keyon

Unleash Microsoft PKI

true-Xtender Suite für Microsoft PKI

Die Microsoft PKI bildet mit der true-Xtender Suite von Keyon eine umfassende Lösung für die Ausgabe und Verwaltung von X.509 Zertifikaten.

Erweitern Sie die Funktionalität Ihrer Active Directory® Certificate Services-Infrastruktur mit der true-Xtender Suite von Keyon, einer umfassenden Sammlung von Diensten und Anwendungen, die Benutzerfreundlichkeit mit mehr Flexibilität und Funktionen verbindet.

Alle Module werden auf Windows 2012 (R2) und 2016 unterstützt und bieten volle Enterprise Funktionalität. Eine Schemaerweiterung ist nicht notwendig. Die true-Xtender Suite besteht aus den folgenden Modulen.

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)

Das true-Xtender Policy Module erweitert die Eigenschaften der Microsoft PKI und ermöglicht eine regelbasierte Ausgabe und Verwaltung von X.509 Zertifikaten. Der Zertifikatsinhalt kann umfangreich erweitert oder verändert werden. Folgend ein paar Beispiele:

- Die einzelnen Komponenten des Subject Distinguished Names (DN) können fest definiert, aus dem ursprünglichen Zertifikatsantrag übernommen oder nach einer beliebigen Regel verändert oder erweitert werden.
- X.509 Zertifikatserweiterungen können beliebig entfernt, angepasst, erweitert oder hinzugefügt werden. Mit dem true-Xtender Policy Modul von Keyon können auch hostspezifische Erweiterungen wie beispielsweise die RACF ID verwaltet werden.
- Zusätzliche Benutzer-, oder Systemattribute können aus einem Verzeichnis oder aus einer Datenbank ausgelesen und in das Zertifikat integriert werden.

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

Die true-Xtender Registration Authority Web Application ermöglicht die nahtlose Integration der Zertifikatsverwaltung in die unternehmensinternen Prozesse und bietet neben einem browserbasierten GUI eine Webservice Schnittstelle für automatisierte Prozesse.

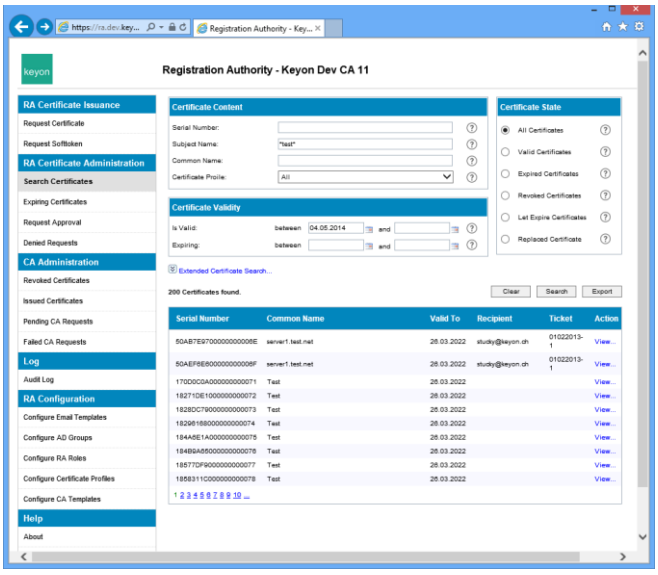
Über Metadaten, welche zusätzlich in der Datenbank der RA gespeichert werden, können unternehmensspezifische Verwaltungsprozesse umgesetzt werden. Beispielsweise können Zertifikate Applikationen, Personen oder Gruppen zugeordnet werden, die im Falle eines Erneuerungsprozesses, einer Revokation oder anderen Aktivitäten, benachrichtigt werden.

Ein umfangreiches Audit-Log speichert jede Aktivität der Antragsteller und der Administratoren. Die Berechtigungen für die einzelnen Funktionen werden über Active Directory-Gruppen gesteuert. Die RA speichert alle Daten in einer Microsoft SQL-Datenbank. Auswertungen und Berichte können mit Microsoft SQL Server Reporting Services (SSRS) oder mit Microsoft Power BI erstellt werden. Die RA unterstützt unterschiedliche Workflows, die für jeden Zertifikatstyp definiert werden können.

Die true-Xtender Registration Authority Web Application bietet die folgenden Funktionen:

- Einfache und Erweiterte Suche nach Zertifikaten (Unterstützung mehrerer CAs)
- Ausstellen von Zertifikaten auf der Basis von PKCS#10-Dateien
- Ausstellen von Schlüsselpaaren und Zertifikaten als PKCS#12-Dateien
- Ausstellen von Schlüsselpaaren und Zertifikaten, welche direkt auf Hardwaretoken (HSM, Smartcard, etc.) gespeichert werden. Die Schlüsselgenerierung findet dabei auf den Hardwaretoken statt.
- Ausliefern von bereits ausgestellten Zertifikaten über unterschiedliche Kanäle (E-Mail, Web-basierter Download)
- Sicherheitskritische Funktionen können über ein Workflow Management (4-Augen-Prinzip) abgebildet werden
- Wiederrufen (Revozieren) von Zertifikaten
- Erneuern von Zertifikaten

Die true-Xtender Registration Authority Web Application basiert auf Microsoft IIS.



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

Der true-Xtender Registration Authority ACME Service stellt das ACME-Protokoll als standardisierte Schnittstelle für die automatisierte Verwaltung von Zertifikaten zur Verfügung. Der RA-ACME Service ist in die RA-Datenbank und deren Benutzeroberfläche integriert. Der RA-ACME Service ist als Proxy-Server-Architektur umgesetzt, welche dadurch den Einsatz von ACME in separaten Netzwerkzonen ermöglicht. Mehrere ACME Adapter fungieren dabei als Proxy zwischen den Enrollment Clients und der RA, bzw. dem RA-ACME Service. Die Validierung der Domains wird von den ACME Adaptern durchgeführt. Die Adapter unterstützen das ACMEv2-Protokoll mit HTTP-Validierung (gemäss RFC 8555). Verschiedene Zertifikatsprofile werden für unterschiedliche Domains unterstützt indem unterschiedliche Endpunkte in der Service-URL der Adapter verwendet werden. Die Adapter sind für Windows- und Linux-Systemen erhältlich.

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

Das true-Xtender Registration Authority Reminder Services Add-on dient zur Überwachung und Protokollierung ablaufender Zertifikate vor deren Ablauf. Es können verschiedene Reminder erstellt werden, um den Ablauf in verschiedenen Intervallen zu überwachen, Benachrichtigungs-E-Mails an Zertifikatsempfänger zu senden und ablaufende Zertifikate im Windows Application Event Log zu protokollieren. Kundenspezifische Monitoring-Systeme können integriert werden, um die erzeugten Windows Application Event Log-Einträge zu überwachen und weiter zu verarbeiten.

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

Mit dem true-Xtender Registration Authority Web CA Add-on können alle Zertifikatsanträge der Microsoft CA verwaltet und Zertifikate gesperrt werden, insbesondere Zertifikate welche mit dem Autoenrollment Mechanismus der Microsoft CA ausgestellt wurden. Analog zur true-Xtender RA-WA können mit dem auf AD-Gruppenmitgliedschaften basierenden Rollenkonzept verschiedene Berechtigungen zur Verwaltung und Sperrung der Zertifikate vergeben werden.

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

Das Registration Authority Web Service Add-on bietet umfangreiche REST und / oder SOAP Schnittstellen für die automatisierte Ausgabe und Verwaltung von X.509 Zertifikaten. Ein Enrollment-Client authentisiert sich gegenüber dem Webservice und erhält aufgrund der entsprechenden AD Gruppenmitgliedschaft und dem Rollenkonzept die entsprechenden Berechtigungen für die einzelnen Funktionen:

- Ausstellen von Zertifikaten basierend auf PKCS#10-Dateien
- Ausstellen von Schlüsselpaaren und Zertifikaten als PKCS#12-Dateien
- Beziehen von ausgestellten Zertifikaten
- Wiederrufen (Revozieren) von Zertifikaten
- Erneuern von Zertifikaten

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

Das true-Xtender Registration Authority DCOM Add-on ermöglicht als DCOM Schnittstelle das Forest-übergreifende Ausstellen und Sperren von Zertifikaten. So wird beispielsweise in einer DMZ anstelle einer separaten Microsoft CA nur das RA-DCOM Add-on benötigt, um Zertifikate von der Corporate CA ausstellen zu können. Zudem kann das Modul auch als Proxy für eine Microsoft CA verwendet werden, um den direkten Zugriff auf die CA für alle Client-Systeme zu verhindern.

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

Das true-Xtender Third Party Certificate Manager Add-on dient zur Überwachung von Drittanbieter-Zertifikaten. Es können mehrere Benachrichtigungsdienste eingerichtet werden, die einen Benutzer informieren, sobald ein Zertifikat das Ende seiner Lebensdauer erreicht. Die zu überwachenden Zertifikate werden über das Web-GUI oder die Webservice Schnittstelle in die RA-Datenbank importiert. Mit dem Upload können zusätzliche Metadaten bereitgestellt werden, die dann bei den Benachrichtigungen vor dem Ablauf der Zertifikate verwendet werden können. Das Rollenkonzept des true-Xtender Third Party Certificate Manager Add-ons basiert auf Active Directory Benutzergruppen.

true-Xtender AutoEnroll PKI Proxy (TX-AEP)

Der true-Xtender AutoEnroll PKI Proxy wird als Proxy zwischen true-Xtender RA und der externen Schnittstelle einer öffentlichen CA verwendet. Alle Zertifikate werden von der true-Xtender RA-WA verwaltet und überwacht. Dies ermöglicht ein einheitliches Cockpit für alle internen und öffentlichen Zertifikate.

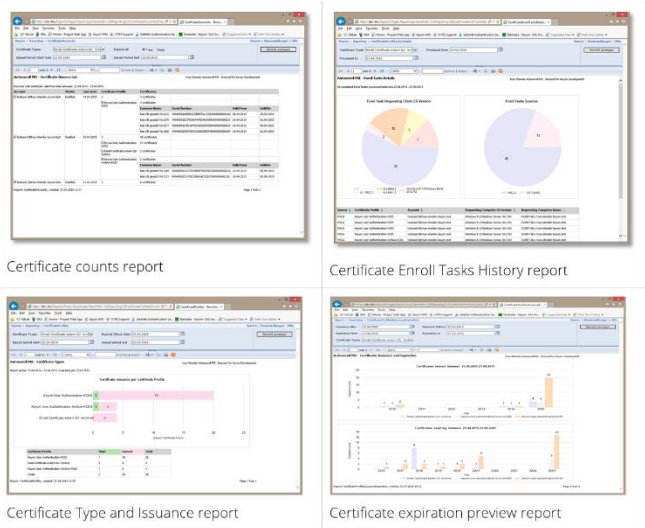
true-Xtender AutoEnroll PKI (TX-AE)

true-Xtender AutoEnroll PKI verbindet die Microsoft Autoenrollment Funktion mit einem öffentlichen PKI Service. Dadurch ergibt sich die Möglichkeit, firmeninterne Zertifikate gewohnt automatisiert auszugeben und zu verwalten, ohne dafür eine eigene Microsoft CA zu betreiben.

Mit dem true-Xtender AutoEnroll PKI kann zudem die Autoenrollment Funktion der Microsoft PKI entscheidend erweitert werden.

- Autoenrollment von öffentlichen Zertifikaten. Jede öffentliche CA die eine Webservice Schnittstelle anbietet kann integriert werden.
- Autoenrollment basierte Erneuerung von Zertifikaten im Falle einer Änderung von Benutzer- oder Serverattributen.
- Flexibles Lifecycle-Management von Benutzer- und Serverzertifikaten.

Ein umfassendes und intuitives Web-GUI sowie umfangreiche Reporting Services bilden das Cockpit für alle im Unternehmen verwendeten Zertifikate.



true-Xtender PKI Services

Die true-Xtender PKI Services bieten zusätzliche Unterstützungsfunktionen für das Lifecycle-Management von Zertifikaten und Sperrlisten.

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

Der true-Xtender Auto-Revocation Service ist das Pendant zu der von Microsoft angebotenen Autoenrollment Funktion. Der true-Xtender Auto-Revocation Service revoziert ein Zertifikat, sobald dessen zugeordnetes Computer- oder Benutzerobjekt im AD entfernt wird. Er widerruft auch doppelte Zertifikate, d.h. Zertifikate desselben Typs, die für denselben Subject DN ausgestellt wurden. Der Schwellenwert der Anzahl zu revozierender Zertifikate kann konfiguriert werden, um einen unbeabsichtigten Wiederruf bei AD-Strukturänderungen zu verhindern (z.B. Verschieben von Benutzern in eine andere Organisationseinheit (OU)). Alle Aktionen des Services werden im Windows Application Event Log aufgezeichnet.

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

Der true-Xtender Standalone Certificate Expiration Service prüft periodisch, ob Zertifikate innerhalb einer bestimmten Zeit ablaufen. Falls Zertifikate ablaufen, sammelt der Service die Daten zu den ablaufenden Zertifikaten aus der Microsoft CA Datenbank und verschickt Erinnerungsemails an Zertifikatsverantwortliche oder Administratoren. Alle Aktionen des Services werden im Windows Application Event Log aufgezeichnet.

true-Xtender CRL Management Service (SE-CD)

Der true-Xtender CRL Management Service wird im Zusammenhang mit der Überwachung von CRL Distribution Points und der Verteilung von Sperrlisten an unterschiedliche CRL Distribution Points (CDPs) eingesetzt. Der Service überwacht, ob die konfigurierten CRL Distribution Points die jeweils aktuellen Sperrlisten bereitstellen. Im Fehlerfall versendet der CRL Distribution Service eine E-Mail an Administratoren und aktualisiert entsprechend den Windows Application Event Log. Der Service unterstützt unterschiedliche Quellen von CRLs und kann diese über LDAP, File Shares oder Script-Aufruf an die CDPs verteilen.

true-Xtender CRL Publication Service (SE-CP)

Der true-Xtender CRL Publication Service publiziert die Zertifikatsperrliste (CRL) unmittelbar nach dem Eingang eines sogenannten Revokations-Antrages auf der Microsoft CA. Im Weiteren wird in einem regelmässigen Intervall (z.B. einmal täglich) eine Sperrliste publiziert, auch wenn kein neuer Sperreintrag vorhanden ist.

Durch die Verwendung des true-Xtender CRL Publication Services entfällt die regelmässige Publikation der Sperrlisten wodurch diese beispielsweise vom einem Online-Responder nicht unnötig neu eingelesen werden müssen. Eine Sperrliste wird nur dann neu eingelesen, wenn diese aufgrund eines neuen Sperreintrages aktualisiert wurde.

Der true-Xtender CRL Publication Service wird als Windows-Service installiert und als sogenanntes Exit-Modul auf der Microsoft CA registriert. Die Publizierungsintervalle sowie weitere Applikationsspezifische Parameter können in einer XML-Datei konfiguriert werden.

Keyon Revocation Provider

Es sind zwei Module für den true-Xtender Revocation Provider erhältlich:

Keyon Caching Resync Revocation Provider (RP-CL)

Die Prüfung gegen Widerruf erfolgt im Windows CryptoAPI über installierbare Revocation Provider, wobei Microsoft Standardmässig einen Revocation Provider zur Verfügung stellt, der die Sperrinformationen über OCSP und Sperrlisten ermitteln kann.

Bei der Verwendung von Sperrlisten durch den Standard Microsoft Revocation Provider kann jedoch nicht davon ausgegangen werden, dass eine Sperrung eines Zertifikats zeitnah festgestellt werden kann, da die Sperrlisten und auch OCSP Antworten aufgrund verschiedener Parameter lokal gecached werden.

Die Keyon Revocation Provider stellen sicher, dass CRLs und OCSP Antworten einer CA nach einer konfigurierbaren Zeit neu geladen statt aus dem Cache gelesen werden.

Anwendungsbeispiel:

Bei der Ausstellung von temporären Smartcards wird die aktive Smartcard suspendiert und temporär auf der Sperrliste aufgeführt. Damit ein Mitarbeiter nach Rückgabe der temporären Smartcard seine alte Smartcard möglichst bald wiederverwenden kann, müssen die Domänencontroller nach Aufhebung der Suspendierung die aktuellste Sperrliste verwenden.

Der Keyon Caching Resync Revocation Provider wird hauptsächlich auf Domänencontrollern und Windows-Servern eingesetzt, wo Benutzerzertifikate gegen Widerruf geprüft werden.

Keyon Fallback and BCM Revocation Provider (RP-DC)

Durch die Verwendung des Keyon Fallback and BCM Revocation Providers kann der Windows Logon mittels Smartcard auch bei einem längeren Totalausfall einer PKI garantiert werden.

Kann ein Domänencontroller beim Start sein eigenes Zertifikat nicht mittels einer gültigen Sperrliste oder OCSP Anfrage überprüfen, dann deaktiviert er die Funktion für den Smartcard Logon.

Kann keiner der installierten Revocation Provider bei einem Smartcard Logon Event das Zertifikat des Clients überprüfen, liefert der Keyon Fallback and BCM Revocation Provider den Status „nicht gesperrt" zurück und erstellt einen Eintrag im Eventlog des Domänencontrollers.

Der Keyon Fallback and BCM Revocation Provider wird hauptsächlich auf Domänencontrollern und Windows-Servern eingesetzt, wo Benutzerzertifikate gegen Widerruf geprüft werden.

Keyon Credential Provider (CP)

Der Keyon Credential Provider ermöglicht die Forcierung des Smartcard Logons, ohne dass das AD Passwort eines Mitarbeiters randomisiert wird. Dies ermöglicht die Kompatibilität mit Anwendungen, die Benutzernamen und Kennwörter anhand von AD prüfen und nicht Kerberos oder zertifikatsbasierte Authentifizierung unterstützen.

Der Keyon CP erlaubt die Anmeldung mit Benutzernamen und Passwörtern nur für lokale Administratoren und für Mitglieder von definierten AD Gruppen. Zusätzlich können so genannte "Deny Password Logon" AD Gruppen definiert werden, welche die AD Gruppen überschreiben, für die die Smartcard-Anmeldung nicht erzwungen wird.

Wenn der Keyon CP nicht feststellen kann, ob ein Benutzer lokaler Admin oder Mitglied einer definierten AD Gruppe ist, ist die Anmeldung mit Benutzername und Passwort nicht möglich. Der Keyon CP speichert Gruppenmitgliedschaften von Benutzern im Cache, um das Offline-Anmeldeszenario zu unterstützen.

Ein zweiter Smartcard Credential Provider Wrapper ermöglicht das AD-Passwort zu ändern, falls die Richtlinien dies erfordern, wenn der Benutzer versucht sich mit einer Smartcard anzumelden. Dadurch wird sichergestellt, dass Passwortänderungsrichtlinien auch für Benutzer durchgesetzt werden können, die sich nur interaktiv mit einer Smartcard anmelden dürfen.

Der Keyon CP unterstützt Windows 7 und Windows 10. Die Konfiguration kann über Gruppenrichtlinien festgelegt werden.

Keyon Certificate Propagator (CE-PR)

Der Microsoft Certificate Propagation Service (CertPropSvc) importiert die Zertifikate beim Einlegen der Smartcard und beim Anmelde- / Entsperrvorgang in den User Certificate Store.

Der Microsoft Certificate Propagation Service (CertPropSvc) läuft standardmäßig für alle auf einem System verfügbaren Smartcards, d.h. die Zertifikate anderer Benutzer werden auch in den Zertifikatsspeicher des aktuell angemeldeten Benutzers übertragen. Diese Zertifikate werden dann in Auswahldialogen angezeigt.

Keyon Certificate Propagator Funktionalität

Der Keyon Certificate Propagator ersetzt den Microsoft Certificate Propagation Service (CertPropSvc) und importiert nur die Zertifikate des aktuell angemeldeten Benutzers, die entsprechend der Konfiguration importiert werden sollen.

Der Keyon CE-PR verfügt über eine Architektur, die es ermöglicht, die Funktionalität bei verschiedenen Ereignissen (Smartcard gesteckt, Smartcard entfernt) durch Plug-ins in Form von DLLs zu erweitern. Durch diese Architektur können Anwendungen oder Scripts bei einem Ereignis wie die anstehende Zertifikatserneuerung gestartet werden.

Beim Start des CE-PRs werden die folgenden Aktionen ausgeführt:

- Die Zertifikate aller derzeit im System verfügbaren Smartcards werden ermittelt.
- Die Smartcard-Zertifikate, die einem Smartcard-CSP / KSP zugeordnet wurden, sich aber auf keiner der eingesetzten Smartcards befinden, werden im Zertifikatsspeicher des Benutzers gelöscht.

Während die Anwendung ausgeführt wird, werden die folgenden Aktionen beim Einlegen einer Smartcard ausgeführt:

- Die Zertifikate auf der eingelegten Smartcard werden ermittelt.
- Die Smartcard-Zertifikate, die die gleiche Benutzer-ID haben, aber auf keiner der eingesetzten Smartcards vorhanden sind, werden im Zertifikatsspeicher des Benutzers gelöscht.

Während die Anwendung ausgeführt wird, werden die folgenden Aktionen beim Entfernen einer Smartcard ausgeführt:

- Wenn die Zertifikate auf der Remote-Smartcard zu dem angemeldeten Windows-Benutzer gehören (UPN im Authentifizierungszertifikat = UPN des Windows-Benutzers), werden keine Aktionen durchgeführt und keine Zertifikate gelöscht.
- Wenn die Zertifikate auf der Remote-Smartcard nicht dem angemeldeten Windows-Benutzer gehören, werden die Zertifikate im Zertifikatsspeicher des Benutzers gelöscht.

Die Anwendung hat keine Benutzeroberfläche und läuft unsichtbar im Hintergrund. Es werden nur Zertifikate mit einem KSP / CSP für Smartcards berücksichtigt. Soft-Token werden nicht behandelt.