PKI-Unterstützung in Windows 2000

Secorvo White Paper

Version 1.1
Stand 29. November 2001

Holger Mack

Secorvo Security Consulting GmbH
Albert-Nestler-Straße 9
D-76131 Karlsruhe

Tel. +49 721 6105-500
Fax +49 721 6105-455

E-Mail info@secorvo.de
Internet http://www.secorvo.de

Inhaltsübersicht

Abkürzungen

ADS	Active Directory Service
ADSI	Active Directory Service Interface
AIA	Authority Information Access
ANSI	American National Standard Institute
CA	Certification Authority
CDP	Certificate Distribution Point
COM	Common Object Model
CRL	Certificate Revocation List
CryptoAPI	Cryptographic Application Programming Interface
CSP	Cryptographic Service Provider
CTL	Certificate Trust Lists
DB	Database
DLL	Dynamic Link Libraries
DNS	Domain Name Service
EFS	Encrypting File System
HSM	Hardware Security Modulen
IE	Internet Explorer
IETF	Internet Engineering Task Force
IIS	Internet Information Server
IPSec	Internet Protocol Security
ISO	Internation Standardisation Organisation
IT	Information Technology
LDAP	Lightweigt Directory Access Protocol
MMC	Mananagement Console
NT	New Technology
OCSP	Online Certifcate Status Protocol
PC/SC	Personal Computer/Smart Card
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure
PKIX	X.509-based Public Key Infrastructure
RFC	Request for Comment
SDK	Software Developement Kit

SSL	Secure Socket Layer
TLS	Transport Layer Security
XP	Experience

1 Zusammenfassung

Microsoft hat in 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.

Microsoft schlägt damit einen ähnlichen Weg ein wie Lotus Notes vor einigen Jahren, mit dem Unterschied, daß die von Microsoft verwendete PKI offener und standardkonformer ist als die in Lotus Notes realisierte Lösung. Die Standardunterstützung ermöglicht es, die Funktionalität außerhalb der reinen Windows-Umgebung einzusetzen bzw. eine Integration mit Umgebungen und Anwendungen anderer Hersteller zu ermöglichen. Hier muß allerdings genau untersucht werden, ob alle Erfordernisse erfüllt sind, um eine solche Unterstützung zu gewährleisten.

Kritisch betrachtet muß man allerdings sehen, daß die effektiv verfügbare PKI-Funktionalität noch nicht ausgereift ist. Die Entwicklung anderer CA-Produkte hat gezeigt, daß bis zu einem ausgereiften PKI-Produkt einige Zeit vergehen kann. So mangelt es hauptsächlich an Flexibilität und Funktionalität, vor allem wenn man sich außerhalb der Windows 2000-Umgebung bewegt.

Mit Windows XP zeichnet sich ab, daß PKI ein wichtiger Baustein der .NET Strategie von Microsoft ist. Mit Windows XP oder .NET scheint die PKI-Funktionalität große Fortschritte zu machen: Einige wichtige Funktionen, die in Windows 2000 noch gefehlt haben, sind dort implementiert. Es bleibt allerdings abzuwarten, ob diese Funktionalitäten den Erwartungen entsprechen und ob Microsoft den Certificate Service so erweitern wird, daß auch die Funktionalität für das Ausstellen von Zertifikaten außerhalb der Windows-Umgebung verbessert wird.

Auch müssen einige Funktionen, wie das automatische und transparente Nachladen von vertrauenswürdigen Zertifikaten, noch genauer untersucht werden. Diese könnten sonst einem Angreifer Werkzeuge in die Hand geben, die PKI Funktionalität dazu zu verwenden, weiterreichende Angriffe vorzubereiten. Da PKI in der Microsoft-Strategie für die Zukunft (z.B. .NET-Architektur, Passport-Service) eine gewichtige Rolle spielen, ist die Sicherheit der PKI-Funktionalität von entscheidender Bedeutung.

Zusammenfassend kann also gesagt werden, daß die PKI-Funktionalität in Windows 2000 alle grundlegenden Funktionen einer PKI anbietet. 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 2000-PKI und Produkten anderer Hersteller oder Dienstleister sinnvoll sein.

2 Einleitung

Mit dem Erscheinen von Windows 2000 hat Microsoft eine große Anzahl von Neuerungen gegenüber der Vorgängerversion Windows NT 4.0 eingeführt. Vor allem auf dem Gebiet Sicherheit hat Microsoft erkennbar Anstrengungen unternommen, seinen bis dahin schlechten Ruf auf diesem Gebiet loszuwerden: An vielen Stellen in Windows 2000 wurden die Sicherheitsfunktionen überarbeitet, erweitert oder komplett neue Funktionalität hinzugefügt.

Eine besondere Rolle spielt dabei die Integration von Public Key-Technologie als Teil des Betriebsystems. Public Key-Technologie wird in Windows 2000 eingesetzt, um bestehende Sicherheitsmechanismen zu verbessern (z.B. die Einführung zertifikatsbasierter Authentifikation), aber auch um neue Sicherheitsmechanismen direkt in Windows 2000 zu unterstützen (z.B. Dateiverschlüsselung, IPSec).

Die Unterstützung für Public Key Infrastrukturen (PKI) in Windows 2000 hat vor allem deshalb viel Beachtung gefunden, da viele Organisationen sich mit der Umsetzung von PKI Lösungen beschäftigen. So spielt bei PKI-Projekten immer häufiger die Frage eine Rolle, ob und gegebenenfalls wie Microsofts Windows 2000 in die PKI-Strategie einer Organisation paßt.

Dies hat zwei Hauptgründe: Zum einen bietet Microsoft an einigen Stellen Funktionalität „umsonst“ als Teil des Betriebssystems an, die bei anderen spezialisierten Herstellern von PKI-Software für viel Geld separat eingekauft werden muß. Zum anderen spielt Microsoft Windows durch seine weltweite Verbreitung und zentrale Marktposition bei Betriebsystemen immer eine gewichtige Rolle, wenn es darum geht, IT-Projekte umzusetzen. Verständlicherweise werden die meisten IT-Projekte bei der Umsetzung bemüht sein, sicherzustellen, daß diese mit den von Microsoft unterstützten Techniken zusammenarbeitet, sei es weil Windows 2000 bereits unternehmensweit eingesetzt wird bzw. eine Umstellung geplant ist, sei es, weil man technische Probleme bei der Zusammenarbeit mit Firmen, die Microsoft einsetzen, vermeiden möchte.

Vor diesem Hintergrund spielt die Frage eine wichtige Rolle, was denn nun wirklich hinter der PKI-Funktionalität von Windows 2000 steckt und inwieweit die PKI-Funktionalität in die Planungen der PKI- oder IT-Projekte einbezogen werden soll. Die technischen Details eines PKI-Produkts und die Auswirkungen der Technik auf die PKI-Strategie sind oft nicht unmittelbar zu erkennen bzw. anhand der Dokumentation ersichtlich. Speziell im Bereich PKI hat sich gezeigt, daß die Angabe einer Funktionalität in der Dokumentation zweier verschiedener Hersteller (z.B. Standardunterstützung) nicht automatisch bedeutet, daß diese beiden Produkte in der Praxis zusammenarbeiten können. Oft sind es nur kleine Unterschiede, die aber bei der Umsetzung eine große Rolle spielen können. Zu berücksichtigen sind dabei auch immer die jeweiligen Rahmenbedingungen (z.B. technische Umgebung, spezielle Anforderungen Sicherheitsanforderungen etc.).

Das vorliegende White Paper enthält eine Beschreibung und Diskussion der Funktionalität des Microsoft Certificate Service, der Certification Authority (CA) Komponente von Windows 2000. 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.

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.

3 PKI Unterstützung in Windows 2000

Die PKI-Unterstützung in Windows 2000 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 (oder Certification Authority (CA)) übernimmt, d.h. das Ausstellen und Sperren von Zertifikaten.

Wie insgesamt in einer Windows 2000 Domäne spielt auch bei der Windows 2000 PKI der integrierte Verzeichnisdienst Active Directory Service(ADS) eine wichtige Rolle. Abhängig von der Betriebsart der CA (siehe unten) 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 2000 Domäne.

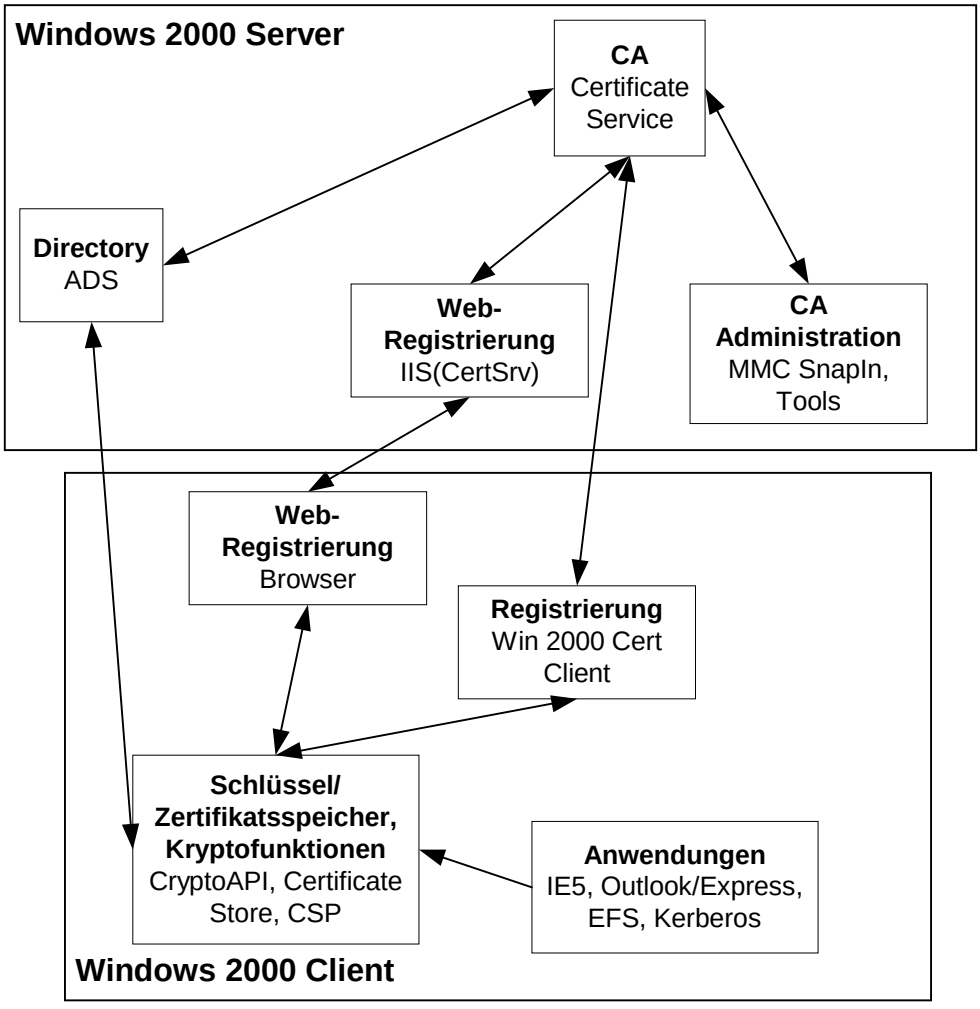

Abbildung 1: Komponenten Windows 2000 PKI

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 Programmieren 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

2000 Domäne von zentraler Stelle verwaltet und vorgegeben werden. Einige Microsoft Anwendungen, wie z.B. Outlook oder Internet Explorer, bedienen sich bereits dieser Funktionalitäten. Mit Hilfe von sogenannten Cryptographic Service Providern (CSP) – das sind Funktionsbibliotheken, die dem Betriebssystem über eine definierte Schnittstelle den Zugriff auf kryptographische Operationen erlauben – kann auch die in Windows 2000 mitgelieferte Standard-Funktionalität erweitert werden, z.B. zur Unterstützung von kryptographischer Hardware.

Der Hauptaugenmerk in den folgenden Abschnitten gilt der CA-Komponente von Windows 2000, dem Certificate Service. Diese Komponente konkurriert mit anderen auf dem Markt verfügbaren Produkten von Herstellern wie Entrust oder Baltimore, die sich auf CA-Komponenten spezialisiert haben.

4 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.

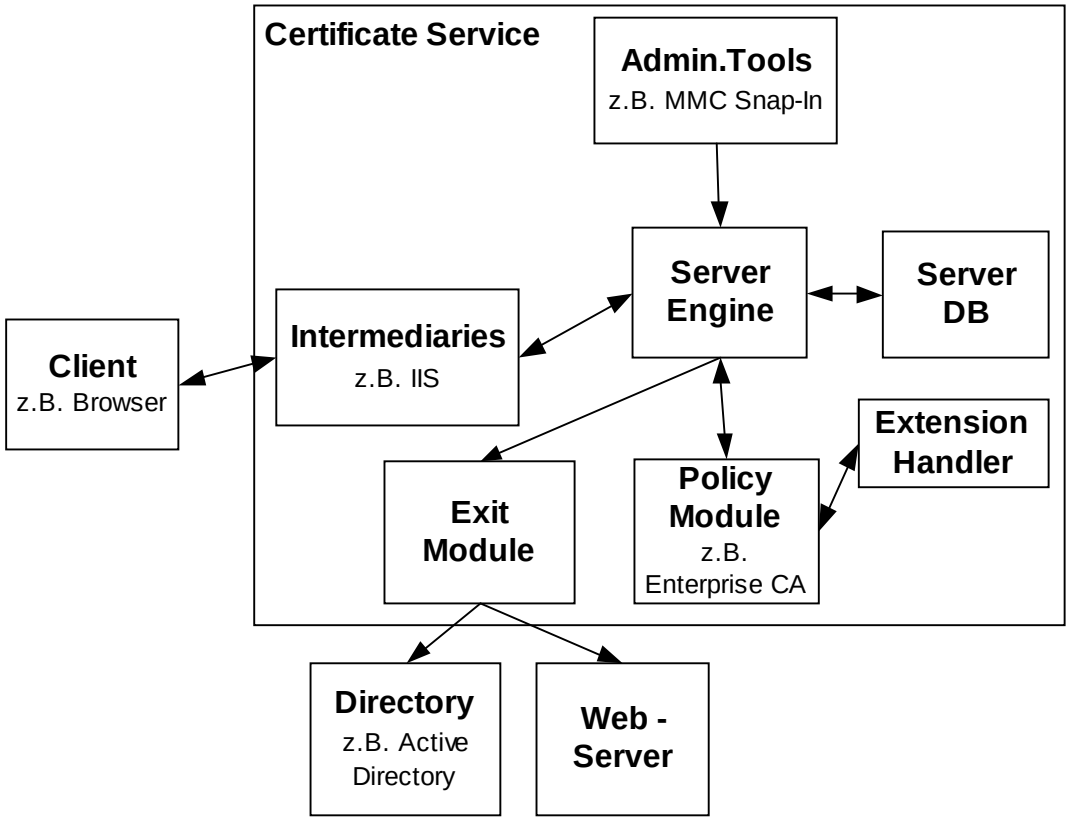

Abbildung 2: Windows 2000 Certificate Service Architektur

Der Server-Engine ist die zentrale Komponente in dieser Architektur. Er ist verantwortlich für das Ausstellen von Zertifikaten und Sperrlisten. Im Server-Engine selber ist nur begrenzte Funktionalität integriert (d.h. das eigentliche Generieren der Zertifikate). Ein wichtiger Teil der PKI-Funktionalität ist in den verschiedenen Modulen implementiert, deren sich der Server-Engine bedient:

- *Policy Module*: Hier sind Funktionen wie die Prüfung und Genehmigung eines Zertifierungsantrags, die Namensgebung und die Gestaltung eines Zertifikates (Nutzung und Belegung der Attribute) implementiert.
- *Exit Module*: Hier sind Funktionen zum Veröffentlichen von Sperrlisten und Zertifikaten z.B. in einem Verzeichnisdienst implementiert.
- *Extension Handler*: Hier werden Zertifikats-Erweiterungen, die im Zertifikat verwendet werden sollen, definiert.
- *Intermediaries*: Von ihnen werden Zertifizierungsanträge von Anwendungen entgegengenommen und an den Server-Engine weitergeleitet.

Alle diese Module sind über definierte Schnittstellen miteinander verbunden, ansonsten aber voneinander unabhängig meistens in Gestalt von Dynamic Link Libraries (DLL) realisiert. Sie sind dadurch anpaßbar und austauschbar. Die Kommunikation der Module mit dem Server-Engine erfolgt meist über COM-Schnittstellen.

Durch die modulare Gestaltung ist zwar eine hohe Flexibilität gewährleistet und die Realisierung einer individuellen Lösung denkbar, in der Praxis ist dies aber mit einigem Aufwand verbunden. Der Hauptgrund dafür ist, daß einzelne Module nur komplett ausgetauscht werden können und die Module zur Realisierung von Modifikationen komplett neu programmiert werden müssen. Im Microsoft Software Development Kit (SDK) [MSDN_01] sind die entsprechenden Funktionen enthalten und in den Programmiersprachen C++ und Visual Basic nutzbar. Standardmäßig sind bei Windows 2000 bereits verschiedene Module enthalten. An einigen Stellen wird auch explizit davon abgeraten, diese (z.B. Policy Module für Enterprise CA) auszutauschen.

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 2000 Umgebung inklusive Active Directory integriert und setzt eine Windows 2000 Domäne und Active Directory voraus. Die Enterprise CA 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 auf die verschiedenen Aspekte der beiden Policy-Module eingegangen.

5 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 nur einige Kriterien die bei einer solchen Bewertung berücksichtigt werden müssen.

Der Betrachtung in diesem Kapitel liegt kein explizites Einsatzszenario zu Grunde. Vielmehr soll hier versucht werden, eine möglichst generell Betrachtung durchzuführen. In diesem Rahmen soll anhand der wichtigsten Kriterien, die bei einem CA-Produkt zu berücksichtigen sind, die Funktionalität der Windows 2000 PKI beurteilt werden. Diese Kriterien sind:

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

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

5.1 Vertrauensmodell

Neben der Möglichkeit eine Windows 2000 CA unabhängig zu betreiben, wird auch 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 2000 CAs zu mischen. So kann z.B. eine Windows 2000 CA als untergeordnete CA unter einer externen CA arbeiten, Windows 2000 kann aber auch Zertifikate für untergeordnete CAs außerhalb der Windows 2000 Umgebung ausstellen. Die Hierachietiefe ist hierbei nicht eingeschränkt. Die Beantragung und Bearbeitung von Zertifizierungen in einer Hierachie geht dabei über die Standardformate PKCS#10 [PKCS_10] und PKCS#7 [PKCS_7], die von nahezu allen Herstellern und Anbieter unterstützt werden.

Cross-Zertifizierung [HAM_01] als zweite Methode zum Aufbau eines Vertrauensmodells wird von Windows 2000 nicht unterstützt, weder durch die CA noch durch die Client-Komponenten, soll aber in Windows XP unterstützt werden (siehe auch Kapitel 7).

Neben der Nutzung des hierarchischen Modells bietet Windows 2000 eine weitere Möglichkeit, Vertrauen zu anderen CAs herzustellen. Der 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. Das Prinzip ist dabei ähnlich einer Sperrliste, mit dem Unterschied, daß die CTL nicht gesperrte Zertifikate, sondern vertrauenswürdige Zertifikate von Zertifizierungsstellen enthält. In einer Windows 2000 Umgebung wird diese von einer vertrauenswürdigen Person (z.B. einem PKI-Administrator) aus der eigenen Hierarchie unterschrieben. Mit Hilfe des Active Directories und des Windows 2000 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 in einer Domäne erklärt bzw. definiert werden. Programme, die die Client-Funktionalität von Windows 2000

verwenden, werden Zertifikate, die von CAs aus einer CTL stammen, automatisch als vertrauenswürdig anerkennen.

Das (proprietäre) Format der CTLs erlaubt es außerdem, das Vertrauen in die in der Liste enthaltenen CA-Zertifikate in zwei Aspekten einzuschränken:

- CTLs haben wie CRLs und Zertifikate eine begrenzte Lebensdauer, d.h. ein Gültigkeitszeitraum kann festgelegt werden.
- Die Verwendung der CA-Zertifikate kann eingeschränkt werden. Es kann festgelegt werden, für welche Verwendung (z.B. Object signing) den in der CTL aufgeführten CAs vertraut wird. Nur für diese Anwendungen werden die Zertifikate somit im Client als vertrauenswürdig anerkannt.

Der CTL-Mechanismus ist eine proprietäre Lösung von Microsoft und entspricht keinem Standard. CTLs werden deshalb zur Zeit auch nur von Microsoft unterstützt. CTLs können zwar als Datei exportiert und verteilt werden, können aber nur in einer Windows 2000 Umgebungen ausgewertet und genutzt werden.

Problematisch ist, daß es in Windows 2000 derzeit noch keinen Mechanismus gibt, um CTLs zu sperren. Wenn einem Zertifikat nicht länger das Vertrauen ausgesprochen werden soll, muß die CTL mit Hilfe der Windows 2000 Mechanismen gelöscht werden und eine neue CTL ausgestellt und verteilt werden. Werden CTLs über die Grenzen einer zentral administrierten Windows 2000 Umgebung verteilt, fällt das Fehlen einer Sperrmöglichkeit ins Gewicht.

5.2 Standardunterstützung

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 2000 inzwischen in weiten Teilen auf internationalen Standards. Die wichtigsten darunter sind:

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

5.2.1 Zertifikate

Bei den Zertifikatsformaten orientiert sich Microsoft an X.509v3 sowie den Zertifikats- und Sperrlistenprofilen, die im RFC2459 definiert sind. Die Architektur des Certificate Service erlaubt dabei prinzipiell flexible Zertifikatsinhalte. Bei den im Lieferumfang von Windows 2000 enthaltenen Policy-Modulen sind diese Möglichkeiten allerdings stark eingeschränkt. Die Inhalte und das Aussehen der ausgestellten Zertifikate sind anhand sogenannter Zertifikats-Templates vordefiniert und können nur in sehr beschränktem Maße angepaßt werden.[1] Enthalten sind eine Reihe von anwendungsspezifischen Zertifikats-Templates, die die meisten üblichen Anwendungen abdecken. Diese Templates werden im Active Directory

[1] Die Zertifikats-Templates enthalten nicht nur Angaben zum Inhalt der Zertifikate, sondern auch Informationen die für die Ausstellung notwendig sind (Überprüfungen etc.) .

verwaltet. Es ist derzeit nicht möglich, diese Zertifikats-Templates anzupassen oder neue zu definieren.

Die in den 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. Dabei sind zwei Fälle zu unterscheiden:

- Der Microsoft Certificate Service wird dazu verwendet um Zertifikate für nicht-Windows Produkte auszustellen,
- Ein CA-Produkt eines anderen Herstellers oder Dienstleisters soll verwendet werden, um Zertifikate für Windows 2000 Anwendungen auszustellen.

Je nachdem welcher dieser beiden Fälle betrachtet wird, haben die unten beschriebenen Fälle verschiedene Auswirkungen.

Über die in den Standards definierten Zertifikatserweiterungen hat Microsoft eigene, sogenannte Private Extensions definiert, die vor allem bei originären Microsoft-Anwendungen benötigt werden (z.B. Encrypting File System(EFS)). Der Standard X.509 erlaubt explizit die Definition solcher eigenen Erweiterungen, allerdings kann es in der Praxis zu Problemen kommen, wenn Anwendungen diese Erweiterungen nicht interpretieren können bzw. Produkte von Drittherstellern die mit einer Erweiterung verknüpfte Funktionalität nicht unterstützen. Viele PKI-Hersteller haben allerdings inzwischen eine Unterstützung der Microsoft-Erweiterungen in ihre aktuellen Produkte eingebaut, d.h. auch mit diesen Produkten können Zertifikate mit den von Microsoft definierten Erweiterungen z.B. für bestimmte Windows 2000 Anwendungen (wie EFS) ausgestellt werden. Da alle diese Erweiterungen nicht als „kritisch“ (critical) markiert sind, sollten andere Client-Produkte sie gemäß Standard schlimmstenfalls ignorieren. In der Praxis gibt es hier aber manchmal Probleme wie z.B. Programmabstürze. Im Zweifelsfall muß daher die Nutzbarkeit von Zertifikaten mit Microsoft-spezifischen Extensionen in Nicht-Microsoft-Produkten getestet werden.

Darüber hinaus hält sich Microsoft in den vordefinierten Zertifikaten nicht in allen Punkten an die Empfehlungen der Standards hinsichtlich der Kennzeichnung der Zertifikatserweiterungen als „kritisch“. In den vordefinierten Zertifikats-Templates werden bei der Verwendung von Erweiterungen diese grundsätzlich nicht als „kritisch“ gekennzeichnet. Dies betrifft auch solche Erweiterungen wie die Schlüsselverwendung (Key Usage), für die im Standard empfohlen wird, sie als „kritisch“ zu markieren.[2]

Es ist allerdings darauf hinzuweisen, daß der Certificate Service prinzipiell schon die Ausstellung von kritischen Erweiterungen unterstützt; diese Funktionalität wird jedoch in den vordefinierten Zertifikatsformaten nicht eingesetzt.

Eine dritte Stelle, an denen die von Microsoft verwendeten Zertifikatsformate Problem bereiten können, ist, daß Microsoft-Anwendungen strikte Anforderungen an das Vorhandensein und das genaue Aussehen bestimmter Zertifikatserweiterungen stellen (z.B. Certificate Distribution Points (CDP)). Dies spielt vor allem bei der Gültigkeitsprüfung von Zertifikaten eine Rolle. Sind diese nicht so vorhanden wie vorgesehen kann es zu Einschränkungen bei der Client-Funktionalität kommen (z.B. beim Suchen und Importieren von Sperrlisten).

---

[2] Dies ist allerdings leider eine sehr verbreitete Praxis, die einige Anbieter wählen, um Interoperabilitätsprobleme auf Kosten der Sicherheitsfunktionalität zu vermeiden.

Insgesamt konnten im Rahmen verschiedener (nicht vollständiger) Tests die von Windows 2000 ausgestellten Zertifikate von Produkten anderer Hersteller in der Regel importiert werden, und es gelang auch, von CA-Produkten anderer Hersteller ausgestellte Zertifikate in Windows 2000 zu nutzen. Es ist allerdings Vorsicht geboten, wenn sichergestellt werden soll, daß es zu keinen funktionalen und sicherheitstechnischen Einschränkungen durch Zertifikatsdetails kommt. Dies kann vor allem dann der Fall sein, wenn bereits existierende Infrastrukturen mit Windows 2000 zusammenarbeiten sollen. 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.

5.2.2 Sperrlisten

Windows 2000 unterstützt standardmäßig Certificate Revocation Lists (CRL) als Mechanismus, um Zertifikate zu sperren. Hierbei werden Sperrlisten nach dem X.509 Standard eingesetzt [X509_97]. Dies entspricht dem heute üblichen Standard. Es handelt sich dabei immer um komplette Sperrlisten, d.h. die CA gibt eine Sperrliste aus, in der alle gesperrten (und noch nicht abgelaufenen) Zertifikate einer CA enthalten sind. Weitergehende im Standard vorgesehene und von vielen CA-Produkten heute unterstützte Mechanismen wie die Unterscheidung von CRLs und ARLs (Authority Revocation List), Delta CRLs oder das Protokoll OCSP [FOX_99] werden in Windows 2000 weder auf CA-Seite noch auf Client-Seite unterstützt.

Wichtig ist, daß Windows 2000 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 2000 nur gegen lokal importierte Sperrlisten prüfen[3].

5.2.3 Austauschformate

Neben den oben beschriebenen Standards für Zertifikate und Sperrlisten, unterstützt Windows 2000 eine Reihe von Standards aus der PKCS-Serie zum Austausch von 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.

5.3 Directory-Unterstützung

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

---

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

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 auf Zertifikate und Sperrlisten zugreifen, 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.

5.4 Flexibilität

Die Architektur des Certificate Service erlaubt durch die verschiedenen Module im Prinzip relativ große Flexibilität. Wie bereits in Kapitel 4 beschrieben, kann diese Flexibilität jedoch an vielen Stellen nur mit erheblichem Programmieraufwand genutzt werden. Bei den mitgelieferten Policy-Modulen für die Enterprise und die Stand-Alone CA sind die Konfigurationsmöglichkeiten beschränkt. Die Einstellmöglichkeiten beschränken sich bei der PKI-Funktionalität auf einige wenige Parameter (CDPs), die entsprechend angepaßt werden können. Auch bei der Gestaltung des Distinguished Name von CAs und Benutzern sind die Attribute vorgegeben.

Auf Client-Seite gibt es Flexibilität durch austauschbare CSP, so können hauptsächlich die kryptographischen Funktionen und die Speicherung der Schlüssel angepaßt werden.

5.5 Registrierung

Die Abläufe bei der Registrierung von Benutzern und Computern unterscheiden sich stark abhängig davon, welches Policy-Modul eingesetzt wird. Im folgenden werden die beiden Module daher separat betrachtet.

5.5.1 Enterprise CA

Bei einer Enterprise CA ist die eigentliche Registrierung des Benutzers oder Computers das Anlegen eines Accounts in der Windows 2000 Domäne. Ist der Benutzer hier angemeldet, kann er sich mit Hilfe des Certification Managers in der MMC oder über die Registrierungswebseite der CA (mit Hilfe des Internet Information Servers (IIS)) ein Zertifikate beantragen. Eine entsprechende Webseite wird von Microsoft mitgeliefert. Der Benutzer wird anhand seines Windows 2000 Accounts mit Hilfe der im Active Directories gespeicherten Informationen authentifiziert, anschließend wird das Zertifikat automatisch ausgestellt. 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), kontrolliert werden.

Eine Ausnahme von dieser Registrierung erfolgt bei der Verwendung des Encrypting File System (EFS). 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.

Bei der Ausgabe von Zertifikaten für Computer gibt es bei der Enterprise CA außerdem die Möglichkeit sogenanntes „Auto-enrollment“ einzusetzen. Wenn dies konfiguriert ist (via Group Policies), werden für Rechner in der Domäne bei der Anmeldung automatisch Zertifikate ausgestellt. Wenn dieses auto-enrollment nicht eingesetzt wird, muß ein Administrator die Zertifizierung jedes einzelnen Rechners manuell durchführen.

Ein Spezialfall ist auch die Ausstellung von Zertifikaten für den in Windows 2000 unterstützen Smart-Card Login. Standardmäßig können diese Zertifikate nicht vom Benutzer selber 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 Smart-Card an den Benutzer weiterleiten muß. Der Vorgang wird standardmäßig über eine entsprechende Webseite durchgeführt.

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.

5.5.2 Stand-Alone CA

Bei der Stand-Alone CA findet keine Integration in eine Domäne statt, es besteht daher nur die Möglichkeit, Zertifikate über die Webseite des IIS zu beantragen. In der Standardeinstellung werden die Zertifikatsanforderungen dann an die CA weitergeleitet, wo dann ein Operator explizit den Antrag freigeben (bzw. ablehnen) muß. Es ist allerdings auch möglich, eine automatische Ausstellung aller eingehenden Anfragen zu konfigurieren. Außer den sehr begrenzten Angaben, die im Zertifikatsantrag enthalten sind, hat der Administrator allerdings keine zusätzlichen Informationen um den Antrag zu prüfen.

Der Zugriff auf die Webseiten kann (wie auch bei der Enterprise CA) über die im IIS üblichen Protokollen und Mechanismen (z.B. TLS) geschützt werden.

5.6 Administration

Neben der reinen PKI-Funktionalität spielt die Administration einer PKI in der Praxis eine wichtige Rolle. Sie ist entscheidend für den für den Betrieb der PKI benötigten Aufwand und damit sowohl die Kosten als auch 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 (siehe Abb 3).

Die Darstellung lehnt sich an den Dateimanager an und ist so relativ einfach und übersichtlich gehalten. Allerdings kann sie bei großen Zahlen von Zertifikaten schnell unübersichtlich werden.

Neben dem Ausstellen und Sperren von Zertifikaten können über dieses Tool Schnittstelle auch noch eine Reihe zusätzlicher Verwaltungsfunktionen wie Starten und Stoppen des Certificate Service, Erneuerung des CA-Zertifikats[4] und das Sichern und Wiederherstellen der CA-Datenbank durchgeführt werden.

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

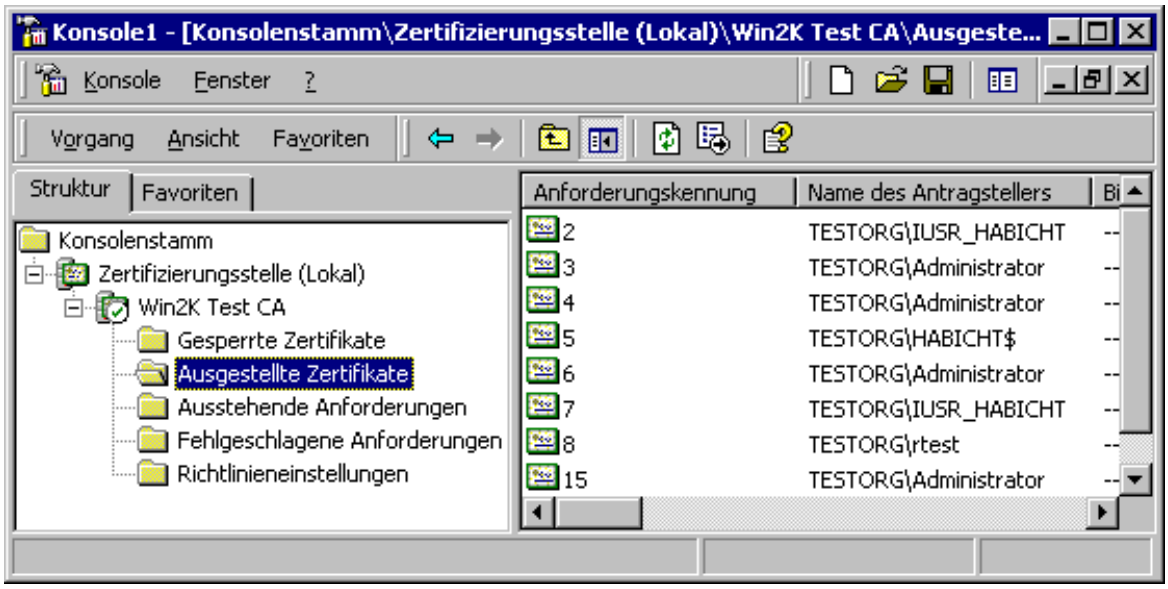

Abbildung 3: MMC SnapIn Administration Zertifizierungsstelle

Zusätzlich zu dieser graphischen Oberfläche gibt es einige sehr hilfreiche Kommandozeilen-Tools, die bei der Administration verwendet werden können. Die beiden wichtigsten sind *certutil.exe* und *dsstore.exe*.

- Certutil stellt im Prinzip die wichtigste Funktionalität der grafischen Oberfläche plus einiger wichtiger Zusatzfunktionen auf Kommandozeilenebene zur Verfügung (siehe Anhang).
- DSStore hat Funktionen, die für das Zusammenspiel von Active Directory und Enterprise CA wichtig sind. Dieses Tool ist vor allem sehr hilfreich bei der Fehlerbehebung von PKI- und Active Directory-Problemen. Im Gegensatz zu Certutil, das mit Windows 2000 Server ausgeliefert wird, ist DSStore nur als Teil des Server Ressource Kit erhältlich (siehe Anhang).

Durch die starke Integration der Enterprise CA in Active Directory sind bei der Fehlerbehebung einige der LDAP- und Active Directory-Tools sehr hilfreich, die teilweise bei Windows 2000 mitgeliefert werden und teilweise im Ressource Kit enthalten sind.

In Bezug auf die Kontrolle des Zugriffs auf die CA-Funktionalität verwendet Microsoft das in Windows 2000 eingesetzte Modell der Rechteverwaltung. Der Certificate Service und einige wichtige Komponenten sind – wie alles in einer Windows 2000 Umgebung – Objekte, für die spezielle Zugriffsrechte vergebenen werden können. So gibt es die Möglichkeit, die Zugriffsrechte auf die CA zu beschränken (siehe Abb 4), hierfür gibt es spezielle Berechtigungen für das CA-Objekt. Außerdem gibt es die Möglichkeit, die Rechte durch Einschränkungen des Zugriffs auf die Zertifikats-Templates für die CA oder den Benutzer anzupassen (Teil der Group Policies im ADS). Auf diese Weise kann konfiguriert werden, welche Art von Zertifikaten von welcher CA ausgegeben werden können und wer welche Arten von Zertifikaten beantragen kann. Eine noch feinere Abstimmung kann auch noch durch die Rechtevergabe an den verschiedenen Enrollment Controls erfolgen, die für die Beantragung von Zertifikaten notwendig sind.

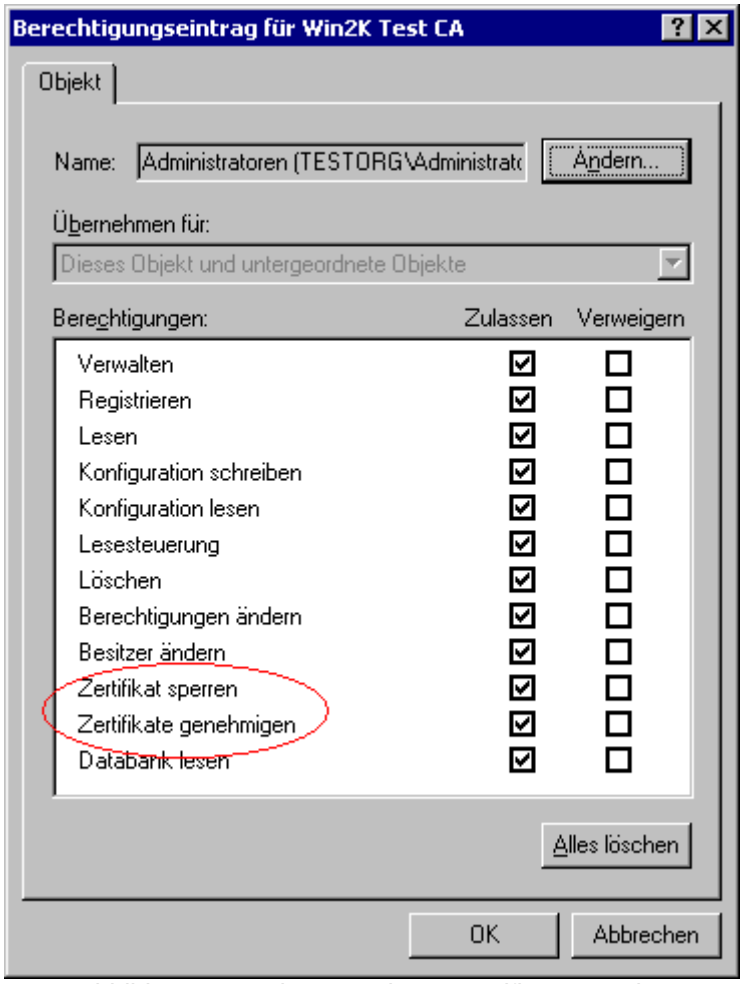

Abbildung 4: Rechteverwaltung Certificate Service

5.7 Spezielle Schutzmaßnahmen (CA)

Zur Sicherung der CA sind neben den üblichen Maßnahmen zum Schutz von Windows 2000 Servern auch noch spezielle Maßnahmen zum Schutz des CA Services notwendig. Die standardmäßig vergebenen Zugriffsrechte auf einige Komponenten sind hier oft zu großzügig. Mehr Details zur sicheren Konfiguration können [NSA_00] entnommen werden.

Sind besondere Anforderungen vorhanden (z.B. 4-Augen Prinzip), können diese nur über organisatorische Maßnahmen (z.B. geteilte Paßwörter) oder durch die Nutzung von Zusatzfunktionen von Drittprodukten (z.B. Hardware Security Modules) realisiert werden.

Allerdings läßt sich durch die enge Verknüpfung von Betriebssystem und CA kaum vermeiden, daß Administratoren auch weitreichende Rechte für die CA-Funktionalität haben. Eine strenge und saubere Rollentrennung läßt sich daher in einer Windows 2000 PKI nicht umsetzen.

6 Sonstiges

In diesem Kapitel werden einige weitere Eigenschaften der Windows 2000 PKI beschrieben, die noch nicht im Rahmen der anderen Punkte erwähnt wurden.

6.1 Gültigkeitsmodell

Der Certificate Service stellt die Gültigkeitszeiträume der Zertifikate nach dem sogenannten Schalenmodell aus [BER_01]. Das bedeutet, daß eine CA nur Zertifikate ausstellt, deren Gültigkeitszeitraum komplett innerhalb des Gültigkeitszeitraums des CA-Zertifikats liegt [MS_CS_00]. In der Praxis heißt dies zum Beispiel, daß eine CA, deren Zertifikat nur noch sechs Monate gültig ist, nur Zertifikate mit einer maximalen Lebensdauer von sechs Monaten ausstellen kann. Bei der Planung des Updates der CA-Zertifikate ist dieser Umstand zu berücksichtigen. In älteren Client-Versionen haben Microsoft-Anwendungen (z.B. Internet Explorer) dieses Schalenmodell abgeprüft und Zertifikate bei Verstoß zurückgewiesen. Neuere Versionen scheinen diese Prüfung allerdings nicht mehr durchzuführen – die Einhaltung dieses Gültigkeitsmodells wird von Microsoft-Anwendungen also nicht (mehr) erzwungen.

6.2 Integration mit anderen Produkten

Andere Hersteller von PKI-Komponenten haben schnell reagiert und die Unterstützung für Windows 2000 in ihre Produkte integriert. Dies umfaßt die simple Möglichkeit, Fremdprodukte für das Betriebssystem Windows 2000 zu implementieren bis hin zu einer weiterreichenden Integration in die Betriebssystemfunktionen. Vor allem die großen Hersteller von CA-Produkten sind bemüht, ihre Produkte so mit Windows 2000 zusammenarbeiten zu lassen, daß den Kunden der Mehrwert ihrer eigenen Produkte gegenüber Windows 2000 dargestellt wird.

Die Unterstützung und die Integration unterscheidet sich von Produkt zu Produkt. Grundsätzlich gibt es verschiedene Strategien und Ansatzpunkte, an denen eine Integration möglich ist. Die wichtigsten sind:

- *Active Directory Unterstützung*: Die Produkte können Zertifikate und Sperrlisten direkt ins Active Directory schreiben.
- *Unterstützung von Zertifikatserweiterung*: Möglichkeit zur Ausstellung von Zertifikaten mit den speziellen Microsoft-Erweiterungen und den Zertifikatserweiterungen in der Gestalt, die Microsoft erwartet.
- *Zertifikatsmanagement*: Bereitstellung eines Benutzer-Zertifikatsmanagements über die CryptoAPI/CSP-Schnittstelle.
- *Integration in die PKI-Hierarchie:* Die Möglichkeit, Fremdprodukte und Windows 2000 CAs innerhalb einer hierarchischen Struktur zu integrieren.

Gibt ein Hersteller also an Windows 2000 zu unterstützen, ist es ratsam, sich über die Details dieser Unterstützung zu informieren

Eine häufige Frage ist, ob es möglich ist, den Microsoft Certificate Service komplett durch ein anderes Produkt zu ersetzen. Für viele der Microsoft-Anwendungen (z.B. Outlook) ist dies grundsätzlich möglich d.h. es können auch Zertifikate aus anderen CAs verwendet werden (z.B. durch PKCS#12-Import). Allerdings ist damit nicht dieselbe umfassende Integration wie bei Verwendung der Enterprise CA zu realisieren. Bei einigen Anwendungen ist das Vorhandensein einer Enterprise CA notwendig, z.B. für das auto-enrollment. Solche Funktionen können daher beim ausschließlichen Einsatz eines externen CA-Produkts nicht unterstützt werden.

6.3 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 Smart-Cards oder speziellen Hardware Security Modulen (HSM).

Derzeit nicht unterstützt wird ein gemanagtes Key Recovery- oder Key Backup-Konzept für die Aufbewahrung der geheimen Teilnehmerschlüssel, um z.B. bei Verlust eines Schlüssels trotzdem noch an verschlüsselte Daten zu gelangen.

Auch eine automatische Erneuerung von Zertifikaten ist derzeit in Windows 2000 nicht integriert. Der Benutzer muß bei Ablauf seines Zertifikats ein neues beantragen. Eine Ausnahme hierfür ist wiederum das auto-enrollment, bei dem automatisch neue Zertifikate ausgestellt werden. Ein Mechanismus zur Verlängerung von CA-Zertifikaten ist vorhanden.

7 Windows XP

Im Herbst 2001 (Client) bzw. Frühjahr 2002 (Server) kommt der Nachfolger von Windows 2000 mit dem Namen Windows XP[5] auf den Markt. Es wird sich hierbei um eine Weiterentwicklung der in Windows 2000 eingeführten Technologien handeln, d.h. Windows XP baut auf der Windows 2000 Technologie auf. Auch im Bereich der PKI-Unterstützung wartet Microsoft mit einer Reihe von Neuerungen auf; die Grundarchitektur ist dabei jedoch die gleiche, die sich schon in Windows 2000 findet. Allerdings hat Microsoft die einzelnen Komponenten weiterentwickelt und um neue Funktionalität erweitert.

Die wichtigsten Neuerungen im PKI-Bereich sollen hier kurz vorgestellt werden:

- Sowohl CA als auch Client-Komponenten werden Cross-Zertifizierung und Bridge CA Szenarien unterstützen[6].
- Auto-enrollment und -update wird auch für Benutzer-Zertifikate unterstützt.
- Zertifikat-Templates können angepaßt werden; dabei können eine Reihe von Attributen wie Zertifikatsinhalte, die Policy für das Ausstellen von Zertifikaten, Gültigkeit, verwendeter CSP etc. konfiguriert werden.
- Ein Key-Archiv zur zentralen Schlüsselhinterlegung ist integriert und über die Certificate Templates konfigurierbar.
- Delta CRLs werden unterstützt
- Für die Verwaltung der CA werden definierte Rollen zur Verwaltung mit jeweils entsprechenden Rechten eingeführt, z.B. CA Administrator, Operator, Auditor etc. Diese Trennung der Rollen steht im Zusammenhang mit den Bemühungen von Microsoft, eine Common Criteria Zertifizierung für Windows XP zu erhalten.

---

5 Die Server-Variante wird dabei als .NET Server vertrieben

6 Was dies im Detail bedeutet konnte noch nicht getestet werden.

Auch auf Seiten der Anwendungen wurde die bestehende Funktionalität erweitert, so wird es z.B. mit EFS möglich sein, daß mehrere Benutzer Zugriff auf eine verschlüsselte Datei haben. Windows XP wird auch die Funktionalität zur Überprüfung von digitalen Signaturen unter zu installierenden Software Paketen besitzen.

Eine weitere Neuerung die Microsoft zusammen mit Windows XP[7] einführt, ist das sogenannte *„Microsoft Root Certificate Program“*[MS_TN_01]. In der Vergangenheit wurden Browser und Betriebsystem mit einer vorkonfigurierten Liste „vertrauenswürdiger Zertifizierungsstellen“ ausgeliefert. Diese Liste wird jetzt durch einen Mechanismus ersetzt, bei dem der Browser automatisch und transparent für den Benutzer, neue „vertrauenswürdige“ CA-Zertifikate von einem Microsoft Server lädt und in den Browser integriert. Der Mechanismus basiert auf dem oben beschriebenen Certificate Trust Lists (CTL) (siehe Kapitel 6.1). Neben dem Mechanismus der Verteilung der CA Zertifikate, ändert Microsoft auch die Anforderungen, die ein CA-Betreiber erfüllen muß, um in das *Root Certificate Program* aufgenommen zu werden. Die Anforderungen reichen dabei von Anforderungen an das Aussehen der Zertifikate (z.B. mindestens gültig bis 2010, Verwendung von CDP Extensions) bis zu einer Zertifizierung unter dem *„WebTrust for Certification Authorities Program“* [WEB_01].

8 Stärken und Schwächen

Die Stärken der Windows 2000 PKI liegen eindeutig in der starken Integration in die Windows 2000 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 aufwendig 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 2000 Domäne ist die Enterprise CA auch durch die vorhandene Anwendungsintegration geeignet.

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 Stand-Alone CA ist eigentlich nur dazu geeignet, eine geringe Anzahl von Zertifikaten (z.B. für SSL-Server oder als Root CA) auszustellen oder um innerhalb begrenzter Pilotversuche mit einer PKI zu experimentieren. Beim Ausstellen von Zertifikaten für eine große Anzahl von Teilnehmern fallen die mangelnden Management-Möglichkeiten und die fehlenden Funktionen (z.B. keine Directory Integration) stark ins Gewicht.

Eins der größten Mankos ist sicherlich die insgesamt eingeschränkte Funktionalität und mangelnde Flexibilität der derzeitigen Implementierung. Schwächen zeigt die Windows 2000 CA vor allem, wenn es darum geht, außerhalb einer Windows 2000 Umgebung zu operieren. Hier liegt die Funktionalität deutlich hinter der anderer auf dem Markt befindlicher Produkte zurück.

Solange die von Microsoft vorgegebenen Einstellungen innerhalb einer „Standard“-IT-Umgebung passen ist die geringe Flexibilität sicherlich kein Problem. Bei einer vielseitig

---

7 Entsprechende Updates werden es auch für ältere Windows Versionen (NT, ME, 98, 95) zur Verfügung gestellt.

einsetzbaren Lösung können hier aber durchaus Probleme auftreten. Für die weitere Entwicklung sind hier von Microsoft verschiedene Verbesserungen angekündigt, die diese Schwächen beheben sollen.

Eins der Hauptargumente für den Certificate Service ist immer wieder der Preis. Der Certificate Service ist bei jeder Windows 2000 Server Version „umsonst“ dabei (bei Windows XP mit vollem Funktionsumfang allerdings nur bei der Advanced Server Variante). 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 aufwendig dies ist im Vergleich zu anderen Produkten ist. Die oftmals bessere Administrierbarkeit anderer Produkte kann durchaus die höheren Anschaffungskosten an anderer Stelle wieder ausgleichen.

9 Literatur

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

[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

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

[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

[MS_TN_01] Microsoft TechNet, *Microsoft Root Certificate Program,* Microsoft Corporation, 2001

[NSA_00] S.Christman, *Guide to the Secure Configuration and Administration of Microsoft 2000 Certificate Services*, National Security Agency, 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) (RFC2251)*, 1997, IETF

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

[WEB_01] AICPA/CICA, *WebTrust Program for Certification Authorities*, Version 1.0, WebTrust

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

Anhang: DSStore, CertUtil Optionen

DSSTORE

Dsstore Usage:
DS Certificate Management Options
dsstore <dn of root domain> [-del][-addcrl][-addroot]
Must specify DN of root domain as first param!
i.e. dsstore DC=ntdev,DC=microsoft,DC=com
-del will give you a list of roots, and you can choose 1 for deletion.
-display Display enterprise roots
-addcrl <.crl file> <CA Name> <Machine Name>
-addroot <.crt file> <CA Name>
-addaia <.crt file> <CA Name> (for intermediate CAs)

Other diagnostic options
dsstore [[-domain] [-dcmon]] [-tcainfo] [-pulse] [-entmon] [-macobj]
-domain <domain name> Modify target domain for DCMon
-dcmon Run KDC Certificate monitoring tool
-checksc Check on smart card certificate validity
-tcainfo Display information about Enterprise CAs on domain
-pulse Pulse autoenrollment event(s)

Following options use SAM style machine names, e.g. domain\machinename$
-entmon <SAM machine name> Examine PKI and autoenrollment on remote machine
-macobj <SAM machine name> List attributes on DS machine object of interest to PKI

CERTUTIL

Syntax:
CertUtil [Opt.] -dump
CertUtil [Opt.] [-config Konfig.] -getconfig

CertUtil [Opt.] -decodehex Eingabedatei Ausgabedatei
CertUtil [Opt.] -decode Eingabedatei Ausgabedatei
CertUtil [Opt.] -encode Eingabedatei Ausgabedatei

CertUtil [Opt.] [-config Konfig.] -deny Anforderungskennung
CertUtil [Opt.] [-config Konfig.] -resubmit Anforderungskennung
CertUtil [Opt.] [-config Konfig.] -setattributes Anford.-kennung Attribute
CertUtil [Opt.] [-config Konfig.] -setextension Anford.-kennung Erweiterungsname Flags {Lang | Datum | Zeichenkette | @InDatei}
CertUtil [Opt.] [-config Konfig.] -revoke Seriennummer [Grund]
CertUtil [Opt.] [-config Konfig.] -isvalid Seriennummer
CertUtil [Opt.] [-config Konfig.] -CRL [Ausgabedatei | -]
CertUtil [Opt.] [-config Konfig.] -GetCRL Ausgabedatei [Index]
CertUtil [Opt.] [-config Konfig.] -importcert Zertifikatsdatei [Flags]

CertUtil [Opt.] [-config Konfig.] -ca.cert AusgStellenZertifikatsdatei [Index]
CertUtil [Opt.] [-config Konfig.] -ca.chain AusgStellenAustauschKettendatei [Index]
CertUtil [Opt.] [-config Konfig.] -ping
CertUtil [Opt.] [-config Konfig.] -pingadmin
CertUtil [Opt.] [-config Konfig.] -shutdown

CertUtil [Opt.] [-config Konfig.] -installCert [Stellenzertifikatdatei]
CertUtil [Opt.] [-config Konfig.] -renewCert [Schlüssel wiederverwenden] [Anforderungsdatei]

CertUtil [Opt.] [-config Konfig.] -schema

```
CertUtil [Opt.] [-config Konfig.] -ConvertMDB

CertUtil [Opt.] [-config Konfig.] -backup Sicherungsverz. [Kennwort [Inkremental] [Protokoll]]
CertUtil [Opt.] [-config Konfig.] -backupDB Sicherungsverz. [Inkremental] [Protkoll]
CertUtil [Opt.] [-config Konfig.] -backupKey Sicherungsverz. [Kennwort]
CertUtil [Opt.] [-config Konfig.] -restore Sicherungsverz. [Kennwort]
CertUtil [Opt.] [-config Konfig.] -restoreDB Sicherungsverzeichnis
CertUtil [Opt.] [-config Konfig.] -restoreKey Sicherungsverz. | PFX-Datei [Kennwort]
CertUtil [Opt.] [-config Konfig.] -dynamicfilelist
CertUtil [Opt.] [-config Konfig.] -databaselocations

CertUtil [Opt.] -store [Zertifikatspeichername [Zert.-index [Ausgabedatei]]
CertUtil [Opt.] -verifystore Zertifikatspeichername [Zert.-index]
CertUtil [Opt.] [-config Konfig.] -verifykeys [Schlüsselcontainername StellenZertDatei [Anbietertyp]]
CertUtil [Opt.] -verify Zertifikatsdatei [StellenZertDatei]

CertUtil [Opt.] -vroot [Löschen]
CertUtil [Opt.] -7f Zertifikatsdatei
CertUtil [Opt.] -error Fehlercode
CertUtil [Opt.] -getreg [{ca|restore|policy|exit}\[Prog.-kennung\]Reg.-wertname
CertUtil [Opt.] -setreg [{ca|restore|policy|exit}\[ProgId\]Reg.-wertname Wert
CertUtil [Opt.] -?

Befehle:
  -dump          -- Bildet Konfigurationsinformationen oder -dateien ab.
  -getconfig     -- Fragt die Standardkonfiguration ab.

  -decodehex     -- Decodiert eine hexadezimal-codierte Datei.
  -decode        -- Decodiert eine Base64-codierte Datei.
  -encode        -- Codiert eine Datei mit Base64.

  -deny          -- Verweigert die ausstehende Anforderung.
  -resubmit      -- Übermittelt die ausstehende Anforderung erneut.
  -setattributes -- Legt Attribute für die ausstehende Anforderung fest.
  -setextension  -- Legt Erweiterung für die ausstehende Anforderung fest.
  -revoke        -- Sperrt das Zertifikat.
  -isvalid       -- "IsValid"-Zertifikat
  -CRL           -- Veröffentlicht Sperrliste [optional in Datei].
  -GetCRL        -- Sperrliste lesen
  -importcert    -- Importiert eine Zertifikatsdatei in eine Datenbank.

  -ca.cert       -- Fragt das Zertifikat der Zertifizierungsstelle ab.
  -ca.chain      -- Fragt die Zertifikatskette der Zertifizierungsstelle ab.
  -ping          -- Sendet Signal zu den Zertifikatsdiensten.
  -pingadmin     -- Sendet Signal zur Adminschnittst. d. Zertifikatsdienste.
  -shutdown      -- Fährt die Zertifikatsdienste herunter.

  -installCert   -- Installiert das Zertifikat der Zertifizierungsstelle.
  -renewCert     -- Erneuert das Zertifizierungsstellen-Zertifikat.

  -schema        -- Bildet das Zertifikatschema ab.
  -ConvertMDB    -- Konvertiert die MDB-Datenbank in aktuelle Version.

  -backup        -- Sichert die Zertifikatsdienste.
  -backupDB      -- Sichert die Zertifikatsdienste-Datenbank.
  -backupKey     -- Sichert Dienstezertifikat und privaten Schlüssel.
  -restore       -- Stellt die Zertifikatsdienste wieder her.
  -restoreDB     -- Stellt die Zertifikatsdienste-Datenbank wieder her.
  -restoreKey    -- Stellt Dienstezertifikat und priv. Schlüssel wieder her.
  -dynamicfilelist -- Zeigt eine dynamische Dateiliste an.
  -databaselocations -- Zeigt den Datenbankpfad an.

  -store         -- Bildet Zertifikatspeicher ab.
```

```
   -verifystore    -- Bestätigt ein Zertifikat ein einem Speicher
   -verifykeys     -- Bestätigt das öffentlich-private Schlüsselpaar.
   -verify         -- Bestätigt die Zertifikatskette.

   -vroot          -- Erstellt/löscht virtuelle Webstammverz. und Freigaben.
   -7f             -- Überprüft das Zertifikat auf 0x7f-Längencodierungen.
   -error          -- Zeigt den Meldungstext des Fehlercodes an.
   -getreg         -- Zeigt den Registrierungswert an.
   -setreg         -- Legt den Registrierungswert fest.
   -?              -- Zeigt diese Syntaxmeldung an.

Optionen:
   -v              -- Führt den Vorgang ausführlich aus.
   -f              -- Erzwingt überschreiben.
   -idispatch      -- Verwendet IDispatch anstelle von COM.
   -user           -- Verwendet HKEY_CURRENT_USER oder Zertifikatspeicher.
   -gmt            -- Zeigt die Uhrzeit in GMT an.
   -silent         -- Verwenden Sie den automatischen Flag, um den Kryptografiekontext abzurufen.
```