ERNW Newsletter 34 /November 2010

Liebe Partner, liebe Kollegen,

willkommen zur 34. Ausgabe des ERNW Newsletters mit dem Thema:

Implementierung von zertifikatsbasierter Netzwerk-Authentifizierung im Unternehmensnetzwerk

Version 1.0 vom 16. November 2010

Autoren: Oliver Roeschke, oroeschke@ernw.de
Christopher Werny, cwerny@ernw.de

Friedwart Kuhn
22.11.2010 22:30:56

Abstract
Im diesem Newsletter wird die Implementierung von IEEE 802.1X™ Netzwerkzugangskontrolle über Cisco-Komponenten, mit EAP-TLS, mit einer Microsoft-PKI mit Software-Zertifikaten in einer Windows Server 2008 R2-basierten Active Directory-Umgebung erläutert.

INHALTSVERZEICHNIS

1 EINLEITUNG 4

2 DAS FRAMEWORK 802.1X 4

2.1 Zugrunde liegende Standards und Technologien 5
2.1.1 802.1X 5
2.1.2 X.509v3-Zertifikate 5
2.1.3 EAP 5
2.1.4 EAP-TLS 6

3 ANFORDERUNGEN UND BESCHREIBUNG DER UMGEBUNG 8

3.1 Nicht-technische Anforderungen an die Lösung 8
3.2 Struktur der Umgebung 9
3.3 Active-Directory 9
3.4 Netzwerk Infrastruktur 10
3.5 Authentifizierungsserver – Cisco Secure ACS 10
3.6 Windows Clients 10
3.7 Zertifikatsinfrastruktur 10

4 VORBEREITENDE MAßNAHMEN IM NETZWERKBEREICH 11

4.1 Netzstruktur 11
4.2 Authentifzierungsmethoden 12
4.3 Vorbereitung Netzwerk-Infrastruktur 12

5 VORBEREITUNG DER ACTIVE-DIRECTORY UMGEBUNG 12

5.1 Konfiguration des Credential Roaming 12
5.2 Anonyme LDAP Anfragen an der Globalen Katalog konfigurieren 14
5.3 Konfiguration des Autoenrollment 20
5.4 Installation des Cisco ACS Remote Agent 21
5.5 Prüfung der Active Directory-Benutzer 21

6 VORBEREITENDE MAßNAHMEN PKI-UMGEBUNG 22

6.1 Zertifikatsvorlagen 22
6.1.1 Vorlage für Computer Zertifikate 22
6.1.2 Vorlage für Benutzer Zertifikate 25
6.1.3 Vorlage für Secure ACS Zertifikate 26
6.1.4 Veröffentlichen der Vorlagen 26
6.2 Autoenrollment Konfiguration 27
6.2.1 Autoenrollment Konfiguration für Computer-Zertifikate 28
6.2.2 Konfiguration für Benutzer-Zertifikate 29
6.2.3 Autoenrollment Logging Konfiguration 30

7 KONFIGURATION CISCO SECURE ACS 30

7.1 Einrichtung des Remote Agents 30

7.2 Import der PKI-Zertifikate in Secure ACS ... 33
7.2.1 Konfiguration der vertrauenswürdigen Zertifizierungsstellen ... 33
7.2.2 Konfiguration der Zertifikatssperrliste ... 34
7.3 Anbindung des Secure ACS an das Active Directory ... 35
7.4 Ausstellung des Secure ACS-Zertifikates ... 38
7.5 Konfiguration EAP-TLS ... 42
7.5.1 Basis Konfiguration EAP-TLS ... 42
7.5.2 Konfiguration von 802.1X VLAN-Zuordnung ... 43
7.6 Konfiguration MAC Authentication Bypass ... 45
8 KONFIGURATION DER SWITCHE ... 47
8.1 802.1X Basis Konfiguration ... 47
8.1.1 Anlegen des RADIUS-Clients ... 48
8.2 Konfiguration MAC Authentication Bypass ... 48
8.3 Konfiguration Wake-on-LAN ... 48
8.4 Konfiguration des PXE ... 49
8.5 Konfiguration des Guest-VLANs ... 49
8.6 Konfiguration des Auth-Fail VLANs ... 49
8.7 Konfiguration von Inaccessible Authentication Bypass ... 49
9 KONFIGURATION DER CLIENT PCS ... 50
10 TROUBLESHOOTING ... 51
10.1 Sperrung von Benutzer- oder Computer-Zertifikaten ... 51
10.2 Ausrollen neuer Benutzer-/Computer-Zertifikate ... 54
10.3 Keine gültigen Zertifikate zur Authentifizierung vorhanden ... 54

1 EINLEITUNG

Eine häufige Anforderung in Unternehmensnetzwerken ist, dass Netzwerke gegen unerlaubte Zugriffe aus Netzen Dritter (beispielsweise dem Internet oder Partnerunternehmen) geschützt sind, jedoch keinerlei Kontrolle für den Zugriff aus den Unternehmensräumen heraus stattfindet. Somit kann durch die Einbringung von Fremdhardware (hierzu zählen alle Netzwerk-fähigen Geräte, die nicht durch die Unternehmens-IT beschafft und betreut werden) ein hohes Risiko für die Sicherheit der Systeme und verarbeiteten Daten entstehen.

Der IEEE Standard 802.1X in Kombination mit EAP basierten Authentifizierungsmethoden stellt die gängigste Technologie im Bereich Netzwerkzugangskontrolle dar. Aufgrund seiner Modularität kann dieses Verfahren sowohl für kabelgebundene Netzwerke, wie auch Funknetzwerke genutzt werden. Es stehen weiterhin eine Reihe unterschiedlicher Authentifizierungsmethoden zur Verfügung. Diese ermöglichen eine auf das Unternehmen abgestimmte Implementierung.

Der folgende Newsletter beschreibt das technische Setup einer 802.1X in einer *Active Directory*-Umgebung. Hierbei wird Zugangskontrolle sowohl durch Authentifizierung von Computern als auch Benutzern erreicht. Durch die Benutzerauthentifizierung wird gleichzeitig eine dynamische VLAN-Zuordnung von Systemen anhand der Benutzeridentität möglich. Als Authentifizierungs-merkmal kommen Zertifikate einer eigenen PKI Infrastruktur zum Einsatz.

2 DAS FRAMEWORK 802.1X

Der von der IEEE (http://www.ieee.org) definierte Standard 802.1X bietet die Möglichkeit für kabelgebundene sowie drahtlose Netzwerke eine Zugangskontrolle zu etablieren. Hierbei können unterschiedliche Authentifizierungsmerkmale wie Benutzername und Kennwort oder Zertifikate genutzt werden, um den geforderten Identitätsnachweis zu erbringen. Anhand dieser Identität wird entschieden ob einem Computer oder Benutzer Zugang zum Netzwerk gewährt wird. Zusätzlich können eine Reihe netzwerkseitiger Konfigurationen, wie beispielsweise die Zuweisung eines Netzwerksegmentes vorgegeben werden.

Innerhalb des 802.1X Konzepts agieren folgende Komponenten miteinander:

- Supplicant
- Authenticator
- Authentication Server

Der *Supplicant* stellt die Software-Komponente auf der Seite der zu authentifizierenden Arbeitsstation dar. Sie ist zuständig für die Übermittlung der Authentifizierungsinformationen an den *Authenticator*.

Der *Authenticator* ist ein Netzwerkgerät, beispielsweise ein Switch. Seine Aufgabe besteht in der Umsetzung der Authentifizierung. Hierzu kommuniziert er mit dem *Supplicant* mittels des EAPoL Protokolls. Mit dem Authentication Server kommuniziert er über das RADIUS Protokoll. Da der Authentifzierungsvorgang zwischen *Supplicant* und *Authentication Server* stattfindet, benötigt der *Authenticator* nur ein geringfügiges Verständnis des Vorganges. Er vermittelt den Vorgang und setzt die Entscheidung des *Authentication Servers* um.

Der *Authentication Server* stellt den Kommunikationsendpunkt vom *Supplicant* aus gesehen, während der Authentifizierung dar. Er benötigt volles Verständnis über den Ablauf der Authentifizierung. Im Ablauf der Authentifizierung identifiziert sich der *Authentication Server* auch gegenüber dem *Supplicant*, um die gegenseitige Authentifizierung sicher zu stellen. Durch die Einbindung externer Datenbanken können Identitäten, beispielsweise gegen Verzeichnisdienste wie das Windows *Active-Directory,* geprüft werden.

2.1 Zugrunde liegende Standards und Technologien

2.1.1 802.1X

Der 802.1X Standard definiert ein Framework zur Authentifizierung von Netzwerkgeräten und –Benutzern. Mittels der beschriebenen Schnittstellen findet eine Integration des *Extensible Authentication Protocol* (EAP) statt, dessen Transport in kabelgebundenen und kabellosen Ethernet-Netzwerken mittels *EAP over LAN* (EAPOL) stattfindet. Diese Konstellation bildet die Grundlage für Authentifizierungsmechanismen wie EAP-TLS, EAP-TTLS oder PEAP.

Die 802.1X Spezifikation kann unter folgender URL abgerufen werden:
http://standards.ieee.org/getieee802/download/802.1X-2010.pdf

Die Spezifikation des EAP Standard steht unter folgender Adresse zur Verfügung:
http://tools.ietf.org/html/rfc3748

2.1.2 X.509v3-Zertifikate

Ein Zertifikat ist eine digital signierte Verknüpfung von Identitäts-Informationen mit einem öffentlichen Schlüssel.

Zertifikate enthalten in der Regel folgende Informationen:

- Subject (Antragsteller): Informationen zur Identität (Benutzer, Computer oder Netzwerkgerät) des Zertifikatsinhabers
- Issuer (Aussteller): Informationen zur Identität der Signatur erzeugenden Zertifizierungsstelle
- Öffentlicher Schlüssel der dem Subject zugeordnet ist
- Name des Signaturalgorithmus, der zur Berechnung der Signatur eingesetzt wurde
- Gültigkeitszeitraum des Zertifikats in Form eines „Gültig ab“ und „Gültig bis“ Zeitstempels
- Angaben zum Sperrlistenverteilungspunkt (CDP)
- Seriennummer des Zertifikats
- Liste der verwendeten X.509 V3-Erweiterungen im Zertifikat
- ggf. weitere Attribute (etwa eine vom Unternehmen beantragte Objekt-ID für einen bestimmten Verwendungszweck (OID))

Die aktuelle Version des X509v3 Standards kann unter folgender Adresse bezogen werden:
http://tools.ietf.org/html/rfc5280

2.1.3 EAP

Der IETF Standard *Extensible Authentication Protocol* (EAP) dient als Authentifizierungs-Framework im Bereich Netzwerkzugangskontrolle. Er definiert einen Transportmechanismus für Authentifizierungsdaten, während die eigentliche Authentifizierungsmethode individuell gewählt werden kann. Es stehen eine Reihe von Methoden, beispielsweise MD5, SIM, Benutzername und Kennwort oder Zertifikate zur Verfügung, um den Authentifizierungsvorgang durchzuführen. Kommen Methoden zum Einsatz, die Verschlüsselungsmaterial erzeugen, kann dieses über EAP ausgehandelt und übertragen werden.

Die aktuelle Version des EAP Standards kann unter folgender Adresse bezogen werden:
http://tools.ietf.org/html/rfc5247

2.1.4 EAP-TLS

Das *Transport Layer Security* (TLS) Protokoll ist eine Weiterentwicklung des von Netscape entworfenen *Secure Socket Layer* (SSL) Protokolls. Es dient der verschlüsselten Übertragung vertraulicher Inhalte über Netzwerke. Es unterstützt die gegenseitige Authentifizierung der Kommunikationsteilnehmer mittels digitaler Zertifikate nach dem X509v3 Standard.

Der IETF Standard EAP-TLS adaptiert das TLS Protokoll für die Nutzung innerhalb des EAP Authentifizierungsframeworks. Hierbei werden die Authentifizierungs- und Schlüsselgenerierungsmechanismen des TLS Standards genutzt, um den Authentifizierungsvorgang sowie den Schlüsselerzeugungsvorgang abzubilden. EAP-TLS eignet sich als Authentifizierungsmethode für gemischte Netzwerke, die sowohl kabelgebunden wie auch funkbasiert arbeiten, da neben der Authentifizierung eine manipulationssichere Schlüsselgenerierung erfolgt. Das hiermit erzeugte Schlüsselmaterial kann beispielsweise als dynamischer Schlüssel für WLAN-Verbindungen eingesetzt werden.

Die (im November 2010) aktuelle Version des TLS Standards kann unter folgender Adresse bezogen werden:

http://tools.ietf.org/html/rfc5246

Die (im November 2010) aktuelle Version des EAP-TLS Standards kann unter folgender Adresse bezogen werden:

http://tools.ietf.org/html/rfc5216

2.1.4.1 EAP-TLS Architektur und Nachrichtenformat

EAP nutzt ein *Request Response* Mechanismus. Innerhalb der Datenpakete zeigt das *Type* Feld an, um welche EAP Methode es sich bei den transportierten Nutzdaten handelt. Der Wert 13 im *Type* Feld zeigt an, dass TLS Daten für EAP-TLS Authentifizierung übertragen werden. Der Transport der TLS Daten wird in Server-to-Client Richtung über *EAP-Request* Nachrichten übertragen, in Client-to-Server Nachrichten werden diese in *EAP-Response* Pakete eingebettet.

Die TLS-Architektur, welche auf dem Client/Server Prinzip basiert widerspricht dem Konzept von EAP, das ein 3-Tier Modell (*Supplicant*, *Network Access Server*/*Authenticator und Authentication Server*). Daher wird die Rolle des NAS stark reduziert. Er verifiziert lediglich die Vollständigkeit von TLS Nachrichten, die Kommunikation findet zwischen *Supplicant* und *Authentication Server* statt.

Abbildung 1: EAP Entitäten

2.1.4.2 Protokoll Übersicht

Da die EAP-TLS Spezifikation zunächst für die Nutzung über PPP Verbindungen vorbereitet war, basiert die ursprüngliche Protokoll-Übersicht auf einem 2 Tier Modell.

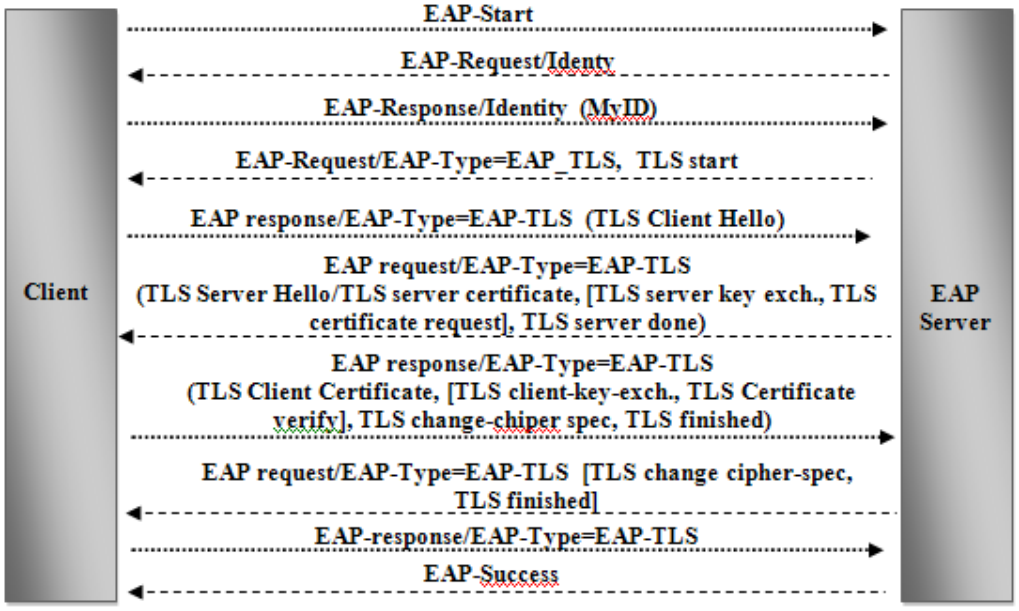


Abbildung 2: EAP-TLS Flow

- Bei Nutzung von EAP über eine PPP Verbindung, startet der Prozess wenn der Client eine PPP LCP Bestätigung sendet, dies zeigt die Übereinstimmung des Clients, EAP als Authentifizierungsprozess zu nutzen.
- Zunächst sendet der Server ein *EAP-Request/Identity* Paket, welches den Client auffordert seine Identität zu übertragen. Diese wird dann mittels dem *EAP-Response/Identity* übertragen.
- Danach folgt der Aufbau der TLS-Verbindung, wobei die *TLS Start* Nachricht in ein *EAP-Request* Packet eingebettet wird. Wird die Methode durch den Client unterstützt, antwortet dieser mit dem *TLS Client Hello* Kommando.
- Die gegenseitige Authentifizierung wird durch den Austausch der digitalen Zertifikate zwischen Client und Server erreicht. Des Weiteren werden in TLS Nachrichten die nötigen Informationen zur Schlüsselerzeugung und Algorithmenwahl übertragen.
- Einen erfolgreichem Ablauf des TLS Handshakes signalisiert der Client durch die Übermittlung eines leeren TLS Pakets innerhalb einer *EAP/Response*. Wird dies durch den Server mit einem *EAP-Success* Paket bestätigt, ist die EAP-TLS Authentifizierung erfolgreich abgelaufen.

3 ANFORDERUNGEN UND BESCHREIBUNG DER UMGEBUNG

Der folgende Abschnitt beschreibt eine technische Umgebung, die sich aus der Historie eines Unternehmens heraus entwickelt hat. Die ab Kapitel 4 dargestellten technischen Maßnahmen beschreiben die vorgenommene 802.1X Implementierung in ihren jeweiligen Schritten.

3.1 Nicht-technische Anforderungen an die Lösung

Im Voraus wurde durch den Kunden eine Reihe von Anforderungen definiert, die durch die neue 802.1X Lösung erfüllt werden sollten:

- Ablösung des Cisco User Registration Tools (URT). URT wird vom Kunden seit einigen Jahren eingesetzt, und implementiert mittels eines Agents auf den Geräten dynamische Zuordnung von Benutzern/Computern zu unterschiedlichen Segmenten. Da dieses Produkt vom Hersteller nicht mehr gepflegt wird, (das *End of Life* Datum ist überschritten) ist ein zeitnaher Ersatz der Technologie notwendig.
- Sichere Authentifzierung von Geräten mittels Zertifikaten, sowohl für Benutzer als auch für Computer.
- Management von Zertifikaten ist ein (soweit möglich) automatischer Prozess, in welchen nur in Problemfällen manuell eingegriffen werden muss. Dies gilt sowohl für die Initiale Ausstellung eines Zertifikates, wie auch für seine Erneuerung und das Widerrufen. Bei diesen Prozessen soll insbesondere keine Interaktion mit dem Endanwender notwendig sein.
- Zur Speicherung von Zertifikaten werden keine Smart-Cards eingesetzt. Die hiermit verbundenen Implikationen auf die Produktivität von Mitarbeitern bei Vergessen oder Verlust/technischem Defekt der Karte werden somit vermieden.

3.2 Struktur der Umgebung

Die folgende Grafik zeigt (die vereinfachte) Netzstruktur, sowie die Positionierung der einzelnen Systeme im Netzwerk.

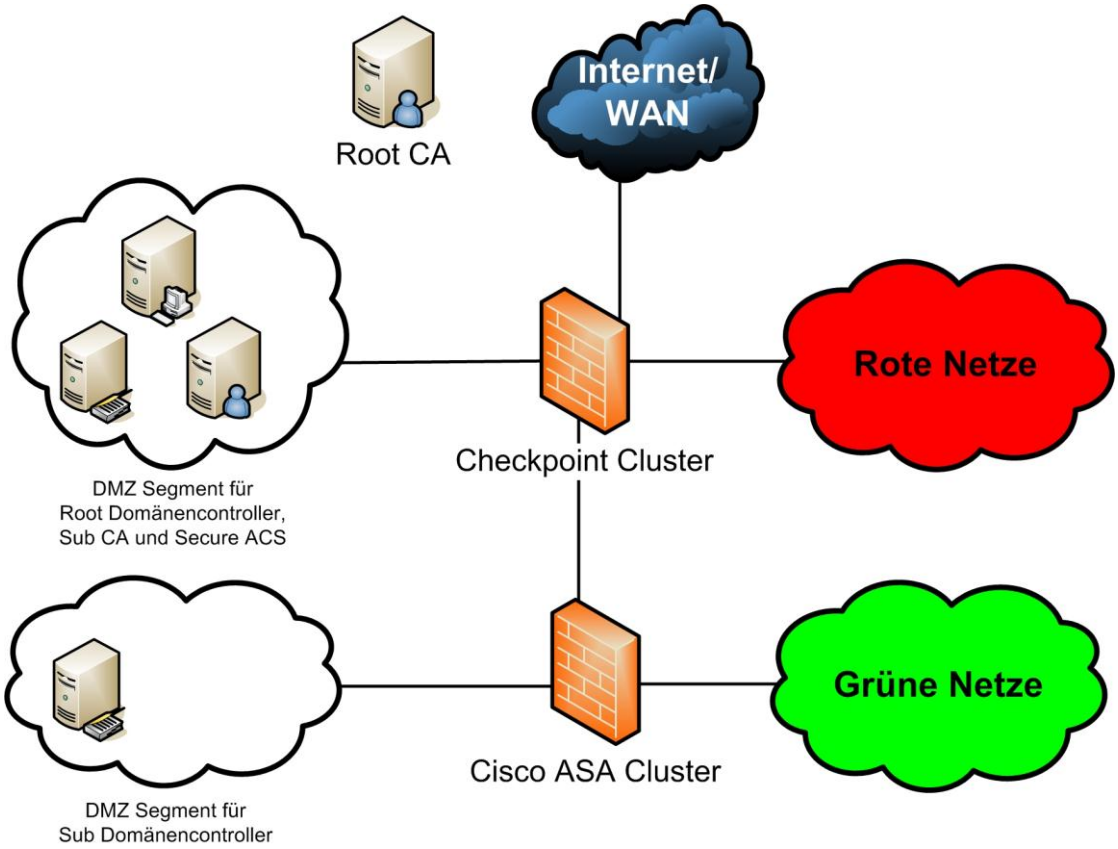


Abbildung 3: Struktur der Umgebung

Unternehmens-PCs sind (mit wenigen Ausnahmen) grünen Netzen zugeordnet, während in roten Netzen Geräte mit hohem Schutzbedarf, Bedrohungspotential zugeordnet werden. Hierzu zählen beispielsweise Produktionssysteme, Drucker, nicht 802.1X fähige Infrastrukturgeräte, Gäste und Weitere. Die Strukturierung ist Resultat der Historie der gesamten Umgebung.

Die *Root CA* besitzt aus Sicherheitsgründen kein Zugang zum Netzwerk, da ihr ein hoher Schutzbedarf (aufgrund der Funktion) zukommt.

3.3 Active-Directory

Das Setup der *Active-Directory* Umgebung entspricht einer hierarchischen Struktur, bestehend aus einer *Root-Domäne*, sowie einer *Sub-Domäne*. Benutzer und Computer die mit 802.1X authentifiziert werden sollen, sind jeweils der *Sub-Domäne* zugeordnet. Alle Domänen-Controller werden auf Basis von Windows Server 2008 R2 betrieben. Während der Umstellung der *Domain Controllers* (DCs) von Server 2003 auf Server 2008 R2 wurden die entsprechenden Schema-Erweiterungen im *Active-Directory* (automatisch vom Setup-Programm) durchgeführt.

Die Domänen-Controller der *Root-Domäne* sind in einem separaten DMZ-Segment platziert. Die Domänen-Controller der *Sub-Domäne* sind in internen Server Segmenten platziert.

3.4 Netzwerk Infrastruktur

Die Netzwerk-Infrastruktur wird praktisch ausschließlich durch Cisco Geräte bereitgestellt. Hierbei kommen im Bereich der *Access Ports*[1] Switches der 3560er Familie zum Einsatz. Diese sind im Backbone-Bereich[2] durch *Catalyst Switches* der 6500er Serie angebunden. Für interne Filterung von Datenverkehr kommen *Cisco ASA*s zum Einsatz, die Anbindung von DMZ Segmenten erfolgt über einen Checkpoint Cluster.

Auf den Access-Switches ist das IOS Release 12.2(50) oder neuer installiert. Dies ist Voraussetzung für eine Reihe von erweiterten Funktionen im Bereich 802.1X. Hierzu zählt die Anpassung der Authentifizierungsreihenfolge. Diese steuert, ob alternative Authentifizierungsverfahren wie *MAC Authentication Bypass* (MAB) eingesetzt werden, und in welcher Reihenfolge die Authentifizierungen erfolgen.

3.5 Authentifizierungsserver – Cisco Secure ACS

Als Authentifizierungsserver setzt das Unternehmen bereits mehrere *Cisco Secure Access Controller Server* (ACS) in Version 4.2.1.15 ein. Bei vorherigen Versionen gibt Cisco eine unvollständige Unterstützung von Windows Server 2008 R2 an. Zur Aufrechterhaltung der Verfügbarkeit in Problemfällen sind die Authentifizierungsserver redundant ausgelegt. Hierbei kommen sowohl *ACS Solution Engine*s in Appliance Form, wie auch eine Software Installation des *Secure ACS* auf Basis von Windows Server 2003[3] zum Einsatz. Es wurde die ACS interne Replikation eingerichtet, um eine Gleichheit der Konfigurationsparameter und lokalen Datenbankinhalten zu gewährleisten.

3.6 Windows Clients

Auf den Arbeitsstationen und Notebooks ist Windows XP mit Service Pack 3 oder höher installiert. Systeme mit älterem Softwarestand können nicht für die 802.1X Authentifizierung genutzt werden und werden nicht berücksichtigt. Dies ergibt sich aus dem Umstand, dass keine Smart-Cards für die Speicherung von Zertifikaten eingesetzt werden. Die Verfügbarkeit der digitalen Zertifikate wird durch Active-Directory Funktion *Credential Roaming* erreicht. Diese Funktion ist jedoch erst mit Windows XP SP3 nutzbar.

3.7 Zertifikatsinfrastruktur

Die für die Authentifizierung von Computern und Benutzern eingesetzten Zertifikate werden von einer unternehmensinternen PKI Infrastruktur erzeugt. Diese wurde zweistufig ausgelegt, da eine Erweiterung der funktionellen Anforderungen über den Bereich Netzwerk-Authentifizierung hinaus nicht ausgeschlossen werden konnte (und sollte).

Initial wurde eine *Stand-Alone Root CA* eingerichtet. Diese ist für die Signatur des Zertifikats der *Subordinate CA* zuständig. Die *Root CA* wird innerhalb der Umgebung ohne Anbindung an das Netzwerk betrieben, Zertifikatsanträge müssen mittels mobiler Datenträger übertragen werden.

Die *Subordinate CA* ist für die Signierung der Computer und Benutzerzertifikate zuständig. Es handelt sich hierbei um eine *Windows Enterprise CA*, basierend auf einem *Windows Server 2008 R2* System, welches in die *Root-Domäne* eingebunden ist. Der gewählte Betriebsmodus der CA ermöglicht die Nutzung von Zertifikatsvorlagen und der *Autoenrollment* Funktion. Dieses gewährleistet die automatische Verteilung und Erneuerung von Computer- und Benutzerzertifikaten.

---

[1] *Ausgehend von einem hierarchischen Netzwerk-Design sind im Access-Bereich Endsysteme wie Arbeitsstationen angeschlossen.*

[2] *Ausgehend von einem hierarchischen Netzwerk-Design stellt der Backbone-Bereich die Spitze der Architektur dar, dessen Aufgabe die schnelle Vermittlung von Daten zwischen den einzelnen Teilbereichen ist.*

[3] *Eine Installation dieser Software auf Windows Server 2008 R2 ist nicht möglich.*

4 VORBEREITENDE MAßNAHMEN IM NETZWERKBEREICH

Der folgende Abschnitt beschreibt die zur Authentifzierung von Geräten mittels 802.1X eingesetzten Methoden, sowie die dazugehörige VLAN Struktur.

4.1 Netzstruktur

Das Netzwerk ist in eine Reihe unterschiedlicher VLANs segmentiert. Eine dynamische Zuordnung der Geräte/Benutzer zu den Segmenten findet bereits durch die vorhandene URT-Lösung statt und soll beibehalten werden. Es wird grundsätzlich zwischen grünen und roten Netzen unterschieden. Innerhalb grüner Netze darf lediglich unternehmensinterne Kommunikation stattfinden. Geräte die an einem solchen Netz angehören gelten als vertrauenswürdig. Einzelne grüne Netzsegmente werden anhand der Funktionalität oder Abteilungszugehörigkeit von Benutzern/Geräten unterschieden. Es findet eine entsprechende dynamische Zuordnung der Benutzer zu einem grünen Benutzersegment statt. Ist keine Zuordnungs-Information für einen Benutzer/Gerät hinterlegt, so wird dieser dem *Global Default* zugewiesen. Maschinen mit Zuordnung sind standardgemäß dem *Global Maschine* Segment zugeordnet.

Rote Netze stellen Segmente mit Benutzern/Geräten dar, die weniger vertrauenswürdig sind. Diese werden durch restriktive Filterung in ihren Kommunikationsmöglichkeiten eingeschränkt. Rote Netze sind beispielsweise das Gäste-Netz, das *InAccessible Authentication VLAN*, welchem Geräte beim Ausfall des Radius-Server zugeordnet werden, und Segmente für spezielle Geräte wie Drucker, Produktionsmaschinen und DECT-to-VoIP Bridges. Geräte, welche dediziert als weniger vertrauenswürdig eingestuft wurden, werden dem entsprechenden roten Netz zugeordnet. Das Gleiche gilt für Geräte die schwächere Formen der Authentifizierung unterstützen, sowie für alle unbekannten Geräte (Gäste).

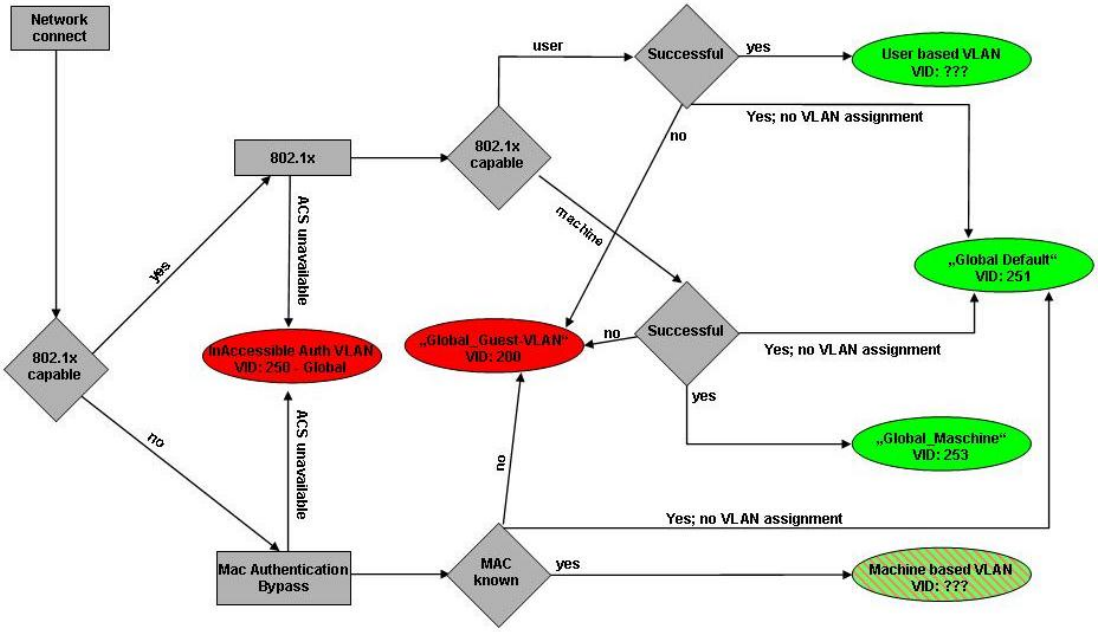


Abbildung 4: Schema der VLAN Zuordnung von Geräten/Benutzern

4.2 Authentifzierungsmethoden

Zur Authentifizierung von Geräten und Benutzern soll, soweit technisch möglich, EAP-TLS eingesetzt werden, da der Identitätsnachweis mittels eines Zertifikats durchgeführt wird. Dies Authentifizierungsmethode ist daher weder anfällig für Man-In-The-Middle Attacken noch für eine Fälschung von Zertifikaten[4].

Geräte, welche nicht mittels Zertifikaten authentifiziert werden können, sind beispielsweise Drucker, DECT-to-VoIP Bridges, Spezialhardware, sowie veraltete Windows Versionen. Diese werden mittels *MAC Authentication Bypass* (MAB) authentifiziert. Es handelt sich hierbei um eine im Cisco Switch integrierte Funktion. Diese ermittelt aus dem ersten Datenpaket, das von einem Endgerät gesendet wird, die Absender MAC-Adresse und versucht den Port anhand dieser Information zu authentifizieren.

4.3 Vorbereitung Netzwerk-Infrastruktur

Die Netzwerk-Infrastruktur muss entsprechend der Authentifizierungsmethode vorbereitet werden. Dies beinhaltet das Anlegen der im vorigen Abschnitt beschriebenen VLANs, die Einrichtung potentiell notwendiger Firewall-Regeln und Routingeinträgen. Wird Netzwerkverkehr, welcher an die Subordinate CA gerichtet ist, durch eine Firewall gefiltert, müssen zusätzlich folgende Ports freigeschaltet werden, um Autoenrollment zu erlauben:

Zielsystem	Protokoll	Port
Subordinate CA	TCP	135
Subordinate CA	TCP	49152 – 65535
Root Domain Controller	TCP/UDP	88
Root Domain Controller	UDP	389

Tabelle 1: Port Übersicht für Firewallregeln

5 VORBEREITUNG DER ACTIVE-DIRECTORY UMGEBUNG

Das folgende Kapitel beschreibt die Konfigurationseinstellungen, welche vorbereitend in der *Active-Directory* Umgebung vorgenommen werden müssen.

5.1 Konfiguration des Credential Roaming

Die Nutzung digitaler Zertifikate zur Authentifizierung erfordert die Nutzung der ab *Windows Server 2008* eingeführten Funktion *Credential Roaming*. Da Benutzer-Zertifikate grundsätzlich im Zertifikatsspeicher des Benutzers abgelegt werden, resultiert dies in einer Neuausrollung des Benutzer-Zertifikates, falls sich der Benutzer an unterschiedlichen Computern anmeldet. Dies führt zu einem Benutzer-Zertifikat pro Computer, an welchem sich der Benutzer angemeldet hat. Mit Hilfe der Funktion *Credential Roaming* werden das Zertifikat sowie der dazugehörige private Schlüssel im *Active-Directory* hinterlegt. Ein Computer kann während des Windows Anmeldevorganges auf diese Informationen zugreifen, sie lokal cachen, und anschließend zur Authentifizierung am Netzwerk nutzen.

[4] *Unter der Voraussetzung der private Schlüssel der signierenden Zertifizierungsstelle wurde nicht kompromittiert.*

Zum Schutz der Informationen sind diese in einem speziellen *Confidential Attribute* hinterlegt. Die Konfiguration von *Credential Roaming* wird durch ein Gruppenrichtlinien-Objekt vorgenommen[5]. Das Gruppenrichtlinien-Objekt ist, wie im folgenden Screenshot gezeigt, unter *Administrative Templates* der Benutzer Konfiguration zu finden. Die Einstellungen werden unter *Certificate Services Client – Credential Roaming* vorgenommen:

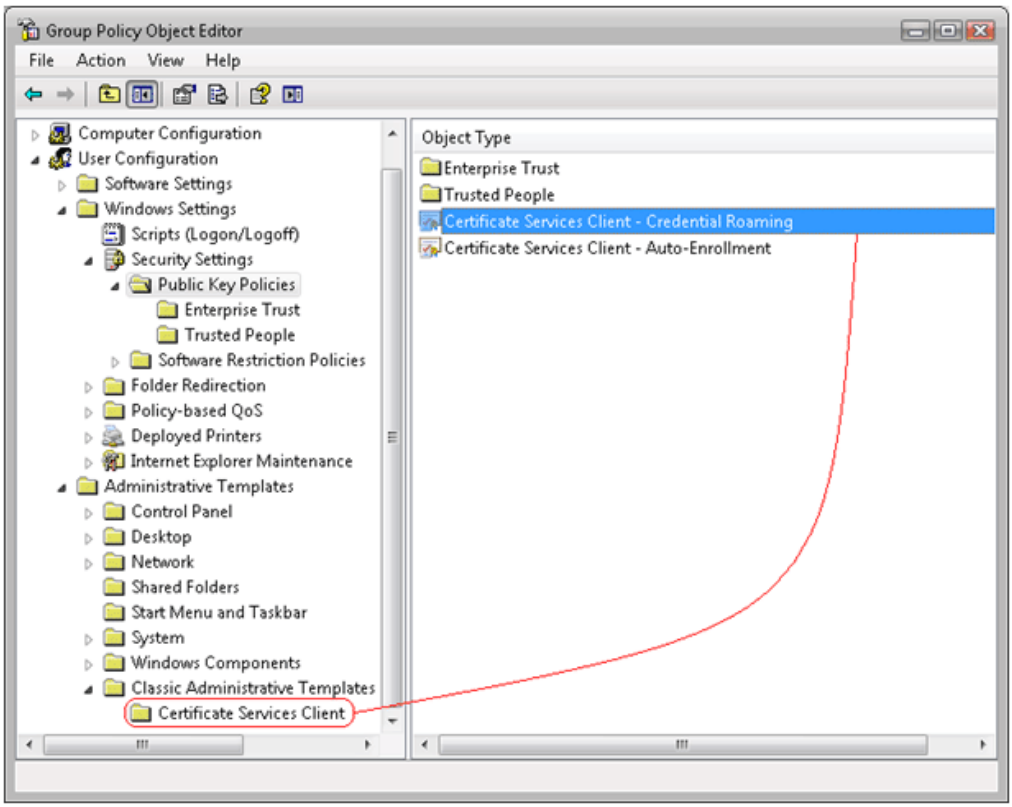


Abbildung 5: Credential Roaming GPO Einstellungen

5 Für Active Directory Umgebungen, die keinen Server 2008 basierenden Domänen-Controller enthalten, müssen separate Konfigurationsschritte vorgenommen werden, um diese Funktionalität nachzurüsten. Eine ausführliche Anleitung ist unter folgender Adresse verfügbar: http://technet.microsoft.com/en-us/library/cc700821.aspx

Die Einstellungen müssen wie abgebildet vorgenommen werden. Neben der Aktivierung ist die Einstellung der *Tombstone Lifetime* und der maximalen Anzahl *Roaming Credentials per user* zu beachten. Die *Tombstone Lifetime* sollte dem in Ihrer Umgebung verwendeten Wert entsprechen.[6] Eine hohe Anzahl von *Credentials* pro Benutzer können bei einer großen Anzahl Benutzer/Computer im *Active-Directory* zur Verlängerung der Replikationsdauer führen.

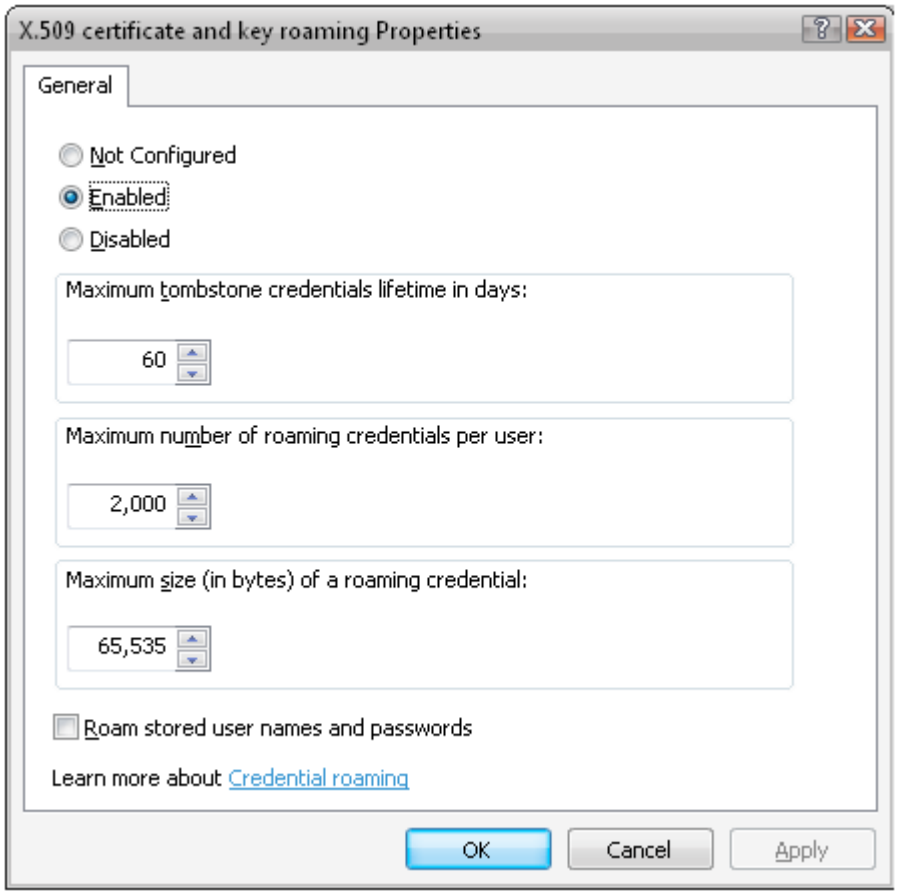


Abbildung 6: X509 GPO Einstellungen

Beim Verknüpfen des Gruppenrichtlinien-Objekts muss auf die korrekte Anwendung innerhalb der AD-Struktur geachtet werden. Es wird empfohlen dies nicht domänenweit, sondern auf die jeweiligen *Organizational Units* zu binden, innerhalb derer die zu authentifizierenden Benutzer angelegt sind.

5.2 Anonyme LDAP Anfragen an der Globalen Katalog konfigurieren

Per Standard ist der Zugriff auf im *Active-Directory* gelegene Informationen nur für Domänen Mitglieder möglich. Alternativ hierzu können von Nicht-Domänen-Mitgliedern LDAP-Anfragen mit Authentifizierung gegen den *Global Catalog/Domain Controller* gestellt werden, um Informationen abzufragen. Bis inklusive Version 4.2.1 beherrscht der *Secure ACS* keine der beiden Möglichkeiten zum Abruf von Informationen, jedoch können anonyme (nicht

[6] *Diese Betrug bis vor Windows Server 2003 SP1 60 Tage, ab Windows Server 2003 SP1 und bis zu Windows Server 2008 R2 180 Tage. Da die betrachtete Umgebung aus einem Upgrade von Windows Server 2003 vor SP1 stammt, sind die 60 Tage beibehalten.*

authentifizierte) LDAP-Anfragen genutzt werden. Um mittels dieser Abfragen die Zertifikatssperrliste zu erhalten, ist es nötig, anonyme LDAP-Abfragen gegen den *Global Catalog* zu erlauben[7], und die Zugriffsrechte für Zertifikatssperrlisten anzupassen. Die dazu nötigen Schritte werden im Folgenden beschrieben.

Zunächst muss die Bibliothek, welche das Schema Management ermöglicht registriert werden. Dies kann mittels der Kommandozeile mit dem Befehl `regsrv schmgmt.dll` vorgenommen werden.

Abbildung 7: Registrierung des Schema Management SnapIn

Im *MMC SnapIn Active-Directory Schema* werden die Änderungen am Attribut *certificateRevocationList* vorgenommen[8]. Dies ist in der Kategorie *Attributes* zu finden:

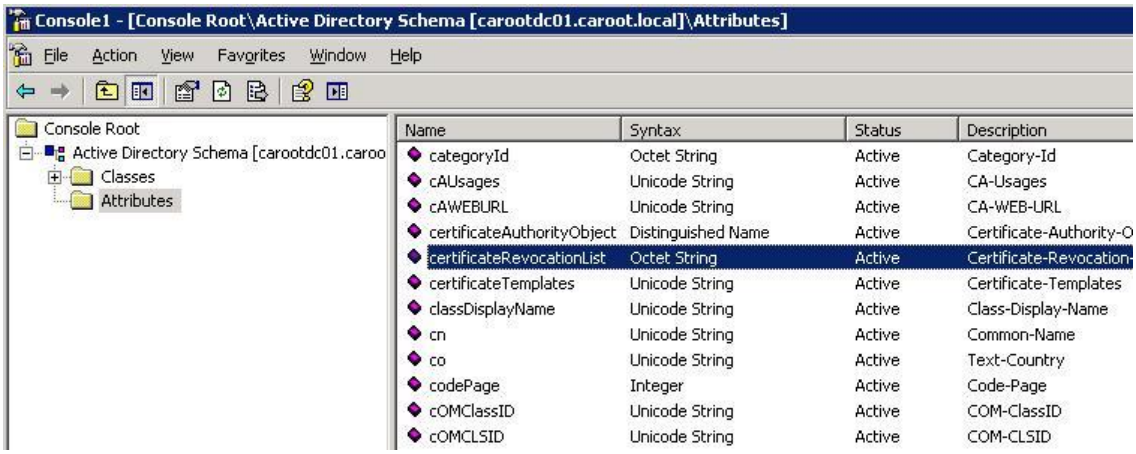


Abbildung 8: certificationRevocationList Attribut

Die Eigenschaften dieses Attributes müssen angepasst werden, so dass die folgenden Optionen aktiviert sind:

- *Index this attribute in the Active Directory*
- *Replicate this attribute to the Global Catalog*
- *Index this attribute for containerized searches in the Active Directory*

---

[7] *Die Deaktivierung von anonymen LDAP-Anfragen stellt eine große Errungenschaft seit Windows Server 2003 SP2 dar. Die geforderte Reaktivierung bringt entsprechende Problematiken mit sich. Ist dies unerwünscht können Sperrlisten von HTTP-Adressen aus abgerufen werden. Hierbei ist jedoch auf die redundante Auslegung dieser Adressen sowie einer einwandfrei funktionierenden Replikation der Sperrlisten zu achten.*

[8] *Bei Änderungen des Active Directory Schema ist eine große Sorgfaltspflicht geboten, da fehlerhafte Änderungen massive Auswirkungen auf die Funktion haben können.*

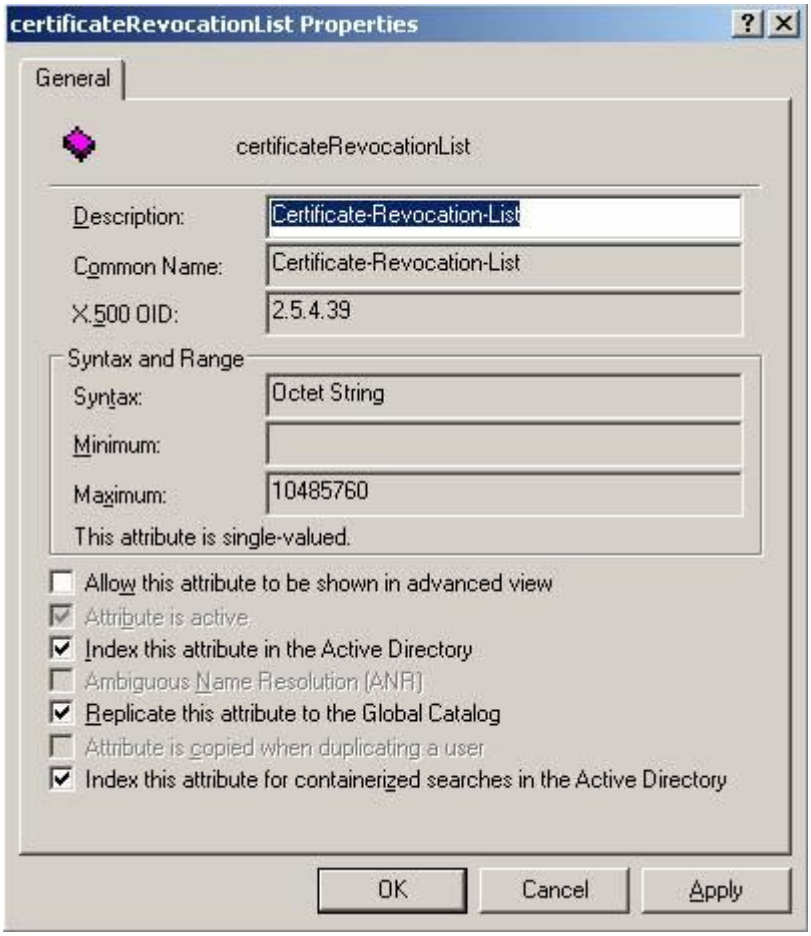


Abbildung 9: Anpassung der Optionen für das CRL Attribut

Aus dem Windows Support Tools Packet wird im nächsten Schritt das *MMC SnapIn ADSI Edit* benötigt. Das Paket kann unter folgender URL heruntergeladen werden:

http://technet.microsoft.com/en-us/library/cc758202.aspx

Zur Durchführung der notwendigen Änderungen am *Global Catalog* muss eine Verbindung zum *Naming Context Configuration* aufgebaut werden.

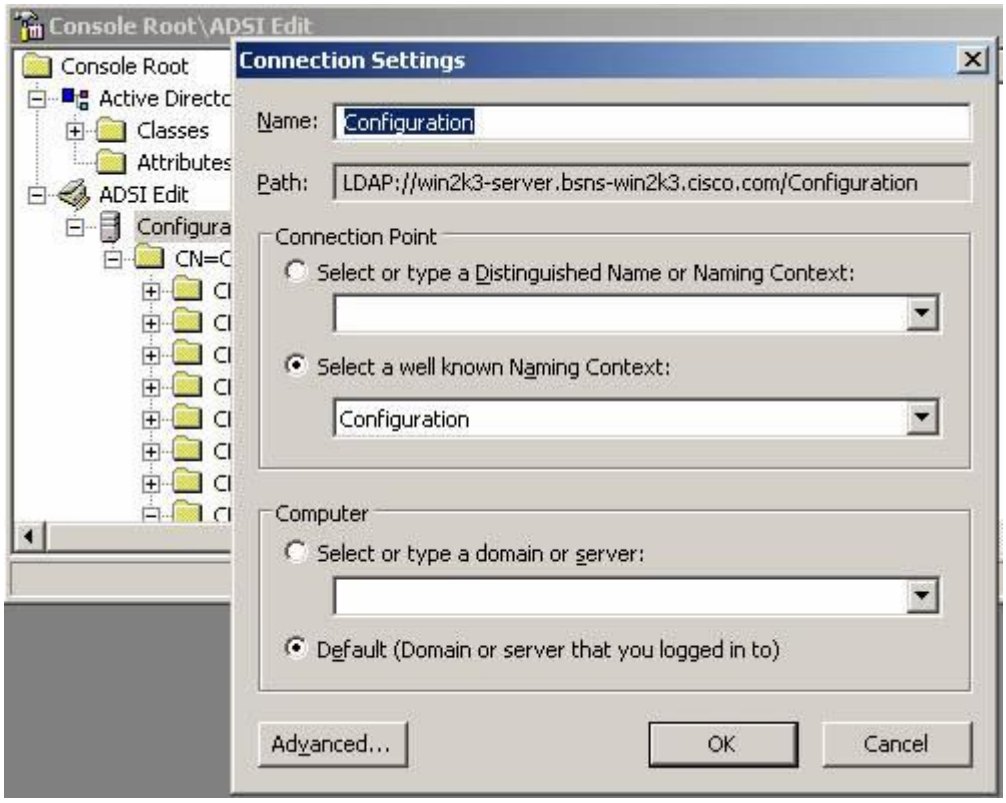


Abbildung 10: Verbindung zum Configuration Context aufbauen

Für alle Verzeichnisse, welche unterhalb von *CN=Services, CN=Public Key Services, CN=CDP* liegen, sowie das darin befindliche Attribut *crlDistributionPoint* müssen die Zugriffsrechte angepasst werden. Hierbei muss der im Reiter *Security* der Benutzer *Anonymous* hinzugefügt und diesem *Read* Rechte zugewiesen werden.

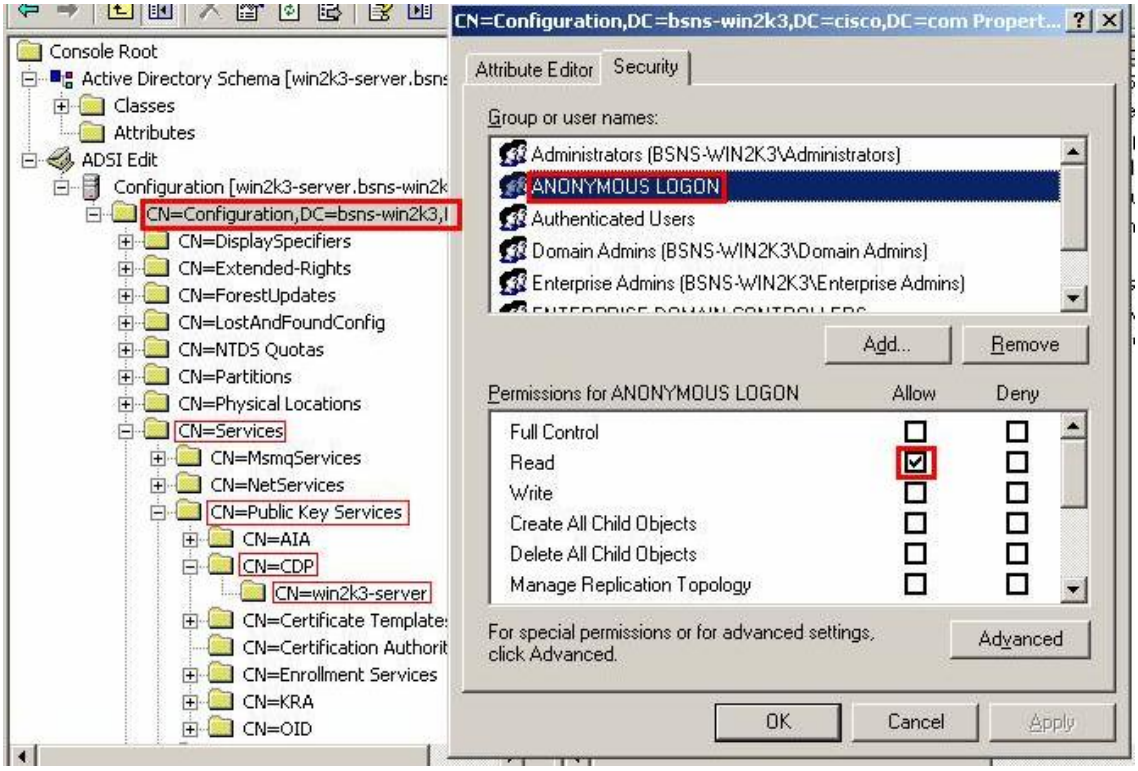


Abbildung 11: Zuweisung von Leserechten für Anonymous

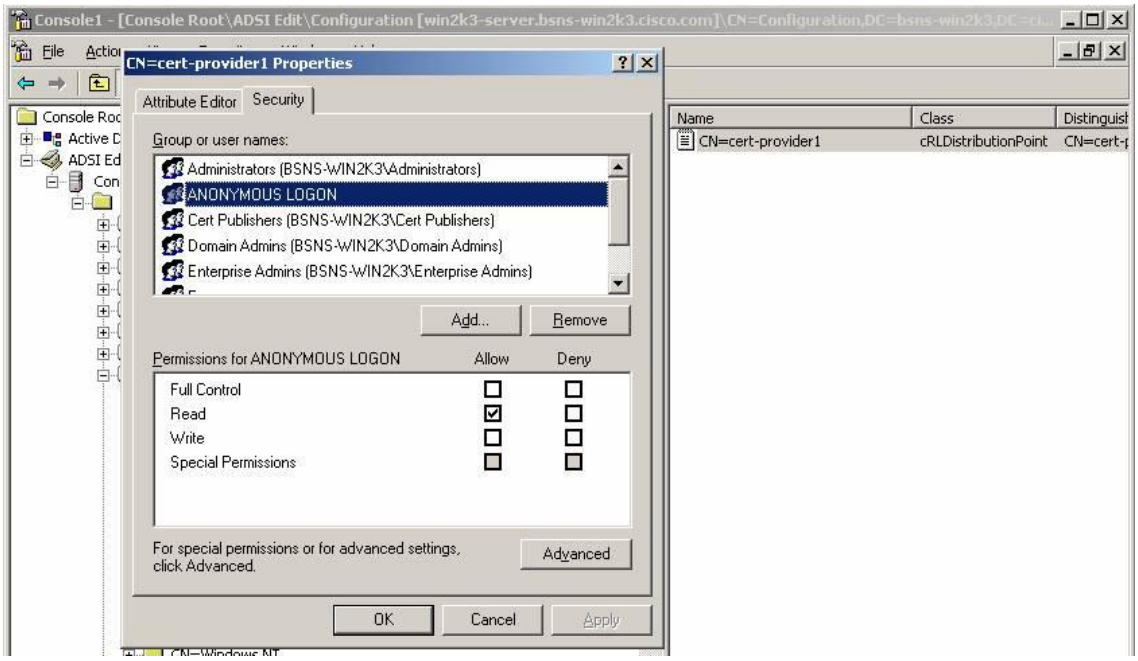
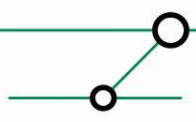


Abbildung 12: Zuweisung der Leserechte auf das crlDistributionPoint Attribut

Ist der *Domain Functional Level* nicht kleiner als *Windows Server 2003 SP1*, müssen anonyme LDAP Anfragen aktiviert werden. In älteren Active Directory Umgebungen ist dies standardgemäß aktiviert. Im *Configuration Context*, muss im Pfad *CN=Configuration,*



CN=Services, CN=WindowsNT dem Attribut *dsHeuristics* der Wert *0000002* zugewiesen werden[9].

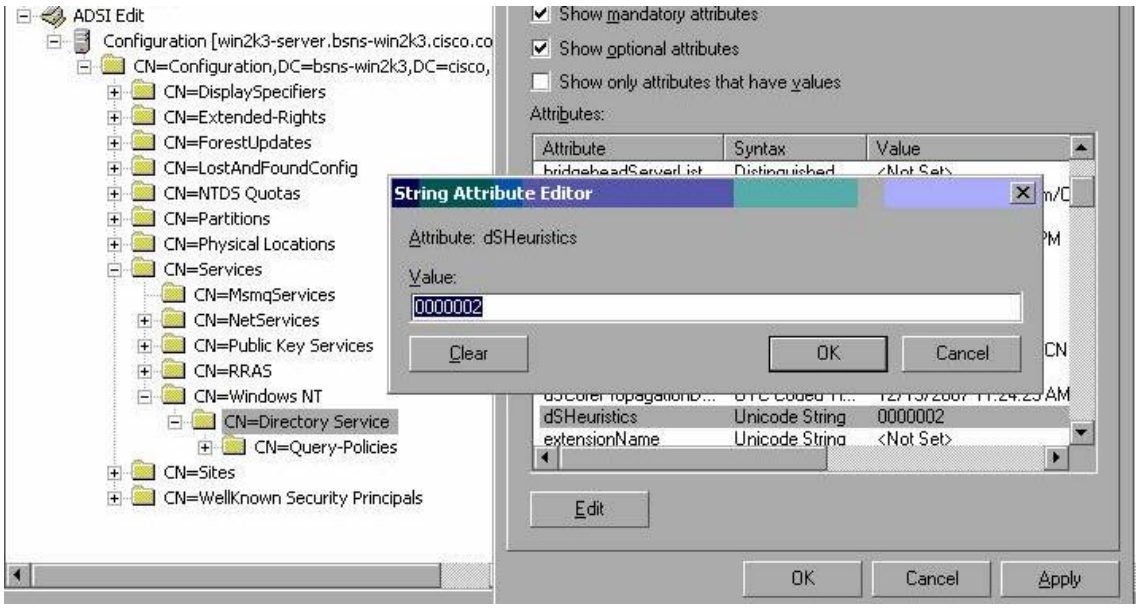


Abbildung 13: Aktivieren der anonymen LDAP Anfragen

[9] *Bei Änderungen des dsHeuristic Wertes ist eine große Sorgfaltspflicht geboten, da fehlerhafte Änderungen massive Auswirkungen auf die Funktion haben können. Die genaue Dokumentation des Parameters kann unter folgender Adresse abgerufen werden: http://msdn.microsoft.com/en-us/library/ms675656(VS.85).aspx*

Im Secure ACS muss die LDAP-Adresse des zum ACS am Nächsten gelegenen *Global Catalog* eingetragen werden. Die LDAP-Adresse lässt sich aus den Zertifikaten im Reiter *Details* unter dem Punkt *CRL Distribution Points* ermitteln.

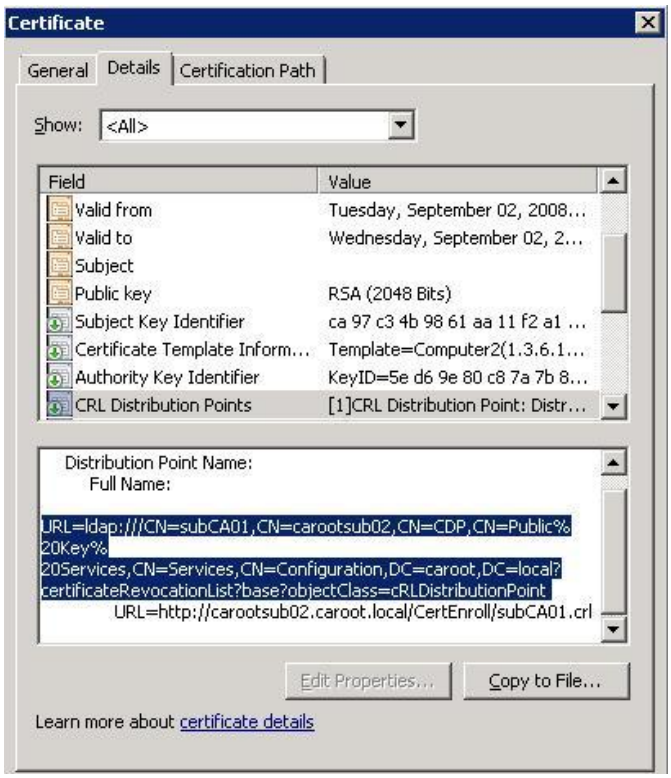
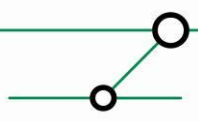


Abbildung 14: CRL Distribution Points der Zertifikate

5.3 Konfiguration des Autoenrollment

Autoenrollment der Benutzer- und Computerzertifikate wird über die Gruppenzugehörigkeit im Active Directory gesteuert. Hierzu muss in der *Root*- wie *Subdomäne* eine Gruppe für das Ausrollen von Benutzerzertifikaten und Computerzertifikaten erstellt werden. Wird ein Benutzer bzw. Computer als Mitglied in einer der Gruppen konfiguriert, so erhält diese Identität automatisch ein Zertifikat.

Die Benennung der Gruppen sollte, wie im folgenden Screenshot gezeigt, sprechend vorgenommen werden.



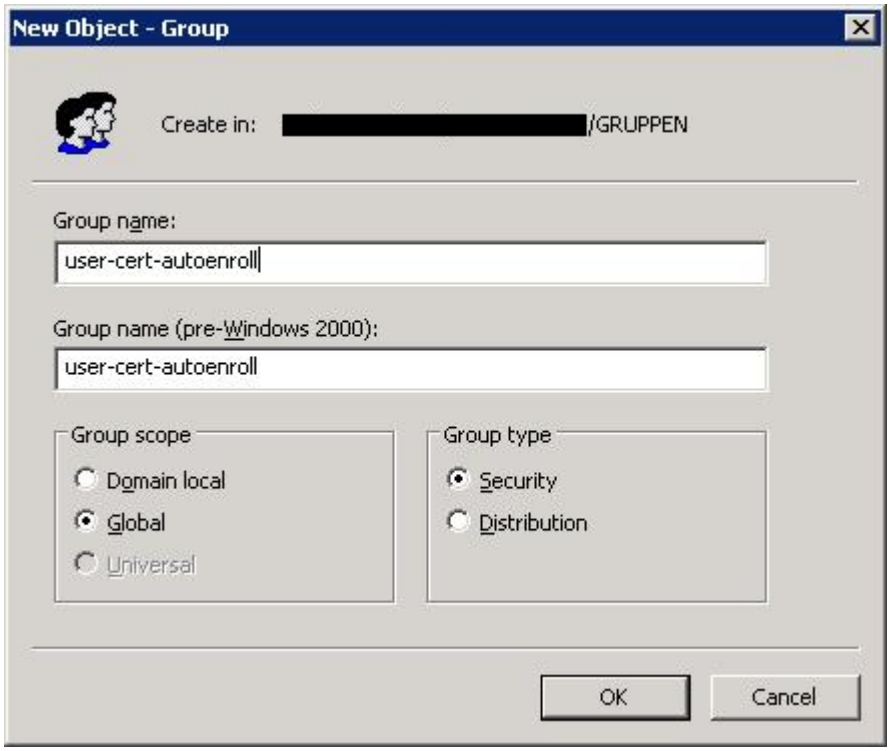


Abbildung 15: Erstellung einer AD-Gruppe für Auto-Enrollment der Benutzer-Zertifikate

Nach Anlegung der min. 4 Gruppen (Benutzer- & Computer-Zertifikate (2 Gruppen) in Sub- und Root-Domäne (2 Domänen)) müssen die Gruppen der Subdomäne in ihren äquivalenten Gruppen innerhalb der Root-Domäne aufgenommen werden. Wie im Abschnitt 6.1 gezeigt, werden auf die Gruppen der Root-Domäne die Zugriffsrechte für Zertifikatsvorlagen gesetzt.

5.4 Installation des Cisco ACS Remote Agent

Die Kommunikation zwischen der *Secure ACS* Appliance und dem *Active Directory* findet mittels eines Agents statt, der auf einem Domänencontroller installiert sein muss. Dieser Agent reicht die Anfragen an den Domänencontroller weiter. Die Ergebnisse der Anfrage werden durch den Agent an die Appliance zurück vermittelt. Dieser *Remote Agent* MUSS auf allen Domänencontrollern installiert sein, welche durch Secure ACS Appliances genutzt werden sollen. Hierbei ist darauf zu achten, dass die installierte Version des Remote Agents mindestens 4.2.1.15 oder aktueller beträgt, da ältere Versionen Windows Server 2008 R2 basierte Domänencontroller nicht unterstützen.

5.5 Prüfung der Active Directory-Benutzer

Für Benutzer die sich via EAP-TLS authentifizieren sollen, müssen in den *Active Directory* Konto Einstellungen für die Felder *User Logon Name* und *User Logon Name (pre-Windows 2000)* jeweils identische Werte gesetzt haben. Andernfalls kommt es zu Problemen während der EAP-TLS Authentifizierung. Diese äußern sich durch Logeinträge im *Secure ACS*, welche aussagen, dass der zu authentifizierende Benutzer im *Active Directory* nicht gefunden wurde.

6 VORBEREITENDE MAßNAHMEN PKI-UMGEBUNG

Im Folgenden werden die Konfigurationsmaßnahmen in der PKI-Umgebung beschrieben, welche notwendig für die automatisierte Ausstellung von Benutzer/Computer Zertifikaten sind. Es wird nicht näher auf die Installation der PKI-Installation eingegangen. Voraussetzung für die Durchführung der in Abschnitt 6 beschriebenen Schritte ist die fehlerfreie Installation der PKI-Umgebung mit einer *Stand-Alone Root-CA* sowie einer *Enterprise Sub-CA*, die im *Active Directory* eingebunden ist. Hierbei ist zu prüfen, dass die Verfügbarkeit der Zertifikatssperrlisten im *Active Directory* gewährleistet ist.

6.1 Zertifikatsvorlagen

Das automatisierte Ausrollen von Zertifikaten basiert auf Vorlagen, die mit der *Enterprise CA* Funktion der Windows *Certificate Services* verfügbar ist. Diese Vorlagen definieren den Aufbau und die Inhalte eines Zertifikates, unter welchen Bedingungen ein Zertifikatsantrag automatisch signiert wird, und für welche *Active Directory* Gruppe die automatische Ausrollung erlaubt ist. Die Konfiguration von Zertifikatsvorlagen wird über das *MMC-SnapIn Certificate Templates* vorgenommen.

6.1.1 Vorlage für Computer Zertifikate

Zunächst muss eine neue Vorlage für Computer Zertifikate erstellt werden. Die Vorlage für Autoenrollment wird von der *Computer* Vorlage durch duplizieren abgeleitet:

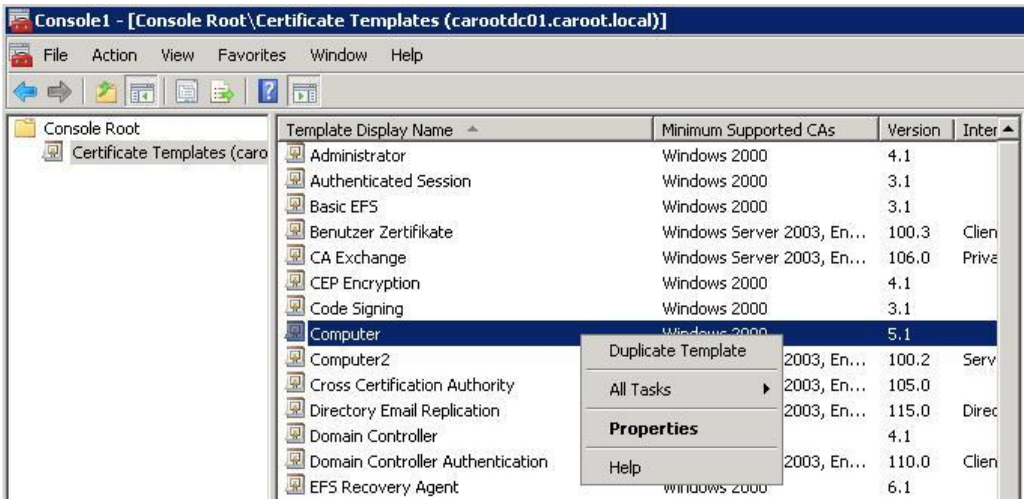


Abbildung 16: Duplizieren der Computer Vorlage

Im *Duplicate Template* Dialog ist als Version der neuen Zertifikatsvorlage *Windows Server 2003, Enterprise Edition* zu wählen. Hierdurch ist eine problemfreie Integration in den *Auto-Enrollment* Mechanismus garantiert.

Abbildung 17: Wahl der Vorlagen Version

In den nachfolgenden Schritten werden die Eigenschaften der Vorlage angepasst. Im Reiter *General* sollte zunächst ein sprechender Name für die Vorlage vergeben werden. Weiterhin ist die *Validity Period* und *Renewal Period* der Zertifikate zu prüfen. Erstere definiert wie lang ein Zertifikat, das anhand dieser Vorlage ausgerollt wurde, gültig ist. Werte kleiner *1 Year* werden nicht empfohlen, da mobile Systeme (beispielsweise Notebooks von Außendienstmitarbeitern) potentiell nicht ausreichend häufig ihr Zertifikat erneuern können. Die *Renewal Period* gibt an, ab welchem Zeitraum vor Ablauf der Zertifikatsgültigkeit versucht wird, mittels *Autoenrollment* ein neues Zertifikat zu beantragen. Auch hier gilt, dass zu kurze Zeiten dazu führen können, dass problematische Geräte kein Computer Zertifikat besitzen.

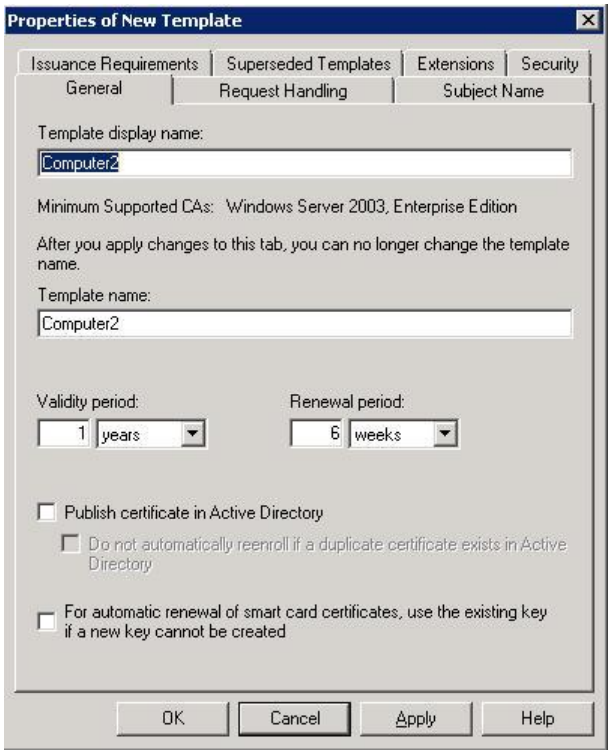
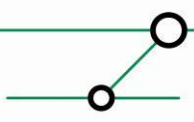


Abbildung 18: Allgemeine Einstellung der Vorlage

Die Einstellungen für Parameter in den Reitern *Request Handling*, *Subject Name*, *Issuance Requirements* und *Extensions* können übernommen werden. Im Reiter *Superseeded Templates* ist es nötig, die Vorlage *Computer* hinzuzufügen.



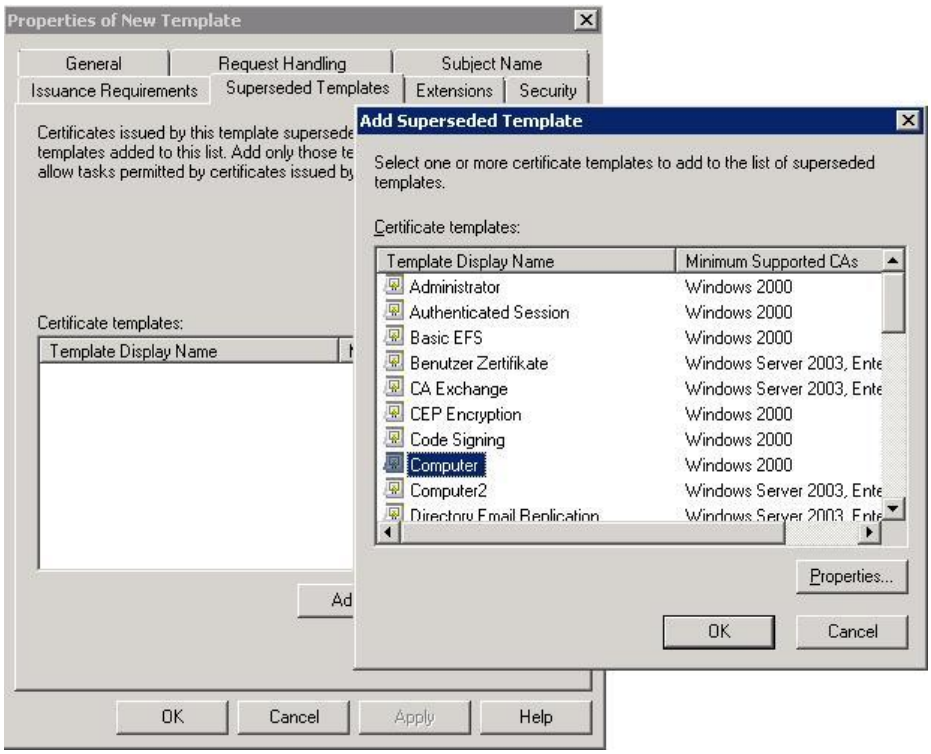


Abbildung 19: Die Computer Vorlage wird durch die neue Vorlage ersetzt

Im Reiter *Security* muss das Objekt *Domain Computers* der *Root-* und *Sub-Domäne* hinzugefügt und mit den folgenden Rechten versehen werden:

- *Read*
- *Enroll*
- *Autoenroll*

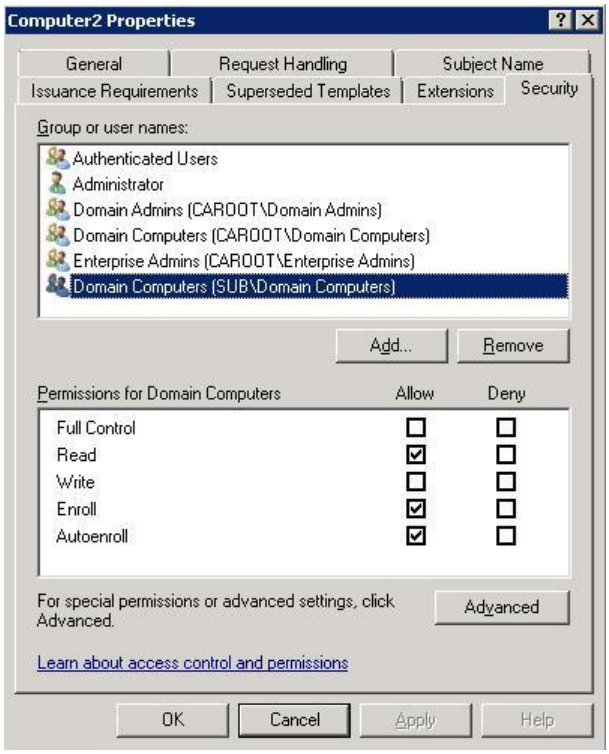


Abbildung 20: Zugriffsrechte der AD-Computer auf Vorlage festlegen

6.1.2 Vorlage für Benutzer Zertifikate

Die Vorlage für Benutzer-Zertifikate wird analog zu der Vorlage für Computer-Zertifikate erstellt. Als zu duplizierende Vorlage kann die Vorlage *Benutzer* dienen. Eine Anpassung der Vorlagen Eigenschaften kann hinsichtlich der gewünschten *Validity Period* und *Renewal Period* nötig sein. Im Reiter *Security* muss der in Abschnitt 5.2 erstellte Gruppe die folgenden Rechte zugewiesen werden:

- *Read*
- *Enroll*
- *AutoEnroll*

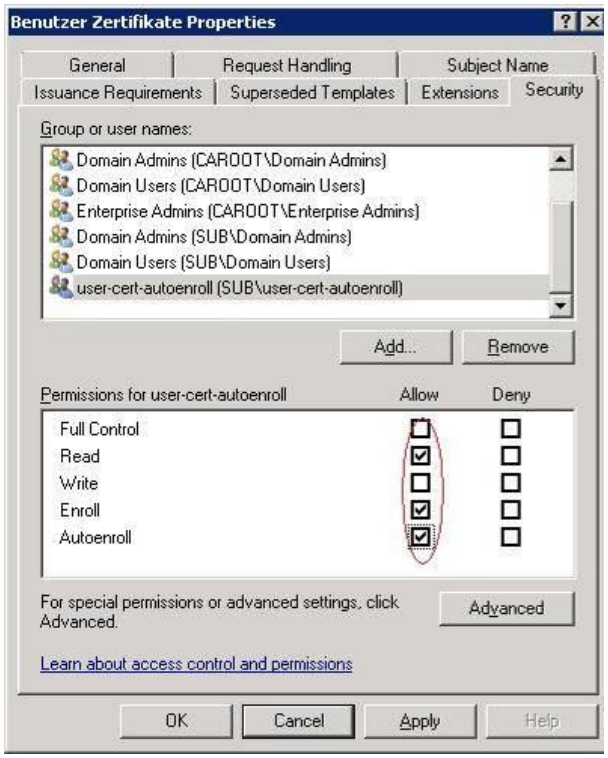


Abbildung 21: Festlegung der Zugriffsrechte auf die Vorlage für Benutzer-Zertifikate

6.1.3 Vorlage für Secure ACS Zertifikate

Die Vorlage für Secure ACS Zertifikate wird analog zu der Vorlage für Computer-Zertifikate erstellt. Als zu duplizierende Vorlage kann die Vorlage *Web Server* dienen. Eine Anpassung der Vorlagen Eigenschaften kann hinsichtlich der gewünschten *Validity Period* und *Renewal Period* nötig sein. Im Reiter *Security* muss den *Active Directory* Gruppen *Enterprise-Admins* und *Domain Admins* die folgenden Rechte zugewiesen werden:

- *Read*
- *Enroll*

6.1.4 Veröffentlichen der Vorlagen

Abschließend müssen im *MMC-SnapIn Certificate Authority* die erstellten Vorlagen im *Active Directory* veröffentlicht werden. Andernfalls ist deren Nutzung durch *Autoenrollment* nicht möglich. Hierzu wird im Kontextmenü des Ordners *Certificate Templates* der Punkt *New* und *Certificate Template to Issue* gewählt.

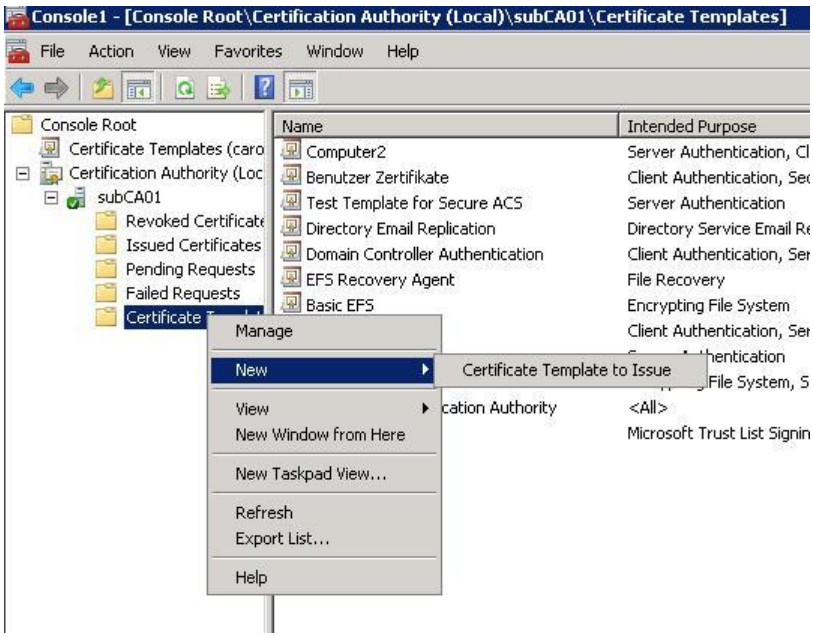


Abbildung 22: Veröffentlichen der Vorlagen im Certificate Authority SnapIn

Im nachfolgenden Dialog müssen die drei zuvor erstellten Vorlagen einzeln ausgewählt werden, und die Veröffentlichung mit *OK* bestätigt werden.

Abbildung 23: Auswahl der zu veröffentlichenden Vorlage

6.2 Autoenrollment Konfiguration

Autoenrollment von Zertifikaten wird mittels Gruppenrichtlinien konfiguriert. Diese können je nach Anforderung und Struktur des *Active Directory* Domänenweit oder eingeschränkt auf eine bestimmte *Organizational Unit* konfiguriert werden. Dies ist abhängig von der *Active Directory* Struktur, in welche 802.1X integriert wird.

Die automatische Zertifikatsaustellung mittels *Group Policy Objects* sollte vor der Aktivierung von 802.1X an den Switchports abgeschlossen sein. Andernfalls kann dies zu massiven Problemen bei der Kommunikation von Computern mit dem Netzwerk führen.

6.2.1 Autoenrollment Konfiguration für Computer-Zertifikate

Die Konfiguration wird im *MMC SnapIn Active Directory Users and Computers* vorgenommen. Im Kontextmenü der Domäne oder OU muss der Punkt *Properties* gewählt werden:

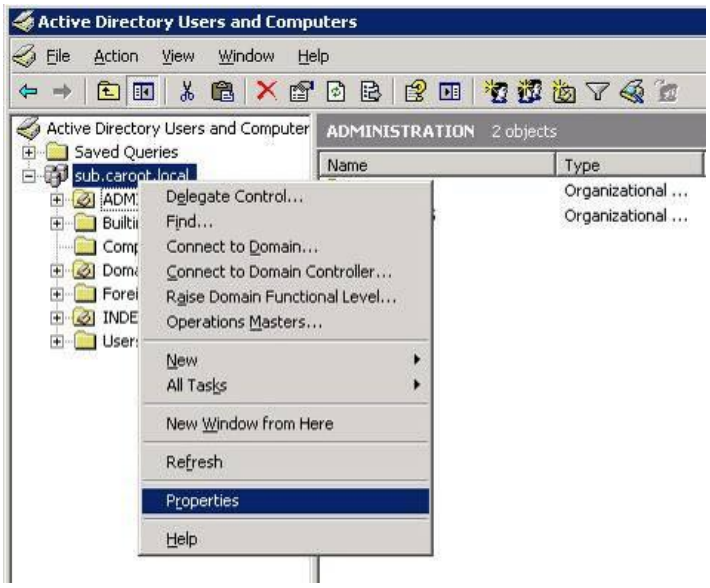


Abbildung 24: Wahl der Domäne/OU für Computer Auto-Enrollment

Die Änderungen sollten in einer separaten *Domain Policy* vorgenommen werden. Dies gilt insbesondere, wenn die neu erstellte GPO auf mehrere *Organizational Units* angewendet werden soll.

Im *Group Policy Object Editor* wird der Unterbaum *Computer Configuration -> Windows Settings -> Security Settings -> Public Key Policies* gewählt. Der *Object Type Autoenrollment Settings* bietet die Möglichkeit die Einstellungen, wie im Screenshot gezeigt, vorzunehmen:

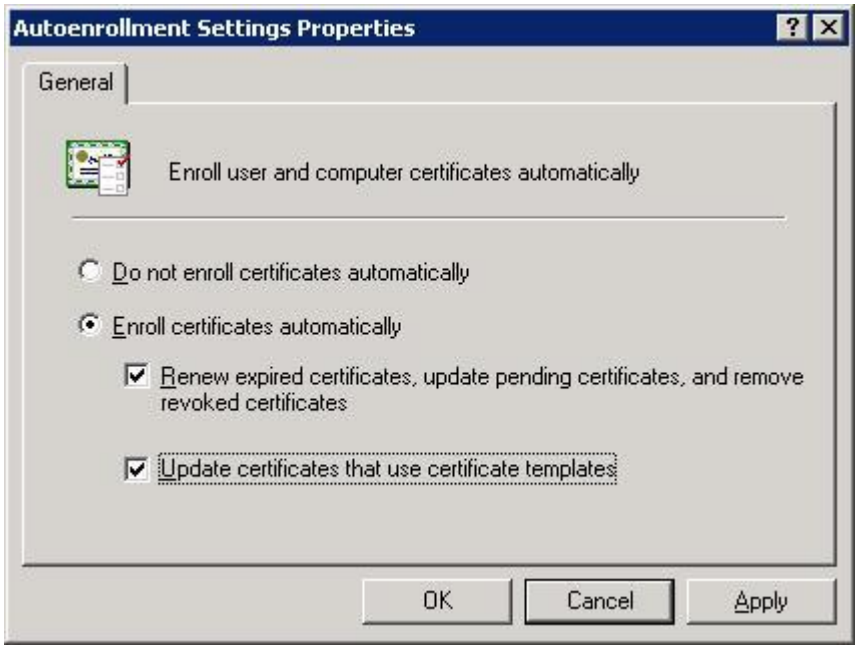


Abbildung 25: Einstellungen für Autoenrollment

6.2.2 Konfiguration für Benutzer-Zertifikate

Die *Autoenrollment* Konfiguration für Benutzer-Zertifikate erfolgt analog zu der Konfiguration von *Autoenrollment* für Computer Zertifikate. Lediglich im *Group Policy Object Editor* wird als Pfad *User Configuration -> Windows Settings -> Security Settings -> Public Key Policies* für das Einrichten der Einstellungen gewählt.

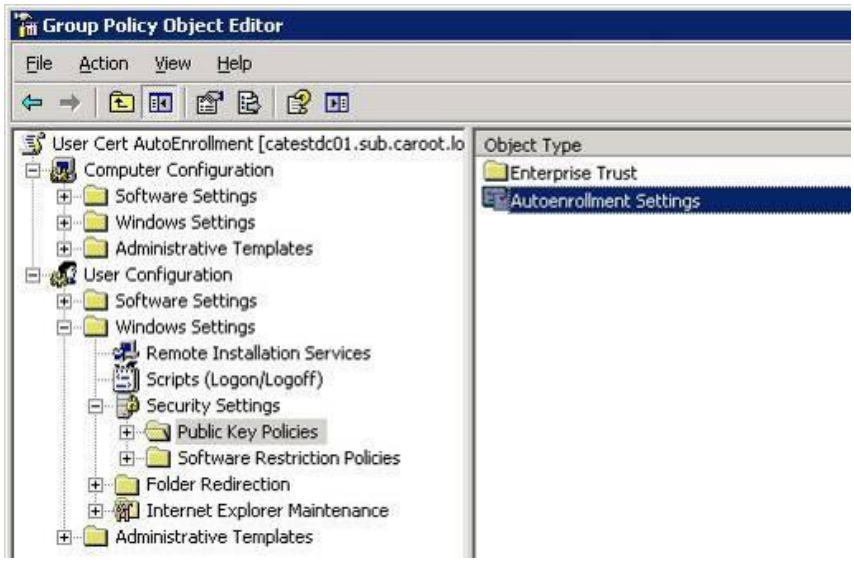


Abbildung 26: Einrichtung Auto-Enrollment Benutzer Zertifikate

6.2.3 Autoenrollment Logging Konfiguration

Um detaillierte Informationen über den Verlauf, insbesondere bei fehlgeschlagenen *Autoenrollment* Vorgängen, zu erhalten, ist es empfehlenswert das erweiterte Logging für Autoenrollment zu aktivieren. Hierzu ist die Modifikation der folgenden Registrierungsschlüssel notwendig (siehe auch http://technet.microsoft.com/en-us/library/cc755801.aspx):

Enrollment für	Registryschlüssel	Wert
Computer Zert.	HKEY_LOCAL_MACHINE\Software\ Microsoft\Cryptography\ Autoenrollment	AEEventLogLevel DWORD = 0
Benutzer Zert.	HKEY_CURRENT_USER\Software\ Microsoft\Cryptography\ Autoenrollment	AEEventLogLevel DWORD =0

Tabelle 2: Übersicht Registry-Keys für Auto-Enrollment Logging

7 KONFIGURATION CISCO SECURE ACS

Der folgende Abschnitt beschreibt die Konfigurationsschritte, um einen *Cisco Secure ACS* als *Authenticator* für EAP-TLS einzurichten. Werden, wie in Abschnitt 3.5, mehr als ein *Secure ACS* verwendet, so empfiehlt sich vor der Konfiguration der EAP-TLS Parameter die *Secure ACS* interne Replikation zu konfigurieren und zu testen. Hierdurch wird die getrennte Konfiguration der einzelnen *Secure ACS* überflüssig, soweit die Optionen von der Replikation abgedeckt werden.

Auf die grundsätzliche Einrichtung des *Secure ACS* wird im Weiteren nicht weiter eingegangen, und die entsprechenden Schritte als fehlerfrei vollzogen vorausgesetzt. Bei der Basiskonfiguration sollte ein besonderes Augenmerk darauf gelegt werden, dass der *Secure ACS* seine lokale Systemzeit mittels NTP gegen die Domänencontroller abgleicht. Dies verhindert Unstimmigkeit bezüglich der Laufzeit von Zertifikate. Einstellungen bezüglich der Zeitzone müssen entsprechend des Standortes vorgenommen werden.

7.1 Einrichtung des Remote Agents

Für den Zugriff einer *Secure ACS Appliance* auf das *Active Directory* muss mindestens ein *Remote Agent* konfiguriert werden. Die Konfiguration weiterer Agents wird aus Verfügbarkeitsgründen dringend empfohlen.

Die Einrichtung des *Remote Agents* wird unter dem Menüpunkt *Network Configuration -> Remote Agents -> Add Entry* vorgenommen:

Abbildung 27: Hinzufügen eines Remote Agents

Im nachfolgenden Dialog muss die IP Adresse des *Remote Agents* angegeben werden. Der Name sollte entsprechend der Namenskonvention gewählt werden. Mit *Submit + Apply* wird die Konfiguration gespeichert:

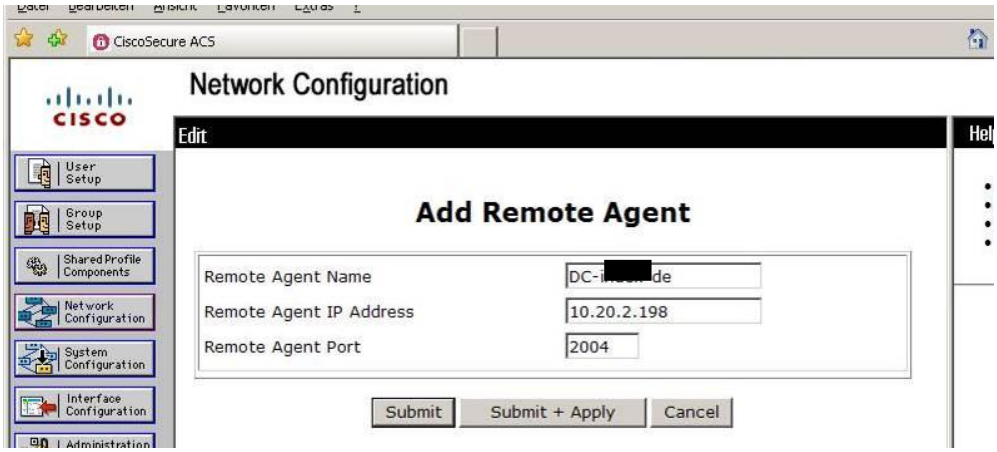


Abbildung 28: Daten des Agents eintragen

Im Menüpunkt *External User Databases -> Database Configuration -> Windows Database -> Configure -> Windows Remote Agent Selection* sollte abschließend eine Priorisierung der *Remote Agent(s)* vorgenommen werden. Wurde mehr als ein Agent konfiguriert, empfiehlt sich die Priorisierung nach geografischer Entfernung vorzunehmen. Mittels *Submit* muss die Konfiguration gespeichert werden:

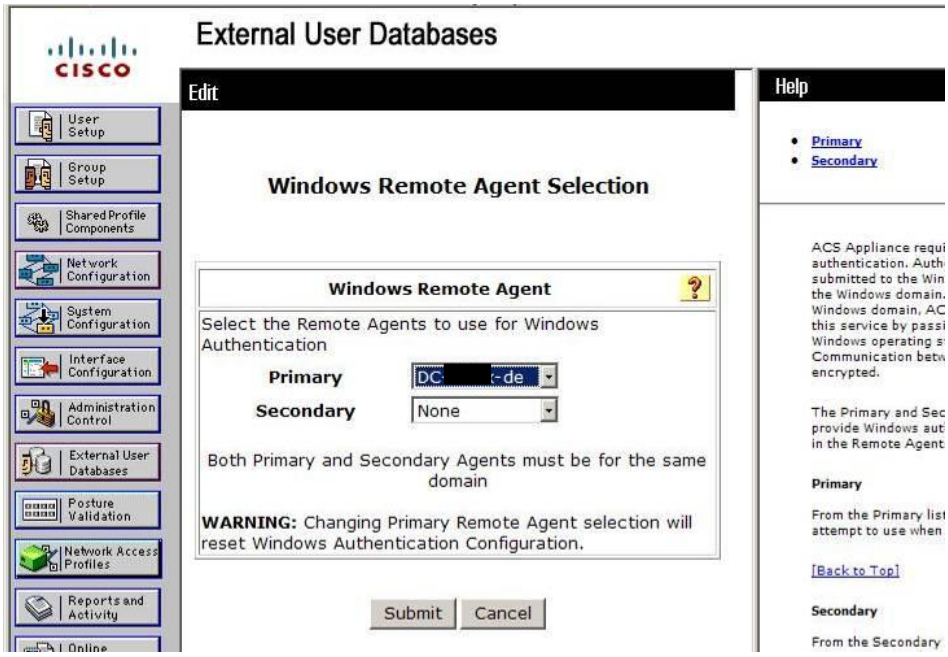


Abbildung 29: Priorisierung der Abfragereihenfolge der Remote Agents

7.2 Import der PKI-Zertifikate in Secure ACS

Im *Secure ACS* können Zertifikate der unternehmensinternen PKI-Umgebung, sowie *Certificate Trust* Einstellungen über das Menü *System Configuration -> ACS Certificate Setup* vorgenommen werden. Zunächst müssen im Untermenü *ACS Certification Authority Setup* die Zertifikate der PKI-Umgebung importiert werden. Auf der *Secure ACS* Appliance gibt es hierbei die Möglichkeit diese über das Web-Interface hochzuladen. Ist die *Secure ACS* Software auf einem Windows Server installiert, müssen die Zertifikate auf dieses System kopiert werden. Zum Importiert muss der vollständige Pfad und Name der Dateien angegeben werden.

Abbildung 30: Importieren eines PKI Zertifikates im Windows basierten Secure ACS

Nach erfolgreichem Import aller PKI-Zertifikate, müssen die *Secure ACS* Dienste neu gestartet werden. Dies geschieht im Menü *System Configuration -> Service Control* durch Anwahl des Buttons *Restart*.

7.2.1 Konfiguration der vertrauenswürdigen Zertifizierungsstellen

Unter *System Configuration -> ACS Certificate Setup* muss im nächsten Schritt *Edit Certificate Trust List* gewählt werden, um die Liste der vertrauenswürdigen Zertifizierungsstellen anzupassen. Hierbei sollte nur jenen Zertifizierungsstellen ein Vertrauen ausgesprochen werden, die Zertifikate für die Umgebung signieren. Die Vertrauensstellung wird durch Aktivieren des Kästchens vor dem Namen konfiguriert.

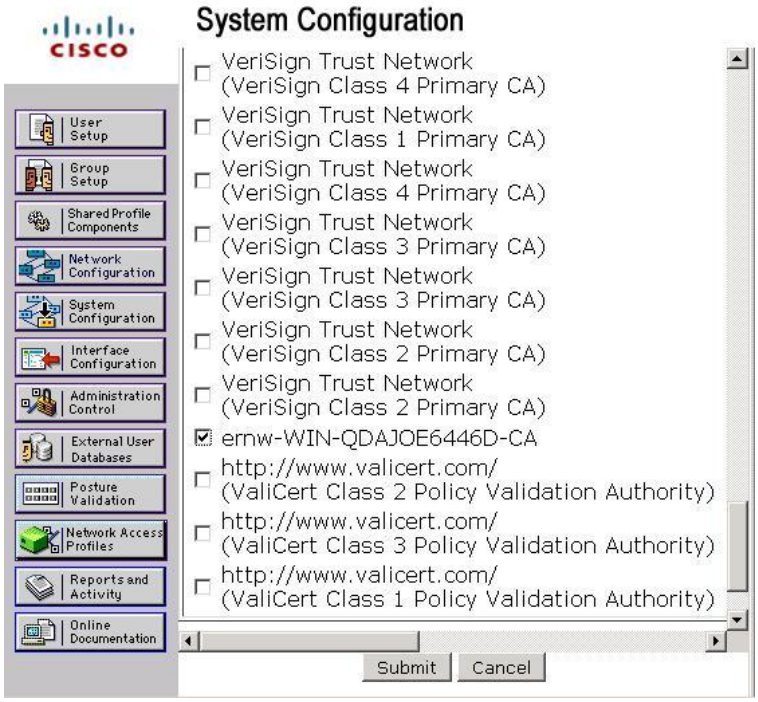


Abbildung 31: Festlegung der Vertrauensstellung für die eigene PKI Infrastruktur

Abschließend müssen die *Secure ACS* Dienste über das Menü *Service Control* neu gestartet werden.

7.2.2 Konfiguration der Zertifikatssperrliste

Der Netzwerkzugang einzelner Benutzer kann durch Zurückziehen des Benutzerzertifikats gesperrt werden. Hierzu prüft der *Secure ACS* das vom Client erhaltene Zertifikat gegen eine Zertifikatssperrliste. Die Verfügbarkeit der Sperrliste wird durch den Replikationsmechanismus im *Active Directory* gewährleistet. Die Veröffentlichung der Sperrliste im *Active Directory* findet auf einer *Enterprise CA* automatisch statt.

Die Sperrlistenkonfigurationist im *Secure ACS* unter dem Menüpunkt *System Configuration -> ACS Certificate Setup -> Certificate Revocation Lists* zu finden. Die Konfiguration muss für die *Sub CA* vorgenommen werden. In die Zeile *CRL Distribution URL* muss eine LDAP-Adresse eingefügt werden. Diese basiert auf der LDAP-URL welche im Zertifikat als CDP angegeben ist. Sie enthält hiervon jedoch nur die Werte linksseitig des ersten Fragezeichens. Zwischen dem zweiten und dritten Schrägstrich muss die IP-Adresse des nächstgelegenen *Global Catalog Servers/Domain Controllers* inklusive Portnummer angegeben werden.

Beispiel:
ldap://192.168.201.198:3268/CN=subCA01,CN=carootsub02,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=caroot,DC=local)

Der Haken *CRL is in use* muss gesetzt werden, und es sollte ein kleiner Zeitwert (beispielsweise 10 Minuten bis 1 Stunde) für *Retrieve CRL* gesetzt werden.

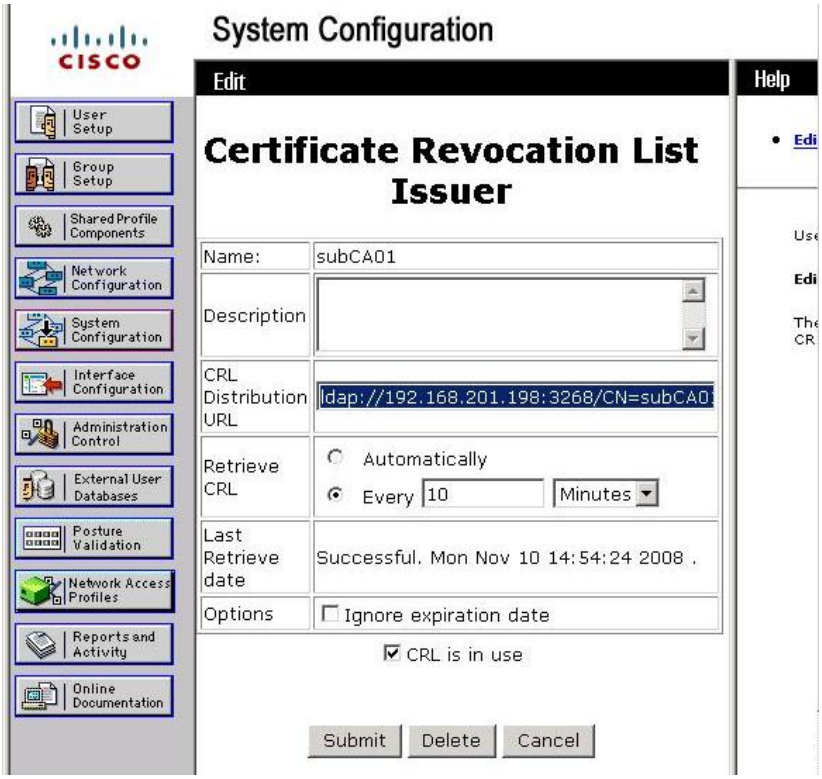


Abbildung 32: Konfiguration des Zertifikatssperrlistenabrufs

Durch Klicken auf den *Submit* Button werden die Änderungen gespeichert. Zur Prüfung ob der Abruf der Zertifikatssperrlisten erfolgreich verläuft, muss der Konfigurationsdialog erneut aufgerufen werden. In der Zeile *Last retrieve date* werden das Datum und der Status der letzten Abfrage angezeigt.

7.3 Anbindung des Secure ACS an das Active Directory

Da der *Secure ACS* Identitäten verifiziert, welche im *Active Directory* hinterlegt sind, ist eine Konfiguration von AD-Paramenter notwendig. Hierzu dient das Menü *External User Databases*. In diesem ist die Konfiguration für die *Unknown User Policy* zu finden. Diese *Policy* definiert, wie Benutzer identifiziert werden können, deren Identität nicht im *Secure ACS* gespeichert wird. In der *Policy* muss die Option *Check the following external user databases* gesetzt werden, und in die externe Datenbank *Windows Databases* in die rechte Liste mit dem Namen *Selected Databases* aufgenommen werden. Diese Konfiguration wird durch Betätigen von *Submit* gespeichert.

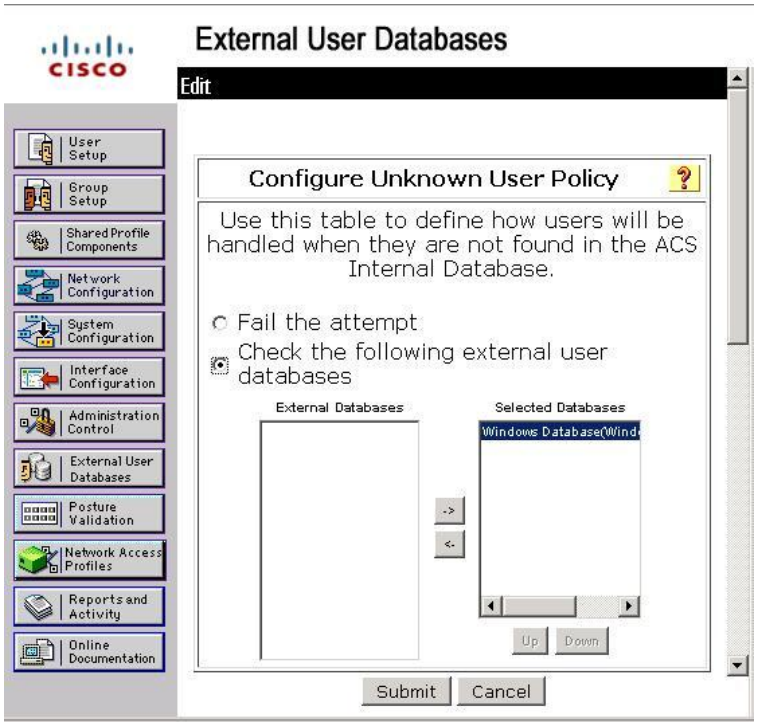


Abbildung 33: Die External User Database ist ein Windows AD

Im nächsten Schritt müssen für die Windows Datenbank genaue Parameter konfiguriert werden. Dies geschieht im Menüpunkt *Database Configuration* durch Auswahl von *Windows Database*. Initial existiert keine Konfiguration, daher muss eine neue Konfiguration durch Auswahl von *Configure* angelegt werden.

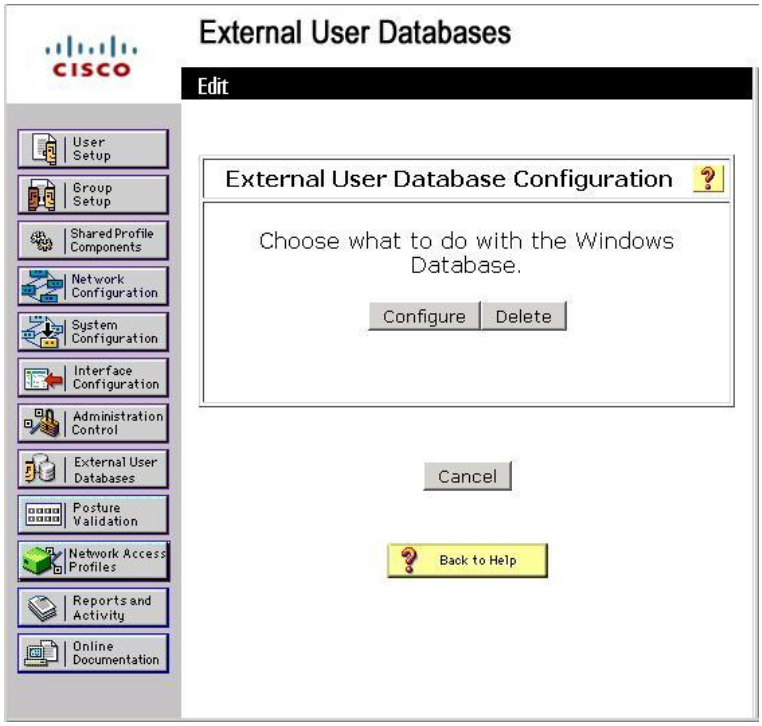


Abbildung 34: Anlegen einer neuen Windows Database Konfiguration

Im Abschnitt *Configure Domain List* müssen alle Domänen ausgewählt werden, welche Benutzer/Computer enthalten die authentifiziert werden sollen.

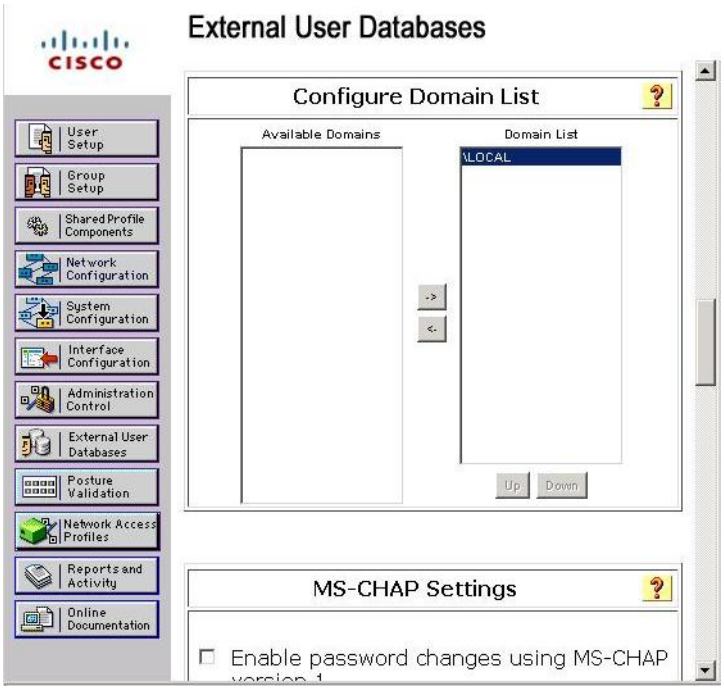


Abbildung 35: Hinzufügen der Domains

Weiterhin muss die EAP-TLS Funktionalität im Abschnitt *Windows EAP Settings* aktiviert werden, bevor die Einstellungen über das Betätigen von *Submit* gespeichert werden.

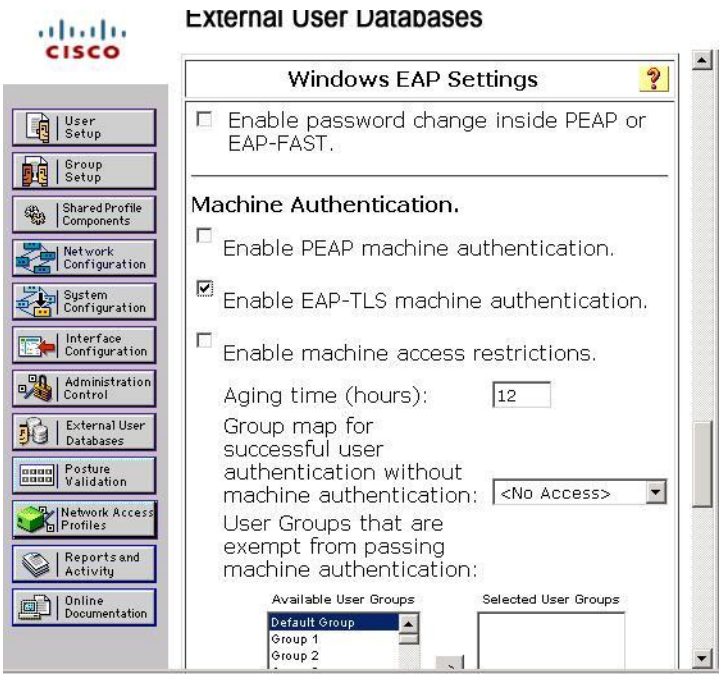


Abbildung 36: Aktivierung von EAP-TLS Authentifizierung für diese Datenbank

Als letzter Schritt wird die Einbindung der Gruppen der *Active Directory* Domäne in den *Secure ACS* vorgenommen. Hierbei wird im Menü *External User Databases -> Database Group Mappings* der Punkt *Windows Database* gewählt. Im nachfolgenden Dialog werden alle bereits konfigurierten Domänen aufgelistet. Die neuen Domänen müssen über *New configuration* hinzugefügt werden. Im erscheinenden Dialog wird die gewünschte Domäne ausgewählt, und durch Betätigen von *Submit* hinzugefügt.

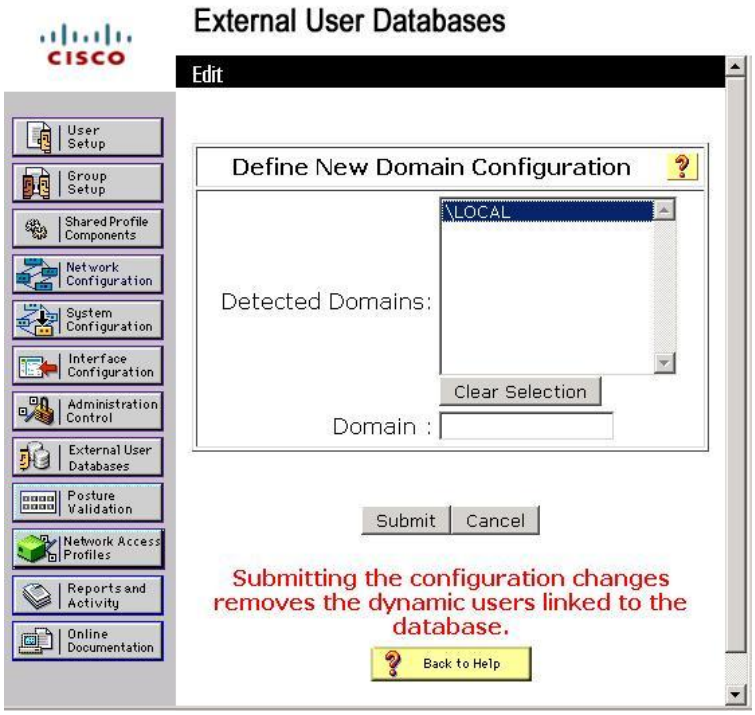


Abbildung 37: Hinzufügen der Domäne

7.4 Ausstellung des Secure ACS-Zertifikates

Nachfolgend wird der Prozess der Zertifikatsaustellung für die *Secure ACS* Appliance beschrieben. Das Zertifikat wird während der EAP-TLS Authentifizierung an den Client gesendet und ermöglicht so die Authentifzierung des Netzwerkes durch den Supplicant. Auf einem Windows basierten *Secure ACS* kann dieser Vorgang über das *Web Enrollment Interface* der *Sub CA* durchgeführt werden. Hierbei ist die in Abschnitt 6.1.3 erstellte Vorlage zu verwenden. Im Dialog *ACS Certificate Setup* kann das erstellte Zertifikat aus der *Select Certificate From Storage* Liste ausgewählt werden. Weitere Konfigurationsschritte sind in diesem Szenario nicht durchzuführen.

Das Austellen eines Zertifikates für eine *Secure ACS* Appliance ist aufwändiger und wird daher nachfolgend im Detail beschrieben.

Unter dem Menüpunkt *System Configuration -> ACS Certificate Setup -> Generate Certificate Signing Request* kann ein Zertifikatsantrag erstellt werden. Das Feld *Certificate Subject* muss hierbei mit der Zeichenfolge *cn=* beginnen, und nachfolgend den Systemnamen der Appliance enthalten.

Im Feld *Private Key File* muss eine Datei angegeben werden in welcher der private Schlüssel gespeichert wird. Dieser sollte mit einem Passwort gesichert werden. Als Parameter für *Key Length* und *Digest to sign with* ist aus Sicherheitsgründen minimal *2048 bits* und *SHA-1* zu wählen.

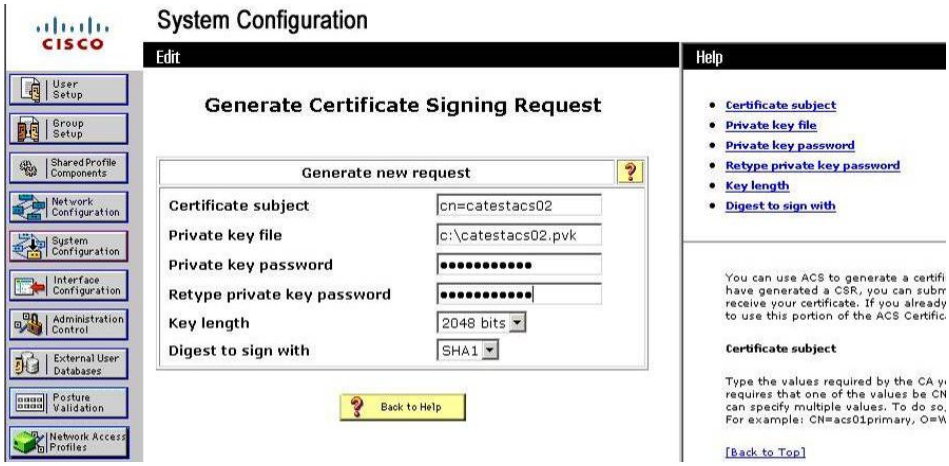


Abbildung 38: Parameter für den Zertifikatsantrag

Nach betätigen des *Submit* Buttons wird der Zertifikatsantrag erzeugt, und im rechten Frame angezeigt:

Abbildung 39: Generierter Zertifikatsantrag

Der gesamte Text des Zertifikatsantrages, inklusive der beiden `BEGIN/END CERTIFICATE REQUEST` Zeilen muss kopiert werden. Der Antrag kann an der *Sub CA* mittels *Web Enrollment* eingereicht werden. Hierzu muss im *Internet Explorer* die Seite *http://<NAME_DER_CA>/CertSrv* aufgerufen werden. Nach Auswahl von *Request a Advanced certificate request -> Submit a certificate request* kann im erscheinenden Dialog der Text des Zertifikatsantrages eingefügt werden. Abschließen muss die in Abschnitt 6.1.3 erzeugte Vorlage gewählt werden.

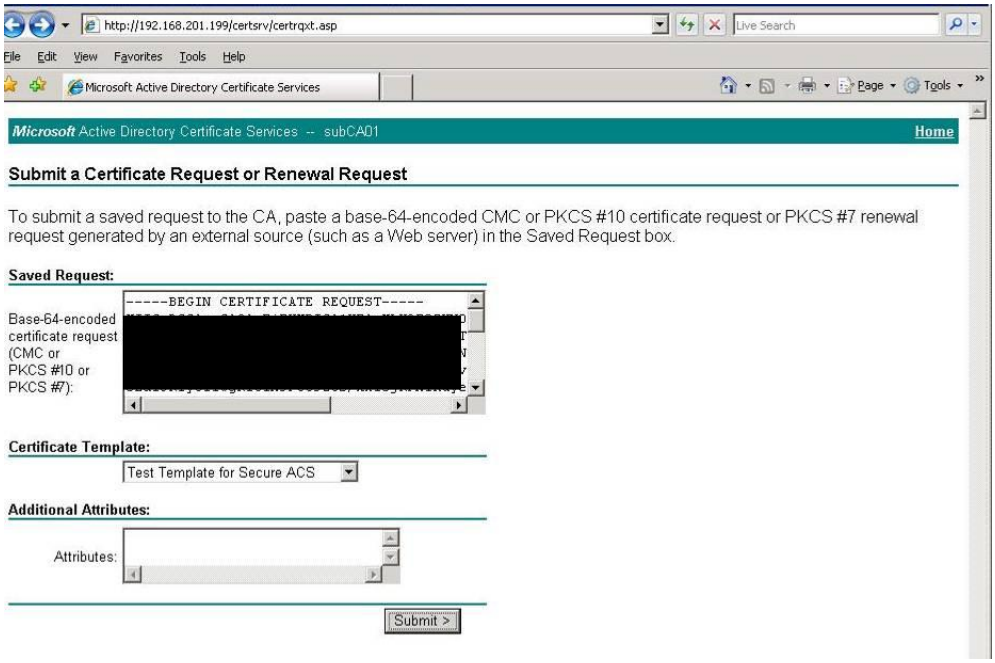


Abbildung 40: Übermittlung der Zertifikatsantrages

Entspricht das Zertifikat den Vorgaben der Vorlage, wird es automatisch signiert, und steht zum Download bereit. Beim Download des Zertifikats muss das Base64 Format gewählt werden, da andernfalls der Import des Zertifikats fehlschlägt:

Abbildung 41: Download des signierten Zertifikats

Zur Installation des Zertifikats muss dieses auf einen FTP Server kopiert werden, mit welchem der *Secure ACS* kommunizieren darf. In der Oberfläche des *Secure ACS* muss im Menü *System Configuration -> ACS Certificate Setup -> Install ACS Certificate* die Option *Download certificate file* gewählt werden. Im nachfolgenden Dialog werden die Zugangsdaten für den FTP-Download eingetragen.

Abbildung 42: FTP Download Informationen

Nach bestätigen durch den *Submit* Schaltknopf, wird die Datei heruntergeladen, und lokal auf dem *Secure ACS* gespeichert. Im folgenden Dialog muss im Feld *Private key password* das Passwort für den Zugriff auf den privaten Schlüssel des Zertifikats hinterlegt werden. Der Dialog wird mit *Submit* bestätigt.

Abbildung 43: Kennwort für privaten Schlüssel konfigurieren

Die korrekte Installation des Zertifikats wird durch den *Secure ACS* wie folgt angezeigt:

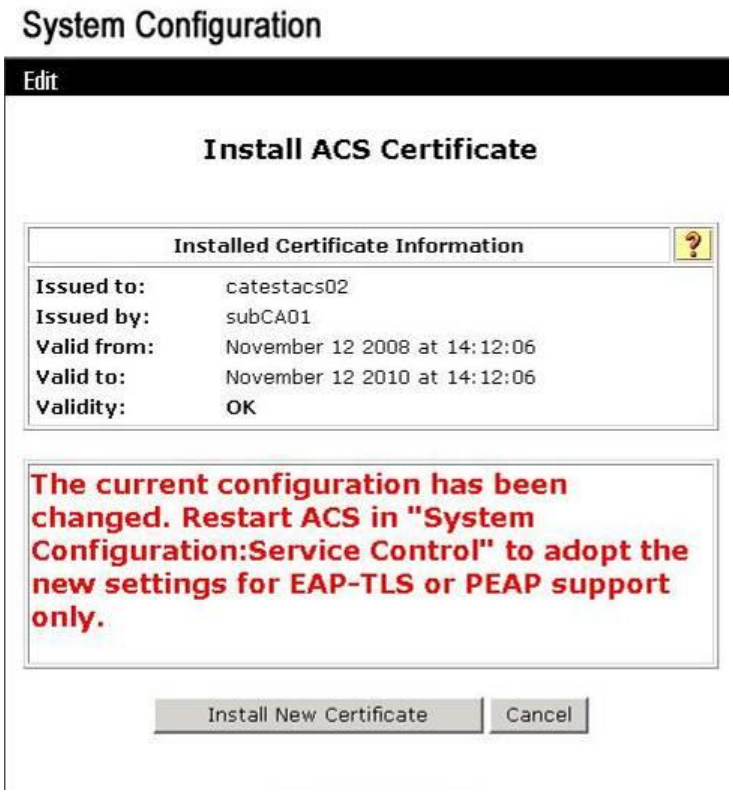


Abbildung 44: Verifizieren der erfolgreichen Zertifikatsinstallation

Zum Abschließen der Konfiguration müssen die *Secure ACS* Dienste neu gestartet werden. Dies geschieht im Menü *System Configuration -> Service Control* durch betätigen der Schaltfläche *Restart*.

7.5 Konfiguration EAP-TLS

Im folgenden Abschnitt wird die Basis Konfiguration zum Betrieb von 802.1X mit dynamischer VLAN Zuordnung beschrieben. Wird letztere Funktion nicht benötigt, so können die im Abschnitt 7.5.2 beschriebenen Schritte übersprungen werden.

7.5.1 Basis Konfiguration EAP-TLS

In der Administrationsoberfläche des *Secure ACS* findet sich im Menü *System Configuration -> Global Authentication Setup* die Konfiguration der Authentifizierungsmethoden. Hier muss die EAP-TLS Option, inklusive der drei *Comparison* Methoden aktiviert werden. Weitere Authentifizierungsverfahren sollten, wenn möglich, durch Entfernen der entsprechenden Haken deaktiviert werden.

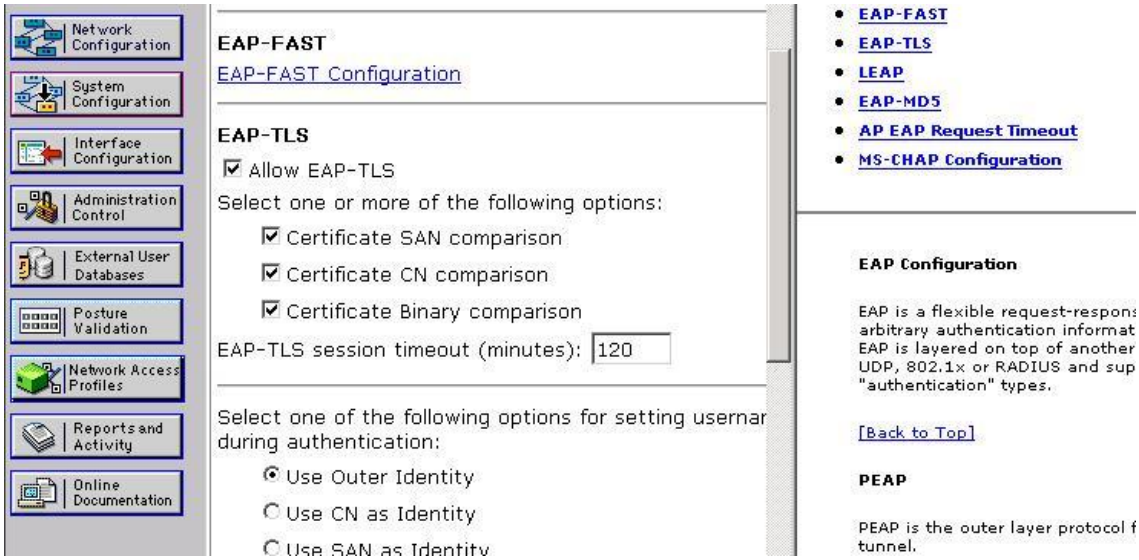


Abbildung 45: Aktivierung von EAP-TLS

Durch Klicken auf die *Submit + Restart* Schaltfläche werden die Änderungen aktiv.

7.5.2 Konfiguration von 802.1X VLAN-Zuordnung

Zusätzlich zu einem erfolgreichen Authentifizierungsvorgang kann eine Zuweisung von authentifizierten Geräten zu einem spezifischen VLAN erfolgen. Das Prinzip sieht hierbei vor, dass die VLAN-Zugehörigkeit über Gruppen im *Active Directory* abgebildet werden. Es müssen daher für alle VLAN-IDs eine zugehörige Gruppe im *Active Directory* angelegt werden. Computer und/oder Benutzer können diesen Gruppen zugeordnet werden. Hierbei ist zu beachten, dass ein Computer/Benutzer jeweils nur Mitglied in einer dieser Gruppen sein darf. Andernfalls kann keine deterministische Zuordnung vorgenommen werden.

Bei einer erfolgreichen Authentifizierung werden diese Gruppeninformationen für einen Computer/Benutzer durch den *Secure ACS* ausgelesen. ACS-intern kann ein Mapping von Windows-Gruppen auf ACS-Gruppen konfiguriert werden. Hierbei wird in den ACS-Gruppen die VLAN Zugehörigkeit hinterlegt.

Im Folgenden wird die *Secure ACS* spezifische Konfiguration dieses Mechanismus beschrieben. Auf die Einrichtung der *Active Directory* Gruppen wird nicht näher eingegangen.

7.5.2.1 Anlegen einer Secure ACS-Gruppe

Das Anlegen von *Secure ACS*-Gruppen erfolgt im Menü *Group Configuration*. Hier muss die entsprechende Gruppe ausgewählt werden, mittels *Edit Settings* können die Einstellungen angepasst werden. Bei dieser Anpassung müssen drei Radius-Attribute festgelegt werden. Dies sind die Attribute *64*, *65* und *81*. Die Werte von *64* und *65* sind für alle Gruppen auf *VLAN* und *802* zu konfigurieren. In Attribut *81* wird die VLAN Zugehörigkeit durch Angabe der entsprechenden *VLAN-ID* konfiguriert.

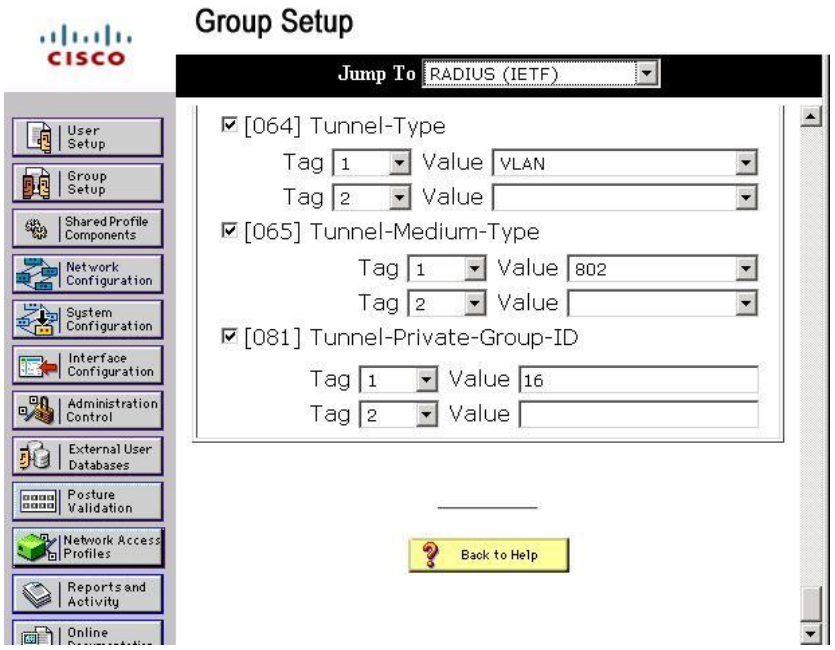


Abbildung 46: Konfiguration der VLAN Zugehörigkeit einer Secure ACS Gruppe

Die Konfiguration wird mit *Submit + Restart* aktiv.

7.5.2.2 Zuordnung einer Windows Active Directory Gruppe zu einer Secure ACS Gruppe

Im Konfigurationsmenü unter *External User Databases -> Database Group Mappings* muss die entsprechende Domäne ausgewählt werden, in welcher die *Active Directory* Gruppen liegen. Im Beispielsfall sei dies *\LOCAL*.

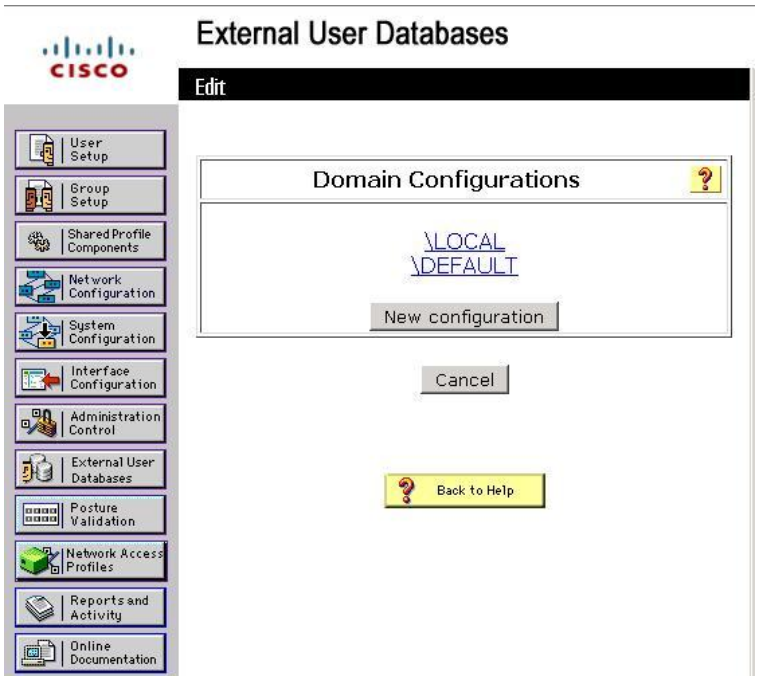


Abbildung 47: Auswahl der AD-Domäne

Im nachfolgenden Dialog kann durch Auswahl einer bestehenden Zuordnung diese geändert werden, oder durch Auswahl von *Add mapping* eine neue Zuordnung hinzugefügt werden. Im erscheinenden Dialog kann jetzt eine (oder mehrere) Gruppen(n) ausgewählt werden, und mittels des Button *Add to selected* der Liste der *Active-Directory* Gruppen hinzugefügt werden. Unterhalb ist die Auswahlliste der *Secure ACS* Gruppe zu finden. Einer ACS-Gruppe können mehrere AD-Gruppen zugeordnet werden. Die umgekehrte mehrfache Zuordnung ist nicht möglich.

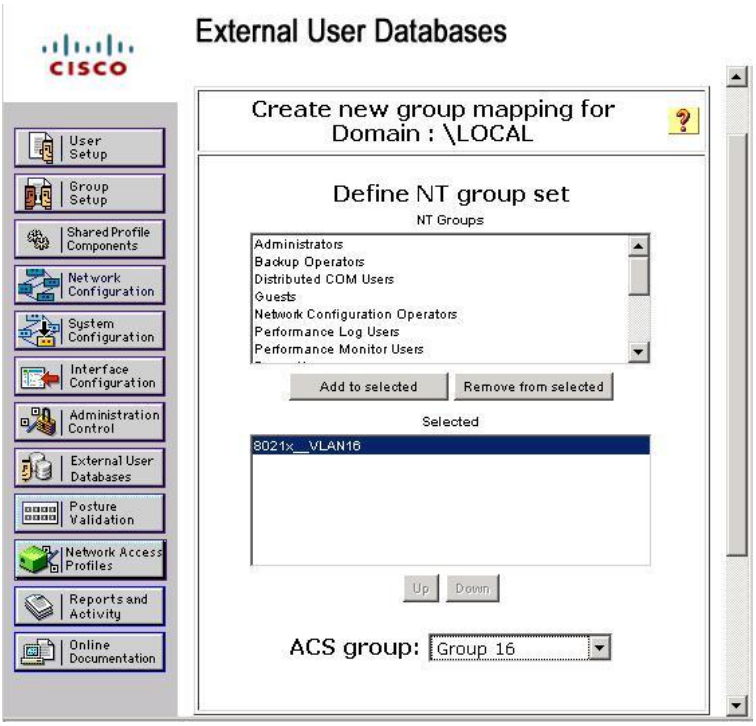


Abbildung 48: Erstellen einer AD zu ACS Gruppenzuordnung

7.6 Konfiguration MAC Authentication Bypass

MAC Authentication Bypass authentifiziert nicht-802.1X fähige Geräte mittels ihrer MAC-Adresse. Hierbei wird die Absenderadresse durch den Switch aus dem ersten Packet ausgelesen, und als Authentifizierungsdaten an den *Secure ACS* gesendet. Kann dieser die Daten erfolgreich gegen seine interne Datenbank verifizieren, wird der Zugang für das Gerät zum Netzwerk gewährt. Hierbei kann eine vorkonfigurierte dynamische VLAN-Zuordnung stattfinden.

Für jedes über MAB zu authentifizierende Gerät muss ein Benutzer auf dem *Secure ACS* angelegt werden. Der Benutzername entspricht der Mac-Adresse des Gerätes ohne Trennzeichen.

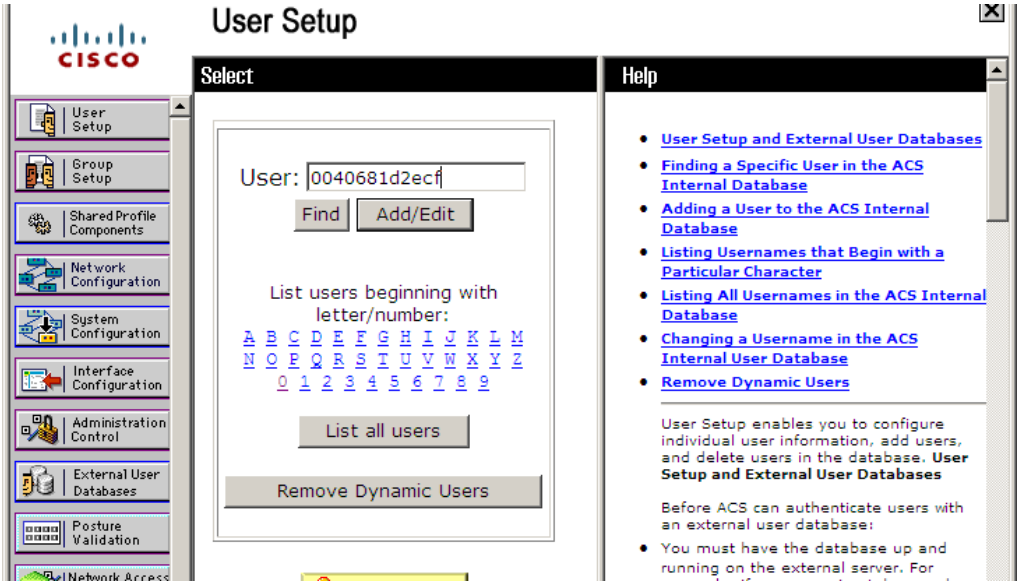


Abbildung 49: Anlegen eines MAB Gerätes als Benutzer im Secure ACS

In den Eigenschaften des neu angelegten Benutzers wird nun das Passwort festgelegt. Dieses muss identisch mit dem Benutzernamen sein, andernfalls schlägt die Authentifizierung fehl.

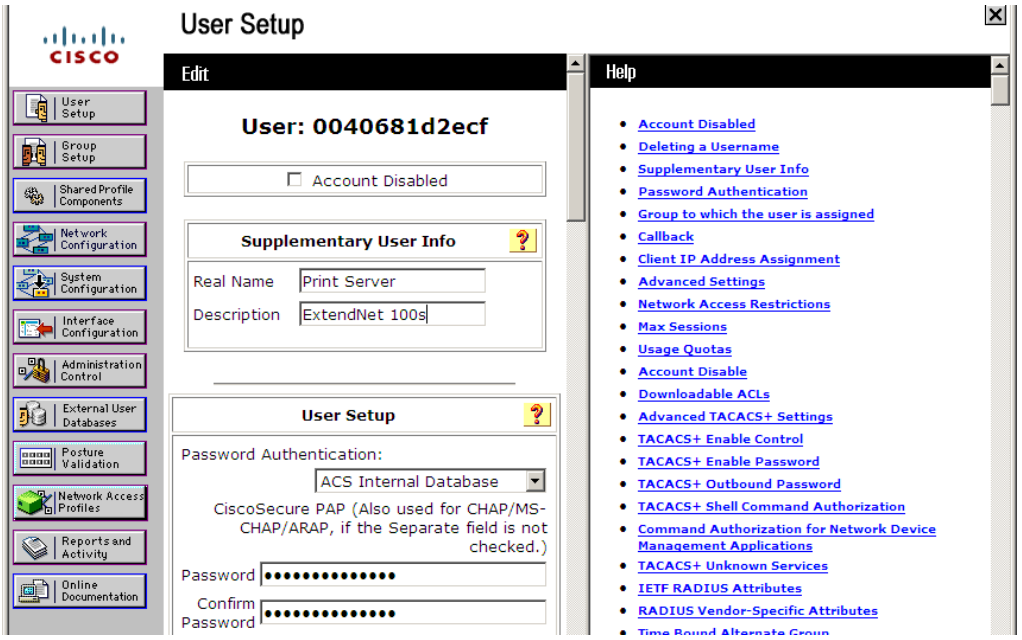


Abbildung 50: Konfiguration des Kennworts für MAB

Soll für das konfigurierte Gerät eine VLAN-Zuordnung hinterlegt werden, kann diese durch die Zugehörigkeit des Benutzers zu einer *Secure ACS* Gruppe konfiguriert werden. Innerhalb dieser Gruppe ist die VLAN-ID hinterlegt, welche dem authentifizierten Switchport zugewiesen wird.

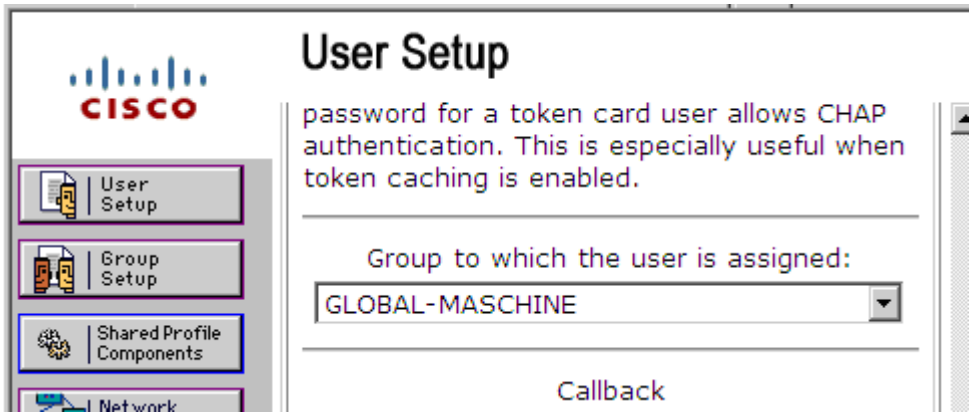


Abbildung 51: Festlegung des VLANs über die ACS Gruppe

8 KONFIGURATION DER SWITCHE

Im folgenden Abschnitt werden die Konfigurationsschritte für die Einrichtung der 802.1X Switche beschrieben. Die Aufteilung in thematische Kapitel ermöglicht eine einfache Auslassung von Konfigurationsschritten, die aus Lesersicht nicht erforderlich sind.

8.1 802.1X Basis Konfiguration

Der Switch vermittelt während des Authentifizierungsvorgangs Informationen zwischen dem EAPoL- und dem Radius-Protokoll. Daher benötigt er eine entsprechende Basiskonfiguration die angibt welcher Radius-Server verwendet werden soll. Des Weiteren aktiviert die nachstehende Konfiguration die 802.1X Funktionen. Zunächst wird im globalen Konfigurationsmodus die Radius-Server Konfiguration vorgenommen.

```
switch(config)#aaa new-model
switch(config)#aaa authentication dot1x default group radius
switch(config)#aaa authorization network default group radius
switch(config)#radius-server host <RADIUS_IP>auth-port 1812 acct-
              port 1646 test username admin ignore-auth-port
              idle-time 2 key <RADIUS_PASSWORT>
switch(config)#radius-server vsa send accounting
switch(config)#radius-server vsa send authentication
switch(config)#dot1x system-auth-control
```

Des Weiteren müssen Ports die 802.1X basierte Authentifizierung durchführen sollen wie folgt konfiguriert werden:

```
switch(config-if)#switchport mode access vlan <VLAN_NUMBER>
switch(config-if)#switchport mode access
switch(config-if)#dot1x port-control-auto
switch(config-if)#dot1x pae authenticator
```

Hierbei verweist <VLAN_NUMBER> auf das VLAN in welchem der Port nach erfolgreicher Authentifizierung aufgenommen sein soll, wenn keine VLAN-Zuordnung durch den *Secure ACS* stattfindet.

8.1.1 Anlegen des RADIUS-Clients

Auf *Secure ACS* Seite muss jeder Switch durch das Erstellen eines *AAA-Clients* bekannt gemacht werden. Dies geschieht im Menü *Network Configuration*. Gegebenenfalls muss hier zunächst die *Network Device Group* ausgewählt werden, zu welcher der Switch zugeordnet ist. Unterhalb der Liste der *AAA-Clients* kann mittels *Add Entry* das Formular zur Erstellung eines neuen *AAA-Clients* aufgerufen werden. In diesem muss ein Name, die IP-Adresse und das zuvor auf dem Switch konfigurierte Radius-Passwort angegeben werden. Im Menü *Authenticate Using* muss *RADIUS (IETF)* ausgewählt werden.

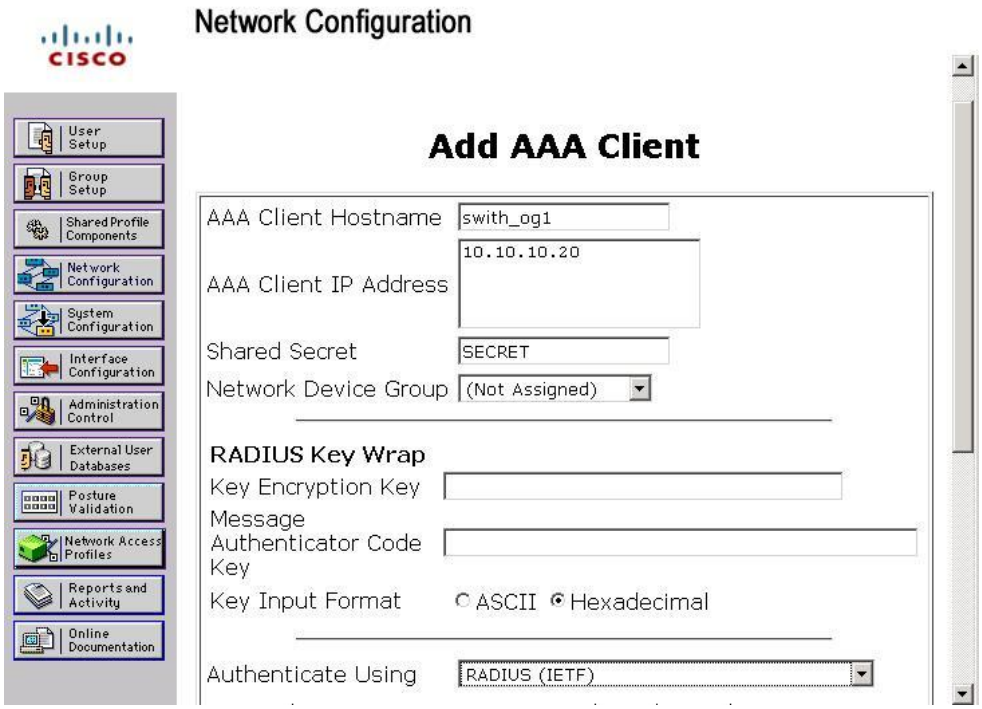


Abbildung 52: Anlegen eines neuen AAA-Clients

8.2 Konfiguration MAC Authentication Bypass

Zur Aktivierung von MAB muss auf den Switches folgende Einstellung vorgenommen werden. Diese Einstellung ist auf jedem Port, welcher Geräte über *MAC Authentication Bypass* authentifizieren soll, vorzunehmen:

```
switch(config-if)# mab
```

8.3 Konfiguration Wake-on-LAN

In der Basiskonfiguration lässt ein 802.1X konfigurierter Port nur *EAPoL*-, *STP*- und *CDP*-Pakete passieren, bis eine erfolgreiche Authentifizierung stattgefunden hat. Wird beispielsweise für die Softwareverteilung *Wake On LAN* (WoL) genutzt, muss diese zusätzliche Funktion auf dem 802.1X Switchport aktiviert werden.

Hierzu wird die Kontrollrichtung des unauthorisierten Ports verändert. Die Standardeinstellung sieht vor, dass Datenpakete, bis auf die oben genannten Ausnahmen, in beide Richtungen blockiert werden. Mit Hilfe des Kommandos `dot1x control-direction` lässt sich die Sperrrichtung explizit konfigurieren. Wird diese lediglich auf `in` konfiguriert, so ist die Nutzung von WoL möglich:

```
switch(config-if)#dot1x control-direction in
```

8.4 Konfiguration des PXE

Wird im Netzwerk *Preboot Execution Environment* (PXE) genutzt, müssen die *Timeout Parameter*, nach deren Ablauf *MAC Authentication Bypass* greift, angepasst werden. Andernfalls bricht der PXE Boot Manager des Computers mit einem Timeout ab. In den Standardeinstellungen beläuft sich der Timeout auf insgesamt 90 Sekunden. Es werden bis zum Abbruch 3 Authentifizierungsversuche mit jeweils 30 Sekunden Timeout durchgeführt. Mit den folgenden Einstellungen wird der Timeout auf 2 Authentifizierungsversuche mit je 10 Sekunden Timeout reduziert:

```
switch(config-if)#dot1x timeout tx-period 10
switch(config-if)#dot1x max-reauth-req 1
```

8.5 Konfiguration des Guest-VLANs

Die Guest-VLAN Funktionalität gewährleistet, das nicht 802.1X fähige Geräte, deren Mac-Adressen nicht im Cisco *Secure ACS* eingetragen ist (z.B. Kunden die ihren Laptop an das Netzwerk anschließen), einem bestimmten VLAN (hier VLAN 200) zugewiesen werden.

```
switch(config-if)#dot1x guest-vlan 200
```

8.6 Konfiguration des Auth-Fail VLANs

Mit dieser Konfiguration wird sichergestellt dass Clients, deren Authentifizierung fehlgeschlagen ist (z.B. bei zurückgezogenem Zertifikat), einem bestimmten VLAN zugewiesen werden. Dies ist erwünscht, damit zu diesen Clients Verbindungen im Rahmen eines Supportvorganges hergestellt werden können. So können diese z.B. mit einem neuen Zertifikat ausgestattet werden.

```
switch(config-if)#dot1x auth-fail vlan 200
switch(config-if)#dot1x auth-fail max-attempts 2
switch(config-if)#dot1x reauthentication
```

8.7 Konfiguration von Inaccessible Authentication Bypass

Inaccessible Authentication Bypass ermöglicht die erfolgreiche Authentifizierung von Benutzern/Computern falls der *Secure ACS* nicht verfügbar sein sollte. Hierbei findet eine Zuordnung in ein spezielles VLAN statt. Ist der *Secure ACS* wieder verfügbar reauthentifiziert der Switch die Geräte und ordnet sie dem entsprechenden VLAN zu. Damit der Switch in einem definierbaren Intervall die Erreichbarkeit des *Secure ACS* überprüfen kann, muss die in Abschnitt 8.1 vorgestellte RADIUS Konfiguration vollständig vorgenommen sein.

Mit diesen Einstellungen überprüft der Switch alle 2 Minuten ob der *Secure ACS* erreichbar ist. Der Switch verwendet dazu einen lokal (auf dem Switch) konfigurierten Benutzernamen. Der Switch sendet hierzu einen *Access-Request* an den *Secure ACS* Server. Da der angegebene Benutzername nicht in der Datenbank des *Secure ACS* vorhanden ist antwortet dieser mit einem *Access-Reject*. Hierdurch weiss der Switch, dass der *Secure ACS* erreichbar ist und markiert diesen als *alive*. Das Anlegen eines passenden Benutzers auf dem Secure ACS ist weder nötig noch möglich.

Wenn der Secure ACS Server als *dead* (derzeit nicht erreichbar) markiert wurde, muss die Zeitspanne konfiguriert werden, in welchen Abständen der Switch versucht ihn wieder zu erreichen. Dies wird mit folgendem Kommando realisiert:

```
switch(config)#radius-server deadtime 2
```

Mit diesem Befehl versucht der Switch alle 2 Minuten den *Secure ACS* zu erreichen, wenn dieser zuvor als *dead* markiert wurde.

Für den Fall, dass der Switch den Secure ACS nicht mehr erreichen kann, ist es notwendig ein VLAN zu definieren in welches die betroffenen Ports aufgenommen werden. Dies muss auf Port Basis konfiguriert werden, mit dem folgenden Befehl

```
switch(config-if)#authentication event server dead action
                  authorize vlan 250
```

Soll die Authentifizierung durchgeführt werden, sobald der Secure ACS wieder erreichbar ist, muss das folgende Kommando auf Port Basis konfiguriert werden.

```
switch(config-if)#authentication event server alive action
                  reinitialize
```

Wenn ein Port im *critical state* authentifiziert wurde, ist es sinnvoll den Switch so zu konfigurieren, dass dieser eine *EAP-Success* Nachricht an den 802.1X Supplicant verschickt. Dies wird im globalen Konfigurationskontext mit folgendem Befehl konfiguriert werden:

```
switch(config)#dot1x critical eapol
```

9 KONFIGURATION DER CLIENT PCS

Die Konfiguration der Client PCs erfordert, dass Windows XP ab Service Pack 3 installiert ist. Bei 64bit Windows XP Systemen enthält ein vollständig gepatchtes System ebenfalls alle nötigen Updates für die korrekte Funktionalität des 802.1X *Supplicant*.

Zunächst muss sichergestellt werden, dass der Dienst *dot3svc* bei Systemstart automatisch gestartet wird. Dieser ist für die 802.1X Anmeldung für kabelgebundene Netzwerke notwendig.

Im Reiter *Authentifizierung* der Eigenschaften der LAN-Verbindung wird die 802.1X Konfiguration vorgenommen. Hierzu ist es notwendig diese zu zunächst zu aktivieren, und als Methode *Smartcard oder anderes Zertifikat* auszuwählen. Unter *Einstellungen* lassen sich nun die *EAP-TLS* Eigenschaften hinterlegen. Hierbei muss darauf geachtet werden, dass folgende Einstellungen vorgenommen wurden:

- *Zertifikat auf diesem Computer verwenden* muss gewählt werden, wobei der Haken für *Einfache Zertifikatsauswahl verwenden* nicht gesetzt werden sollte
- *Serverzertifikat überprüfen* muss aktiviert werden, andernfalls wird das Zertifikat des *Secure ACS* nicht geprüft
- Die Option *Verbindung mit diesem Server herstellen* ermöglicht die explizite Angabe der *Secure ACS* DNS-Namen. Die Hinterlegung dieser im Profil verhindert Man-In-The-Middle Angriffe gegen den Client
- In der Liste *Vertrauenswürdige Stammzertifizierungsstellen* muss der eigenen PKI-Umgebung das Vertrauen ausgesprochen werden. Werden nur Zertifikate aus der eigenen PKI-Umgebung für die *Secure ACS* Server eingesetzt, so sollte geprüft werden, dass allen weiteren PKIs das Vertrauen, durch Entfernen des Hakens, entzogen wurde.

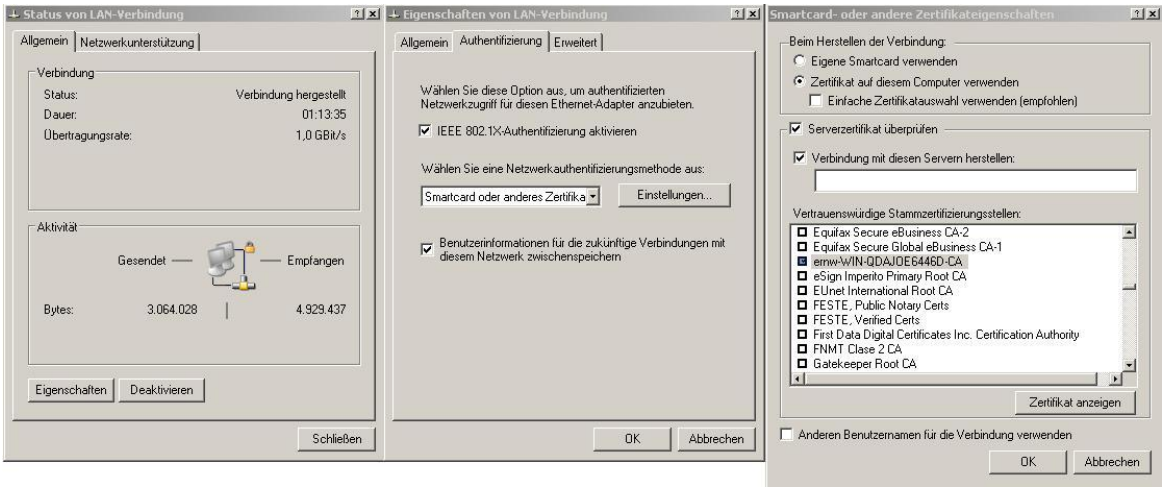


Abbildung 53: Konfiguration des 802.1X Supplicant auf Windows XP

Eine globale Konfiguration dieser Eigenschaften kann mittels GPO ausgerollt werden[10].

10 TROUBLESHOOTING

Der folgende Abschnitt beschreibt die wichtigsten Troubleshooting Prozesse, welche im Betrieb von 802.1X mit Zertifikaten auftreten können.

10.1 Sperrung von Benutzer- oder Computer-Zertifikaten

Die Sperrung von Zertifikaten kann aus unterschiedlichen Gründen erfolgen:

- Computer/Benutzer scheidet aus Umgebung aus
- Benutzer tritt längerfristigen Urlaub an
- Notebook des Benutzers wird gestohlen
- Verdacht auf Kompromittierung des privaten Schlüssel

Die Sperrung von Zertifikaten kann im *MMC SnapIn Certificate Authority* der ausstellenden Zertifizierungsstelle vorgenommen werden. Hierbei sollte das zu sperrende Zertifikat immer über seine Seriennummer identifiziert werden, da dieses eine eindeutige Identifizierung ermöglicht:

[10] *Unter folgender Adresse ist eine ausführliche Dokumentation zur Vorgehensweise zu finden:* http://technet.microsoft.com/en-us/library/cc731213.aspx

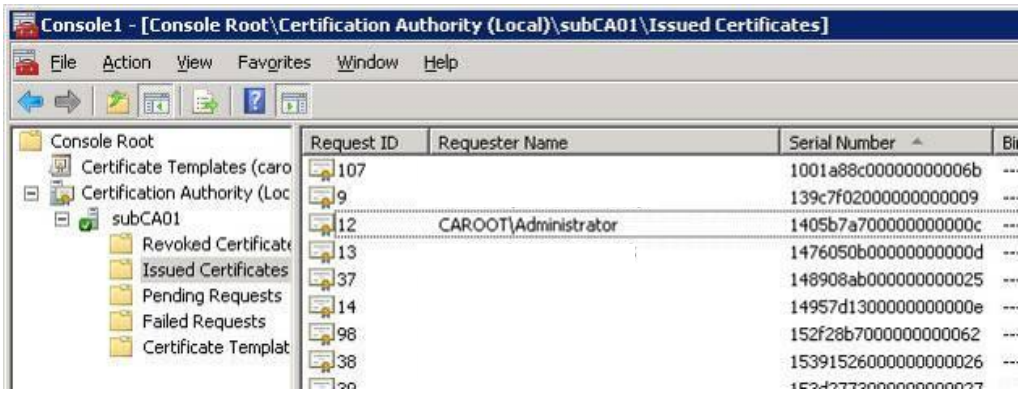


Abbildung 54: Liste der ausgestellten Zertifikate

Wurde das Zertifikat identifiziert, muss im Kontextmenü unter *All Tasks -> Revoke Certificate* das Zertifikat gesperrt werden:

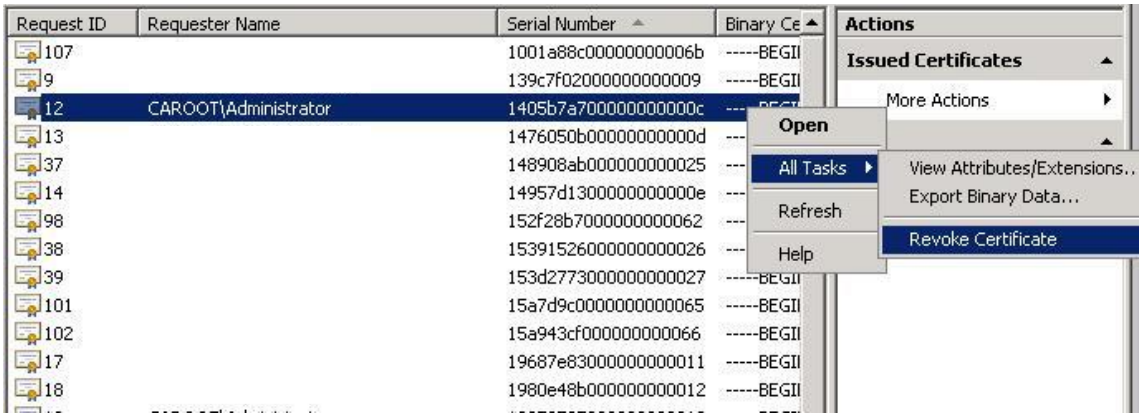


Abbildung 55: Zertifikat sperren

Im nachfolgenden Dialog werden der Grund für die Sperrung, sowie der Zeitpunkt der Sperrung angegeben:

Abbildung 56: Grund und Zeitpunkt der Zertifikatssperrung

Es steht eine Reihe von Gründen zur Verfügung, aufgrund derer ein Zertifikat gesperrt werden kann. Soll ein Zertifikat nur für einen bestimmten Zeitraum gesperrt werden, muss als Grund *Certificate Hold* gewählt werden. Andere Gründe können je nach Szenario passend gewählt werden:

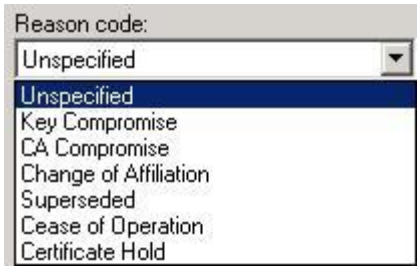


Abbildung 57: Listing der Sperrgründe für Zertifikate

Ist das Zertifikat gesperrt worden, muss die Zertifikatssperrliste neu veröffentlicht werden. Andernfalls ist die Sperrung erst gültig, nach Ablauf der Gültigkeit der aktuellen Sperrliste. Im Kontextmenü der Liste *Revoked Certificates* kann die Generierung der Liste durch Auswahl von *All Tasks -> Publish* gewählt werden:

Abbildung 58: Erzeugen einer neuen Zertifikatssperrliste

Im nachfolgenden Dialog muss *New CRL* ausgewählt werden da die *Secure ACS Appliance* keine Delta-Sperrlisten verarbeiten kann[11]:

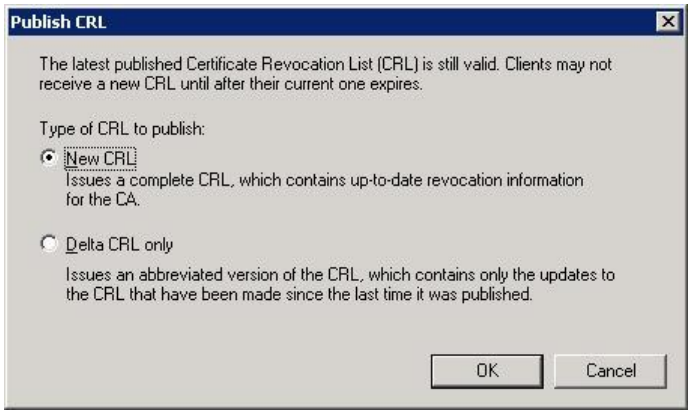


Abbildung 59: Eine neue Sperrliste wird erzeugt

[11] *Delta-Sperrlisten beschreiben lediglich die Veränderungen innerhalb der Zertifikatssperrliste seit der Veröffentlichung der letzten vollständigen, oder Delta-Sperrliste.*

Nach Bestätigung des *OK* Buttons wird die neue Sperrliste generiert und automatisch im *Active Directory* veröffentlicht. Weitere Schritte sind nicht notwendig, da der *Secure ACS* die aktuelle Sperrliste via LDAP aus dem *Active-Directory* herunterlädt, und somit automatisch über die aktuellste Version verfügt.

10.2 Ausrollen neuer Benutzer-/Computer-Zertifikate

Das Ausrollen neuer Zertifikate kann unter einer Reihe von Umständen nötig sein. Beispielsweise wenn eine Aktualisierung der Zertifikatsvorlage vorgenommen wurde oder das Zertifikat der signierenden CA getauscht wurde.

Hierzu kann die Funktion *Reenroll All Certifcate Holders* genutzt werden. Diese findet sich im *Server Manager* der signierenden Zertifizierungsstelle, unter *Active-Directory Certificate Services*. Nach Auswahl des entsprechenden *Templates* ist die Aktion im Kontextmenü zu finden:

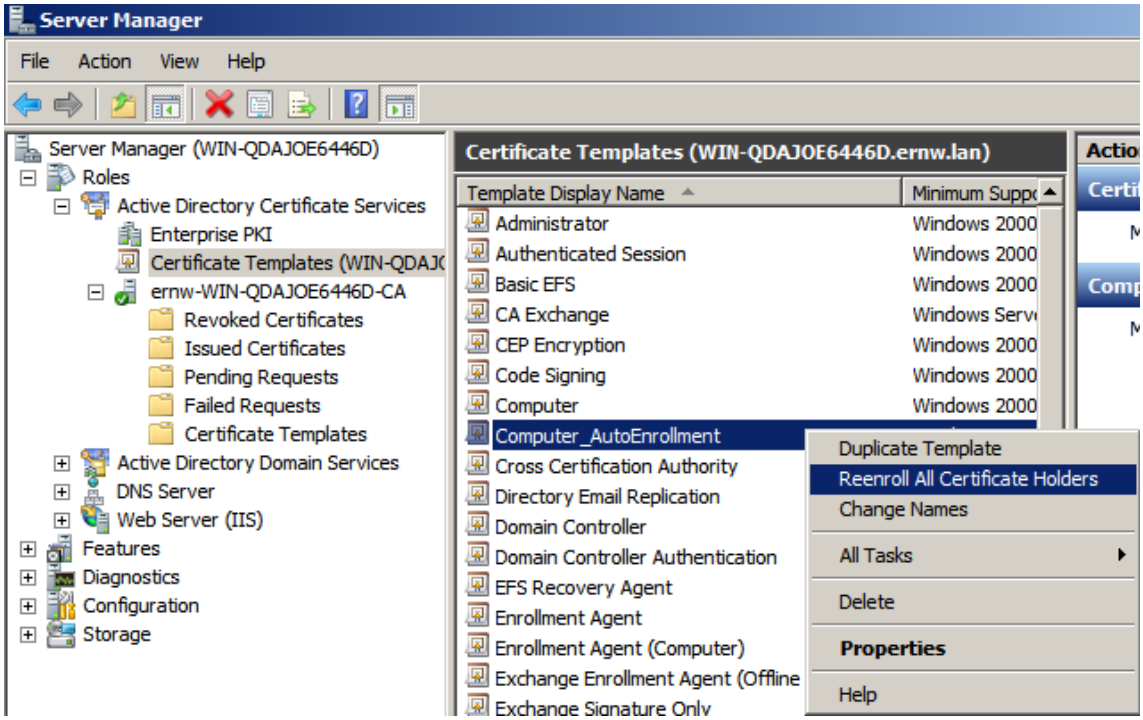


Abbildung 60: Erneutes Ausrollen aller Zertifikate einer Vorlage

10.3 Keine gültigen Zertifikate zur Authentifizierung vorhanden

Existiert auf einem zu authentifizierenden System kein gültiges Computerzertifikat, kann dies dazu führen, dass sich Benutzer nicht am Netzwerk authentifizieren kann. Hintergrund ist, dass der für die Benutzerauthentifizierung benötigte Schlüssel aufgrund von *Credential Roaming* im *Active Directory* befindet, und hierauf nicht zugegriffen werden kann.

Dieser Fehlerfall lässt sich durch kurzfristige Aufnahme der Mac-Adresse des betroffenen Computers, in die Liste der Geräte die mit *MAC Authentication Bypass* authentifiziert werden, lösen.

Hierzu wird im *Secure ACS* ein Benutzer angelegt, dessen Name und Kennwort der Mac-Adresse des Computers entsprechen. Während der Anlegung des Nutzers, muss auf die Angabe der korrekten *Secure ACS* Gruppe geachtet werden, damit der Computer einem VLAN zugeordnet wird, in welchem er ein neues Zertifikat beantragen kann.

Weiterhin sollte eine automatische Deaktivierung des neu angelegten Benutzers konfiguriert werden. Dies kann durch Aktivierung der Option *Disable account if* und die Angabe eines Datums, sowie der Aktivierung des Kontrollkastens *Date exceeds* konfiguriert werden. Somit wird sichergestellt, dass die Authentifizierung mittels *Mac-Adresse* nur kurzfristig möglich ist.

Abbildung 61: Konfiguration der automatischen Deaktivierung für neue Benutzer

Mit freundlichen Grüßen,

Oliver Roeschke und Christopher Werny.

ERNW - ERNW Enno Rey Netzwerke GmbH
Breslauer Str. 28
69124 Heidelberg
Tel. +49 6221 480390
Fax +49 6221 419008

www.ernw.de