keyon true-Xtender

The keyon true-Xtender suite for Enterprise PKI provides a comprehensive solution for the issuance and management of X.509 certificates.

The keyon true-Xtender suite from SITS is a comprehensive collection of services and applications that combine ease of use with added flexibility and features for the manual and automated management of certificates, while supporting crypto-agility to ensure adaptability to evolving cryptographic standards.

Our solution for your certificate management

Modules and features:

- true-Xtender **Policy Module** extends the features of Microsoft ADCS
- true-Xtender **RA Web Application** enables the seamless integration of certificate management
- true-Xtender **RA ACME Service** provides the ACME protocol
- true-Xtender **RA Enrollment Server** provides the CMPv2 and the EST protocol
- true-Xtender **RA Web Service Add-on** offers extensive REST and / or SOAP interfaces
- true-Xtender **RA DCOM Add-on** enables as a DCOM interface the cross-forest certificate issuance and revocation
- true-Xtender **Third-Party Certificate Manager Add-on** is used to monitor third-party certificates
- true-Xtender **Discovery** enables comprehensive detection and inventory of certificates
- true-Xtender **PKI Services** provide additional supporting features for the lifecycle management of certificates
- **true-CA** is a self-contained multi-tenant Certification Authority solution
- **Revocation Provider** makes sure that CRLs and OCSP responses from a CA are reloaded after a configurable time instead of being read from the cache.
- true-Xtender **AutoEnroll PKI** extends the Microsoft auto-enrollment feature to manage S\MIME certificates from a public CA including key archival and key recovery.

Your advantages with SITS:

- **Building trust**: Globally recognized solutions that build trust and promote digitization.
- **Tailored consulting**: Individual consulting and solution finding according to your specific requirements.
- **Comprehensive service:** From consulting to SaaS solutions – we offer the complete package.
- **Seamless integration**: Support with connecting to specialist applications and integration into existing systems.
- **Experience:** Decades of experience in the field of Public Key Infrastructure guarantee professionalism and data protection.

LEARN MORE

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

keyon true-Xtender Registration Authority

RA-WA

true-Xtender RA Web Application

The true-Xtender Registration Authority Web Application enables the seamless integration of certificate management into the company's internal processes and offers next to a browser-based GUI multiple enrollment protocols (ACME, CMPv2, EST) and a web service interface for automated processes.

Company specific management processes can be implemented through metadata, which are additionally stored in the registration authority (RA) database. For example, certificates can be mapped to applications, individuals or groups, who will be notified in case of a renewal process, a revocation, or other activities.

An extensive audit log stores every activity of the applicants and the administrators. The permissions for the individual features are controlled by role-based access control after successful authentication based on Kerberos or OIDC/OAuth2.

The RA stores all data in a Microsoft SQL database. Evaluations and reports can be created using Microsoft SQL Server Reporting Services (SSRS) or Microsoft Power BI. The RA supports different workflows, which can be defined for each certificate type Services (SSRS) or Microsoft Power BI. The RA supports different workflows, which can be defined for each certificate type

RA-Web Application Features

- simple and advanced **search for certificates**
- issuing certificates based on **PKCS#10 files**
- issuing key pairs and certificates as **PKCS#12 files**
- **delivering certificates via different channels**
  E-mail
  Web-based download
- safety-critical features can be mapped through a **workflow management** (four-eye-principle)
- **revocation** of certificates
- **renewal** of certificates
- **monitoring for expiring certificates**
- **multi-CA-support**
  (SwissSign, DigiCert, GlobalSign, Telekom, etc.)

RA-ACME+

true-Xtender RA ACME Service

The true-Xtender Registration Authority ACME Service provides the ACME protocol as a standardized interface for automated certificate management.

The RA-ACME Service is integrated into the RA database and its user interface. The RA-ACME Service is implemented as a proxy server architecture, which enables the use of ACME in separate network zones. Several ACME adapters act as a proxy between the enrollment clients and the RA, or the RA-ACME Service. The ACME adapters perform the validation of the domains.

The adapters support the ACMEv2 protocol with http-01 and dns-01 validation (according to RFC 8555). Various certificate profiles are supported for different domains by using different endpoints in the service URL of the adapters. The adapters are available for Windows and Linux systems.

RA-CMP+, RA-EST+

true-Xtender RA Enrollment Server

The true-Xtender Registration Authority enrollment server provides the CMPv2 and the EST protocol as a standardized interface for automated certificate management.

The enrollment server is implemented as a proxy server architecture, which enables the use of CMPv2 and EST in separate network zones.

RA-WS+

true-Xtender RA Web Service Add-on

The true-Xtender Registration Authority Web Service Add-on offers extensive REST and / or SOAP interfaces for the automated issuance and management of X.509 certificates.

An enrollment client authenticates itself against the web service and receives based on the corresponding role concept the appropriate permissions for the individual features:

- issuing certificates based on PKCS#10 files,
- issuing key pairs and certificates as PKCS#12,
- obtaining issued certificates,
- revocation of certificates, and
- renewal of certificates
- Certificate profile and role configuration

RA-DCOM+

true-Xtender RA DCOM Add-on

The true-Xtender Registration Authority DCOM Add-on enables as a DCOM interface the cross-forest certificate issuance and revocation.

For example, in a DMZ only the RA-DCOM Add-on is required instead of a separate Microsoft CA to issue certificates from the corporate CA. In addition, the module serves as a proxy for a Microsoft CA to prevent direct access to the CA for all client systems.

RA-CM-3RD+

true-Xtender 3rd-Party Certificate Manager

The true-Xtender Third Party Certificate Manager Add-on is used to monitor third-party certificates. Multiple notification services can be set up, which will notify a user as soon as a certificate reaches the end of its lifetime.

Certificates to be monitored are imported into the RA database via the web GUI or the web service interface. With the upload, additional metadata can be provided, which can then be used in the notifications before the certificates expire.

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

INQUIRE NOW AND REQUEST A DEMO

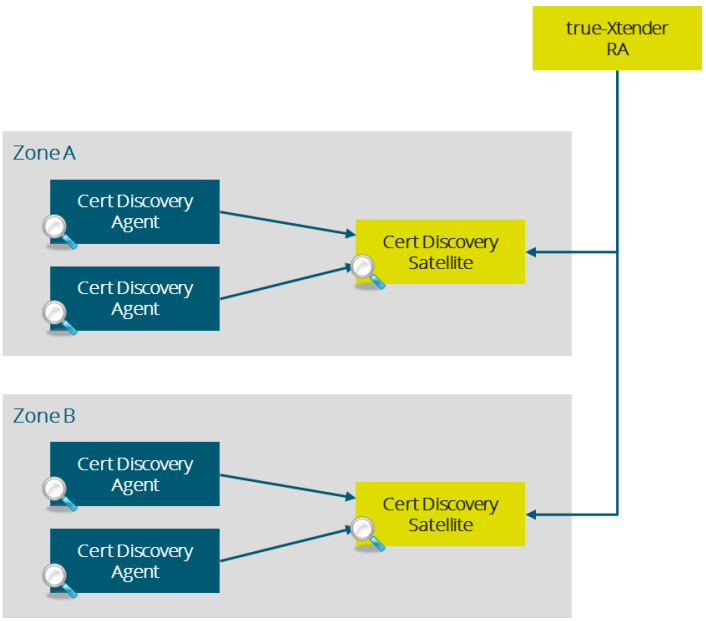
Policies and Discovery

Certificate Discovery

true-Xtender Discovery

The true-Xtender Discovery module enables comprehensive detection and inventory of certificates within the IT environment

Various search methods can be adapted to specific requirements, enabling efficient discovery of certificates. The certificates found are imported into the true-Xtender RA. The resulting monitoring increases both the security and operational reliability of IT systems.



Remote discovery via Satellites:

- Uses so-called satellites to locate certificates through remote port scanning.
- Supports SSL/TLS and StartTLS (FTP/SMTP/POP3/IMAP) protocols.
- Pv4 & IPv6 support.
- Configurable address ranges (IP ranges, IP subnets, hostnames).
- Configurable port ranges.

The satellite collects scan results from the so-called agents. The true-Xtender Discovery agent is deployed as a single binary executable on target systems (Windows, Linux, MacOS) to perform local certificate searches.

Local discovery by Agents:

- Local port scans
- Local file scan
- Local certificate store scan

The agents are managed by the satellites and receive their configuration from them.

TX-PMSA

true-Xtender Policy Module

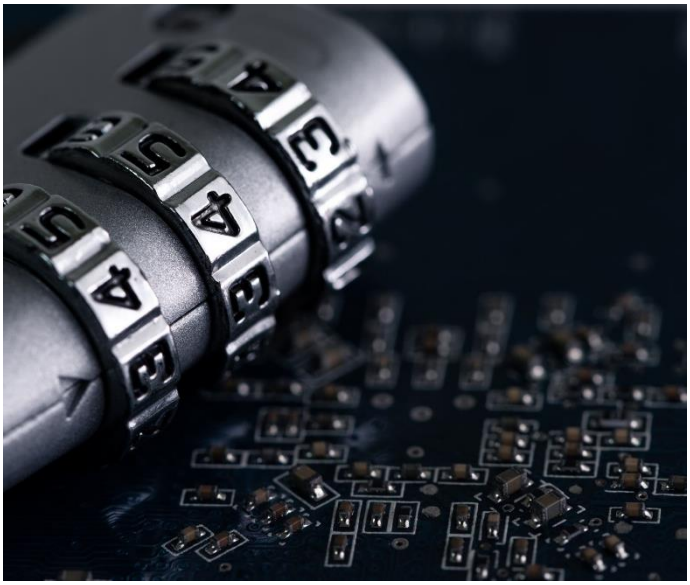
The true-Xtender Policy Module extends the features of Microsoft ADCS based Enterprise PKI and allows a rule-based issuance and management of X.509 certificates.

The certificate content can be considerably extended or modified

Policy examples

- The individual components of the subject distinguished name (DN) can be defined, taken from the original certificate application, or modified and extended by any rule.
- X.509 certificate extensions can be randomly removed, adjusted, enhanced, or added. Host specific extensions such as the RACF ID can also be managed with the true-Xtender Policy Module.
- Prevent or block unattended issuance of user certificates, especially for privileged accounts such as enterprise or domain administrators.
- Additional user or system attributes can be selected from a directory or database and integrated into the certificate.

LEARN MORE

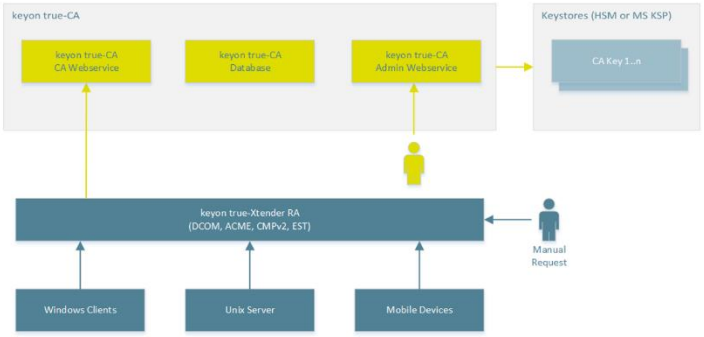


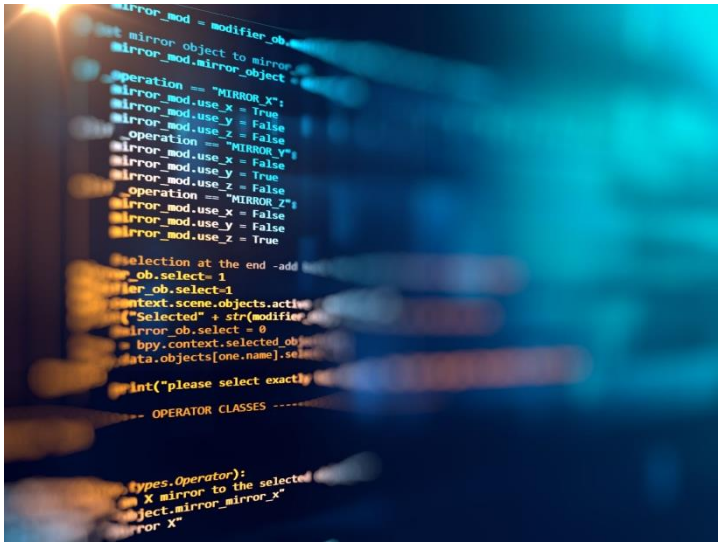
Certification Authority and Revocation

Certification Authority

keyon true-CA

true-CA is a self-contained multi-tenant Certification Authority solution.





true-CA features

- Central operating and managing multiple CA hierarchies
- Easily and quickly deploy and manage new Root CAs and Issuing CAs
- Supports multiple certificate profiles per CA
- Supports multiple CRL profiles per CA
- Supported key algorithms are RSA, ECDSA_P256 and ECDSA_P384. (*Post-Quantum algorithms on the roadmap)
- Fully integrated in keyon true-Xtender Registration Authority
- RA provided enrollment protocols: Microsoft DCOM, ACME, CMPv2 and REST API
- Can easily be clustered for availability and performance
- CA private keys may be stored on Hardware Security Modules (HSM) or as Softtoken (Microsoft Software KSP)

Revocation

keyon Revocation Provider

There are two modules available of the true-Xtender Revocation Provider.

RP-CL

Caching Resync Revocation Provider

The check against revocation takes place in the Windows CryptoAPI through installable revocation providers, whereby Microsoft provides a revocation provider by default that can detect the revocation details via OCSP and revocation lists.

When using CRLs through the standard Microsoft revocation provider, it cannot be assumed that the revocation of a certificate can be detected in a timely manner because the CRLs and the OCSP responses are cached due to various parameters.

The keyon revocation provider makes sure that CRLs and OCSP responses from a CA are reloaded after a configurable time instead of being read from the cache.

Revocation example

When issuing temporary smart cards, the active smart card is suspended and temporarily listed on the CRL.

In order for an employee to use his old smart card as soon as possible after returning the temporary smart card, the domain controller must use the latest CRL after the suspension.

The keyon Caching Resync Revocation Provider is primarily used on domain controllers and Windows Servers where user certificates are checked against revocation.

LEARN MORE

RP-DC

keyon Fallback and BCM Revocation Provider

By using the keyon Fallback and BCM Revocation Provider, a Windows login using a smart card can be guaranteed even after a longer total failure of a PKI.

If a domain controller can't check its own certificate at the start with a valid CRL or OCSP request, it then deactivates the feature for the smart card logon.

If none of the installed revocation providers can retrieve valid revocation details, then the Keyon Fallback and BCM Revocation Provider return the status "not revoked" for the domain controller certificate. The Keyon Fallback and BCM Revocation Provider is primarily used on domain controllers and Windows clients.

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

INQUIRE NOW AND REQUEST A DEMO

keyon true-Xtender AutoEnroll PKI

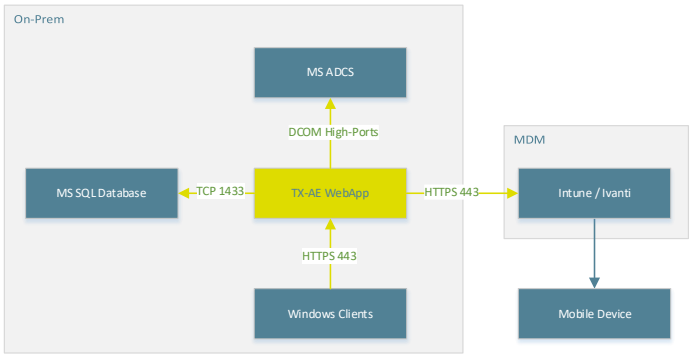
Automation

AutoEnroll PKI

true-Xtender AutoEnroll PKI extends the Microsoft auto-enrollment feature to obtain certificates from a public CA of your choice and allows the automated issuance and management of certificates on Windows domain joined Systems, and Mobile Devices (iOS, Android and Windows Mobile).

true-Xtender AutoEnroll PKI (TX-AE PKI) enables automated and easy issuance and management of personal S\MIME certificates for all Microsoft operating systems.

An internal Microsoft PKI or a public PKI can be used for this purpose.



AutoEnroll PKI Features

- **Automatic issuance of certificates**

  Active Directory and respective policies will determine whether a certificate must be issued. TX-AE PKI allows in addition to re-issue certificates in case of attribute changes. This is practiced, for instance, in a change of name or change of department (change of common name (CN) or organizational unit (OU) or other certificate attributes).
- **Automatic renewal of certificates**

  The certificates are renewed automatically before they expire. The time between the first renewal attempts and the expiration of the certificates can be configured (renewal time).
- **Automatic revocation of certificates**

  Certificates can be revoked automatically based on a flexible set of rules. This is applied, in particular, for personnel leaving the company or the decommissioning of equipment.
- **Key-Archival and Key-Recovery**

  The cryptographic keys for S/MIME certificates are stored in the TX-AE database and can be retrieved either by the owner or through an audited four-eyes recovery workflow.
- **Interfaces and CA integration**

  The integration of TX-AE PKI into a public CA is based on the commonly used RFC 2797 interface or a CA-specific interface.
- **Zero footprint installation**

  TX-AE PKI requires no software installation on the client side. However, a client can be rolled out to terminal devices if a key history import of encryption certificates within an auto-enrollment process is required. The standard Microsoft auto-enrollment feature does not offer such a solution.
- **Parallel operation of internal and public CA**

  The outsourcing of in-house certificates, used for example, for personal and device authentication, could not be implemented due to a lack of integration into a public CA.

  TX-AE PKI connects your business with a public CA of your choice. This allows you to fully outsource the operation of a CA without losing the benefits of automated certificate distribution and management. It also allows the simultaneous integration of multiple internal and public CAs and enables, for example, the seamless migration of an internal CA into a public CA.
- **Deployment of issued certificates to MDM**

  Certificates can be deployed to mobile devices via MDM. Intune is supported by default. Any MDM that provides a certificate import can be integrated.
- **Comprehensive cockpit**

  TX-AE PKI provides a web-based GUI for all activities or queries. Comprehensive reports provide insight into the progress of a process or system state. They may be used, for example, for cost distribution of the certificate usage according to organizational units.

LEARN MORE

Other offerings from our Applied Crypto Solutions:

- **keyon true-Sign:** Comprehensive suite for Digital Signatures. Supports Code Signing, Document Signing and Archiving.
- **PKI Consulting:** Benefit from our decades of experience in the enterprise PKI environment

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