DuD
Datenschutz und Datensicherheit

PKI-Unterstützung in Windows Server 2003

Holger Mack

Microsoft Windows 2003 Server verspricht PKI Funktionalitäten „umsonst“ als Teil des Betriebsystems, die man an von anderen Herstellern für viel Geld kaufen muss. Der folgende Beitrag gibt einen kurzen Überblick darüber was hinter der PKI Funktionalität, und besonders der CA Komponente von Windows Server 2003 steckt und wie diese genutzt werden kann.

Holger Mack

Konzeption und Umsetzung von PKI Lösungen, Anwendungsintegration, Sicherheitsanalysen

E-Mail: mack@secorvo.de

Einleitung

Eine besondere Rolle bei den Sicherheitsfunktionalität im Windows Server 2003 spielt die Integration von Public Key-Technologie als Teil des Betriebsystems. Public Key-Technologie wurde von Microsoft schon seit Windows 2000 konsequent eingesetzt, um bestehende Sicherheitsmechanismen zu verbessern (z. B. die Einführung zertifikatsbasierter Authentifikation), aber auch um neue Sicherheitsmechanismen direkt im Windows Betriebssystem zu unterstützen (z. B. Dateiverschlüsselung, IPSec). Diese Funktionen wurden in den aktuellen Versionen von Windows (XP Professional und Windows 2003 Server) weiterentwickelt.

Der vorliegende Beitrag beschäftigt sich hauptsächlich mit der Funktionalität des Microsoft Certificate Service, der Certification Authority (CA) Komponente von Windows 2003 Server. Hierbei wird untersucht, welche Dienste der Microsoft Certificate Service zu dem Aufbau einer PKI beitragen kann und welche Randbedingungen dabei zu beachten sind. Dies soll helfen, den Microsoft Certificate Service besser einordnen zu können, um über dessen Einsatz und geeignete Verwendung zu urteilen. Im Fokus dieses Beitrags steht der Windows Server 2003 als neuste Version des Microsoft Betriebsystems. An einigen Stellen wird aber auch auf Unterschiede und Abhängigkeiten zu den Versionen XP und 2000 eingegangen. Eine detailliertere Betrachtung der Funktionalitäten der Windows PKI findet sich in [MAC2_03].

Die PKI-Unterstützung von Microsoft umfasst allerdings nicht nur die CA-Funktionalität des Certificate Service, sondern schließt auch Client-Funktionalität ein wie z. B. die Zertifikatsverwaltung, die im Betriebssystem integriert ist. Durch die enge Verzahnung über das Windows Betriebssystem sind diese Punkte nicht immer komplett zu trennen, deshalb wird an einigen Stellen auch auf Client-Funktionalitäten eingegangen.

1 PKI Unterstützung in Windows 2003

Die PKI-Unterstützung in den betrachteten Windows Versionen (hauptsächlich XP/ 2003) zieht sich durch viele Bereiche des Betriebsystems. In Abbildung 1 sind deren wichtigste Komponenten dargestellt.

Eine zentrale Rolle spielt dabei der Certificate Service, der die Funktionen einer Zertifizierungsstelle (Certification Authority, CA) übernimmt, d. h. das Ausstellen und Sperren von Zertifikaten. Wie insgesamt in einer Windows 2003 Domäne spielt auch bei der Windows PKI der integrierte Verzeichnisdienst Active Directory Service (ADS) eine wichtige Rolle. Abhängig von der Betriebsart der CA dient das Active Directory sowohl zum Veröffentlichen von Zertifikaten und Sperrlisten und zur Registrierung der Teilnehmer als auch zur zentralen Steuerung der PKI-Funktionalität auf den Clients in einer Windows Domäne.

Auf Seiten der Zertifikatsbenutzer sind Funktionen zur Verwaltung von Zertifikaten, Sperrlisten und Schlüsseln sowie die Prüfung der Zertifikate und Zertifikatsketten in das Betriebsystem integriert. Über entsprechende Schnittstellen (z. B. CryptoAPI) können diese Funktionen von Programmierern in Anwendungen integriert werden. Diese Funktionalität ermöglicht es, den Benutzern PKI-Funktionalität in einer einheitlichen Weise zur Verfügung zu stellen. Teile dieser Zertifikatsverwaltung des Benutzers können innerhalb einer Windows 2003 Domäne von zentraler Stelle verwaltet und vorgegeben werden. Einige Microsoft Anwendungen, wie z. B. Outlook oder der Internet Explorer, bedienen sich bereits dieser Funktionalitäten, und immer mehr Hersteller von Drittprodukten machen sich diese zu Nutze. Mit Hilfe von sogenannten

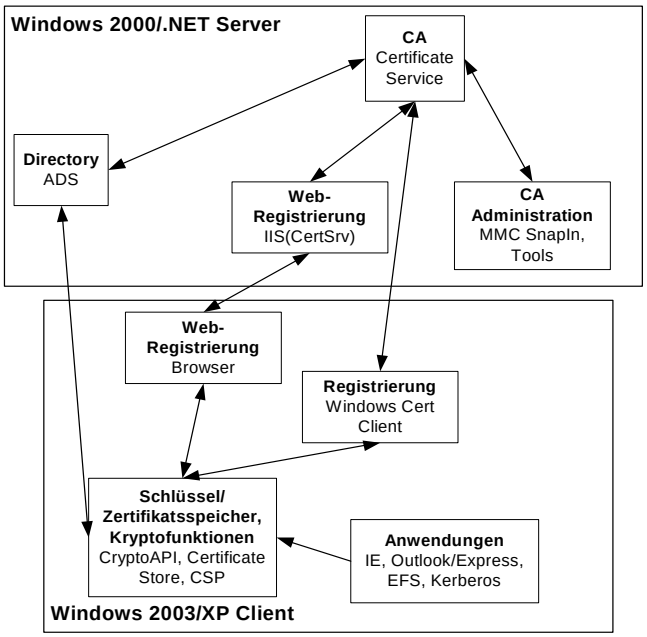

Abbildung 1: Komponenten Windows 2003 PKI

Cryptographic Service Providern (CSP) kann auch die in Windows 200x mitgelieferte Standard-Funktionalität erweitert werden, z. B. zur Unterstützung von kryptographischer Hardware, insbesondere von Smartcards.

Das Hauptaugenmerk in den folgenden Abschnitten gilt der CA-Komponente von Windows 2003 Server, dem Certificate Service. Diese Komponente konkurriert mit anderen auf dem Markt verfügbaren Produkten von Herstellern wie Entrust oder Betrusted, die sich auf CA-Komponenten spezialisiert haben.

2 Architektur

Der Certificate Service ist in eine größere Zahl von Modulen gegliedert, die unterschiedliche Aufgaben des Zertifikatsmanagements übernehmen. Abbildung 2 zeigt die Architektur des Certificate Service mit dazugehörigen Komponenten.

Die Server-Engine ist die zentrale Komponente in dieser Architektur. Sie ist verantwortlich für das Ausstellen von Zertifikaten und Sperrlisten. In der Server-Engine selber ist nur begrenzte Funktionalität integriert, nämlich das eigentliche Generieren der Zertifikate. Ein wichtiger Teil der PKI-Funktionalität ist in den verschiedenen Modulen implementiert, deren sich die Server-Engine bedient. Sie sind prinzipiell anpassbar und austauschbar, auch wenn in der Praxis meist mit den mitgelieferten Standardmodulen gearbeitet wird.

Für die PKI-Funktionalität sind vor allem die beiden Policy-Module Enterprise CA und Stand-Alone CA von Bedeutung, die Teil des Standard-Lieferumfangs von Microsoft sind. Welches dieser beiden Policy-Module eingesetzt wird, wird bei der Installation entschieden. Das Hauptkriterium ist dabei der Einsatzzweck der CA:

- Die *Enterprise CA* ist sehr tief in die Windows 200x Umgebung inklusive Active Directory integriert und setzt eine Windows 200x Domäne und Active Directory voraus.

Sie ist ausschließlich für die Zertifizierung von Benutzern und Rechnern innerhalb einer Domäne vorgesehen.

- Die *Stand-Alone CA* dagegen ist weitgehend unabhängig von anderen Komponenten (z. B. dem Active Directory) und kann unabhängig von einer Windows 2000 Domäne betrieben werden.

Die Zertifizierung erfolgt unabhängig von Domänen-Accounts. Im folgenden wird hauptsächlich auf die Enterprise CA eingegangen, da die Stand-Alone CA nur begrenzte Funktionalitäten anbietet.

3 Vergleichskriterien

Die Bewertung eines PKI-Produkts hängt in der Praxis sehr stark von wichtigen Rahmenbedingungen ab: Die Art des Einsatzes, die zu unterstützenden Anwendungen, die technische Einsatzumgebung und das geforderte Sicherheitsniveau sind einige der Kriterien, die bei einer solchen Bewertung berücksichtigt werden müssen.

Der Betrachtung in diesem Beitrag liegt kein explizites Einsatzszenario zu Grunde. Vielmehr soll hier versucht werden, eine möglichst generelle Einschätzung vorzunehmen. In diesem Rahmen soll anhand der wichtigsten Kriterien, die bei einem CA-Produkt zu berücksichtigen sind, die Funktionalität der Windows 2003 PKI beurteilt werden. Die folgenden Kriterien wurden dazu herangezogen:

- Vertrauensmodelle
- Standardunterstützung
- Registrierung und Schlüssel-/Zertifikatsverteilung
- Flexibilität
- Administration
- Directory-Unterstützung (Zertifikats- und Sperrlistenveröffentlichung)

In den folgenden Abschnitten wird auf diese Kriterien im Detail eingegangen.

3.1 Vertrauensmodell

Neben der Möglichkeit, eine Windows 2003 CA unabhängig zu betreiben, wird sowohl in Windows 2000 als auch in 2003 ein hierarchisches Vertrauensmodell (d. h. die Integration in oder der Aufbau einer PKI-Hierarchie) unterstützt. Dabei ist es möglich, CA Produkte anderer Hersteller oder Dienstleister beliebig mit Windows CAs in einer Hierachie zu verbinden. Cross-Zertifizierung [HAM_01] als zweite Methode wird seit der 2003 CA offiziell unterstützt. Neben dem reinen Ausstellen von Cross-Zertifikaten unterstützt Microsoft die sog. Qualified Subordination, mit der die Gültigkeit der Vertrauensbeziehung beschränkt werden kann (z. B. nur für bestimmte Anwendungen). Obwohl eine durchaus sinnvolle Methode, sind diese Einschränkungen in der Praxis nur wirksam, wenn sie von den verwendeten Clients richtig interpretiert werden. Es muss deswegen geprüft werden, in wie weit diese Einschränkungen in der spezifischen Umgebung (d. h. mit den eingesetzten Anwendungen) auch technisch durchgesetzt werden können.

Neben der Nutzung des hierarchischen Modells und der Cross-Zertifizierung bietet Windows weitere Möglichkeiten, Vertrauen zu anderen CAs herzustellen, zumindest innerhalb einer entsprechenden Windows Domänenstruktur. Diese Möglichkeiten

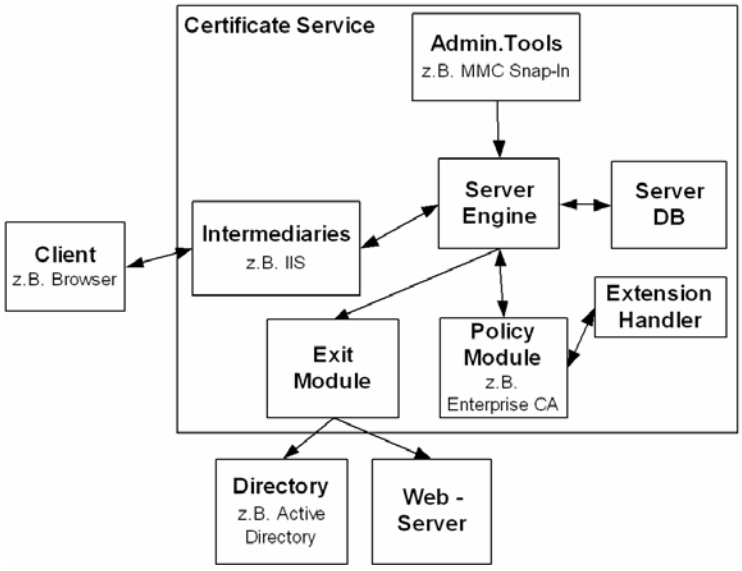

Abbildung 2: Windows 2003 Certificate Service Architektur

werden sowohl von Windows 2000 als auch von 2003 unterstützt. Ein Mechanismus, der dabei verwendet wird, sind die sogenannten Certificate Trust Lists (CTL).

Bei einer CTL handelt es sich um eine signierte Liste mit vertrauenswürdigen CA-Zertifikaten. Mit Hilfe des Active Directories und des Windows Group-Policy Mechanismus kann diese Liste an die Clients innerhalb einer Domäne verteilt und auch wieder gelöscht werden.

Auf diese Weise können von zentraler Stelle aus CAs als vertrauenswürdig innerhalb einer Domäne erklärt bzw. definiert werden. Programme, die die Client-Funktionalität von Windows 200x/XP verwenden, werden Zertifikate, die von CAs aus einer CTL stammen, automatisch als vertrauenswürdig anerkennen. Der CTL-Mechanismus ist eine proprietäre Lösung von Microsoft und entspricht keinem Standard.

3.2 Standardkonformität

Im Zuge der allgemeinen Öffnung von Windows zu etablierten IETF-, ISO- und ANSI-Standards in vielen Bereichen (z. B. DNS) basiert auch die PKI-Funktionalität von Windows 200x inzwischen in weiten Teilen auf internationalen Standards. Die wichtigsten darunter sind:

- X.509v3/v2 [X509_97] und PKIX RFC 2459/3280 [RFC2459] für Zertifikats- und Sperrlistenformate,
- PKCS für Signaturformate [PKCS_1] und Austauschformate [PKCS_7], [PKCS_10], [PKCS_12],
- LDAPv3 [RFC2251],
- PC/SC zur Smartcard Integration [PC/SC_97].

Zertifikatsformate

Bei den Zertifikatsformaten orientiert sich Microsoft an X.509v3 sowie den Zertifikats- und Sperrlistenprofilen, die in PKIX (RFC 3280) definiert sind.

In der 2003 CA werden die Zertifikatsinhalte über sogenannte Templates definiert. Hier gibt es weitreichende Möglichkeiten sowohl die Zertifikats-Inhalte als auch gewisse Verhaltensweisen bei der Verarbeitung der Zertifikate anzupassen. Die Zertifikatsinhalte können dabei nicht komplett flexibel gestaltet werden, d. h. einige Teile lassen sich nicht oder nur beschränkt anpassen.

Neben den Zertifikatsinhalten können über die Templates auch noch eine Reihe von anderen Parametern, die die Bearbeitung dieses Zertifikatstyps betreffen, konfiguriert werden. Auf die Details wird an den entsprechenden Stellen in diesem Beitrag eingegangen.

Die in den mitgelieferten Zertifikats-Templates definierten Zertifikatsinhalte entsprechen bis auf einige Details den in wichtigen Standards definierten Formaten. Diese Details können allerdings in der Praxis eine wichtige Rolle spielen. So verwendet Microsoft z. B. eigene, sogenannte Private Extensions, die vor allem bei originären Microsoft-Anwendungen benötigt werden (z. B. Encrypting File System, EFS), und einige Extensions werden nicht wie im Standard vorgesehen als „critical“ markiert.

Über die Zertifikats-Templates in Windows 2003 lassen sich aber die meisten dieser Probleme anpassen. Ein wichtiger Punkt bei der Anpassung der verwendeten Zertifikatsformate ist aber, dass Microsoft Anwendungen strikte Anforderungen an das Vorhandensein und das genaue Aussehen bestimmter Zertifikatserweiterungen stellen (z. B. Certificate Distribution Points, CDP). Sind diese nicht so vorhanden wie vorgesehen, kann es zu Einschränkungen bei der Client-Funktionalität kommen (z. B. beim Suchen und Importieren von Sperrlisten).

Der bekannt gewordene Fall eines falschen Verisign-Zertifikats für Microsoft [MAC1_00] hat die Bedeutung von Problemen, die an dieser Stelle auftreten können, deutlich aufgezeigt. Diese Problematik betrifft auch die CAs anderer Hersteller, sofern diese Zertifikate für Microsoft Anwendungen ausstellen wollen.

Insgesamt konnten im Rahmen verschiedener (nicht vollständiger) Tests die von Windows 2003 ausgestellten Zertifikate von Produkten anderer Hersteller in der Regel importiert und genutzt werden. Auch Interoperabilitätstests gegen das ISIS-MTT Testbed und im Rahmen der Federal Bridge CA in den USA deuten darauf hin, dass im Fall der Zertifikate weitgehende Interoperabilität erreicht werden kann.

Sperrlisten

Windows 2003 Certificate Service unterstützt standardmäßig Certificate Revocation Lists (CRLv2) als Mechanismus, um Zertifikate zu sperren. Hierbei werden Sperrlisten nach dem X.509 Standard eingesetzt [X509_97]. In der Windows 2003 CA werden zusätzlich sogenannte Delta-CRLs unterstützt.

Wichtig ist, dass Windows 200x/XP Clients Sperrlisten nur dann in Directories finden können, wenn im Zertifikat die CDP Extension mit der entsprechenden Information im richtigen Format enthalten ist. Ist diese Erweiterung nicht vorhanden (was vor allem bei älteren Zertifikaten der Fall ist) kann Windows 200x/XP nur gegen lokal importierte Sperrlisten prüfen.[1]

Austauschformate

Neben den oben beschriebenen Standards für Zertifikate und Sperrlisten unterstützt Windows 200x eine Reihe von Standards aus der PKCS-Serie zum Austausch von

[1] Die Prüfung gegen lokal importiere Sperrlisten wird allerdings nicht in allen Fällen und von allen Anwendungen unterstützt (siehe [MAC1_00]).

Zertifikatsanträgen, Schlüsseln und Zertifikaten. Die hier unterstützten Standards sind

- PKCS #10 für Zertifikatsanträge [PKCS_10],
- PKCS #7 zum Austausch von Zertifikaten und Zertifikatsketten [PKCS_7],
- PKCS #12 zum Austausch von privaten Schlüsseln [PKCS_12].

Diese Standards werden von nahezu allen anderen PKI-Produkten unterstützt.

3.3 Directory-Unterstützung

Eine direkte Directory-Unterstützung bietet der Certificate Service nur bei Verwendung der Enterprise Policy und des dabei installierten Exit Moduls. In diesem Fall werden Zertifikate und Sperrlisten automatisch im Active Directory veröffentlicht. Eine automatische Veröffentlichung in anderen Verzeichnissen via LDAP wird nicht unterstützt. Im Stand-Alone-Modus ist keine direkte Integration mit einem Directory vorhanden.

Active Directory unterstützt LDAPv3 in der Form, dass Anwendungen per LDAPv3 auf das Active Directory und die Zertifikate und Sperrlisten zugreifen können. So können auch Anwendungen anderer Hersteller Zertifikate und Sperrlisten nutzen, hierzu müssen die Clients allerdings die CDP (Certificate Distribution Point) und AIA (Authority Information Access) Erweiterungen zum Auffinden der Sperrlisten bzw. CA-Zertifikate im Active Directory unterstützen. Auch ein Abgleich (z. B. Replikation) mit anderen LDAP-Directories ist daher möglich. Im Rahmen des Verzeichnisdienstkozepts der PKI-1 Verwaltung [BSI_02] wurde eine solche Teilreplikation realisiert.

Da die Directory Struktur des Active Directory in der Praxis nicht der Namensstruktur in den Zertifikaten und Sperrlisten entspricht, kann es für Anwendungen, die nicht diese Erweiterungen unterstützen schwierig sein, die richtigen Informationen zu finden.

3.4 Flexibilität

Die Architektur des Certificate Service erlaubt durch die verschiedenen Module im Prinzip relativ große Flexibilität. Diese Flexibilität kann jedoch an vielen Stellen nur mit erheblichem Programmieraufwand genutzt werden. Mit entsprechendem Programmieraufwand lässt sich nahezu jede beliebige Funktion implementieren. Hier wird allerdings nur auf die Anpassungsmöglichkeiten eingegangen, die ohne Programmieraufwand genutzt werden können.

Durch Methoden wie die Anpassbarkeit der Zertifikats-Templates bietet Windows Server 2003 weitreichende Möglichkeiten, das Verhalten der CA zu gestalten. Die Einstellungen der Zertifikats-Templates haben Auswirkungen sowohl auf die Technik (z. B. Zertifikatsinhalte) als auch auf Abläufe (z. B. manuelle Freischaltung von Anträgen) in der PKI.

3.5 Registrierung und Erneuerung

Bei einer Enterprise CA ist die eigentliche Registrierung des Benutzers oder Computers das Anlegen eines Accounts in der Windows 2003 Domäne. Ist der Benutzer hier angemeldet, kann er z. B. mit Hilfe des Certification Managers in der MMC oder über die Registrierungswebseite der CA (mit Hilfe des Internet Information Servers, IIS) ein Zertifikat beantragen. Eine entsprechend vorkonfigurierte Webseite wird von Microsoft mitgeliefert. Der Benutzer wird anhand seines Windows Domänen Accounts mit Hilfe der im Active Directory gespeicherten Informationen authentifiziert, anschließend wird das Zertifikat automatisch ausgestellt.

Bei Windows Server 2003 gibt es zusätzlich die Option, dass eine manuelle Freigabe eines Zertifikatsantrags durch einen Administrator erfolgen muss. Dies kann entweder für jeden Zertifikatstyp individuell als Parameter des Zertifikats-Templates oder für eine CA insgesamt festgelegt werden. Die Anzahl der Zertifikate, die sich ein Benutzer so ausstellen lassen kann, ist nicht begrenzt, allerdings kann die Art von Zertifikaten, die ein Benutzer beantragen kann, über die Zugriffsrechte auf die Zertifikats-Templates im Active Directory eingeschränkt und kontrolliert werden. Der Zugriff auf die Zertifikats-Web-Seite kann außerdem durch die im IIS üblichen Mechanismen (Passwort, SSL/TLS etc.) kontrolliert werden.

Neben diesen vom Benutzer initiierten Methoden gibt es zwei weitere Möglichkeiten, Zertifikate auszustellen. Die erste ist das sogenannte Autoenrollment, bei dem automatisch, ohne manuelle Einwirkung, Zertifikate ausgestellt werden. Bei der Verwendung des Encrypting File System (EFS) kommt dieses Verfahren zum Einsatz: Beim ersten Versuch eines Benutzers, eine Datei zu verschlüsseln, wird ein entsprechender Schlüssel generiert und von der Enterprise CA signiert. Dieser Vorgang läuft automatisch und unsichtbar für den Benutzer ab.

Das Autoenrollment lässt sich über das Active Directory und die Group Policies zentral steuern, d. h. es kann zentral festgelegt werden, wer oder was bei der nächsten Anmeldung automatisch ein Zertifikat erhält. Bei Windows 2000 ist die Funktionalität nur für Computerzertifikate umgesetzt. Ab Windows 2003 können auf diese Weise auch Benutzerzertifikate ausgestellt werden. Der Mechanismus für das Autoenrollment schließt auch eine automatische Erneuerung der Zertifikate ein.

Der zweite Spezialfall ist die Ausstellung von Zertifikaten für das in Windows 2003 unterstützte Smartcard Login. Standardmäßig können diese Zertifikate nicht vom Benutzer selbst beantragt werden; der Antrag muss von einem speziellen Administrator (z. B. einem PKI-Officer), d. h. einem Administrator mit einem speziellen Zertifikat, gestellt werden, der dann die Smartcard an den Benutzer weiterleiten muss. Der Vorgang wird standardmäßig über eine entsprechende Webseite durchgeführt und ist daher mit relativ hohem manuellen Aufwand verbunden. Für große Benutzerzahlen ist dieser Weg daher kaum praktikabel.

Wenn man die Enterprise CA aus PKI-Sicht betrachtet, sind die Registrierungsstellen somit die Stellen, an denen Accounts für Benutzer oder Rechner eingerichtet werden. Die Sicherheit ist hier also stark vom Prozess beim Einrichten von Accounts in einer Domäne abhängig. Gegebenenfalls sollte man hier also überprüfen, ob die Vorgehensweise an dieser Stelle den Sicherheitsanforderungen genügt, die man an die Zertifikate (bzw. die zugehörigen Anwendungen) stellt. In der 2003 CA könnte durch zusätzliche organisatorischen Maßnahmen über die Möglichkeit einer expliziten Freischaltung eines Zertifikatsantrags zusätzliche Sicherheit eingebaut werden.

Bei allen Arten der Registrierung werden die Schlüssel und Zertifikate im Microsoft Zertifikatsspeicher abgelegt und sind dann über die Crypto-API Schnittstelle für alle Anwendungen nutzbar. Damit steht ein einheitliches Zertifikatsmanagement zur Verfügung. Bei Anwendungen, die nicht auf den Microsoft Zertifikatsspeicher zugreifen, ist die Integration aufwändiger und ggf. nur mit manuellem Aufwand möglich.

3.6 Administration

Neben der reinen PKI-Funktionalität spielt die Administration einer PKI in der Praxis eine wichtige Rolle. Sie ist entscheidend für den zum Betrieb der PKI benötigten Aufwand und damit sowohl für die Kosten als auch für die Sicherheit der PKI. Durch die Integration in das Betriebssystem und die Verwendung von bereits existierenden Informationen aus dem Active Directory kann der Administrationsaufwand bei der Enterprise CA relativ klein gehalten werden, sofern keine weiteren speziellen Daten oder Abläufe benötigt werden.

Microsoft bietet eine Reihe von Tools an, mit deren Hilfe die PKI verwaltet werden kann. Das wichtigste graphische Tool ist ein Snap-In für die Management Console (MMC), mit dem die grundlegendsten CA-Funktionalitäten wie das Sperren von Zertifikaten durchgeführt werden können.

Neben dem Ausstellen und Sperren von Zertifikaten können über dieses Tool auch noch eine Reihe zusätzlicher Verwaltungsfunktionen wie das Starten und Beenden des Certificate Service, Erneuerung des CA-Zertifikats[2] und das Sichern und Wiederherstellen der CA-Datenbank durchgeführt werden.

Zusätzlich zu dieser graphischen Oberfläche gibt es einige sehr hilfreiche Kommandozeilen-Tools, die bei der Administration verwendet werden können. Das wichtigste ist Certutil. Certutil stellt im Prinzip die wichtigste Funktionalität der grafischen Oberfläche plus einiger wichtiger Zusatzfunktionen auf Kommandozeilenebene zur Verfügung. Einige wichtige Funktionen wie z. B. Key-Recovery lassen sich nur über dieses Tool nutzen.

In Bezug auf die Kontrolle des Zugriffs auf die CA-Funktionalität verwendet Microsoft das in Windows 2003 eingesetzte Modell der Rechteverwaltung. Der Certificate Service und einige wichtige Komponenten (wie z. B. die Zertifikats-Templates) sind – wie alles in einer Windows 2003 Umgebung – Objekte, für die spezielle Zugriffsrechte vergebenen werden können. So gibt es die Möglichkeit, die Zugriffsrechte auf die CA zu beschränken; hierfür gibt es spezielle Berechtigungen für das CA-Objekt.

Die Rechte wurden von Windows 2000 zu Windows 2003 von einfachen Rechten zu einem Rollenkonzept zusammengefasst und weiterentwickelt. Kern dieses Rollenkonzeptes ist es, einzelne Berechtigungen zu typischen Rollen innerhalb der PKI Verwaltung zusammenzufassen. In der Windows 2003 CA gibt es jetzt Rollen für CA Administrator und CA Manager als direkte PKI-Rollen. Ergänzt werden diese Rollen durch die üblichen Backup-Operator und Auditor Rollen, die über die normalen Windows Zugriffsrechte und Rechte definiert werden.

Eine Besonderheit dieses Rollenkonzepts ist, dass eine technische Unterstützung für eine Trennung der Rollen CA Administrator und CA Manager vorgesehen ist, d. h. wenn gewünscht, kann erreicht werden, dass keine Person (bzw. kein Account!) beide Berechtigungen (CA Manager und CA Administrator) bekommt. Auf diese Weise ist eine Rollentrennung möglich, und auch eine Trennung von normalem Administrator und CA Administration lässt sich umsetzen. Um dies zu erreichen muss aber bei der Vergabe von Rechten sehr genau aufgepasst werden (z. B. sind lokale Administratoren anfangs als Default auch CA Administratoren).

Zusätzlich gibt es die Möglichkeit, die Rechte durch Einschränkungen des Zugriffs auf die Zertifikats-Templates für die CA oder den Benutzer anzupassen. Auf diese Weise kann konfiguriert werden, welche Art von Zertifikaten von welcher CA ausgegeben werden können und wer welche Arten von Zertifikaten beantragen kann.

An einigen Stellen lässt sich durch Kombination der verschiedenen Einschränkungen auch ein 4-Augen Prinzip durchsetzen (z. B. Beantragung durch Enrollment-Agent, manuelle Freischaltung durch CA Manager). Insgesamt kann die Verwaltung der Berechtigungen, durch die Anzahl der verschiedenen Möglichkeiten schnell unübersichtlich werden.

3.7 Schlüsselmanagement

Die Generierung von Schlüsselpaaren für Benutzer und Computer erfolgt in der Regel dezentral, d. h. beim Benutzer selber. Bei Microsoft-Clients hängt die Art und Qualität der Schlüsselgenerierung und Speicherung daher vom dort verwendeten Cryptographic Service Provider (CSP) ab. Standardmäßig ermöglicht Microsoft mit integrierten CSPs die Erzeugung und Speicherung von Schlüsseln (nur) in Software. Es gibt jedoch eine Reihe von Herstellern, die es ermöglichen, CSPs mit speziellen Eigenschaften zu integrieren, z. B. zur Generierung und Speicherung der Schlüssel auf Smartcards oder speziellen Hardware Security Modulen (HSM).

Die Archivierung von Teilnehmerschlüsseln wird ab der Version 2003 durch ein optionales Key Archival unterstützt. Welche Schlüssel hier archiviert werden sollen, ist über die jeweiligen Templates zertifikatsspezifisch konfigurierbar. Hierbei werden aber nur solche Schlüssel archiviert, die für die Verschlüsselung vorgesehen werden; eine Archivierung von Signaturschlüsseln wird nicht unterstützt.

Wird ein Schlüssel archiviert, so wird er nach der Erzeugung an die CA weitergeleitet, die dann für eine gesicherte (d. h. verschlüsselte) Ablage sorgt. Die Schlüssel werden dabei individuell mit einem symmetrischen Schlüssel verschlüsselt. Dieser Schlüssel wird dann mit dem öffentlichen Schlüssel einer oder mehrerer Recovery Agents verschlüsselt. Die Recovery Agents sind dabei unabhängig von den CA Rollen und für eine CA frei konfigurierbar. Zur Wiederherstellung eines Schlüssels muss ein CA Manager in einem ersten Schritt das verschlüsselte Schlüsselpaar aus der Datenbank exportieren. Anschließend muss einer der Recovery Agents die Datei entschlüsseln und mit einem Passwort versehen als PKCS #12 Datei an den entsprechenden Nutzer schicken. Dieser Prozess kann nur über Kommandozeilen-Tools durchgeführt werden.

4 Stärken und Schwächen

Die Stärken der Windows 2003 PKI liegen eindeutig in der starken Integration in die Windows 2003 Umgebung. An vielen Stellen ist durch diese Integration ein hohes Maß an Transparenz oder Automatisierung möglich, so dass Aufgaben, die oft beim Einsatz von PKIs aufwändig sind, z. B. Registrierung, Verteilung von Zertifikaten etc., relativ einfach realisiert werden können. Beim Einsatz einer Enterprise CA ist der Administrationsaufwand daher auf ein Minimum reduziert. Für die Verbesserung der Sicherheit innerhalb einer Windows 2003 Domäne ist die Enterprise CA auch durch die vorhandene Anwendungsintegration geeignet.

[2] Es besteht die Möglichkeit, sowohl das Zertifikat zu verlängern als auch einen neuen Schlüssel zu generieren.

Die starke Integration hat allerdings auch Nachteile. Durch die Verknüpfung mit der Betriebssystemfunktionalität kann es sein, dass Änderungen, Updates und das Einbauen neuer Funktionalität schwieriger ist, da das Zusammenspiel mit anderen Betriebsystemfunktionen beachtet werden muss. Schließlich sind sehr hohe Sicherheitsanforderungen nur mit hohem Aufwand zu realisieren.

Die Entwicklung, dass immer mehr Hersteller den Microsoft Zertifikatsspeicher verwenden, verbreitert auch die Anwendbarkeit der Microsoft CA, da nun auch solche Anwendungen von der Windows Integration der CA profitieren können und die CA nicht auf reine Microsoft-Anwendungen beschränkt ist.

Es zeichnet sich ab, dass PKI ein wichtiger Baustein der zukünftigen Strategie von Microsoft ist. Im Windows 2003 Server hat die PKI-Funktionalität große Fortschritte gegenüber Windows 2000 gemacht. So sind z. B. einige wichtige Funktionen, die in Windows 2000 noch gefehlt haben, dort implementiert (wie Key-Backup, Anpassbarkeit). Zielrichtung ist aber immer noch die Ausstellung von Zertifikaten für Komponenten (z. B. Benutzer, Rechner) einer Windows Domäne; die Funktionalität für das Ausstellen von Zertifikaten außerhalb der Windows-Umgebung ist weiterhin begrenzt.

Zusammenfassend kann also gesagt werden, dass die PKI-Funktionalität in Windows 2003 sehr weitreichende Funktionen einer PKI anbietet und eigentlich keine wichtigen Funktionen fehlen. Im Vergleich mit anderen PKI-Produkten ist Windows 2000 ebenfalls ein Produkt mit Stärken und Schwächen. Es ist also durchaus empfehlenswert, Microsoft in die Produktauswahl einzubeziehen. Wenn die Rahmenbedingungen stimmen (z. B. die betrieblichen Anwendungen überwiegend in einer Windows-Umgebung realisiert sind), ist Microsoft eine ernstzunehmende Alternative zu anderen Spezialprodukten.

Andere Produkte zeichnen sich meistens dadurch aus, dass sie flexibler auch in heterogenen Umgebungen einsetzbar sind. Da in der Praxis heterogene Umgebungen überwiegen und die PKI-basierte Sicherheitsfunktionalität nicht nur in internen Netzen, sondern vor allem auch mit externen Partnern und Kunden genutzt werden soll, kann durchaus auch eine Kombination aus einer Windows PKI und Produkten anderer Hersteller oder Dienstleister sinnvoll sein.

Durch die Erweiterungen bei Windows 2003 hat sich das grundsätzliche Einsatzszenario (Ausstellung von Zertifikaten für interne Komponenten) der Microsoft CA nicht verändert, durch die Erweiterungen und Veränderungen hat Microsoft aber hier erheblich Boden gut gemacht und einige Probleme beseitigt (z. B. Schlüsselarchivierung). Auch die Tatsache, dass mehr Anwendungen die Zertifikatsverwaltung von Microsoft verwenden, beschränkt die Anwendung nicht länger auch reine Microsoft-Umgebungen.

Eines der Hauptargumente für den Certificate Service ist immer wieder der Preis. Der Certificate Service ist bei jeder Windows 2000 Server Version „umsonst“ dabei; CA-Produkte von anderen Herstellern verursachen dagegen zusätzlich hohe Kosten oder haben Lizenzmodelle, die von der Anzahl der ausgestellten Zertifikaten abhängen. Dieser Preisunterschied ist nicht von der Hand zu weisen. Abhängig von der Art und dem Einsatz der PKI spielt der Anschaffungspreis bei den Gesamtkosten für den Aufbau und den Betrieb einer PKI allerdings in der Regel die geringste Rolle. Hier muss also berücksichtigt werden, in wie weit sich das angestrebte Konzept mit Hilfe einer Windows 2000 PKI umsetzen lässt bzw. wie aufwändig dies ist im Vergleich zu anderen Produkten ist. Die oftmals bessere Administrierbarkeit anderer Produkte kann durchaus die höheren Anschaffungskosten an anderer Stelle wieder ausgleichen.

5 Fazit

Microsoft hat seit Windows 2000 PKI-Funktionalität zu einem Kernbestandteil seiner Sicherheitsarchitektur gemacht – das ist zweifellos ein wichtiger Schritt. Der Fokus der PKI-Funktionalität liegt dabei jedoch eindeutig auf der integrierten Unterstützung in einer Microsoft-Umgebung. Hier bietet Microsoft auch einige elegante Lösungen (z. B. zur Verteilung vertrauenswürdiger CA-Zertifikate) für Fragestellungen, die in anderen Umgebungen oft nur mit großem Aufwand gelöst werden können.

Die Standardunterstützung erlaubt es, die Funktionalität auch außerhalb der reinen Windows-Umgebung einzusetzen bzw. eine Integration mit Umgebungen und Anwendungen anderer Hersteller zu ermöglichen. Hier muss allerdings im Einzelfall untersucht werden, ob alle Erfordernisse erfüllt sind, um eine solche Unterstützung zu gewährleisten.

Literatur

[BER_01] Bertsch, Andreas, *Digitale Signaturen*, Springer, 2001

[BSI_02] Hammer, Neundorf, Rosenhauer, *Zertifizierungsinfrastruktur für die PKI-1-Verwaltung*, Verzeichnisdienstkonzept, V1.2, Bundesamt für Sicherheit in der Informationstechnik

[FOX_99] Fox, Dirk: *Zum Problem der Gültigkeitsprüfung von Schlüsselzertifikaten*. Tagungsband 6. Deutscher IT-Sicherheitskongreß des BSI 1999, SecuMedia Verlag, Ingelheim 1999, S. 215-230.

[HAM_01] Hammer, Volker, Cross-Zertifikate verbinden, DuD 2/2001, Verlag Vieweg

[IBMMS_02] *Security in a Web Service World: A Proposed Architecture and Roadmap*, Version 1.0, IBM, Microsoft, April 7, 2002

[ISIS-MTT_02] ISIS-MTT Specification v1.02, 19. Juli 2002

[MAC1_00] Mack, Holger: *Sperren von Zertifikaten in der Praxis – eine Fallanalyse*, DuD 8/2001, Verlag Vieweg,

[MAC2_03] Mack, Holger: *PKI-Unterstützung in Windows 2000 und Windows 2003 Server, v*2.01, Secorvo Whitepaper

[MSDN_01] MSDN Library, *Platform Software Developement Kit*, 2001, Microsoft Corporation www.msdn.microsoft.com

[MS_CS_00] *Windows 2000 Certificate Service*, Microsoft Corporation, 2000

[PC/SC_97] *Interoperability Specification for ICCs and Personal Computer Systems, Part 1. Introduction and Architecture Overview,* PC/SC Workgroup, 1997

[PKCS_1] *PKCS #1: RSA Encryption Standard*, v1.5, 1993, RSA Laboratories

[PKCS_7] PKCS #7 : *Cryptographic Message Syntax Standard*, v1.5, 1993, RSA Laboratories

[PKCS_10] *PKCS #10 v1.0: Certification Request Syntax Standard*, 1993, RSA Laboratories

[PKCS_12] *PKCS #12 v1.0: Personal Information Exchange Syntax*, 1999, RSA Laboratories

[RFC2251] M. Wahl u.a., *Lightweight Directory Access Protocol (v3) (RFC 2251)*, 1997, IETF

[RFC2459] R. Housley u.a., *Internet X.509 Public Key Infrastructure Certificate and CRL Profile*, IETF, January 1999

[X509_97] ITU-T Recommendation X.509 „*Information Technology – Open Systems Interconnection – The Directory: Authentication Framework*“, June 1997