keyon

Unleash Enterprise PKI

true-Xtender Suite for Enterprise PKI

The Enterprise PKI builds together with the true-Xtender Suite from Keyon a comprehensive solution for the issuance and management of X.509 certificates.

Enhance the functionality of your Active Directory® Certificate Services infrastructure with the true-Xtender suite from Keyon, a comprehensive collection of services and applications that combine ease of use with added flexibility and features.

All modules are supported on Windows 2012 (R2) and 2016 and offer full enterprise functionality. There is no schema extension required. The true-Xtender Suite comprises of the modules as follows.

keyon AG
Schlüsselstrasse 6
8645 Jona
Switzerland

Phone: +41 55 220 64 00
Fax: +41 55 220 64 01

www.keyon.ch
info@keyon.ch

true-Xtender Policy Module (TX-PMSA)

The true-Xtender Policy Module extends the features of Enterprise PKI and allows a rule-based issuance and management of X.509 certificates. The certificate content can be considerably extended or modified. Here are some 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.
- Additional user or system attributes can be selected from a directory or database and integrated into the certificate.

true-Xtender Registration Authority Web Application (RA-WA)

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 a web service interface for automated processes.

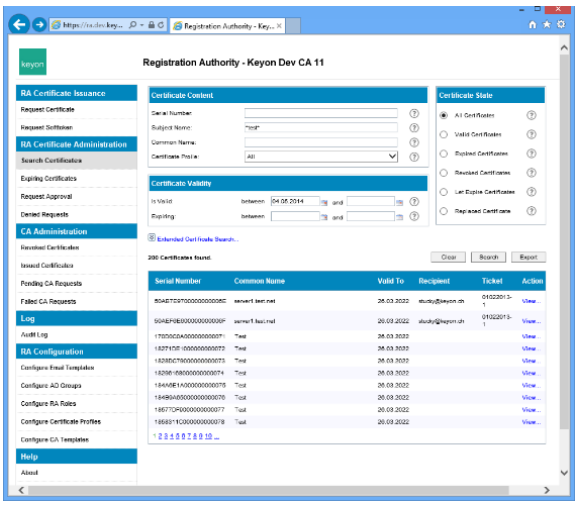
Company specific management processes can be implemented through metadata, which are additionally stored in the registration authority (RA) database. For example, certificates can be mapped to applications, individuals or groups, who will be notified in case of a renewal process, a revocation, or other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

An extensive audit log stores every activity of the applicants and the administrators. The permissions for the individual features are controlled via Active Directory groups. 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.

The true-Xtender Registration Authority Web Application provides the following features:

- simple and advanced search for certificates,
- issuing certificates based on PKCS#10 files,
- issuing key pairs and certificates as PKCS#12 files,
- issuing key pairs and certificates which are directly stored to hardware tokens (HSM, smart card, etc.). The key generation takes place on the token,
- delivering already issued 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, and
- renewal of certificates.

The true-Xtender Registration Authority Web Application is based on Microsoft IIS.



true-Xtender Registration Authority ACME Service (RA-ACME+)

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

true-Xtender Registration Authority Reminder Services Add-on (RA-SE-CE+)

The true-Xtender Registration Authority Reminder Services Add-on is used to monitor and log expiring certificates prior to their expiration. Different reminders can be created to monitor expiration at different intervals, send notification e-mails to certificate recipients, and log expiring certificates into the Windows Application Event Log. Customer-specific monitoring systems can be integrated to monitor and to further process the generated Windows Application Event Log entries.

true-Xtender Registration Authority Web CA Add-on (RA-WCA+)

With the true-Xtender Registration Authority Web CA Add-on all certificate requests of the Microsoft CA can be managed and certificates can be revoked, in particular certificates issued with the auto-enrollment feature of the Microsoft CA. As with the true-Xtender RA-WA, the role concept based on AD group memberships can be used to assign different authorizations for managing and revoking certificates.

true-Xtender Registration Authority Web Service Add-on (RA-WS+)

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 AD group membership and the 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.

true-Xtender Registration Authority DCOM Add-on (RA-DCOM+)

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.

true-Xtender Third-Party Certificate Manager Add-on (RA-CM-3RD+)

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. The role concept of the true-Xtender Third Party Certificate Manager Add-on is based on Active Directory user groups.

true-Xtender AutoEnroll PKI Proxy (TX-AEP)

The true-Xtender AutoEnroll PKI Proxy is used between true-Xtender RA and the external web service interface of a public CA. All certificates are managed and monitored with the true-Xtender RA-WA. This allows a uniform cockpit for all internal and public certificates.

true-Xtender AutoEnroll PKI (TX-AE)

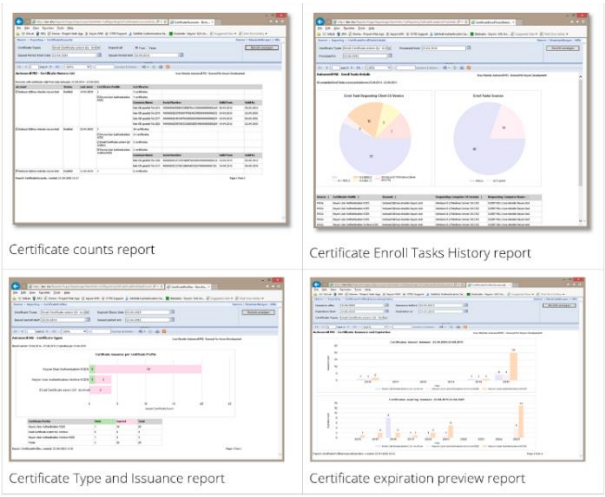
true-Xtender AutoEnroll PKI connects the Microsoft auto-enrollment feature with a public PKI service. This makes it possible to automatically issue and manage in-house certificates, as usual, without having to operate your own Microsoft CA.

Furthermore, the Microsoft PKI auto-enrollment feature can be extended significantly with true-Xtender TX-AE.

- Auto-enrollment of public certificates. Any public CA with a web service interface can be integrated.

- Auto-enrollment based renewal of certificates in the case of modifications of user or server attributes.
- Flexible lifecycle management of user and server certificates.

A comprehensive and intuitive web GUI as well as extensive reporting services make up the cockpit for all certificates used within the company.



For further details please see section true-Xtender AutoEnroll PKI (TX-AE PKI)

true-Xtender PKI Services

The true-Xtender PKI Services provide additional supporting features for the lifecycle management of certificates and certificate revocation lists.

true-Xtender Auto-Revocation Service (SE-CE-AR)

The true-Xtender Auto-Revocation Service is the counterpart of Microsoft's auto-enrollment feature. The true-Xtender Auto-Revocation Service revokes a certificate as soon as its associated computer or user object is deleted in AD. It also revokes duplicate certificates, i.e. certificates of the same type issued to the same subject DN.

The threshold value of the number of certificates to be revoked can be configured to prevent unintentional revocation in case of AD structure changes (e.g. moving users to a different OU). All actions of the service are recorded in the Windows Application Event Log.

true-Xtender Standalone Certificate Expiration Service (SE-CE-AR)

The true-Xtender Standalone Certificate Expiration Service checks periodically whether certificates expire within a certain time. If certificates expire, the service collects data on the expiring certificates from the Microsoft CA database and sends reminder e-mails to certificate managers and administrators. All actions of the service are recorded in the Windows Application Event Log.

true-Xtender CRL Management Service (SE-CD)

The true-Xtender CRL Management Service is applied in connection with the monitoring of CRL distribution points and the distribution of revocation lists to different certificate revocation list (CRL) distribution points (CDPs) and the monitoring of CRL distribution points. The service monitors whether the configured CRL distribution points provide the current revocation lists. In case of failure, the CRL distribution service sends an e-mail to administrators and updates the Windows Application Event Log accordingly. The service supports different sources of CRLs and can distribute them to the CDPs over LDAP, file shares, or script calls.

true-Xtender CRL Publication Service (SE-CP)

The true-Xtender CRL Publication Service publishes the certificate revocation list (CRL) immediately after the input of a so-called revocation request on the Microsoft CA. Furthermore, a blacklist is published in a regular interval (e.g. once a day) even if no new entry exists on the revocation list.

By using the SE-CP, the regular publication of revocation lists is omitted whereby no unnecessary rereading of an online responder is required. The revocation list is only reread when the list is updated due to a new revocation request.

The SE-CP is installed as Windows Service and is registered as a so-called exit module on the Microsoft CA. The publication interval and other application specific parameters can be configured in an XML file.

Keyon Revocation Provider

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

Keyon Caching Resync Revocation Provider (RP-CL)

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 make sure that CRLs and OCSP responses from a CA are reloaded after a configurable time instead of being read from the cache.

Example of us:

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.

Keyon Fallback and BCM Revocation Provider (RP-DC)

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.

Keyon Credential Provider (CP)

The Keyon Credential Provider allows the enforcement of the smart card logon without randomizing the Active Directory (AD) password of an employee. This allows compatibility with applications that check user names and passwords against AD and do not support Kerberos or certificate-based authentication.

The Keyon Credential Provider allows the username /password logon only for local administrators and for members of defined AD groups. In addition, so-called "deny password logon" AD groups can be defined, which overrides AD groups for which smart card logon is not enforced.

If the Keyon Credential Provider cannot determine whether a user is local admin or member of a defined AD group, the login with username and password is not possible. The Keyon Credential Provider caches group memberships of users to support the offline logon scenario.

A second smart card credential provider wrapper allows to change the AD password, if required by policy, when the user tries to login with a smart card. This guarantees that password change policies can be enforced even for users that are only allowed to interactively login with a smart card.

The Keyon Credential Provider supports Windows 7 and Windows 10. The configuration can be set by group policies.

Keyon Certificate Propagator (CE-PR)

The Microsoft certificate propagation service (CertPropSvc) imports the certificates into the user certificate store when the smart card is inserted and during the logon/unlock process.

The Microsoft certificate propagation service (CertPropSvc) runs as a standard for all smart cards available on a system, which means that the certificates of other users are also propagated into the certificate store of the currently logged in user. These certificates are then displayed in selection dialogs.

Keyon Certificate Propagator functionality

The Keyon Certificate Propagator replaces the Microsoft certificate propagation service (CertPropSvc) and imports only the certificates of the currently logged in user, which are to be imported according to the configuration.

The Keyon Certificate Propagator has an architecture that allows to extend the functionality at various events (smart card plugged, smart card removed) through plug-ins in the form of DLLs. This architecture allow applications or scripts to be started on an event such as the pending certificate renewal.

When the CE-PR is started, the following actions are performed:

- The certificates of all smart cards currently available on the system are identified.
- Smart card certificates that have been assigned to a smart card CSP / KSP but are not found on any of the smart cards used are deleted from the user's certificate store.

While the application is running, the following actions are performed when inserting a smart card:

- The certificates on the inserted smart card are identified.
- Smart card certificates that have the same user ID but do not exist on any of the inserted smart cards are deleted from the user's certificate store.

While the application is running, the following actions are performed when a smart card is removed:

- If the certificates on the remote smart card belong to the logged in Windows user (UPN in authentication certificate = UPN of the Windows user), no actions are taken and no certificates are deleted.
- If the certificates on the remote smart card do not belong to the logged in Windows user, then the certificates are deleted from the user's certificate store.

The application has no user interface and runs invisibly in the background. Only certificates with a KSP / CSP for smart cards are considered. Soft tokens are not handled.

true-Xtender AutoEnroll PKI (TX-AE 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 and non-domain joined Systems, Mac OS, Linux/Unix, iOS, Android and Windows Mobile.

true-Xtender AutoEnroll PKI (TX-AE PKI) enables automated and easy issuance and management of personal certificates and device certificates for all Microsoft operating systems, Mac OS, Linux and other non-Microsoft clients. An internal Microsoft PKI or a public PKI can be used for this purpose. An in-house Enterprise PKI must be set up and operated autonomously. The operation of such a PKI requires an appropriate infrastructure, hardware security modules, and continuous know-how.

TX-AE PKI allows you to fully outsource the operation of a CA without losing the benefits of automated certificate distribution and management.

Features

TX-AE PKI provides comprehensive lifecycle management of certificates and impresses with the following 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.

- **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 (see figure 1 and 2 below).

Figure 1

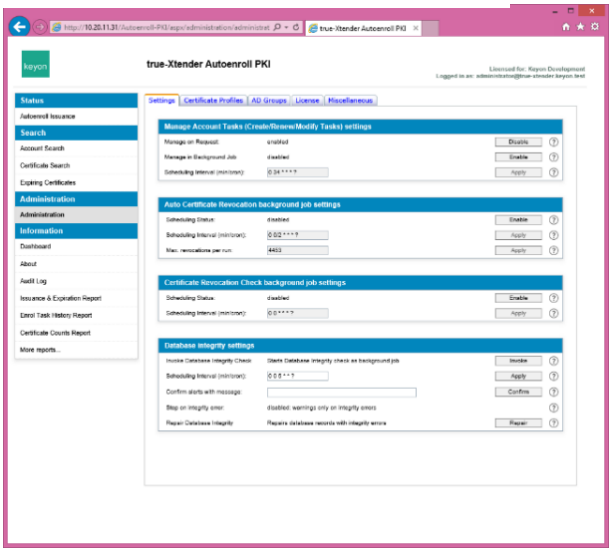
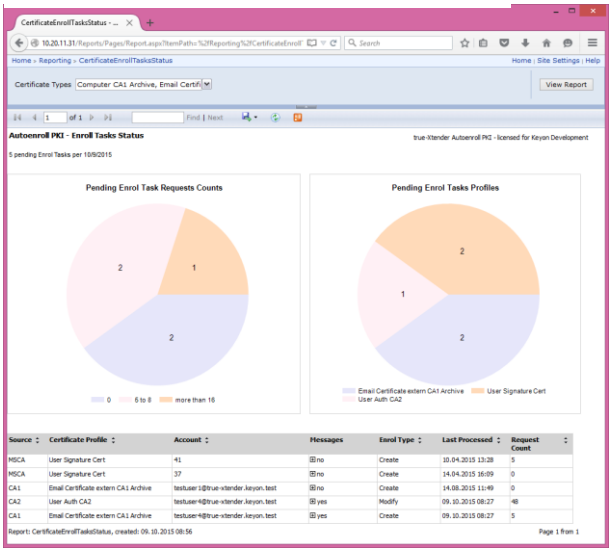


Figure 2



Extended features for automated certificate enrollment

TX-AE PKI provides with additional interfaces the following features:

Operating system	Description
Microsoft Windows	Microsoft auto-enrollment of domain joined Windows systems or users via CES or DCOM. Microsoft auto-enrollment of non-domain joined Windows systems or users via CES.
Mac OS	Certificate enrollment for Mac OS via DCOM or SCEP.
Linux / Unix	Certificate enrollment for Linux / Unix via DCOM or SCEP.
Mobile devices (iOS, Android, Blackberry)	Certificate enrollment for mobile devices / MDM via DCOM or SCEP.
Mobile devices (iOS, Android, Blackberry)	Certificate deployment to mobile devices via MDM (Intune or other MDM solutions).