

keyon true-Xtender

Für Ihr Enterprise PKI

Die keyon true-Xtender Suite der Swiss IT Security AG ergänzt Ihre Enterprise PKI zu einer umfassenden Lösung für die Ausgabe und Verwaltung von X.509 Zertifikaten.

Erweitern Sie die Funktionalität Ihrer Enterprise PKI mit der keyon true-Xtender Suite, einer umfassenden Sammlung von Diensten und Anwendungen, die Benutzerfreundlichkeit mit mehr Flexibilität und Funktionen verbindet.

Alle Module werden auf Windows 2016 und 2019 unterstützt und bieten volle Enterprise Funktionalität. Eine Active Directory Schemaerweiterung ist nicht notwendig. Die keyon true-Xtender Suite besteht aus den folgenden Modulen.

keyon true-Xtender Policy Module (TX-PMSA)

Das keyon true-Xtender Policy Module erweitert die Eigenschaften der Enterprise 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 keyon true-Xtender Policy Modul von der Swiss IT Security AG 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.



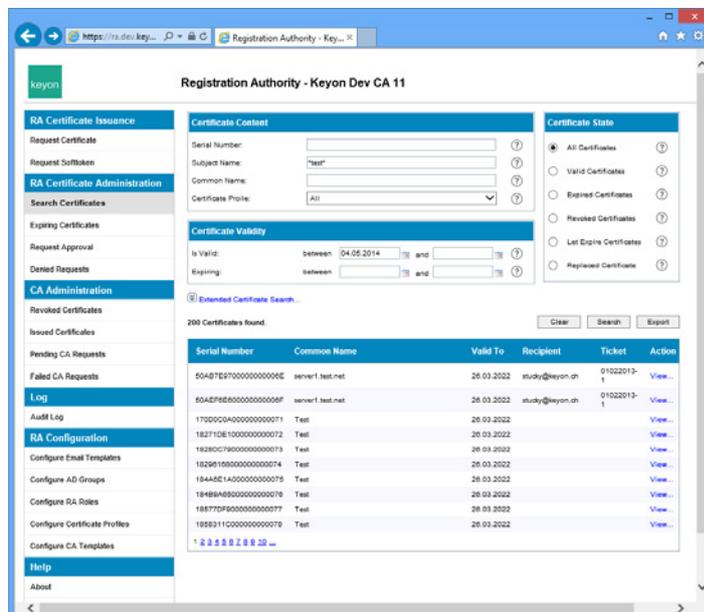
keyon true-Xtender Registration Authority Web Application (RA-WA)

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

Die keyon 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

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

Der keyon 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.



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

Das keyon 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 Zertifikatempfänger 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.

keyon 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

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

Das keyon 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 keyon true-Xtender Third Party Certificate Manager Add-ons basiert auf Active Directory Benutzergruppen.

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

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

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

Das keyon 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.

keyon true-Xtender AutoEnroll PKI Proxy (TX-AEP)

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



keyon true-Xtender PKI Services

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

KEYON TRUE-XTENDER AUTO-REVOCAION SERVICE (SE-CE-AR)

Der keyon true-Xtender Auto-Revocation Service ist das Pendant zu der von Microsoft angebotenen Autoenrollment Funktion. Der keyon 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 Widerruf 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.

KEYON TRUE-XTENDER STANDALONE CERTIFICATE EXPIRATION SERVICE (SE-CE-AR)

Der keyon 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.

KEYON TRUE-XTENDER CRL MANAGEMENT SERVICE (SE-CD)

Der keyon 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.

KEYON TRUE-XTENDER CRL PUBLICATION SERVICE (SE-CP)

Der keyon 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 keyon 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 keyon 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.



Revocation Provider

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

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

FALLBACK AND BCM REVOCATION PROVIDER (RP-DC)

Durch die Verwendung des 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 Fallback and BCM Revocation Provider den Status „nicht gesperrt“ zurück und erstellt einen Eintrag im Event Log des Domänencontrollers.

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

Credential Provider (CP)

Der 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 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 CP nicht feststellen kann, ob ein Benutzer lokaler Admin oder Mitglied einer definierten AD Gruppe ist, ist die Anmeldung mit Benutzernamen und Passwort nicht möglich. Der 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 CP unterstützt Windows 7 und Windows 10. Die Konfiguration kann über Gruppenrichtlinien festgelegt werden.

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.

Certificate Propagator Funktionalität

Der 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 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.



keyon true-Xtender AutoEnroll PKI (TX-AE PKI)

Keyon true-Xtender AutoEnroll PKI erweitert die Microsoft Autoenrollment Funktion mit dem Bezug von Zertifikaten einer öffentlichen CA Ihrer Wahl und ermöglicht auch die automatisierte Ausgabe und Verwaltung von Zertifikaten auf Windows domain- und non-domain joined Systemen, Mac OS, Linux/Unix, iOS, Android und Windows Mobile

Der keyon true-Xtender AutoEnroll PKI (TX-AE PKI) ermöglicht die automatisierte und einfache Ausgabe und Verwaltung von Personen- und Gerätezertifikaten für alle Microsoft Betriebssysteme sowie für Mac

OS, Linux und weitere non-Microsoft Clients. Dazu kann eine interne Enterprise PKI oder eine öffentliche PKI genutzt werden. Eine firmeninterne Enterprise PKI muss jeweils eigenständig aufgebaut und betrieben werden. Das Betreiben einer solchen PKI erfordert eine entsprechende Infrastruktur, Hardware Security Module und nachhaltiges Know-how.

TX-AE PKI ermöglicht Ihnen den Betrieb einer CA vollständig auszulagern, ohne auf die Vorteile der automatisierten Zertifikatsverteilung und Verwaltung zu verzichten.

Eigenschaften

TX-AE PKI bietet ein umfangreiches Life-Cycle Management von Zertifikaten und überzeugt mit folgenden Eigenschaften:

AUTOMATISCHES AUSSTELLEN VON ZERTIFIKATEN

Auf Basis von Active Directory und entsprechenden Richtlinien wird geprüft, ob ein Zertifikat ausgestellt werden muss. Zusätzlich erlaubt TX-AE PKI das erneute Ausstellen von Zertifikaten im Falle von Attributs Wechsel. Dies findet beispielsweise Anwendung bei einer Namensänderung oder bei einem Abteilungswechsel (Änderung vom CN oder OU oder anderen Zertifikatsattributen).

AUTOMATISCHES ERNEuern VON ZERTIFIKATEN

Die Zertifikate werden vor Ablauf ihrer Gültigkeit automatisch erneuert. Die Zeitspanne zwischen den ersten Erneuerungsversuchen und dem Ablauf der Zertifikate ist konfigurierbar (renewal time).

AUTOMATISCHE REVOZIEREN VON ZERTIFIKATEN

Basierend auf einem flexiblen Regelwerk können Zertifikate automatisch revoziert werden. Dies findet insbesondere Anwendung bei Austritten von Personen aus der Firma oder Dekommissionierung von Geräten.

SCHNITTSTELLEN UND CA INTEGRATION

Die Anbindung von TX-AE PKI an die öffentliche CA basiert auf der weit verbreiteten RFC 2797 Schnittstelle oder einer CA spezifischen Schnittstelle.

ZERO FOOTPRINT INSTALLATION

TX-AE PKI benötigt keine clientseitige Software Installation. Falls im Rahmen eines autoenrollment Prozesses die Key-History von Verschlüsselungszertifikaten importiert werden soll, kann ein Client auf die Endgeräte ausgerollt werden. Die Standard Autoenrollment Funktion von Microsoft bietet hierzu keine off-the-shelf Lösung.



PARALLELBETRIEB INTERNE UND ÖFFENTLICHE CA

Die Auslagerung der firmeninternen Zertifikate, die beispielsweise im Bereich der Personen- oder Geräteauthentisierung genutzt werden, konnte aus Mangel der Integration in eine öffentliche CA nicht umgesetzt werden.

TX-AE PKI verbindet ihr Unternehmen mit einer öffentlichen CA Ihrer Wahl. Dies ermöglicht Ihnen den Betrieb einer CA vollständig auszulagern, ohne auf die Vorteile der automatisierten Zertifikatsverteilung- und Verwaltung zu verzichten. Die gleichzeitige Integration von mehreren internen und öffentlichen CAs ist ebenfalls möglich. Dies lässt beispielsweise eine nahtlose Migration von einer internen zu einer öffentlichen CA zu.

BEREITSTELLUNG AUSGESTELLTER ZERTIFIKATE AN MDM

- ✘ Automatisierte Verteilung von Personen- oder Gerätezertifikaten auf O365 Intune MDM*1 verwaltete iOS oder Android Geräte unter Verwendung einer Microsoft PKI oder einer öffentlichen PKI.
- ✘ Key Archive und Recovery Optionen für S/MIME Zertifikate

UMFANGREICHES COCKPIT

TX-AE PKI stellt ein Web-basiertes GUI für sämtliche Aktivitäten oder Abfragen zu Verfügung. Umfangreiche Reports geben Einsicht in Prozessfortschritte oder Systemzustände, die beispielsweise auch für eine Kostenverteilung der Zertifikatsnutzung nach Organisationseinheiten genutzt werden kann (siehe Abbildung 1 und 2 unten).

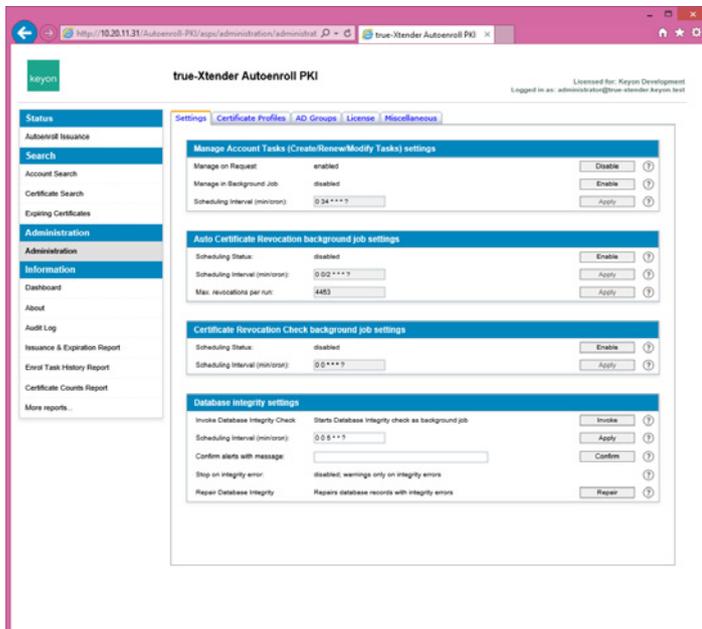


Abbildung 1

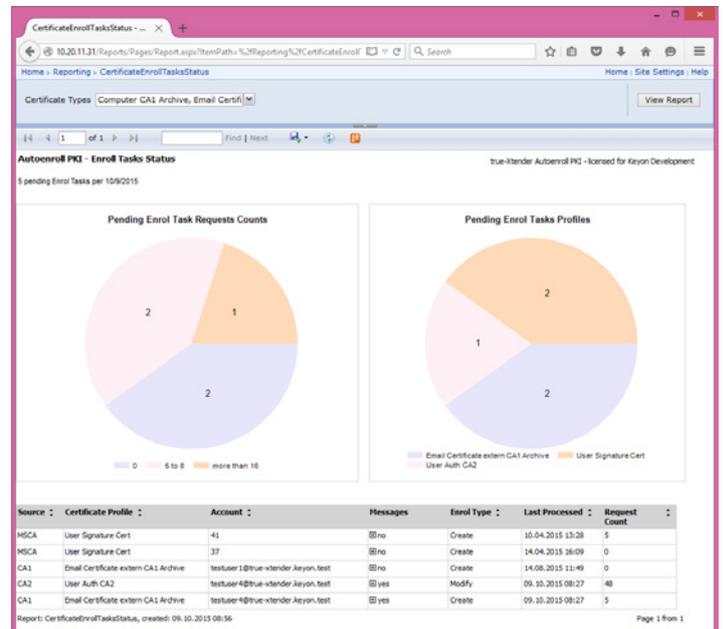


Abbildung 2



Erweiterte Funktion

TX-AE PKI bietet mit zusätzlichen Schnittstellen folgende Möglichkeiten:

| BETRIEBSSYSTEM | BESCHREIBUNG |
|---|--|
| Microsoft Windows | Microsoft Autoenrollment von Domain joined Windows Systemen oder Benutzern über CES oder DCOM. Microsoft Autoenrollment von nicht Domain joined Windows Systemen oder Benutzern über CES. |
| Mac OS | Certificate Enrollment für Mac OS über DCOM oder SCEP. |
| Linux / Unix | Certificate Enrollment für Linux / Unix über DCOM oder SCEP. |
| Mobile Geräte (iOS, Android, Blackberry) | Certificate Enrollment für mobile Geräte / MDM über DCOM oder SCEP. |
| Mobile Geräte (iOS, Android, Blackberry) | Certificate Enrollment zu mobilen Geräten durch MDM (Intune oder andere MDM-Lösungen). |

