PKI-Unterstützung in Windows 2000 und Windows 2003 Server

Secorvo White Paper

Version 2.01
Stand 08. Mai 2003

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

1 Vorwort zu Version 2 6
2 Zusammenfassung 7
3 Einleitung 9
4 PKI Unterstützung in Windows 2000/2003/XP 11
5 Architektur 13
6 Vergleichskriterien 15
6.1 Vertrauensmodell 15
6.1.1 Hierarchisches Modell 15
6.1.2 Cross-Zertifizierung 15
6.1.3 Weitere Verfahren 16
6.2 Standardunterstützung 18
6.2.1 Zertifikate 18
6.2.2 Sperrlisten 20
6.2.3 Austauschformate 21
6.3 Directory-Unterstützung 21
6.4 Flexibilität 21
6.5 Registrierung und Erneuerung 22
6.5.1 Enterprise CA 22
6.5.2 Stand-Alone CA 23
6.6 Administration 23
6.7 Spezielle Schutzmaßnahmen (CA) 26
7 Sonstiges 27
7.1 Gültigkeitsmodell 27
7.2 Integration mit anderen Produkten 27
7.3 Schlüsselmanagement 28
8 Gemischte Umgebungen Windows 2000 & 2003 29
9 Zusatzprodukte 30
10 Praktische Erfahrungen 31
10.1 Interoperabilität 31
10.2 Verzeichnisdienst-Anbindung 32
11 Stärken und Schwächen 33
11.1 Windows 2000 33
11.2 Windows 2003 34

12 Weitere Entwicklungen 35
13 Literatur 36

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	Lightweight Directory Access Protocol
MMC	Management Console
NT	New Technology
OCSP	Online Certificate Status Protocol
PC/SC	Personal Computer/Smartcard
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure
PKIX	X.509-based Public Key Infrastructure
RFC	Request for Comment
SDK	Software Development Kit

SSL	Secure Socket Layer
TLS	Transport Layer Security
XML	Extensible Markup Language
XP	Experience

Historie

Version	Datum	Änderung	Autor
1.1	29.11.01	1. Veröffentlichte Version	Holger Mack
2.0	10.04.03	2. überarbeitete Fassung, Ergänzung um Windows Server 2003 PKI	Holger Mack
2.01	08.05.03	Kleinere Fehlerkorrekturen	Holger Mack

1 Vorwort zu Version 2

Angesichts der Downloadzahlen der ersten Version dieses Whitepapers in dem einen Jahr seit seinem Erscheinen und den positiven Reaktionen auf die Inhalte, kann man darauf schließen, dass die Windows PKI für viele Leute ein interessantes Thema darstellt. Seit dem letzten Erscheinungstermin hat sich in diesem Umfeld so viel getan, dass es sich jetzt lohnt, eine neue, überarbeitete Version des Whitepapers zu veröffentlichen.

Zum einen hat ein Jahr Erfahrung mit der Windows 2000 CA an einigen Stellen die Möglichkeit gebracht, Informationen aus der ersten Version zu verfeinern oder zu ergänzen. Zum anderen steht mit der im Windows 2003 Server (ehemals .NET Server) integrierten PKI auch eine neue Version vor der Tür, für die eine Reihe von Verbesserungen der PKI-Funktionalität angekündigt waren. Zum Zeitpunkt der Erstellung dieses Whitepapers lag der Windows 2003 Server (noch unter dem Namen .NET) in seiner endgültigen Version noch nicht vor. Die Tests und Angaben beziehen sich auf den Release Candidate (RC) 1 der Enterprise Server Version. Inzwischen wurde noch ein RC2 angekündigt, laut Microsoft haben sich hier aber keine Änderungen in der PKI-Funktionalität ergeben. Es ist zu erwarten, dass sich gegenüber der endgültigen Version hier keine wichtigen Änderungen ergeben, garantiert werden kann dies aber nicht.

Obwohl Windows 2000 bereits seit über 2 Jahren auf dem Markt ist und mit der Version 2003 bereits ein Nachfolger vor der Tür steht, gibt es im Markt die Situation, dass viele Firmen es erst jetzt geschafft haben, ihre Netzwerkserver auf Windows 2000 umzustellen, bzw. sich gerade erst in der Umsetzungsphase befinden. Dies hat mit den doch erheblichen Umstellungen (z.B. Active Directory Server) zu tun, die bei einer Umstellung von Windows NT auf Windows 2000 notwendig sind und die eine gute Vorbereitung erforderlich machen. Ein Einsatz des Windows 2003 Servers ist daher bei vielen vorerst kein Thema, Windows 2000 wird daher auf der Server-Seite noch eine Weile eine wichtige Rolle spielen.

Auf der Client-Seite dagegen haben viele Firmen Windows 2000 „übersprungen“ und setzen Windows XP ein, was ja bereits seit längerem auf dem Markt ist. Dieses Whitepaper ist deswegen so aufgebaut, dass Nutzer aller aktuellen Windows Versionen (d.h. Windows 2000, XP, 2003) auf ihre Kosten kommen. Auf diese Weise kann hoffentlich jeder die Informationen bekommen, die für die jeweilige Umgebung und die eingesetzte Kombination der Versionen relevant sind. Ziel ist es dabei, einen Einblick zu geben, welche effektiven Auswirkungen die Unterschiede zwischen den verschiedenen Lösungen mit sich bringen, um z.B. die Entscheidung zu erleichtern, ob sich ein Warten auf die Version 2003 lohnt, oder ob man möglicherweise auch mit der Windows 2000 CA die geplanten Funktionen abbilden kann. In einem extra Kapitel wird daher darauf eingegangen, wie sich Mischformen, d.h. Netze die nicht rein auf Windows 2000 oder Windows .NET aufbauen, im Bezug auf die PKI-Funktionalitäten verhalten können bzw. ob ein Update möglich ist.

Diese Vorgehen wird dadurch erleichtert, dass sich keine grundlegenden Änderungen an der Architektur der Windows PKI ergeben haben. Die Struktur des Dokuments kann deshalb auch weitestgehend erhalten bleiben.

2 Zusammenfassung

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.

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[1]. Die Standardunterstützung erlaubt 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 in Windows 2000 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.

Inzwischen sind mit dem Windows 2003 und Windows XP die nächsten Version des Microsoft Betriebssystems auf dem Markt. In diesen Versionen wurde die PKI-Funktionalität noch einmal erweitert. Hiermit zeichnet sich ab, dass PKI ein wichtiger Baustein der zukünftigen Strategie von Microsoft ist. Im Windows 2003 Server hat die PKI-Funktionalität große Fortschritte gemacht. So sind z.B. einige wichtige Funktionen, die in Windows 2000 noch gefehlt haben, dort implementiert. Zielrichtung ist aber immer noch die Ausstellung von Zertifikaten für Komponenten (z.B. Benutzer, Rechner) einer Windows 2000 Domäne; die Funktionalität für das Ausstellen von Zertifikaten außerhalb der Windows-Umgebung ist weiterhin begrenzt.

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 spielt, 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,

[1] Seit der Version 5 hat Lotus auch eine X.509 konforme PKI Lösung in Notes integriert, die Notes interne PKI läuft allerdings weiterhin mit den proprietären Zertifikaten.

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.

3 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 wurden in Windows 2000 die Sicherheitsfunktionen überarbeitet, erweitert oder komplett neue Funktionalität hinzugefügt. Dieser Weg wird auch bei Windows XP oder dem Windows 2003 Server, der nächsten Version des Microsoft Server Betriebssystems, weiter verfolgt. Die Änderungen die in Windows XP und 2003 umgesetzt wurden, stellen allerdings bei weitem keinen so großen Schritt dar, wie bei der Umstellung von NT4 auf 2000. Vielmehr wird der in Windows 2000 begonnene Weg mit kleineren Erweiterungen und Verbesserungen weitergegangen.

Eine besondere Rolle in der neuen Sicherheitsfunktionalität in Windows 200x spielt dabei die Integration von Public Key-Technologie als Teil des Betriebsystems. Public Key-Technologie wird ab 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).

Die Unterstützung für Public Key Infrastrukturen (PKI) in Windows 200x/XP hat vor allem deshalb viel Beachtung gefunden, da PKI in vielen Bereichen (z.B. sichere E-Mail) eine Rolle spielt und 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 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/XP (oder vielleicht sogar schon 2003) 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 steckt und inwieweit die PKI-Funktionalität in die Planungen der PKI- oder IT-Projekte einbezogen werden soll. Durch das (angekündigte) Erscheinen des 2003 Servers und den darin enthaltenen Erweiterungen der PKI-Funktionalität, kommt eine zusätzliche Fragestellung hinzu: Lohnt es sich, jetzt mit der Windows 2000 CA zu starten, oder soll man besser auf die neue Version der CA warten; bzw. welche Auswirkungen hat die 2003 CA auf die Planung oder müssen neue Aspekte berücksichtigt werden. 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 immer auch die jeweiligen Rahmenbedingungen (z.B. technische Umgebung, spezielle Sicherheitsanforderungen etc.).

Das vorliegende White Paper enthält hauptsächlich eine Beschreibung und Diskussion der Funktionalität des Microsoft Certificate Service, der Certification Authority (CA) Komponente von Windows 200x. 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. Bei der Betrachtung der einzelnen Punkte wird auf Unterschiede zwischen der PKI in Windows 2000 und Windows 2003 explizit eingegangen. Wenn nicht explizit erwähnt, beziehen sich die Kommentare auf beide Lösungen.

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. Es ist auf jeden Fall festzuhalten, dass bei der 2003 CA nichts gegenüber der Windows 2000 PKI weggefallen ist, d.h. alle Funktionalitäten der Windows 2000 PKI lassen sich auch mit der Windows 2003 PKI umsetzen.

4 PKI Unterstützung in Windows 2000/2003/XP

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

Wie insgesamt in einer Windows 200x Domäne spielt auch bei der Windows 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 Domäne.

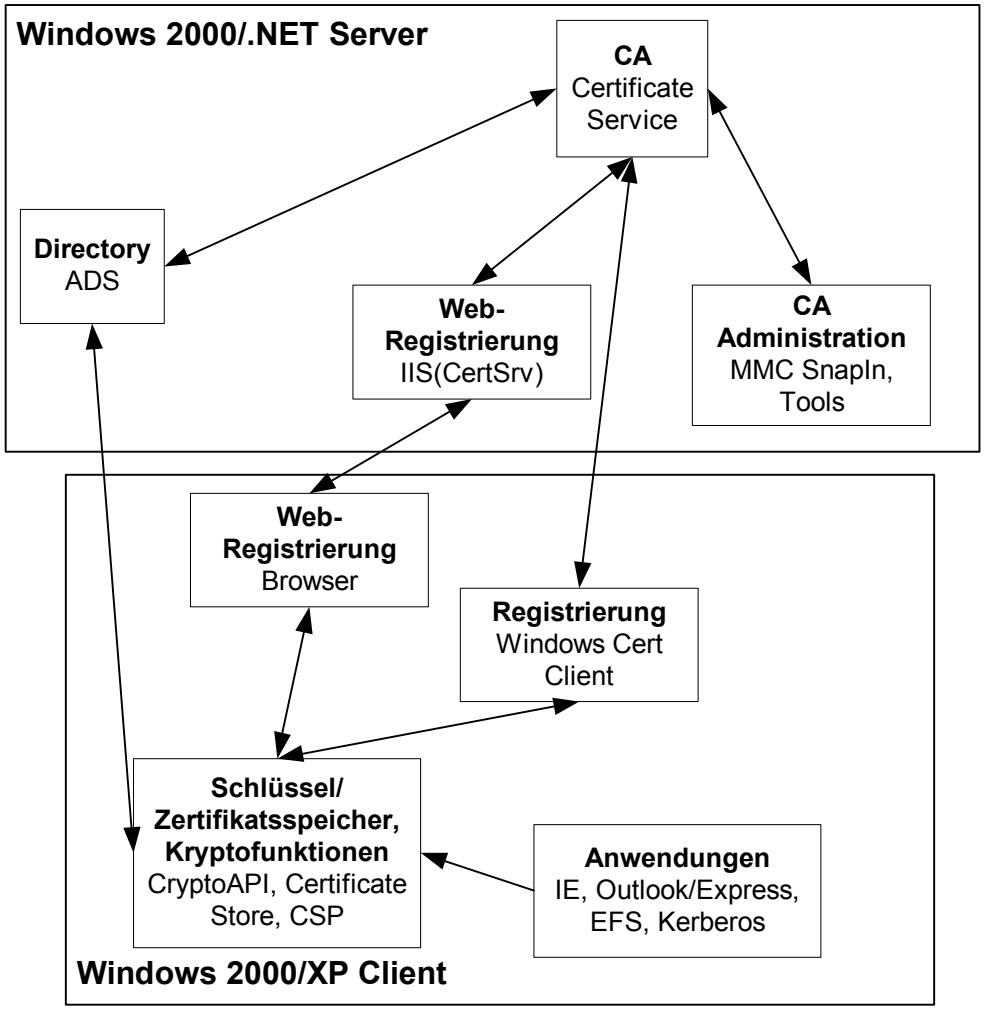

Abbildung 1: Komponenten Windows 2000 PKI

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 200x Domäne von zentraler Stelle verwaltet und vorgegeben werden. Einige Microsoft Anwendungen, wie z.B. Outlook oder Internet Explorer, bedienen sich bereits dieser Funktionalitäten und immer mehr Hersteller von Drittprodukten machen sich diese Funktionalität zu Nutze. 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 200x mitgelieferte Standard-Funktionalität erweitert werden, z.B. zur Unterstützung von kryptographischer Hardware.

Der Hauptaugenmerk in den folgenden Abschnitten gilt der CA-Komponente von Windows 2000/2003, 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.

5 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.

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 Zertifizierungsantrags, die Namensgebung und die Gestaltung eines Zertifikats (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.

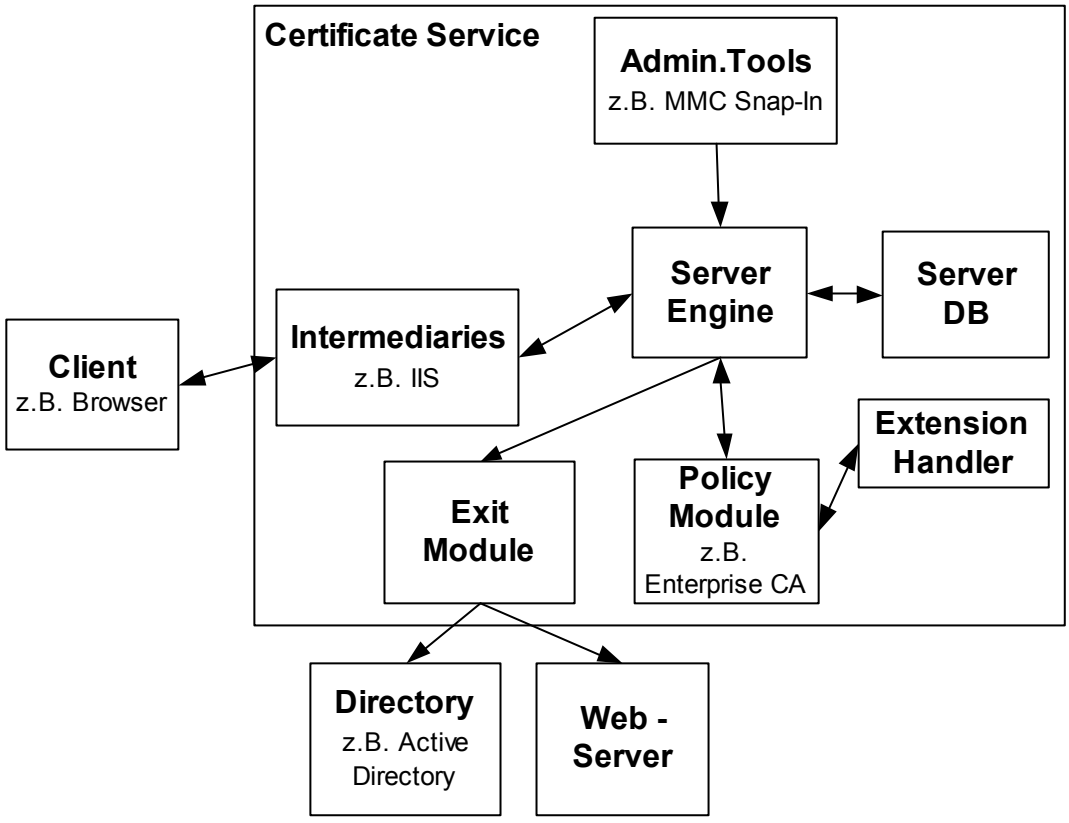

Abbildung 2: Windows 2000/.NET Certificate Service Architektur

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 200x 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 200x Umgebung inklusive Active Directory integriert und setzt eine Windows 200x 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.

6 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 generelle Betrachtung durchzuführen. In diesem Rahmen soll anhand der wichtigsten Kriterien, die bei einem CA-Produkt zu berücksichtigen sind, die Funktionalität der Windows 200x 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.

6.1 Vertrauensmodell

6.1.1 Hierarchisches Modell

Neben der Möglichkeit eine Windows 200x 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 zu mischen. So kann z.B. eine Windows CA als untergeordnete CA unter einer externen CA arbeiten, Windows kann aber auch Zertifikate für untergeordnete CAs ausstellen, die sich außerhalb der Windows Umgebung befinden. Die Hierarchietiefe ist hierbei grundsätzlich nicht eingeschränkt. Die Beantragung und Bearbeitung von Zertifizierungen in einer Hierarchie funktioniert dabei über die Standardformate PKCS#10 [PKCS_10] und PKCS#7 [PKCS_7], die von nahezu allen Herstellern und Anbieter unterstützt werden.

6.1.2 Cross-Zertifizierung

Cross-Zertifizierung [HAM_01] als zweite Methode wird erst ab der 2003 CA und Windows XP offiziell unterstützt.

Dabei muss man zwischen der Cross-Zertifizierung auf Seiten der CA und auf Seiten der Anwendungen unterscheiden. Wenn sich zwei CAs cross-zertifizieren wollen, bedeutet dies nichts anderes als, dass sich die CAs gegenseitig Zertifikate ausstellen. Diese Zertifikate unterscheiden sich prinzipiell nicht von den Zertifikaten für untergeordnete CAs. So ist das Ausstellen eines Cross-Zertifikats für eine andere CA beim 2003 Certificate Service nichts anderes als das Ausstellen eines Zertifikats für eine untergeordnete CA. Dies entspricht so auch dem Standard. So betrachtet können auch mit Windows 2000 Cross-Zertifikate ausgestellt werden.

Das Problem bei Cross-Zertifizierungen ist häufig die Tatsache, dass die Vertrauensstellungen durch Cross-Zertifizierungen unübersichtlich und schwer kontrollierbar werden können, außerdem sollen Cross-Zertifizierungen auf bestimmte Anwendungen oder Bereiche beschränkt werden können: zwei Firmen wollen z.B. eine Cross-Zertifizierung um gegenseitiges Vertrauen für die E-Mail Kommunikation zu ermöglichen, allerdings sollen Zertifikate für die Benutzerauthentifikation am Firmennetz nicht gegenseitig akzeptiert werden.

Um die Akzeptanz und das Vertrauen, dass der anderen PKI entgegengebracht wird kontrollieren und beschränken zu können, unterstützt die Microsoft CA ab der Version 2003 die Möglichkeit der sogenannten Qualified Subordination. Hiermit ist es möglich, das Vertrauen in die ausgestellten Zertifikat auf bestimmte Bereiche (z.B. Anwendungen) zu beschränken Auf diese Weise kann verhindert werden, dass durch eine Cross-Zertifizierung eine uneingeschränkte Vertrauensbeziehung ausgestellt wird.

Die Einschränkungen werden bei der Ausstellung des Zertifikats in das Zertifikat in Form von Zertifikatserweiterungen (Extensions) aufgenommen. Die Einschränkungen können sich dabei auf verschiedene Parameter beziehen, z.B. den Namensraum, die Policies nach denen die Zertifikate ausgestellt werden oder die Anwendungen für die die Zertifikate verwendet werden dürfen. Diese Einschränkungsmöglichkeiten sind bis auf eine Ausnahme Teil des X.509 Standards, die Einschränkungen bezogen auf den Anwendungstyp sind Microsoft-spezifische Erweiterungen des Zertifikats. Hinter der Unterstützung von Cross-Zertifikaten in Windows 2003 steht also hauptsächlich die Funktionalität der Qualified Subordination.

In der Praxis ist das eigentliche Ausstellen von Cross-Zertifikaten häufig das geringste Problem bei der Umsetzung einer Cross-Zertifizierung. Wichtig ist, dass die Anwendungen (z.B. das E-Mail-Programm) auch mit den Cross-Zertifikaten umgehen können. Die Hauptprobleme liegen dabei bei der Zusammenstellung der Zertifikatsketten und der anschließenden Gültigkeitsprüfung. Diese Funktionalitäten sind in den Windows XP Clients inzwischen vorhanden, andere Produkte tun sich hier oft schwer. Auch die Microsoft XP Client-Implementierung setzt ein gewisse der Zertifikatsinhalte und die Verfügbarkeit der Informationen (d.h. Zertifikate und Sperrlisten) in den entsprechenden Verzeichnissen (z.B. ADS) voraus. Ein kritischer Punkt bei Cross-Zertifizierungen ist häufig die Bereitstellung von Zertifikaten und Sperrinformationen über Unternehmensgrenzen hinaus.

Die Schwierigkeit der richtigen Auswertung der Zertifikate durch die Anwendung betrifft auch die Qualified Subordination. Auch diese Einschränkungen erzielen nur ihre Wirkung, wenn alle Anwendungen sie richtig interpretieren können. Bei Produkten die nicht auf den Implementierungen von Windows XP oder 2003 aufzusetzen, ist dies nicht überall gegeben und es muss deshalb getestet werden um die Gesamtsicherheit zu gewährleisten.

6.1.3 Weitere Verfahren

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 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. 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 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 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.

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. Sie können zwar als Datei exportiert und verteilt werden, können aber nur in einer Windows Umgebungen ausgewertet und genutzt werden.

Problematisch ist, dass es in Windows 200x derzeit noch keinen Mechanismus gibt, CTLs zu sperren. Wenn einem Zertifikat nicht länger das Vertrauen ausgesprochen werden soll, muss die CTL mit Hilfe der Windows 200x Mechanismen gelöscht und eine neue CTL ausgestellt und verteilt werden. Werden CTLs über die Grenzen einer zentral administrierten Windows 200x Umgebung verteilt, fällt das Fehlen einer Sperrmöglichkeit ins Gewicht.

Über die Zertifikatsspeicher vertrauenswürdiger CAs, die im Microsoft Betriebssystem integriert sind, können in einer Windows 200x/XP Umgebung auch über Group-Policies CA-Zertifikate an die Benutzerrechner verteilt werden. Zertifikaten, die von diesen CAs ausgestellt werden, wird dann automatisch vertraut. Problematisch an dieser Funktion ist, dass ein Windows Client bereits mit einer vorkonfigurierten Liste solcher Zertifikate kommt, die von Microsoft eingestellt wurden und denen der Benutzer so „automatisch“ vertraut. In einer Windows 2000 Umgebung sind diese nicht ohne weiteres zentral vom Rechner des Benutzer zu entfernen, es ist nur möglich zentral neue hinzuzufügen und auch diese neuen wieder zu löschen. In 2003 ist es dagegen jetzt möglich das Vertrauen in alle diese automatisch eingefügten Zertifikate zentral abzuschalten. Dies setzt allerdings einen Windows XP Client voraus.

Vor allem im Firmenumfeld ist diese Funktion hilfreich, um kontrollieren zu können, welchen Zertifikaten innerhalb des Firmennetzes vertraut werden soll.

Die Funktion der automatisch vertrauten CA-Zertifikate wird in 2003 und XP noch durch eine weitere Funktion erweitert, das automatische Nachladen von CA-Zertifikaten (Automatic Root Update). Hier werden im Hintergrund, ohne Einwirken oder Information des Benutzer, neue von Microsoft als vertrauenswürdig eingestufte CA-Zertifikate in den Speicher der vertrauenswürdigen Zertifikate nachgeladen. Diese Funktion kann abgeschaltet werden, in der Standardkonfiguration ist sie aber eingeschaltet. Ob man diese Funktion nutzen will oder nicht sollte zumindest gut überlegt sein.

6.2 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 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].

6.2.1 Zertifikate

Bei den Zertifikatsformaten orientiert sich Microsoft an X.509v3 sowie den Zertifikats- und Sperrlistenprofilen, die in PKIX (RFC3280) definiert sind. Die Architektur des Certificate Service erlaubt dabei prinzipiell flexible Zertifikatsinhalte. Bei der Umsetzung unterscheiden sich die CAs in Windows 2000 aber erheblich:

- Bei den im Lieferumfang von Windows 2000 enthaltenen Policy-Modulen sind die Möglichkeiten, Zertifikatsinhalte anzupassen sehr 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.[2] In Windows 2000 enthalten sind eine Reihe von anwendungsspezifischen Zertifikats-Templates, die die meisten üblichen Anwendungen abdecken. Diese Templates werden im Active Directory verwaltet. In Windows 2000 ist es nicht vorgesehen, diese Zertifikats-Templates anzupassen oder neue zu definieren.
- Auch in der 2003 CA werden die Zertifikatsinhalte über die oben genannten Templates definiert, im Gegensatz zu Windows 2000 gibt es hier aber weitreichende Möglichkeiten, die Zertifikats-Templates anzupassen. Für die Zertifikatsinhalte können über diesen Mechanismus Faktoren wie die minimale Schlüssellänge, die Gültigkeit oder einige Zertifikatserweiterungen individuell definiert werden. 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 Dokument eingegangen.

Die in den mitgelieferten Zertifikats-Templates definierten Zertifikatsinhalte (diese sind bei beiden Versionen gleich) 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:

---

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

- 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/XP 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)) oder zur internen Verarbeitung genommen werden.

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 200x/XP 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.[3] Über die Zertifikats-Templates in Windows 2003 lassen sich aber z.B. die Key Usage Extensions auf „kritisch“ setzen.

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 Probleme bereiten können, ist die Tatsache, 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).

In der 2003 Version lassen sich die Zertifikatsinhalte so anpassen, dass einige dieser Probleme behoben werden können. Es muss allerdings im Einzelfall geprüft werden, ob die Anpassungsmöglichkeiten den Anforderungen der jeweiligen Umgebung gerecht werden. Es sollte allerdings darauf geachtet werden (am besten durch Tests), dass man durch

---

3 Dieses Verhalten ist allerdings eine leider sehr verbreitete Praxis, die einige Anbieter wählen, um Interoperabilitätsprobleme auf Kosten der Sicherheitsfunktionalität zu vermeiden.

Änderungen in den Zertifikatsinhalte nicht die Funktionalität der Windows-Anwendungen einschränkt.

Insgesamt konnten im Rahmen verschiedener (nicht vollständiger) Tests die von Windows 200x ausgestellten Zertifikate von Produkten anderer Hersteller in der Regel importiert werden, und es gelang auch, von CA-Produkten anderer Hersteller ausgestellte Zertifikate in Windows 200x 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 200x 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.

6.2.2 Sperrlisten

Windows 2000 unterstützt standardmäßig Certificate Revocation Lists (CRLv2) 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.

In der Windows 2003 CA werden zusätzlich sogenannte Delta-CRLs unterstützt. Mit Hilfe von Delta-CRLs kann die Größe der notwendigen Downloads minimiert werden, da hier nicht jedes Mal eine komplette Sperrliste mit allen Einträgen erzeugt wird, sondern nur ein Zusatz mit den Sperrungen seit Veröffentlichung der letzten Sperrliste. D.h. es wird nicht nur regelmäßig (z.B. einmal pro Woche) eine komplette Sperrliste ausgestellt, sondern zusätzlich in kürzeren Abständen (z.B. einmal am Tag) eine Delta-CRL, die nur die Sperrungen seit Ausstellung der letzten kompletten CRL enthält. Die Gültigkeitsdauer der beiden Sperrlisten ist dabei bei der 2003 CA unabhängig voneinander einstellbar. Auch ein manuelles Ausstellen einer neuen CRL oder Delta-CRL außerhalb der normalem Update-Periode ist möglich. Die Einstellungen der Gültigkeit sind abhängig von den jeweiligen Sicherheitsanforderungen. Bei der Umsetzung einer PKI Lösung ist aber darauf zu achten, dass nicht alle Produkte diese Delta-CRLs unterstützen und es somit zu Problemen kommen kann.

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[4].

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

6.2.3 Austauschformate

Neben den oben beschriebenen Standards für Zertifikate und Sperrlisten, unterstützt Windows 200x 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.

6.3 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 (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.

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. 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.

6.4 Flexibilität

Die Architektur des Certificate Service erlaubt durch die verschiedenen Module im Prinzip relativ große Flexibilität. Wie bereits in Kapitel 5 beschrieben, kann diese Flexibilität, vor allem bei der Windows 2000 CA, 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 bei der 2000 CA beschränken sich bei der PKI-Funktionalität auf einige wenige Parameter (z.B. CDPs), die entsprechend angepasst werden können. Auch bei der Gestaltung des Distinguished Name von CAs und Benutzern sind die Attribute vorgegeben.

Hier ist aber auch einer der größten Unterschiede zur 2003 CA. Durch die Möglichkeit die Zertifikats-Templates anzupassen, wird die Flexibilität der Lösung stark verbessert. Die Einstellungen der Zertifikats-Templates hat Auswirkungen sowohl auf die Technik (z.B. Zertifikatsinhalte) als auch auf Abläufe (z.B. manuelle Freischaltung von Anträgen) in der PKI. An den verschiedenen Stellen in diesem Dokument wird auf diese Auswirkungen eingegangen

Auf die Möglichkeiten, die Funktionalität durch Drittprodukte zu ergänzen, wird in Kapitel 9 eingegangen.

Auf Client-Seite gibt es Flexibilität durch austauschbare CSPs; so können hauptsächlich die kryptographischen Funktionen und die Speicherung der Schlüssel angepasst werden. Eine weitere Möglichkeit ist der Einsatz von Revocation Providern mit deren Hilfe die in Windows

enthaltenen Prüfroutinen ergänzt werden können. Auf diese Weise könnte z.B. ein Windows 2000/XP Client auch OCSP zur Prüfung von Zertifikaten verwenden.

6.5 Registrierung und Erneuerung

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.

6.5.1 Enterprise CA

Bei einer Enterprise CA ist die eigentliche Registrierung des Benutzers oder Computers das Anlegen eines Accounts in der Windows 200x Domäne. Ist der Benutzer hier angemeldet, kann er sich 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 entsprechende 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 2003 gibt es zusätzlich die Möglichkeit, auch bei der Enterprise CA durchzusetzen, 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 2 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. In Windows 2000 ist dies nicht konfigurierbar, ab Windows 2003 können über die Zertifikats-Templates die Parameter für die Zertifikatserneuerung konfiguriert werden.

Der zweite Spezialfall ist die Ausstellung von Zertifikaten für den in Windows 200x unterstützen 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. Einige Hersteller arbeiten gerade daran Erweiterungen zu entwickeln, die hier Verbesserung bringen (siehe auch Kapitel 9).

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.

6.5.2 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 auch möglich, eine automatische Ausstellung aller eingehenden Anfragen zu konfigurieren, dabei erfolgt allerdings keinerlei Authentisierung. Außer den sehr begrenzten Angaben, die im Zertifikatsantrag enthalten sind, hat der Administrator allerdings keine zusätzlichen Informationen um den Antrag zu prüfen.

Der Zugriff bzw. die Authentisierung und Autorisierung des Zugriffs auf die Webseiten kann (wie auch bei der Enterprise CA) über die im IIS üblichen Protokollen und Mechanismen (z.B. SSL, TLS) geschützt werden.

Die Funktionalität der Stand-Alone CA hat sich bei Windows 2003 weniger gegenüber der Windows 2000 CA geändert. Einige Änderungen wie z.B. Delta-CRLs oder das Rollenkonzept sind auch in der Stand-Alone Version vorhanden, allerdings arbeitet die Stand-Alone CA nicht mit Zertifikats-Templates und lässt deshalb auch keine Änderungen an den darin definierten Einstellungen zu.

6.6 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 (siehe Abb. 3).

Die Darstellung lehnt sich an den Dateimanager an und ist so relativ einfach und übersichtlich gehalten. Die Bedienung entspricht dem, was man von einer Microsoft-Umgebung erwartet und ist daher relativ einfach zu bedienen. Allerdings kann die Darstellung bei großen Mengen von Zertifikaten schnell unübersichtlich werden, entsprechende Filtermöglichkeiten für die Darstellung bestehen aber.

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[5] und das Sichern und Wiederherstellen der CA-Datenbank durchgeführt werden.

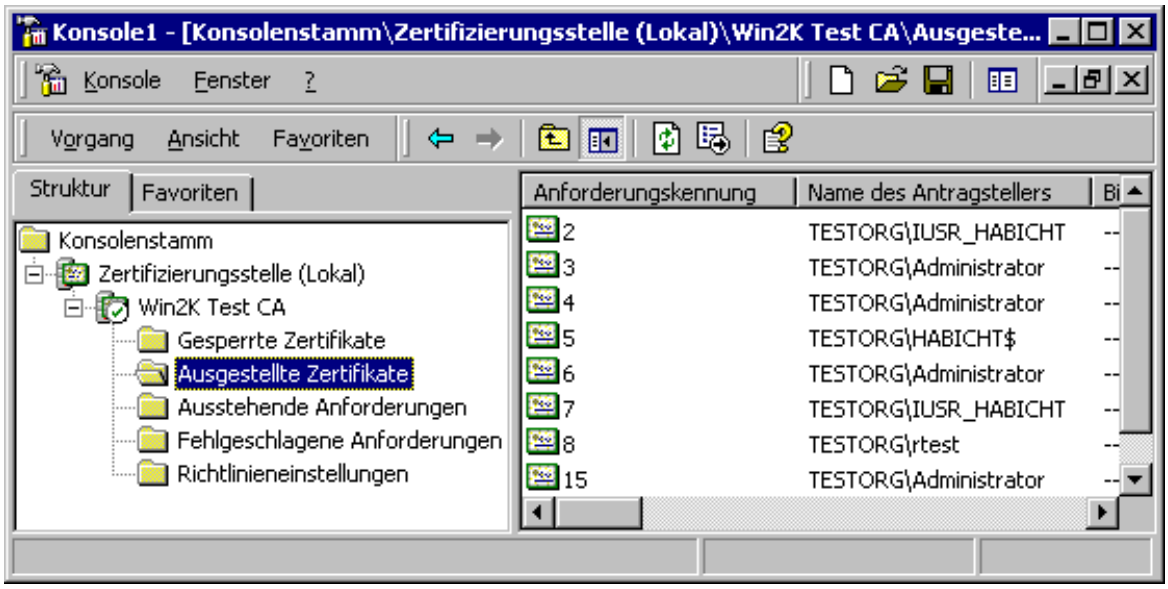

Abbildung 3: MMC Snap-In Administration Zertifizierungsstelle (Windows 2000)

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.
- 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.

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 200x 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 200x eingesetzte Modell der Rechteverwaltung. Der Certificate Service und einige wichtige Komponenten (wie z.B. die Zertifikats-Templates) sind – wie alles in einer Windows 200x 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

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

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 normalen Backup-Operator und Auditor Rollen, die über die normalen Windows Zugriffsrechte und Rechte definiert werden.

Eine Besonderheit dieses Rollenkonzepts ist es, 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 ist möglich. 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). Anders als bei Windows 2000 bei welchem sich die PKI-Funktionalität bei den verschiedenen Server Versionen (Enterprise, Datacenter, etc.) nicht unterscheidet, unterscheidet sich die PKI-Funktionalität bei Windows 2003. Die Möglichkeit einer Rollentrennung ist Teil des Enterprise-Servers oder des Datacenters. Die anderen Server-Versionen (Standard, Web) unterstützen zwar die Rollen, allerdings nicht die Rollentrennung.

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. Eine noch feinere Abstimmung kann auch noch durch die Rechtevergabe an den verschiedenen Enrollment Controls erfolgen, die für die Beantragung von Zertifikaten notwendig sind.

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.

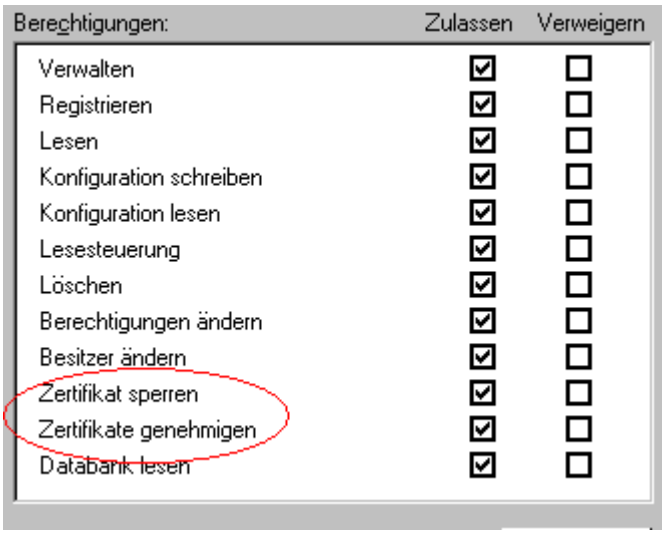

Abbildung 4: Rechteverwaltung Certificate Service (Windows 2000)

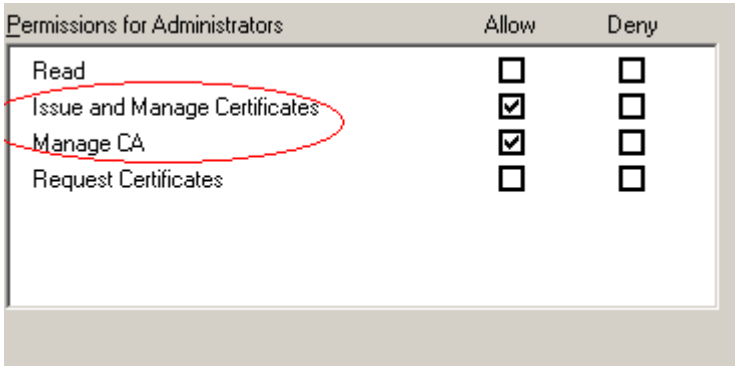

Abbildung 5: Rechteverwaltung Certificate Service (Windows 2003)

6.7 Spezielle Schutzmaßnahmen (CA)

Je nach den spezifischen Sicherheitsanforderungen müssen zur Sicherung des CA Servers und der PKI Komponenten (z.B. Zertifikats-Templates) entsprechende Maßnahmen ergriffen werden. Dies kann von der Härtung der Betriebssystem Plattform (z.B. Abschalten unnötiger Dienste, restriktive Vergabe von Zugriffrechten, Patch-Management) bis hin zu speziellen physikalischen Schutzmaßnahmen reichen (z.B. abschließbarer Schrank, Trennung vom Netzwerk). Für die Sicherung des CA Services und der anderen PKI-relevanten Komponenten, sind außerdem spezielle Konfigurationen notwendig, da die Standardzugriffsrechte hier oft zu großzügig sind. Beim Einsatz in komplexen Windows 2000 Domänenstrukturen kommt dieser Konfiguration besondere Bedeutung zu.

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 Modul) realisiert werden. Auch das Rollenkonzept und die Rollentrennung in der Windows 2003 Version ermöglichen kein 4-Augen-Prinzip für die CA Verwaltung.

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. Mit Hilfe des Rollenkonzepts in der Windows 2003 PKI (siehe oben) ist eine bessere Trennung zwischen Betriebsystemadministration und PKI Administration möglich.

7 Sonstiges

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

7.1 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.

7.2 Integration mit anderen Produkten

Andere Hersteller von PKI-Komponenten haben schnell reagiert und die Unterstützung für Windows PKI in ihre Produkte integriert. Dies umfasst die simple Möglichkeit, Fremdprodukte für das Betriebssystem Windows 2000 zu implementieren bis hin zu einer weitreichenden Integration in die Betriebssystemfunktionen. Vor allem die großen Hersteller von CA-Produkten sind bemüht, ihre Produkte so mit Windows 200x zusammenarbeiten zu lassen, dass den Kunden der Mehrwert ihrer eigenen Produkte gegenüber Windows 200x 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 Zertifikatserweiterungen*: 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 bzw. Cross-Zertifizierung:* Die Möglichkeit, Fremdprodukte und Windows CAs innerhalb einer hierarchischen Struktur zu integrieren.

Gibt ein Hersteller also an, die Windows PKI 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 Autoenrollment. Solche Funktionen können daher beim ausschließlichen Einsatz eines externen CA-Produkts nicht unterstützt werden.

7.3 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 Smartcards oder speziellen Hardware Security Modulen (HSM).

Die automatische und konfigurierbare Archivierung oder Wiederherstellung von Benutzerschlüsseln (sog. Key Recovery- oder Key Backup) wird von der Windows 2000 CA nicht unterstützt.

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 Autoenrollment für EFS- und Computer-Zertifikate, bei dem automatisch neue Zertifikate ausgestellt werden. Ein Mechanismus zur Verlängerung von CA-Zertifikaten ist vorhanden.

Für beide Punkte gibt es in der Windows 2003 CA erweiterte Funktionalitäten:

Die Archivierung von Teilnehmerschlüsseln wird 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.

Auch bei der automatischen Zertifikatserneuerung unterscheidet sich die 2003 CA gegenüber ihrer Vorgängerin. Über das Zertifikats-Template lassen sich wichtige Parameter für die Erneuerung von Zertifikaten konfigurieren. Zusammen mit dem erweiterten Autoenrollment (siehe oben) kann damit auch ein automatisches und transparentes Erneuern der Zertifikate erfolgen.

8 Gemischte Umgebungen Windows 2000 & 2003

Wie bereits angesprochen, ist in vielen Organisationen gerade erst die Umstellung nach Windows 2000 abgeschlossen oder sogar erst in der Umsetzung. Eine komplette Umstellung auf Windows 2003 Server wird also noch eine Weile auf sich warten lassen. Mit Hinblick auf PKI und den deutlich erweiterten Funktionsumfang der Windows 2003 Server CA gegenüber der Windows 2000 CA, stellt sich natürlich die Frage, ob man die erweiterten PKI-Funktionalitäten der Windows 2003 CA nicht auch schon in einer Windows 2000 Umgebung nutzen kann.

Grundsätzlich lässt sich sagen, dass ein Windows 2003 Certificate Service nur auf einem Windows 2003 Server läuft, ein Update der Umgebung ist also notwendig. Für die Unterstützung der neuen Features wie z.B. die veränderbaren Zertifikats-Templates muss ein Update des Schemas des Active Directories durchgeführt werden. Dies gilt dann auch für die anderen angeschlossenen Domain-Controller und ADS-Instanzen. Microsoft stellt hierfür Tools zur Verfügung, mit deren Hilfe ein solches Update durchgeführt werden kann. Die gilt allerdings nur für die Enterprise CA, eine Windows 2003 Stand-Alone CA kann auch ohne dieses Update in einer Windows 2000 Umgebung betrieben werden.

Auch auf Seiten der Client-Versionen unterscheiden sich die Versionen, so dass nur bei einer richtigen Kombination von Windows XP Client und Windows 2003 Server die volle PKI-Funktionalität genutzt werden kann. Sind noch Windows 2000 Clients im Einsatz, können diese Funktionen wie Autoenrollment für Benutzer, das Archivieren von Schlüsseln oder die veränderbaren Zertifikats-Templates nicht verwendet werden.

9 Zusatzprodukte

Wie bereits oben erwähnt, gibt es Schnittstellen und Ansatzpunkte in der Windows 200x CA, über die die Standardfunktionalität der Windows 200x PKI ergänzt bzw. ersetzt werden können.

Die im Betriebsystem integrierten grundlegenden Kryptografiefunktionen, die über die Microsoft CryptoAPI zugreifbar sind und die von allen Microsoft-Anwendungen und auch dem Certificate Service verwendet werden, können mit Hilfe sogenannter Provider erweitert bzw. ersetzt werden. Die häufigste Methode sind hierbei die Cryptographic Service Provider (CSP) die es z.B. ermöglichen, Hardware-Module wie Smartcards oder HSMs zu integrieren. Für die Anwendungen ist es weitestgehend transparent, ob die Kryptofunktionen in Software oder Hardware implementiert sind. Nahezu all Hersteller von Smartcards, USB-Token oder auch Hardware Security Modulen (HSMs) bieten für ihre Produkte eine CSP-Implementierung an, mit deren Hilfe die Produkte für Anwendungen zur Verfügung gestellt werden können. Vorsicht ist hier aber geboten, da nicht alles CSPs Hersteller den vollen Funktionsumfang (z.B. Generierung von Schlüsseln) implementieren.

Der zweite Typ von Providern sind die Revocation Provider. Hiermit können die standardmäßig in Windows enthaltenen Routinen und Techniken zur Überprüfung des Sperrstatus von Zertifikaten durch zusätzliche ergänzt werden. Auf diese Weise kann Windows z.B. um Funktionalitäten wie OCSP zur Sperrprüfung erweitert werden. Auch hier bieten einige Hersteller entsprechende Lösungen, vor allem für OCSP an.

Auf Seite der Client-Anwendungen unterstützt eine steigende Zahl von Herstellern den in Windows integrierten Zertifikatsspeicher, d.h. die Anwendungen greifen über die Microsoft-Schnittstelle CryptoAPI auf die Schlüssel (und ggf. Kryptofunktionen) zu. Dies wird entweder als Alternative zu einer herstellereigenen Schlüsselspeicherung oder auch als einzige Lösung angeboten. Auf diese Weise können diese Anwendungen auch von der integrierten Lösung der Windows PKI profitieren und die von der Windows CA ausgestellten Zertifikate nutzen. Bei Produkten, die diese Schnittstelle nicht verwenden, ist die Integration in eine Windows 200x CA oft schwierig und mit manuellem Aufwand verbunden (z.B. manueller Export und Import von PKCS#12 Dateien).

Eine Serie von Produkten, die relativ neu oder sogar erst in der Entwicklung sind, sind solche die die PKI-Kernfunktionalität der Microsoft CA erweitern sollen. Diese Lösungen sind dabei um die Microsoft CA „herumgebaut" und erweitern sie hauptsächlich um PKI Management-Funktionalitäten wie z.B. flexiblere und erweiterte Registrierungsmöglichkeiten oder das Management von Zertifikaten bis hin zu Smartcard-Management Systemen. Die Art der Integration kann dabei verschieden sein, einige Produkte schalten sich als Proxy vor die Windows CA, andere nutzen die Architektur der Microsoft PKI und ersetzen Policy Module. In wie weit diese Produkte eine sinnvolle Ergänzung darstellen muss sich noch erweisen.

10 Praktische Erfahrungen

Bei der Erstellung der ersten Version dieses Whitepapers konnte auf relativ wenig Erfahrung mit dem Umgang mit der Windows 2000 CA außerhalb der Laborumgebungen zurückgegriffen werden. Inzwischen hat die Windows 2000 PKI aber auch in einigen praktischen Projekten eine große Rolle gespielt, so dass entsprechende Erfahrungen gesammelt werden konnten. Einige der gelernten Aspekte sind in diesem Kapitel zusammengefasst.

10.1 Interoperabilität

Einer der kritischen Faktoren bei der Umsetzung von PKI-Projekten ist immer wieder die Interoperabilität zwischen den Produkten verschiedener Hersteller. Besonders Microsoft hatte in der Vergangenheit und auch noch heute den Ruf, durch eigene Ergänzungen von Standards die Interoperabilität zu anderen Produkten zu erschweren. Interessant ist deshalb, wie Microsoft in diesem Bereich abschneidet.

In Deutschland ist ein wichtiges Projekt in diesem Bereich die ISIS-MTT Spezifikation [ISIS-MTT_02], die in Zusammenarbeit zwischen dem TeleTrusT Verein[6] und dem Zusammenschluss von CA Dienstleistern[7] entstanden ist. Diese Initiative hat als Ziel, die Interoperabilitätsprobleme in heutigen PKI-Implementierungen zu beseitigen. Die erste Zielanwendung ist dabei sichere E-Mail, eine Erweiterung zu TLS/SSL ist aber in Arbeit. ISIS-MTT ist kein neuer Standard, sondern baut auf den wesentlichen PKI-Standards (X.509, PKIX, LDAP, PKCS#11, S/MIME) auf und versucht durch sog. Tailoring, d.h. Ergänzungen, Detailvorgaben und Klärung offener Punkte Interoperabilitätsprobleme mit den existierenden Standards zu beseitigen. Ziel ist es die Interoperabilität von Produkten, die konform zur ISIS-MTT-Spezifikation sind, zu gewährleisten.

Um die Konformität von Produkten zu ISIS-MTT testen zu können, wurde ein frei verfügbares Testbed[8] entwickelt, auf dessen Basis man PKI Produkte verschiedener Ausprägung auf Konformität testen kann. Lässt man jetzt das CA-Zertifikat der Microsoft CA[9] ausgestellten Zertifikate durch das ISIS-MTT Testbed prüfen, so stellt man fest, dass diese Zertifikate bis auf eine Ausnahme ISIS-MTT-konform sind: Die Erweiterung für die Schlüsselverwendung (Key Usage) ist auf nicht kritisch gesetzt. Diese Einstellung ließ sich für das eigene CA-Zertifikat allerdings nicht anpassen. Für Zertifikate die von der CA ausgestellt werden (Sub-CAs, Benutzer etc.), lassen sich diese Einstellungen konfigurieren. Allerdings sind (wie oben erwähnt) keine Zertifikatsdetails konfigurierbar, so dass nicht in allen Fällen ein komplett ISIS-MTT konformes Zertifikat erstellt werden konnte.

In den USA gibt es seit einigen Jahren das Projekt Federal Bridge CA[10], bei dem über den Mechanismus der Cross-Zertifizierung Vertrauensbeziehungen zwischen den PKIs der verschiedenen Behörden in den USA ermöglicht werden sollen. Auch hier spielt die Interoperabilität eine sehr große Rolle und die Hersteller müssen mit ihren Produkten einen

6 http://www.teletrust.de

7 http://www.t7-isis.de

8 Das Testbed ist zu beziehen über http://www.teletrust.de

9 Getestet wurde ein CA Zertifikate einer Windows 2003 CA mit den Standardeinstellungen von Microsoft.

10 http://csrc.nist.gov/pki/fbca/

Interoperabilitätstest bestehen, um teilnehmen zu können. Die Microsoft CA hat diesen Test bestanden.

10.2 Verzeichnisdienst-Anbindung

Ein weiteres Problem von PKI-Projekten ist immer wieder die Anbindung an Verzeichnisdienste. Diese Probleme tauchen verstärkt dann auf, wenn über Firmengrenzen hinaus sicher kommuniziert werden soll. Vor allem die Verteilung von Sperrlisten aber auch Zertifikaten ist hierbei von Bedeutung. Probleme macht hier, dass Verzeichnisdienste im Allgemeinen nicht außerhalb der Firmennetzwerke zur Verfügung stehen, es Probleme mit verschiedenen Namensgebungungen und Verzeichnisstrukturen in verschiedenen Organisationen gibt und die Tatsache, dass Produkte verschiedener Hersteller verschiedene Voraussetzungen für das Auffinden von Sperrinformationen haben.

Die von Microsoft verwendete Methode ist der Einsatz der sogenannten CDPs und AIA Extensions, d.h. im Zertifikat wird der Standort der Sperrinformationen bzw. der CA-Zertifikate kodiert. Die Zertifikate werden so von der Microsoft CA ausgestellt und auch der Microsoft Client erwartet einen solchen CDP. Eine andere Art, für einen Client die Sperrlisten zu holen, besteht nicht. Wenn also ein Zertifikat geprüft werden soll, welches keinen passenden CDP enthält oder wenn der Ort im CDP nicht erreichbar ist (z.B. da das Directory durch Firewalls nicht erreichbar ist) kann der Client keine Prüfung durchführen. Genauso können andere Produkte, die CDPs nicht unterstützen die Sperrlisten im Active Directory nicht ohne weiteres finden, da der Name der CA und die Ablage der Sperrliste im Directory nicht übereinstimmen.

Im Rahmen der PKI1-Verwaltung, sollte dieses Problem durch ein zentrales Directory gelöst werden. Da hier auch Windows 2000 im Einsatz war, mussten die Anforderungen berücksichtigt werden. In [BSI_02] kann nachgelesen werden, welche Probleme auftraten und welcher Aufwand für die Zusammenstellung der Verzeichnisdienste notwendig ist.

11 Stärken und Schwächen

Diese Kapitel ist in zwei Teile aufgeteilt, da eine Bewertung für die beiden Versionen der Microsoft PKI nur getrennt sinnvoll ist. Allerdings ist die Bewertung der 2003 CA nicht alleinstehend, sondern bezieht sich sehr stark auf die der Windows 2000 CA, und stellt die entscheidenden Unterschiede dar.

11.1 Windows 2000

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 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 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.

Eines 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. Die Entwicklung, dass 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.

Solange die von Microsoft vorgegebenen Einstellungen innerhalb einer „Standard“-IT-Umgebung passen, ist die geringe Flexibilität sicherlich kein Problem. Bei einer vielseitig einsetzbaren Lösung in heterogenen Umgebungen können hier aber durchaus Probleme auftreten.

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 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.

11.2 Windows 2003

Da der Windows 2003 Certificate Service eine Weiterentwicklung der Windows 2000 CA darstellt, sind einige der Kernaussagen der Bewertung der Windows 2000 PKI auch hier noch gültig. Die prinzipiellen Vorteile (z.B. einfache Registrierung) und Nachteile (z.B. sehr starke Bindung an Betriebssystem-Funktionen) bleiben bestehen.

Mit dem 2003 Server hat Microsoft eine ganze Reihe von wichtigen PKI-Funktionen ergänzt und erweitert, die bei der Windows 2000 PKI noch fehlten. Dazu gehören hauptsächlich Funktionalitäten wie Key-Archival, die Kontrolle einer Cross-Zertifizierung durch Qualified Subordination, das erweiterte Autoenrollment, das Rollenkonzept sowie die Anpassungsmöglichkeiten bei den Zertifikats-Templates. Dies hat vor allem die Flexibilität erhöht und an einigen Stellen (z.B. User Autoenrollment) noch weitere Vereinfachungen möglich gemacht. Auf diese Weise hat Microsoft an einigen Stellen gegenüber anderen Herstellern aufgeholt. Der Einsatz der Windows PKI lässt sich so deutlich besser an die jeweiligen Bedürfnisse einer Organisation anpassen.

Das prinzipiell geeignete Einsatzszenario der Windows 2003 CA hat sich dabei nicht wesentlich gegenüber der Windows 2000 CA verändert. Auch weiterhin ist die klare Stärke und Ausrichtung die Ausstellung von Zertifikaten für Komponenten (Benutzer, Computer etc.) in einer Windows Domäne. Die Veränderungen an der Stand-Alone CA in Windows 2003 haben kaum Einfluss auf die Bewertung gegenüber der Windows 2000 Lösung, so dass auch die Windows 2003 Stand-Alone CA für eine Ausstellung von Zertifikaten außerhalb der Windows Domäne nur beschränkt geeignet ist. Die Auswirkungen der Änderungen der Windows 2003 Enterprise CA liegen daher vor allem bei:

- Durch die höhere Flexibilität der Zertifikatsinhalte lässt sich die Zusammenarbeit mit Anwendungen außerhalb der Windows 2000 Domäne verbessern. Das gleiche gilt auch wenn es darum geht, mit anderen PKIs und CAs zusammenzuarbeiten. Es muss aber weiterhin im Einzelfall geprüft werden ob die trotzdem vorhandenen Einschränkungen akzeptabel sind.
- Funktionen wie die automatische Ausstellung von Zertifikaten und die automatische Verlängerung vereinfachen ein Reihe von Abläufen. Außerdem können über die Anpassungen an den Templates Abläufe besser gesteuert und an die Anforderungen angepasst werden.
- Die Rollentrennung und die Konfigurationsmöglichkeiten ermöglichen ein erhöhtes Sicherheitsniveau.

Während bei der Windows 2000 CA, bedingt durch die fehlenden Konfigurationsmöglichkeiten, relativ wenig Planung erforderlich ist, sollte man vor der Nutzung der 2003 CA mehr Planung und Tests vorsehen. Einige der Verbesserungen, z.B. Anpassung der Templates etc. kommen nur zum Tragen, wenn man diese entsprechend bei der Planung berücksichtigt. Durch solche Anpassungen verlässt man auch den geprüften und getesteten Rahmen von Microsoft. Wie bei allen Herstellern und PKI-Umsetzungen ist es daher in diesem Fall unumgänglich, die vorgenommenen Änderungen ausgiebig zu testen um sicherzustellen, dass man sich nicht durch eine Öffnung nach außen, Probleme in der internen Umsetzung einhandelt.

Vorsicht ist auch geboten, in wie weit sich die Flexibilität in der Praxis nutzen lässt, vor allem da der Konfigurationsspielraum durch die Vorgaben und Bedingungen der Anwendungen an die Zertifikate beschränkt sind.

12 Weitere Entwicklungen

Wenn man die Entwicklung der Windows 2000 PKI zur Windows 2003 PKI betrachtet, dann sieht man hier klar, dass es sich um ein Evolution und nicht um eine Revolution handelt. Es entsteht der Eindruck, dass viele der jetzt vorhandenen Möglichkeiten, prinzipiell auch schon in der 2000 Implementierung vorhanden waren, sie aber, wahrscheinlich aus Zeit und Stabilitätsgründen in der 2000 Version noch nicht zugänglich gemacht wurden (z.B. Anpassungen der Zertifikats-Templates). In der jetzigen Version scheinen solche „versteckten" Features nicht mehr vorhanden zu sein, große Sprünge können daher nicht erwartet werden. Im Enterprise Modus deckt die Windows 2000 CA so ziemlich alle Funktionen ab, die man für eine solche integrierte Lösung erwartet. Noch nicht vorhandene Funktionen, z.B. Smartcard-Management etc. werden eher von Drittherstellern ergänzt als das Microsoft sie in das Kernprodukt einfügen wird.

Sicherlich noch Verbesserungsspielraum ist bei der Stand-Alone CA vorhanden, die weiterhin sehr stark eingeschränkt ist. Allerdings sind hier auch keine großen Neuerungen zu erwarten, da die Stand-Alone CA in der Microsoft-Strategie hauptsächlich die Rolle einer Root-CA oder einer „Notfall-Lösung“ für kleine Anzahl von Zertifikaten erfüllt und nicht der Versuch erkennbar ist, mit den unabhängigen PKI-Herstellern auf dem Markt der Ausgabe von Zertifikaten für heterogene Umgebungen zu konkurrieren. Durch die derzeit entwickelten Erweiterungen einiger Hersteller, könnte die Stand-Alone CA allerdings in diese Richtung entwickelt werden. Da diese Produkte allerdings nur die Kernfunktionalität des Certificate Service verwenden, unterscheiden sie sich zum Teil kaum noch von anderen Drittprodukten.

Große Funktionalitätssprünge sind also in den nächsten Versionen der Windows CA nicht zu erwarten, eher kleine Verbesserungen und Ergänzungen; die PKI-Funktionalität ist allerdings (sowohl Client- als auch Server-seitig) ein wichtiger und fester Bestandteil der Sicherheitsfunktionen zukünftiger Anwendungen und Plattformen bei Microsoft.

In der .NET Plattform spielt die digitale Signierung von Programmteilen eine Rolle und die von Microsoft und IBM vorgeschlagene Roadmap [IBMMS_02] für die Realisierung von sicheren XML-Web-Services baut in vielen Teilen auf PKI-Funktionalität auf. Beispiele sind hierfür XML-Signaturen und daraus resultierend gesicherte SOAP Nachrichten. Auch bei den Themen Digital Rights Management (DRM) und Trusted Computing Plattform, spielt PKI eine Rolle, auch wenn hier die Ausprägungen noch nicht klar erkennbar sind.

Es scheint also klar, dass die PKI-Integration in Microsoft-Produkte ein strategische Entscheidung bei Microsoft ist, die auch noch in der absehbaren Zukunft eine gewichtige Rolle spielen dürfte.

13 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,

[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