Unterrichtseinheit 5:

Konfigurieren der Netzwerksicherheit mit Hilfe von PKI (Public Key Infrastructure)

Verschlüsselung mit öffentlichen Schlüsseln ist eine bedeutende Technologie für E-Commerce, Intranets, Extranets und Webanwendungen

Verschlüsselung mit öffentlichen Schlüsseln:

Die Verschlüsselung mit öffentlichen Schlüsseln stellt Datensicherheit bereit. Bei der Verwendung von öffentlichen Schlüsseln werden zwei Schlüssel verwendet, die einen mathematischen Bezug zueinander haben.

- Privater Schlüssel (bleibt geheim)
- Öffentlicher Schlüssel (wird an alle potenziellen Korrespondenten ausgegeben)

Das Ziel einer Verschlüsselung ist es, Daten auf eine Weise zu verändern dass sie nur vom Empfänger gelesen werden können, für denn sie bestimmt ist. Nur der Empfänger verfügt über den zugehörigen privaten Schlüssel.

Authentifizierung mit öffentlichen Schlüsseln:

Wie bei der Verschlüsselung mit öffentlichen Schlüsseln wird auch bei der Authentifizierung mit öffentlichen Schlüsseln ein Schlüsselpaar verwendet. Es wird eine Digitale Signatur erstellt. Bei einer digitalen Signatur sind die Funktionen des privaten und des öffentliches Schlüssels vertauscht.

Digitale Signatur

Eine digitale Signatur ist ein Mittel für den Absender einer Nachricht, einer Datei oder anderer codierter Informationen mit seiner Identität zu verbinden.

- Nur eine Person die über den privaten Schlüssel verfügt, kann die digitale Signatur erstellt haben.
- Jede Person mit Zugriff auf den öffentlichen Schlüssel kann die digitale Signatur überprüfen.

Zertifizierung

Zertifikate sind signierte Dokumente, mit denen öffentliche Schlüssel zu anderen Informationen, wie einem Namen oder einer E-Mail-Adresse, zugeordnet werden.
Die Signatur einer Zertifizierungsstelle (kann eine externe Ausstellungsfirma oder auch eine interne Abteilung einer Firma sein) garantiert, dass der öffentliche Schlüssel tatsächlich zu der Person oder Organisation gehört, die ihn angibt.

Nur *Stammzertifizierungsstellen* sind vertrauenswürdig, dagegen sind die *untergeordnete Zertifizierungsstellen* nicht vertrauenswürdig. Obwohl Stammzertifizierungsstellen verwendet werden können, um Zertifikate für Endbenutzer für Aufgaben wie das Senden von sicheren E-Mails auszustellen, werden sie in den meisten Organisationen nur verwendet, um Zertifikate für andere Zertifizierungsstellen, die sogenannten untergeordnete Zertifizierungsstellen, auszustellen.

Primäre Windows 2000 PKI-Komponenten

- *Zertifikatsdienste* (Hauptbetriebssystemdienst) ermöglichen als ihre eigenen Zertifizierungsstellen zu agieren und digitale Zertifikate auszustellen und zu verwalten
- *Active Directory* (Veröffentlichungsdienst) macht Zertifikate und Zertifikationssperrlisten innerhalb einer Organisation öffentlich verfügbar.

Es werden verschiedene Arten von Sicherheitsprotokollen verwendet
SSL (Secure Sockets Layer)
IPSec (Internet Protocol Security)
TSL (Transport Layer Security)

Bereitstellen der Zertifikatsdienste

In Windows 2000 Server gibt es zwei Typen von Zertifizierungsstellen: Organisationszertifizierungsstelle und eigene Zertifizierungsstellen.
Eine Organisationszertifizierungsstelle erfordert, dass alle Benutzer und Computer, die Zertifikate anfordern, über ein Konto in Active Directory verfügen.
Eine eigenständige Zertifizierungsstelle erfordert kein Active Directory.

Organisationszertifizierungsstelle

Eine **Organisationszertifizierungsstelle** (für Zertifikate nur für Benutzer und Computer innerhalb der Organisation) ist die Zertifizierungsstelle auf der höchsten Ebene in einer Zertifikatshierarchie. Für eine Organisationszertifizierungsstelle sind folgende Einstellungen nötig: Active Directory (um die Identität und die Sicherheitsberechtigungen des Anforderers zu bestimmen), DNS-Server-Dienste, Administratorberechtigung auf dem DNS-, Active Directory- und Zertifizierungsstellenserver, man muss Mitglied der Gruppe Organisations-Admins sein.

Wichtig:
Um Zertifikate in Active Directory zu veröffentlichen, muss der Server, auf dem die Zertifizierungsstelle installiert ist, ein Mitglied der Gruppe Zertifikatherausgeber sein.

Eine **untergeordnete Organisationszertifizierungsstelle** muss über eine übergeordnete Zertifizierungsstelle verfügen.
Eine **eigenständige Stammzertifizierungsstelle** (höchste Ebene in einer Zertifikatshierarchie) kann vom Netzwerk getrennt und in einem sicheren Bereich platziert werden. Für Einheiten außerhalb einer Organisation sollte eine eigenständige Stammzertifizierungsstelle installiert werden.
Eine Stammzertifizierungsstelle stellt üblicherweise nur Zertifikate für untergeordnete Zertifizierungsstellen aus. Für die Installation einer eigenen Zertifizierungsstelle benötigt man Administratorberechtigungen auf dem lokalen Server.
Eine eigenständige untergeordnete Zertifizierungsstelle fungiert als Einzelzertifikatsserver innerhalb einer Zertifizierungsstellenvertrauenshierarchie. Für die Installation dieser benötig man folgende Einstellungen: eine übergeordnete Zertifizierungsstelle, Administratorberechtigung auf dem lokalen Server.

Installieren der Zertifikatsdienste

Ein Computer kann nicht umbenannt oder mit einer Domäne verbunden, bzw. entfernt werden, nachdem die Zertifikatsdienste installiert wurden. Um eine dieser Aktionen durchzuführen, müssen die Zertifikatsdienste zunächst vom Computer entfernt werden.

Installieren der Zertifikatsdienste:

- Auswählen eines Zertifizierungsstellentyps
- Festlegen erweiterter Optionen
  Es gibt folgende Kryptografieeinstellungen: **Kryptografiedienstanbieter**, **Hashalgorithmus**, **Schlüssellänge** (Standard sind 512 Bit; für Stammzertifizierungsstellen sollten mindestens 2048 Bit verwendet werden) und **vorhandene Schlüssel verwenden**
- Eingeben von Identifikationsinformationen
- Angeben von Speicherorten für die Datenbank und die Protokolldateien
  Standardverzeichnis für Zertifikate „**%SystemRoot%\System32\CertLog**“

Erstellen einer untergeordneten Zertifizierungsstelle

Eine untergeordnete Zertifizierungsstelle muss einer Zertifizierungsstelle zugeordnet sein, welche die Zertifikatsanforderungen bearbeitet.

- Erhalten eines Zertifikats für eine untergeordneten Zertifizierungsstelle
  Anforderung eines Zertifikatsstellenzertifikats ⇒ Anforderung direkt an eine im Netzwerk vorhandene Zertifizierungsstelle senden ⇒ Computername ⇒ Übgeordnete Stelle
- Installieren eines Zertifikats aus einer Datei
  Verwaltung ⇒ Zertifizierungsstelle ⇒ Vorgang ⇒ alle Tasks ⇒ Zertifizierungsstellenzertifikat installieren ⇒ Öffnen
- Sichern der Zertifikatsdienste
  (nur durch Sicherungsoperatoren oder Administratoren)
  Verwaltung ⇒ Zertifizierungsstelle ⇒ alle Tasks ⇒ Zertifizierungsstelle sichern
- Wiederherstellen der Zertifikatsdienste
  (nur durch Sicherungsoperatoren oder Administratoren)
  Verwaltung ⇒ Zertifizierungsstelle ⇒ alle Tasks ⇒ Zertifizierungsstelle wiederherstellen

Zertifikatsanforderungs-Assistenten

Der Zertifikatsanforderungs-Assistent ist nur verfügbar, wenn ein Zertifikat von einer Organisationszertifizierungsstelle angefordert wird.

- Verwenden von Zertifikatsvorlagen
  Administrator, Domänencontroller, Computer, Basis-EFS, EFS-Wiederherstellungs-Agent, Benutzer, Webserver

- Anforderung eines Zertifikats
  MMC-Konsole öffnen ⇒ Snap-In hinzufügen/entfernen ⇒ Hinzufügen ⇒ Zertifikat auswählen ⇒ Hinzufügen ⇒ Eigenes Benutzerkonto, Dienstkonto oder Computerkonto auswählen ⇒ Fertig stellen ⇒ OK ⇒ Zertifikate - Aktueller Benutzer Zertifikate (Lokaler Computer) ⇒ mit rechter Maustaste auf Zertifikate klicken ⇒ Alle Task ⇒ Neues Zertifikat anfordern ⇒ Weiter ⇒ Zertifikatsvorlage ⇒ Erweiterte Optionen ⇒ Weiter ⇒ Zertifikat installieren

Zertifikatsdienste-Webseiten

- Senden einer Zertifikatsanforderung
  http://*<Servername auf dem sich die Zertifizierungsstelle befindet>*/Certsrv
  ⇒ Ein Zertifikat anfordern ⇒ Weiter ⇒ Anforderungstyp wählen ⇒ Weiter ⇒ Einsenden

- Senden einer erweiterten Zertifikatsanforderung (z.B. für IPSec)
  http://*<Servername auf dem sich die Zertifizierungsstelle befindet>*/Certsrv
  ⇒ Ein Zertifikat anfordern ⇒ Weiter ⇒ Anforderungstyp wählen ⇒ Erweiterte Anforderung ⇒ Weiter ⇒ Senden Sie ein Zertifikatsanforderungsformular an diese Zertifizierungsstelle ⇒ Einsenden

Wichtig:
Wird ein Zertifikat für einen Computer angefordert, so muss das Kontrollkästchen „Lokalen Speicherplatz verwenden“ aktiviert werden.

- Überprüfen einer ausstehenden Anforderung
  http://*<Servername auf dem sich die Zertifizierungsstelle befindet>*/Certsrv
  ⇒ auf ein ausstehendes Zertifikat überprüfen ⇒ Weiter ⇒ Weiter ⇒ Hier stehen drei Zertifikatsstatus zur Verfügung: 1) Noch ausstehend ⇒ Entfernen
  2) Ausgestellt ⇒ Dieses Zertifikat installieren
  3) Verweigert

Anzeigen von Zertifikaten

Windows2000 speichert Computerzertifikate lokal auf dem Computer, die diese angefordert hat.
Indem eine MMC-Konsole geöffnet wird, kann der Zertifikatsspeicher, der folgendermaßen strukturiert sein kann, angezeigt werden:
Eigene Zertifikate, Vertrauenswürdige Stammzertifizierungsstellen, Organisations-vertrauen, Zwischenzertifizierungsstellen, Active-Directory-Benutzerobjekt, Request, SPC

Verwalten von Zertifikaten

- Ausstellen von Zertifikaten
  *Öffnen der Konsole **Zertifizierungsstelle** ⇒ Ausstehende Anforderungen*

- Sperren von Zertifikaten
  *Öffnen der Konsole **Zertifizierungsstelle** ⇒ ausgestellte Zertifikate ⇒ mit rechter Maustaste auf das Zertifikat klicken ⇒ Alle Tasks ⇒ Zertifikat sperren ⇒ Grund auswählen ⇒ Ja*

- Veröffentlichen einer Zertifikatsperrliste
  - befindet sich im Ordner **%SystemRoot%\System32\CertSrv\CertEnroll**
  *Öffnen der Konsole **Zertifizierungsstelle** ⇒ mit rechter Maustaste auf **Gesperrte Zertifikate** klicken ⇒ Alle Tasks ⇒ Veröffentlichen ⇒ Ja*

Importieren und Exportieren von Zertifikaten

Folgende Formate können importiert und exportiert werden:

- Personal Information Exchange (PKCS #12)
- Cryptographic Message Syntax Standard (PKCS #7)
- DER Encoded Binary X.509
- Base64 Encoded X.509

- Importieren eines Zertifikats
  *Öffnen einer MMC-Konsole die das Snap-In **Zertifikat** enthält ⇒ Eigene Zertifikate ⇒ mit rechter Maustaste auf **Zertifikate** klicken ⇒ Alle Tasks ⇒ Importieren*

- Exportieren eines Zertifikats
  *Öffnen einer MMC-Konsole die das Snap-In **Zertifikat** enthält ⇒ Eigene Zertifikate ⇒ mit rechter Maustaste auf **Zertifikate** klicken ⇒ Alle Tasks ⇒ Exportieren*

Konfigurieren von Active Directory für Zertifikate

- Der externe Benutzer muss ein Zertifikat haben
- Der externe Benutzer muss ein Benutzerkonto haben
- Das Zertifikat des Externen Benutzers muss von einer vertrauenswürdigen Zertifizierungsstelle ausgestellt werden
- Eine Namenszuordnung muss zwischen dem Zertifikat des externen Benutzers und dem Activ-Directory-Konto erstellt werden

Problembehandlung

- Überprüfen von Ereignisprotokollen
- Verwenden des Diagnosemodus
- Problembehandlung bei einer Zertifizierungsstelle
- Bestätigen der Gültigkeit eines Zertifikats