Server Reporting Services (SSRS) oder Microsoft Power BI erstellt werden.

Die RA unterstützt unterschiedliche Workflows, die für jeden Zertifikatstyp definiert werden können.

Funktionen der RA-Webanwendung

- Einfache und erweiterte **Suche nach Zertifikaten**
- Ausstellen von Zertifikaten auf Basis von **PKCS#10-Dateien**
- Ausgabe von Schlüsselpaaren und Zertifikaten als **PKCS#12-Dateien**
- **Bereitstellen von Zertifikaten über verschiedene Kanäle** (E-Mail, webbasierter Download)
- Sicherheitskritische Merkmale können durch **Workflow-Management** abgebildet werden (Vier-Augen-Prinzip)
- **Revozierung** von Zertifikaten
- **Erneuerung** von Zertifikaten
- **Überwachung auf ablaufende Zertifikate**
- **Multi-CA Unterstützung** (SwissSign, DigiCert, GlobalSign, Telekom, etc.)

RA-ACME+

true-Xtender RA ACME-Service

Der ACME-Service der true-Xtender Registration Authority stellt das ACME-Protokoll als standardisierte Schnittstelle für das automatisierte Zertifikatsmanagement bereit.

Der RA-ACME Service ist in die RA-Datenbank und deren Benutzeroberfläche integriert. Der RA-ACME Service ist als Proxy-Server-Architektur implementiert, die die Verwendung von ACME in separaten Netzwerkzonen ermöglicht. Mehrere ACME-Adapter fungieren als Proxy zwischen den Registrierungsclients und der RA oder dem RA-ACME-Dienst. Die ACME-Adapter führen die Validierung der Domänen durch.

Die Adapter unterstützen das ACMEv2-Protokoll mit http-01- und dns-01-Validierung (gemäß RFC 8555). Verschiedene Zertifikatprofile werden für verschiedene Domänen unterstützt, indem unterschiedliche Endpunkte in der Dienst-URL der Adapter verwendet werden. Die Adapter sind für Windows- und Linux-Systeme verfügbar.

RA-CMP+, RA-EST+

true-Xtender RA-Enrollmentserver

Der true-Xtender Registration Authority-Enrollmentserver stellt das CMPv2- und das EST-Protokoll als standardisierte Schnittstelle für das automatisierte Zertifikatsmanagement bereit.

Der Registrierungsserver ist als Proxyserverarchitektur implementiert, die die Verwendung von CMPv2 und EST in separaten Netzwerkzonen ermöglicht.

RA-WS+

true-Xtender RA Web Service Add-on

Das true-Xtender Registration Authority Web Service Add-on bietet umfangreiche REST- und/oder SOAP-Schnittstellen für die automatisierte Ausstellung und Verwaltung von X.509-Zertifikaten.

Ein Enrollment-Client authentifiziert sich gegenüber dem Web-Service und erhält auf Basis des entsprechenden Rollenkonzepts die entsprechenden Berechtigungen für die einzelnen Features:

- Ausstellung von Zertifikaten auf der Grundlage von PKCS#10-Dateien
- Ausgabe von Schlüsselpaaren und Zertifikaten als PKCS#12
- Erhalt ausgestellter Zertifikate
- Widerruf von Zertifikaten und
- Erneuerung von Zertifikaten
- Konfiguration des Zertifikatprofils und der Rolle

RA-DCOM+

true-Xtender RA DCOM Add-on

Das true-Xtender Registration Authority DCOM-Add-on ermöglicht als DCOM-Schnittstelle die gesamtstrukturübergreifende Ausstellung und Sperrung von Zertifikaten.

In einer DMZ ist z. B. nur das RA-DCOM-Add-on erforderlich, anstatt eine separate Microsoft-Zertifizierungsstelle, um Zertifikate von der Unternehmenszertifizierungsstelle auszustellen. Darüber hinaus dient das Modul als Proxy für eine Microsoft CA, um den direkten Zugriff auf die CA für alle Client-Systeme zu verhindern.

RA-CM-3RD+

true-Xtender 3rd-Party Certificate Manager

Das true-Xtender Third Party Certificate Manager Add-on wird zur Überwachung von Zertifikaten von Drittanbietern verwendet. Es können mehrere Benachrichtigungsdienste eingerichtet werden, die einen Benutzer benachrichtigen, sobald ein Zertifikat das Ende seiner Lebensdauer erreicht hat.

Zu überwachende Zertifikate werden über die Web-GUI oder die Webservice-Schnittstelle in die RA-Datenbank importiert. Mit dem Upload können zusätzliche Metadaten bereitgestellt werden, die dann in den Benachrichtigungen verwendet werden können, bevor die Zertifikate ablaufen.

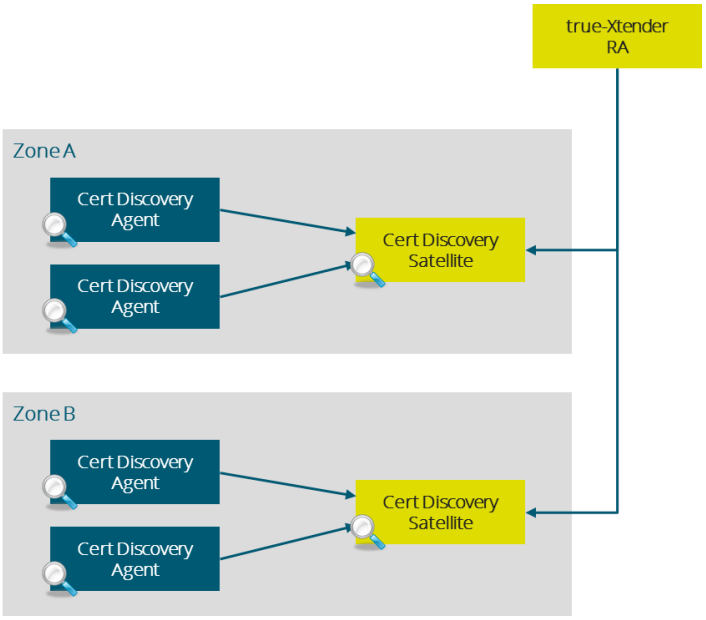
Policies und Discovery

Erkennung von Zertifikaten

true-Xtender Discovery

Das true-Xtender Discovery Modul ermöglicht die umfassende Erkennung und Inventarisierung von Zertifikaten innerhalb der IT-Umgebung

Verschiedene Suchmethoden können an spezifische Anforderungen angepasst werden und ermöglichen so eine effiziente Erkennung von Zertifikaten. Die gefundenen Zertifikate werden in die true-Xtender RA importiert. Das daraus resultierende Monitoring erhöht sowohl die Sicherheit als auch die Betriebssicherheit von IT-Systemen.



Fernerkundung über Satelliten:

- Verwendet sogenannte Satelliten, um Zertifikate durch Remote Port Scanning zu lokalisieren.
- Unterstützt die Protokolle SSL/TLS und StartTLS (FTP/SMTP/POP3/IMAP).
- Pv4- und IPv6-Unterstützung.
- Konfigurierbare Adressbereiche (IP-Bereiche, IP-Subnetze, Hostnamen).
- Konfigurierbare Portbereiche.

Der Satellit sammelt Scan-Ergebnisse von den sogenannten Agenten. Der true-Xtender Discovery Agent wird als einzelne ausführbare Binärdatei auf Zielsystemen (Windows, Linux, MacOS) bereitgestellt, um lokale Zertifikatssuchen durchzuführen.

Lokale Erkennung durch Agenten:

- Lokale Port-Scans
- Lokaler Datei-Scan
- Scan des lokalen Zertifikatspeichers

Die Agenten werden von den Satelliten verwaltet und erhalten von diesen ihre Konfiguration.

TX-PMSA

true-Xtender Policy-Modul

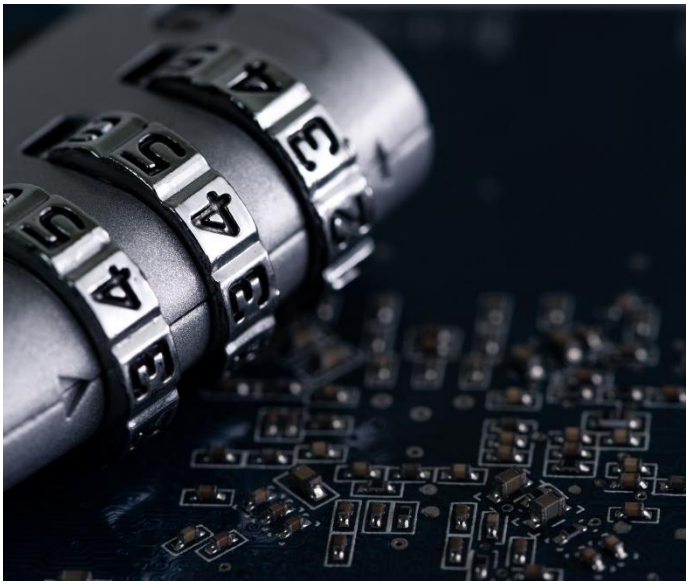
Das true-Xtender Policy Modul erweitert die Funktionen der Microsoft ADCS-basierten Enterprise PKI und ermöglicht eine regelbasierte Ausstellung und Verwaltung von X.509-Zertifikaten.

Der Inhalt des Zertifikats kann erheblich erweitert oder geändert werden.

Beispiele für Richtlinien

- Die einzelnen Komponenten des Subject Distinguished Name (DN) können definiert, aus der ursprünglichen Zertifikatsanwendung übernommen oder durch eine beliebige Regel modifiziert und erweitert werden.
- X.509-Zertifikaterweiterungen können nach dem Zufallsprinzip entfernt, angepasst, erweitert oder hinzugefügt werden. Host-spezifische Erweiterungen, wie z. B. die RACF-ID, können ebenfalls mit dem true-Xtender Policy Module gemanagt werden.
- Verhindern oder blockieren Sie die unbeaufsichtigte Ausstellung von Benutzerzertifikaten, insbesondere für privilegierte Konten wie Unternehmens- oder Domänenadministratoren.
- Zusätzliche Benutzer- oder Systemattribute können aus einem Verzeichnis oder einer Datenbank ausgewählt und in das Zertifikat integriert werden.

WEITERE INFOS

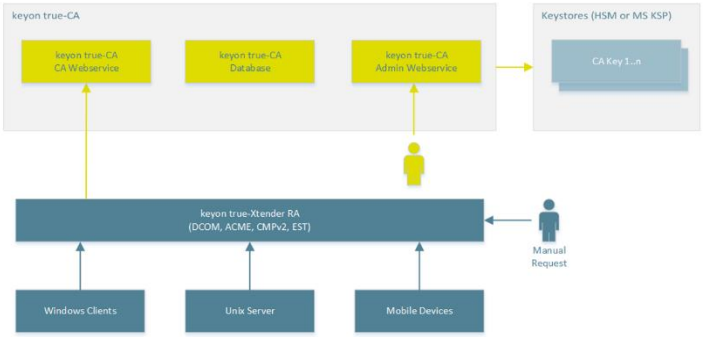


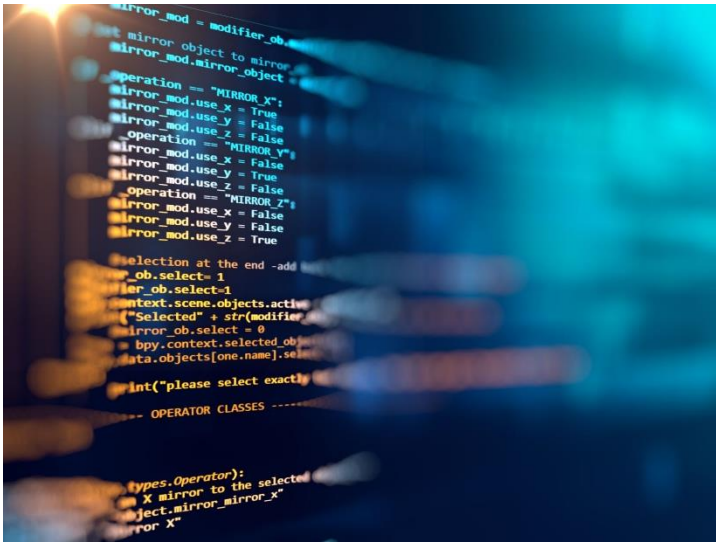
Zertifizierungsstelle und Revozierung

Zertifizierungsstelle

keyon true-CA

true-CA ist eine eigenständige, mandantenfähige Zertifizierungsstelle.





true-CA Funktionen

- Zentrale Bedienung und Verwaltung mehrerer CA-Hierarchien
- Einfaches und schnelles Bereitstellen und Verwalten neuer Root-CAs und ausstellender CAs
- Unterstützt mehrere Zertifikatsprofile pro Zertifizierungsstelle
- Unterstützt mehrere CRL-Profile pro Zertifizierungsstelle
- Unterstützte Schlüsselalgorithmen sind RSA, ECDSA_P256 und ECDSA_P384. (*Post-Quantum-Algorithmen auf der Roadmap)
- Vollständig integriert in keyon true-Xtender Registration Authority
- Von RA bereitgestellte Registrierungsprotokolle: Microsoft DCOM, ACME, CMPv2 und REST API
- Kann für Verfügbarkeit und Leistung einfach geclustert werden
- Private CA-Schlüssel können auf Hardware Security Modulen (HSM) oder als Softtoken (Microsoft Software KSP) gespeichert werden

Revozierung

keyon Revocation Provider

Es stehen zwei Module des true-Xtender Revocation Provider zur Verfügung.

RP-CL

Anbieter für die Sperrung der erneuten Synchronisierung zwischenspeichern

Die Prüfung gegen Sperrung erfolgt in der Windows CryptoAPI durch installierbare Sperranbieter, wobei Microsoft standardmäßig einen Sperranbieter bereitstellt, der die Sperrdetails über OCSP und Sperrlisten erkennen kann.

Bei der Verwendung von Zertifikatsperrlisten über den standardmäßigen Microsoft-Sperranbieter kann nicht davon ausgegangen werden, dass die Sperrung eines Zertifikats zeitnah erkannt werden kann, da die Zertifikatsperrlisten und die OCSP-Antworten aufgrund verschiedener Parameter zwischengespeichert werden.

Der keyon Revocation Provider stellt sicher, dass CRLs und OCSP-Antworten von einer CA nach einer konfigurierbaren Zeit neu geladen werden, anstatt aus dem Cache gelesen zu werden.

Der keyon Caching Resync Resync Revocation Provider wird hauptsächlich auf Domänencontrollern und Windows-Servern verwendet, auf denen Benutzerzertifikate auf Widerruf überprüft werden.

Beispiel für eine Sperrung

Beim Ausstellen temporärer Smartcards wird die aktive Smartcard angehalten und vorübergehend in der Zertifikatsperrliste aufgeführt.

Damit ein Mitarbeiter seine alte Smartcard so schnell wie möglich nach der Rückgabe der temporären Smartcard verwenden kann, muss der Domänencontroller nach der Sperrung die neueste Zertifikatsperrliste verwenden.

WEITERE INFOS

RP-DC

keyon Fallback und BCM Revocation Provider

Durch den Einsatz des keyon Fallback und BCM Revocation Providers kann eine Windows-Anmeldung mit einer Smartcard auch nach einem längeren Totalausfall einer PKI gewährleistet werden.

Wenn ein Domänencontroller sein eigenes Zertifikat zu Beginn nicht mit einer gültigen CRL- oder OCSP-Anforderung überprüfen kann, deaktiviert er das Feature für die Smartcard-Anmeldung.

Wenn keiner der installierten Sperrprovider gültige Sperrdetails abrufen kann, geben der Keyon Fallback und der BCM Revocation Provider den Status "not revoked" für das Domain Controller-Zertifikat zurück. Der Keyon Fallback und BCM Revocation Provider wird hauptsächlich auf Domänencontrollern und Windows-Clients verwendet.

keyon true-Xtender AutoEnroll PKI

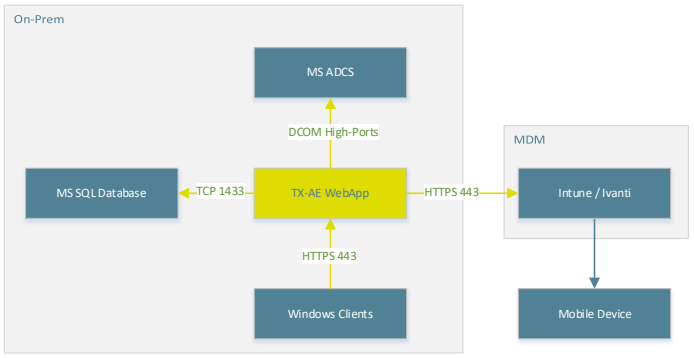
Automatisierung

AutoEnroll PKI

true-Xtender AutoEnroll PKI erweitert die Microsoft-Funktion für die automatische Registrierung, um Zertifikate von einer öffentlichen Zertifizierungsstelle Ihrer Wahl zu erhalten. AutoEnroll PKI ermöglicht die automatische Ausstellung und Verwaltung von Zertifikaten auf Windows-Systemen, die in die Domäne eingebunden sind, und auf mobilen Geräten (iOS, Android und Windows Mobile).

true-Xtender AutoEnroll PKI (TX-AE PKI) ermöglicht die automatisierte und einfache Ausstellung und Verwaltung von persönlichen S\MIME-Zertifikaten für alle Microsoft-Betriebssysteme.

Hierfür kann eine interne Microsoft PKI oder eine öffentliche PKI verwendet werden.



AutoEnroll PKI

- **Automatisierte Ausstellung von Zertifikaten**

  Active Directory und die entsprechenden Richtlinien bestimmen, ob ein Zertifikat ausgestellt werden muss. TX-AE PKI erlaubt neben der Neuausstellung von Zertifikaten auch bei Attributänderungen. Dies ist z.B. bei einer Namensänderung oder einem Abteilungswechsel (Änderung des Common Name (CN) oder der Organisationseinheit (OU) oder anderer Zertifikatsattribute) der Fall.
- **Automatische Erneuerung von Zertifikaten**

  Die Zertifikate werden automatisch erneuert, bevor sie ablaufen. Die Zeit zwischen den ersten Erneuerungsversuchen und dem Ablauf der Zertifikate kann konfiguriert werden (Verlängerungszeitpunkt).
- **Automatischer Widerruf von Zertifikaten**

  Zertifikate können auf der Grundlage eines flexiblen Regelwerks automatisch widerrufen werden. Dies gilt insbesondere für Personal, das das Unternehmen verlässt oder die Stilllegung von Anlagen.
- **Schlüsselarchivierung und Schlüsselwiederherstellung**

  Die kryptografischen Schlüssel für S/MIME-Zertifikate werden in der TX-AE-Datenbank gespeichert und können entweder vom Eigentümer oder über einen geprüften Vier-Augen-Wiederherstellungs-Workflow abgerufen werden.
- **Schnittstellen und CA-Integration**

  Die Integration von TX-AE PKI in eine öffentliche CA basiert auf der gängigen RFC 2797-Schnittstelle bzw. einer CA-spezifischen Schnittstelle.
- **Installation ohne Fussabdruck**

  Für die TX-AE PKI ist keine Softwareinstallation auf der Client-Seite erforderlich. Ein Client kann jedoch auf Endgeräte ausgerollt werden, wenn ein Schlüsselhistorienimport von Verschlüsselungszertifikaten im Rahmen eines Auto-Enrollment-Prozesses erforderlich ist. Die standardmäßige Microsoft-Funktion für die automatische Registrierung bietet eine solche Lösung nicht.
- **Paralleler Betrieb von interner und öffentlicher CA**

  Die Auslagerung von Inhouse-Zertifikaten, die z.B. für die Personen- und Geräteauthentifizierung verwendet werden, konnte aufgrund der fehlenden Integration in eine öffentliche CA nicht umgesetzt werden.

  Die TX-AE PKI verbindet Ihr Unternehmen mit einer öffentlichen Zertifizierungsstelle Ihrer Wahl. Auf diese Weise können Sie den Betrieb einer Zertifizierungsstelle vollständig auslagern, ohne die Vorteile der automatisierten Zertifikatsverteilung und -verwaltung zu verlieren. Es ermöglicht auch die gleichzeitige Integration mehrerer interner und öffentlicher CAs und ermöglicht beispielsweise die nahtlose Migration einer internen CA in eine öffentliche CA.
- **Bereitstellen von ausgestellten Zertifikaten in MDM**

  Zertifikate können über MDM auf mobilen Geräten bereitgestellt werden. Intune wird standardmäßig unterstützt. Jedes MDM, das einen Zertifikatsimport bereitstellt, kann integriert werden.
- **Umfassendes Cockpit**

  TX-AE PKI bietet eine webbasierte GUI für alle Aktivitäten oder Abfragen. Umfassende Berichte geben Einblick in den Fortschritt eines Prozess- oder Systemzustands. Sie können z.B. für die Kostenverteilung der Zertifikatsnutzung nach Organisationseinheiten verwendet werden.

WEITERE INFOS

Weitere Angebote unserer Applied Crypto Abteilung:

- **keyon true-Sign:** Umfassende Suite für digitale Signaturen. Unterstützt Code Signing, Dokumentensignierung und Archivierung.
- **PKI Consulting:** Profitieren Sie von unserer jahrzehntelangen Erfahrung im Enterprise PKI Umfeld.

JETZT ANFRAGEN UND BERATEN LASSEN

Swiss IT Security AG – SITS
www.sits.com
info@sits.ch