

Windows PKI

Secardeo GmbH, 2008

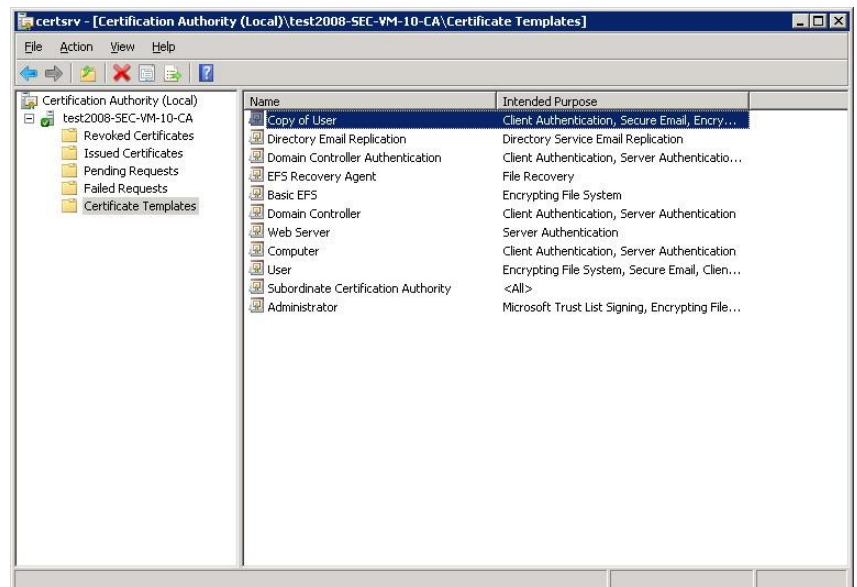
Windows PKI

Was ist PKI?

Eine Public Key Infrastruktur (PKI) stellt Schlüssel, Zertifikate und weitere Dienste bereit, mit denen ein effizientes und verlässliches IT-Security Management möglich ist. Mit digitalen Zertifikaten, die von einer Certification Authority (CA) ausgestellt werden, kann heute eine Vielzahl von Anwendungen auf einem äußerst hohen Niveau abgesichert werden. Die Zertifikate einer PKI können für sichere E-Mail, Web-Security, Windows SmartCard-Logon, VPN, Verschlüsselung von Dateisystemen und Dokumenten sowie digitale Signaturen verwendet werden.

Worin liegt der Nutzen?

PKI macht den Einsatz kryptographischer Sicherheitsmechanismen in großen Unternehmen beherrschbar. PKI ermöglicht die Verschlüsselung von Daten, die starke Authentisierung von Benutzern und IT-Komponenten sowie die digitale Signatur. Das Sicherheitsniveau kann damit signifikant angehoben werden. Probleme mit vergessenen oder geknackten Passwörtern und damit verbundenen Helpdesk-Kosten sowie der systemübergreifenden Verwaltung digitaler Identitäten (Identity Management) lassen sich mit einer PKI minimieren. Der Zugriff auf vertrauliche Informationen kann auch beim Outsourcing sensibler Teile des IT-Betriebs sicher kontrolliert werden. Erst mit einer PKI ist auch der Einsatz digitaler Signaturen und die damit verbundene weit reichende Automatisierung von Geschäftsprozessen möglich. PKI bietet



- hohe Sicherheit
- Erfüllung von Compliance
- durchgängige Basis für Sicherheitsanwendungen
- effizientes Identity Management
- erhöhten Benutzer-Komfort und
- Kostenreduktion bei Administration und Helpdesk.

Warum Windows PKI?

Die Basis für eine Windows PKI steht mit Windows Server und den darin enthaltenen Active Directory Certificate Services (AD CS) kostengünstig zur Verfügung. Erstmals war dieser Dienst in Windows NT 4.0 enthalten und kann heute mit der in Windows Server 2008 enthaltenen Version als äußerst ausgereift bezeichnet werden. Somit konnte sich die Windows PKI inzwischen am Markt etablieren und neben kleineren und mittleren Installationen existieren inzwischen auch globale Infrastrukturen mit einigen tausend Benutzern. In einer reinen Windows Infrastruktur spielen die Certificate Services in der Kombination mit Active Directory ihre Vorteile als Enterprise CA klar aus. Aber auch in heterogenen Umgebungen werden Produkte von anderen Herstellern wie Adobe, Cisco oder Open Source Tools durch die unterstützten Standardformate und –schnittstellen gut unterstützt. Mit Windows können Zertifikate kostengünstig und benutzertransparent mit Autoenrollment verteilt oder mit manuellen Registrierungsverfahren und Enrollment Agents zuverlässig ausgestellt werden. Dabei werden Softwareschlüssel als auch SmartCards unterstützt. Microsoft hat in der Architektur eine Reihe von Schnittstellen für Erweiterungen und unternehmensspezifische Anpassungen vorgesehen. Damit können auch SmartCard oder Token Management Systeme angebunden werden.

Was leistet die Windows PKI?

Die Windows PKI unterstützt wichtige PKI-Standards wie X.509, PKIX und PKCS. Mit der Windows PKI können unterschiedliche Vertrauensmodelle und Zertifizierungsstrukturen abgebildet werden. Eine Windows CA kann in einer mehrstufigen Hierarchie die Rolle einer Root, Intermediate oder Issuing CA einnehmen.

Die Windows CA kann in zwei verschiedenen Varianten betrieben werden:

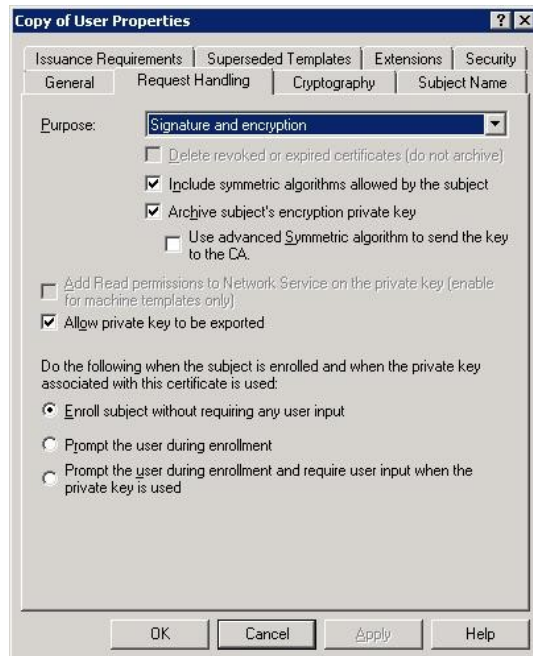
Als Standalone CA ist der Einsatz ohne Active Directory möglich. Eine Standalone CA kann auch logisch in die AD Domäne integriert sein, ohne ständig verfügbar sein zu müssen. Ein Beispiel dafür ist eine Offline Root-CA für eine Domäne. Diese Variante kann einerseits ein hohes Maß an Sicherheit bieten, andererseits sind die Möglichkeiten der Benutzerregistrierung und der Zertifikatsverwaltung eingeschränkt.

Die Variante Enterprise CA ist vollständig in eine AD Domäne integriert. Ausgestellte Zertifikate und Sperrlisten werden automatisch in das AD publiziert. Zur komfortablen und flexiblen Beantragung von Zertifikaten werden sogenannte Zertifikatsvorlagen (Certificate Templates) verwendet. Damit können unterschiedliche Registrierungsszenarien bis hin zur automatischen Beantragung und Zertifizierung (Autoenrollment) ohne Benutzerinteraktion realisiert werden. Mit einer Zertifikatsvorlage können auch individuelle Zertifikatsprofile mit anwendungsspezifischen Erweiterungen entworfen werden.

Windows unterstützt eine Reihe von Krypto-Algorithmen und so genannte Crypto Service Provider (CSP). Über solche CSPs werden Schlüsselpaare entweder innerhalb des Betriebssystems oder mit externen Hardwarekomponenten wie SmartCards generiert. In einer Windows PKI können somit Softwareschlüssel als auch SmartCards zur Verschlüsselung, Authentisierung oder digitalen Signatur verwendet werden.

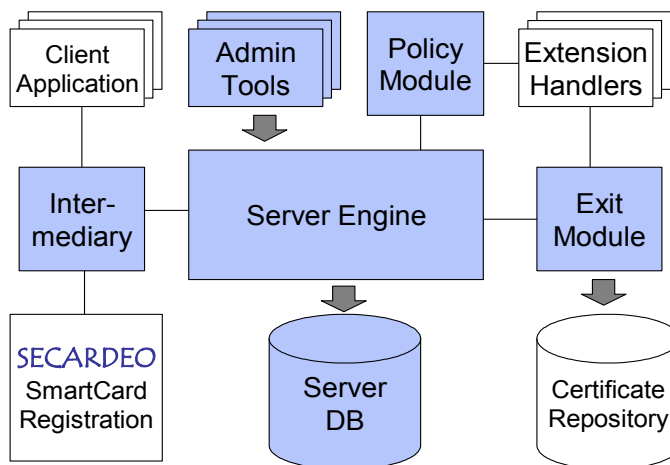
Die Windows CA kann auch für die Sicherung und das Wiederherstellen von privaten Deciffrierschlüsseln genutzt werden. Diese werden verschlüsselt in der Datenbank der CA gespeichert und können über so genannte Wiederherstellungsagenten (KRA) mit speziellen Zertifikaten wieder hergestellt werden. Das ist wichtig, um beispielsweise nach einem möglichen Verlust des Schlüssels chiffrierte E-Mails wieder lesen zu können.

Periodisch von AD CS ausgestellte Sperrlisten (CRL) und Delta-Sperrlisten ermöglichen die Prüfung der Gültigkeit eines Zertifikats. Ab Server 2008 wird ferner die direkte Abfrage der Gültigkeit eines Zertifikats über das Online Certificate Status Protocol (OCSP) unterstützt. Dieses Verfahren ist effizienter und vermeidet das Herunterladen großer CRLs über das Netzwerk.



Wie funktioniert die Windows CA?

Die Windows CA ist modular aufgebaut und verfügt über eine Vielzahl von Schnittstellen. Eine Client-Anwendung wie beispielsweise der Internet Explorer erzeugt ein Schlüsselpaar und sendet eine Zertifikatsanforderung an einen Vermittler (Intermediary). Von diesem erhält er später das ausgestellte Zertifikat zurück. Der Intermediary, beispielsweise die Internet Information Services, stellt dem Client eine Schnittstelle, in diesem Beispiel als Web-ASP Seite, bereit und kommuniziert mit der zentralen CA Server Engine über COM-Schnittstellen. Die Server Engine übergibt empfangene Zertifikatsanforderungen an das zuständige Policy-Modul und erzeugt und signiert das beantragte Zertifikat. Zertifikate und optional zu archivierende private Schlüssel werden in der lokalen Zertifikatsdatenbank gespeichert und an ein Exit-Modul übergeben.



Das Policy Modul überprüft Zertifikatsanforderungen und ergänzt oder modifiziert diese bei Bedarf. Es trifft die Entscheidung über die Ablehnung, direkte Ausstellung oder die Zurückstellung einer Anfrage. Eine Enterprise CA verwendet das mit installierte Enterprise Policy Modul, eine Standalone CA verwendet eine andere Default-Policy. Ein Exit-Modul wird aufgrund bestimmter Ereignisse, beispielsweise Ausstellung eines neuen Zertifikats, aufgerufen. Die Hauptaufgabe ist die Publikation von Zertifikaten und CRLs, beispielsweise in das AD. Es besteht die Möglichkeit, individuelle Policy- und Exit-Module zu implementieren und zu integrieren.

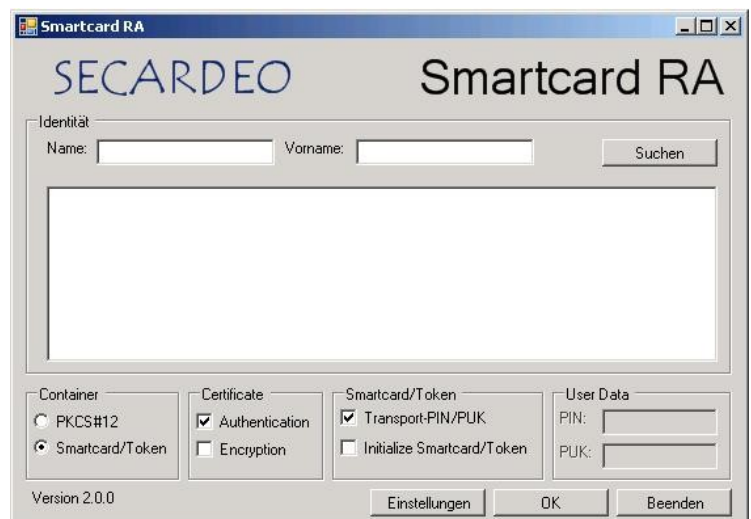
Über die Administrationsschnittstelle können Zertifikatsanforderungen freigegeben oder abgelehnt werden. Bestehende Zertifikate können auf Gültigkeit geprüft oder gesperrt werden. Ferner kann die Ausstellung einer CRL ausgelöst werden.

Was ist beim Einsatz von SmartCards zu beachten?

Windows und AD CS unterstützen SmartCards und andere Komponenten wie USB Crypto Tokens und Hardware Security Module (HSM). Hierfür muss der jeweilige CSP der SmartCard installiert sein und der Zugriff über ein Kartenlesegerät ermöglicht werden. Ursprünglich war die Nutzung von SmartCards von Microsoft eingeschränkt für Authentisierungszwecke wie beispielsweise Windows SmartCard Logon. Schlüssel zur Authentisierung und digitalen Signatur können hoch sicher auf einer SmartCard generiert werden und jederzeit problemlos durch neue Schlüssel oder SmartCards ersetzt werden. Für den Einsatz von SmartCards zur Ver- und Entschlüsselung existieren höhere Anforderungen. Insbesondere müssen eine Archivierung des privaten Schlüssels und eine jederzeitige Rekonstruktion desselben möglich sein. Viele SmartCards und zugehörige CSPs bieten hierfür keine geeignete Unterstützung.

Auf dem Markt gibt es dazu inzwischen Produkte wie Kartenverwaltungssysteme oder Token Managementsysteme. Microsoft bietet das Produkt Identity Lifecycle Manager (ILM) an, das die Komponente Certificate Lifecycle Manager (CLM) enthält und ein umfassendes, mächtiges Werkzeug darstellt. CLM erfordert die Installation eigener Policy- und Exit-Module auf einer Enterprise CA sowie eines Client-Moduls auf allen angebotenen Windows-Systemen. CLM unterstützt derzeit nur eine Auswahl von SmartCards und Tokens.

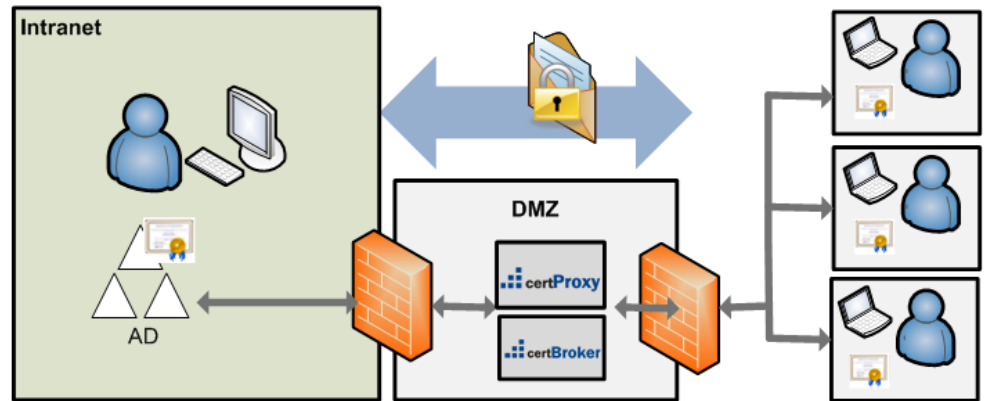
Eine schlanke, adaptierbare Alternative hierzu stellt die SECARDEO SmartCard RA (Registration Authority) dar. Die SmartCard RA ist ein universelles, SmartCard-unabhängiges Registrierungswerkzeug mit Key Backup Funktion. Eine Karte kann damit flexibel initialisiert und sicher parametrisiert werden. Zertifikate für bestehende öffentliche Schlüssel können ohne Neugenerierung verlängert und in beliebige LDAP Verzeichnisse publiziert werden. Die SmartCard RA kann in bestehende Kartenverwaltungssysteme integriert werden. Damit können multifunktionale Mitarbeiterausweise, die originär als Lichtbildausweis mit Zutrittskontrolle und Bezahlungsfunktionen ausgestattet sind, mit Kryptochip für PKI erweitert werden.



Wie kann man sicher mit anderen PKIen kommunizieren?

Zur Verschlüsselung, beispielsweise von E-Mails, wird das Zertifikat des Empfängers benötigt. Das ist im internen Firmennetz (Intranet) normalerweise problemlos möglich. Aber wie sieht es bei der Kommunikation mit externen Partnern aus? Innerhalb eines Windows AD Forests kann der Zugriff vom Client, z.B. Outlook, direkt auf das AD erfolgen.

Üblicherweise ist das AD aus Sicherheitsgründen jedoch nur aus dem Intranet und nicht von Extern erreichbar. Auf der anderen Seite ist eine Suche nach einem externen Zertifikat aus dem Intranet über mehrere LDAP-Verzeichnisse hinweg heute nicht oder nur sehr eingeschränkt möglich. Diese Einschränkungen werden mit SECARDEO certProxy und certBroker aufgehoben. Um



das externe Zertifikat eines Empfängers zu finden, ermittelt certBroker für den Client aufgrund der E-Mail Adresse das zuständige Verzeichnis und leitet die Suchanfrage dorthin weiter. Das zurück gelieferte Zertifikat wird an den Client übergeben, der die Verschlüsselung nun durchführen kann. Wenn ein externer Partner Daten für einen internen Empfänger verschlüsseln möchte, benötigt er dessen Zertifikat aus dem internen AD. Hierfür nimmt der certProxy LDAP-Suchanfragen von Extern entgegen und leitet sie an das interne AD weiter. Der Proxy sorgt dabei für die Zugangskontrolle und Blockierung systematischer Probianfragen sowie die Vertraulichkeit von Daten durch ein patentiertes Verfahren. certBroker und certProxy stellen zusätzlich die Interoperabilität verschiedener Client-Anwendungen mit unterschiedlichen LDAP-Servern her.

Was können Sie von SECARDEO erwarten?

Die Windows AD CS können mit wenigen Mausclicks und den entsprechenden Berechtigungen installiert und in Betrieb genommen werden. Eine von Microsoft vordefiniert Standardinstallation kann von einem versierten Systemadministrator mit wenig Aufwand durchgeführt werden. Ob eine solche Standardinstallation den Sicherheitsanforderungen entspricht, die im Unternehmen eingesetzten Systeme und Anwendungen abdeckt und langfristig zuverlässig und effizient betreibbar und erweiterbar ist – diesen Fragen sollte man sich vorab als IT-Verantwortlicher stellen. SECARDEO kann hierbei helfen, denn SECARDEO hat eine Vielzahl von PKI-Projekten erfolgreich durchgeführt und weiß, worauf es bei mittleren bis hin zu sehr große PKIen mit mehreren hunderttausend Benutzern ankommt!

SECARDEO unterstützt ein PKI-Projekt bereits bei der Vorbereitung und der technischen und organisatorischen Planung. Die Realisierung einer Windows PKI inklusive projektspezifischer Anpassungen und die Integration in individuelle IT-Landschaften gehört zu unseren Kernkompetenzen. Auch während des Betriebs bieten wir zuverlässige, kontinuierliche Support-, Check- und Troubleshooting-Leistungen an. SECARDEO hilft Ihnen dabei durch

- Know-how Transfer in Inhouse-Seminaren und Workshops zur Windows PKI,
- Erstellen eines technischen und organisatorischen PKI-Konzepts,
- Installation, sichere Konfigurierung und zuverlässige Inbetriebnahme von Windows AD CS,
- Generierung von hoch sicheren CA Schlüsseln mit Hardware,
- Erweiterung für die Verwaltung von SmartCards und Token mit MS CLM, Aladdin TMS oder SECARDEO SmartCard RA,
- Integration mit der Kartenverwaltung für multifunktionale Mitarbeiterausweise,
- Anbindung von externen Zertifikatsverzeichnissen,
- Bereitstellung eines sicheren Zugriffs auf interne Zertifikate,
- Anbindung bestehender Anwendungen und Systeme,
- Pilotierung und Unterstützung beim PKI-Rollout.

Benötigen Sie weitere Informationen?

Wenn Sie weitere Informationen wünschen, wenden Sie sich bitte an

Secardeo GmbH
Hohenadlstr. 4
85737 Ismaning
Tel. 089/18935890